A Complete Bibliography of Publications in *Cryptologia*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

29 July 2022
Version 3.69

Title word cross-reference

References

Winkel:1977:WC

[1] Brian J. Winkel. Why Cryptologia? *Cryptologia*, 1(1):1–3, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865249~db=all~order=page`.

Mellen:1977:CMSa

[2] Greg E. Mellen and Lloyd Greenwood. The cryptology of multiplex system: Part I: Simulation and cryptanalysis. *Cryptologia*, 1(1):4–16, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865250~db=all~order=page`.

Harris:1977:DKC

[3] Barbara Harris. A different kind of column. *Cryptologia*, 1(1):17–19, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865251~db=all~order=page`.

Reeds:1977:CRN

[4] James A. Reeds. "Cracking" a random number generator. *Cryptologia*, 1(1):20–26, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://alumni.cs.ucr.edu/~jsun/random-number.pdf`; `http://www.dean.usma.edu/math/pubs/cryptologia/ClassicArticleReprints/V01N1PP20-26JamesReeds.pdf`; `http://www.informaworld.com/smpp/content~content=a748865252~db=all~order=page`. Reprinted in [1789, pp. 509–515].

Kahn:1977:BB

[5] David Kahn. The biggest bibliography. *Cryptologia*, 1(1):27–42, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a748865253~db=all~order=page.

Shulman:1977:RKR

[6] David Shulman. A reply to Kahn's review. *Cryptologia*, 1(1):43–45, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865254~db=all~order=page.

Deavours:1977:UPC

[7] Cipher A. Deavours. Unicity points in cryptanalysis. *Cryptologia*, 1(1):46–68, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865255~db=all~order=page.

Kruh:1977:CECa

[8] Louis Kruh. Cipher equipment: Cipher disks. *Cryptologia*, 1(1):69–75, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865256~db=all~order=page.

Levine:1977:SCA

[9] Jack Levine and Joel V. Brawley. Some cryptographic applications of permutation polynomials. *Cryptologia*, 1(1):76–92, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865257~db=all~order=page.

Winkel:1977:PCCa

[10] Brian J. Winkel. Poe challenge cipher finally broken. *Cryptologia*, 1(1):93–96, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865258~db=all~order=page.

Anonymous:1977:BCa

[11] Anonymous. Biographies of contributory. *Cryptologia*, 1(1):97–99, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865259~db=all~order=page.

Hiatt:1977:AD

[12] Blanchard Hiatt. Age of decipherment. *Cryptologia*, 1(2):101–105, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865262~db=all~order=page.

Hiatt:1977:CFT

[13] Blanchard Hiatt. "Count forward three score and ten ...". *Cryptologia*, 1 (2):106–115, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865263~db=all~order=page.

Schatz:1977:AAC

[14] Bruce R. Schatz. Automated analysis of cryptogram cipher equipment. *Cryptologia*, 1(2):116–142, April 1977. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865264~db=all~order=page.

Kruh:1977:CECb

[15] Louis Kruh. Cipher equipment: Converter M-325(T). *Cryptologia*, 1 (2):143–149, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865265~db=all~order=page.

Mellen:1977:CMSb

[16] Greg E. Mellen and Lloyd Greenwood. The cryptology of multiplex system: Part II. *Cryptologia*, 1(2):150–165, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865266~db=all~order=page.

Kahn:1977:GYS

[17] David Kahn. "Get out your secret decoders, boys and girls ...". *Cryptologia*, 1(2):166, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865267~db=all~order=page.

Deavours:1977:AHC

[18] Cipher A. Deavours. Analysis of the Hebern cryptograph using isomorphs. *Cryptologia*, 1(2):167–185, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865268~db=all~order=page.

Reeds:1977:RA

[19] James A. Reeds. Rotor algebra. *Cryptologia*, 1(2):186–194, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865269~db=all~order=page.

Penney:1977:GR

[20] Walter Penney. Grille reconstruction. *Cryptologia*, 1(2):195–201, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865270~db=all~order=page.

Anonymous:1977:BCb

[21] Anonymous. Biographies of contributors. *Cryptologia*, 1(2):202–204, April 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865271~db=all~order=page.

Kahn:1977:SCI

[22] David Kahn. The significance of codebreaking and intelligence in Allied strategy and tactics. *Cryptologia*, 1(3): 209–222, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845268~db=all~order=page.

Deavours:1977:KT

[23] Cipher A. Deavours. The kappa test. *Cryptologia*, 1(3):223–231,

July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845269~db=all~order=page.

Winkel:1977:WWJ

[24] Brian J. Winkel. Word ways, a journal worth going your way. *Cryptologia*, 1(3):232–234, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845270~db=all~order=page.

Reeds:1977:ECP

[25] James A. Reeds. Entropy calculations and particular methods of cryptanalysis. *Cryptologia*, 1(3):235–254, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845271~db=all~order=page.

Kruh:1977:CEH

[26] Louis Kruh. Cipher equipment: Hagelin pocket cryptographer, type CD-57. *Cryptologia*, 1(3):255–260, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845272~db=all~order=page.

Leighton:1977:EUD

[27] Albert C. Leighton. The earliest use of a dot cipher. *Cryptologia*, 1(3):261–274, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845273~db=all~order=page.

Mint:1977:DDC

[28] Royal Canadian Mint. DPEPE DPJO: a Canadian coin piece with a message. *Cryptologia*, 1(3):275–277, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845274~db=all~order=page.

Deavours:1977:KSM

[29] Cipher A. Deavours. Kullback's "Statistical Methods in Cryptanalysis", a book review. *Cryptologia*, 1(3):278–280, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845275~db=all~order=page.

Morris:1977:ANB

[30] Robert Morris, Neil J. A. Sloane, and Aaron D. Wyner. Assessment of the National Bureau of Standards Proposed Federal Data Encryption Standard. *Cryptologia*, 1(3):281–291, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845276~db=all~order=page.

NBS:1977:PFI

[31] National Bureau of Standards. Proposed Federal Information Processing Data Encryption Standard. *Cryptologia*, 1(3):292–306, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~

content=a758845277~db=all~order=page.

Anonymous:1977:BCc

[32] Anonymous. Biographies of contributors. *Cryptologia*, 1(3):307–308, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a758845278~db=all~order=page.

Winkel:1977:E

[33] Brian J. Winkel. Epilogue. *Cryptologia*, 1(3):309, July 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Deavours:1977:ICC

[34] Cipher A. Deavours. The Ithaca connection: Computer cryptography in the making — a special report. *Cryptologia*, 1(4):312–317, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865284~db=all~order=page.

Winkel:1977:PCCb

[35] Brian J. Winkel. Poe challenge cipher solutions. *Cryptologia*, 1(4):318–325, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865285~db=all~order=page.

Eckler:1977:RYN

[36] A. Ross Eckler. A rapid yes–no computer-aided communicator. *Cryptologia*, 1(4):326–333, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865286~db=all~order=page.

Kruh:1977:CEM

[37] Louis Kruh. Cipher equipment: MA4210 alphanumeric pocket cipher. *Cryptologia*, 1(4):334–336, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865287~db=all~order=page.

Kahn:1977:ECR

[38] David Kahn. Ecclesiastical cryptography — a review. *Cryptologia*, 1(4):337, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865288~db=all~order=page.

Brawley:1977:EVS

[39] Joel V. Brawley and Jack Levine. Equivalence of Vigenère systems. *Cryptologia*, 1(4):338–361, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865289~db=all~order=page.

Marsh:1977:CCC

[40] D. C. B. Marsh. Courses in cryptology — cryptography at the Colorado School of Mines. *Cryptologia*, 1(4):362–363, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865290~db=all~order=page.

Straight:1977:CCC

[41] David W. Straight. Courses in cryptology — cryptanalysis and data security course at the University of Tennessee. *Cryptologia*, 1(4):363–365, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865291~db=all~order=page`.

Bright:1977:CAD

[42] Herbert S. Bright. Cryptanalytic attack and defense: Ciphertext only, known-plaintext, chosen-plaintext. *Cryptologia*, 1(4):366–370, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865292~db=all~order=page`.

Kahn:1977:RR

[43] David Kahn. Reports from the Reich. *Cryptologia*, 1(4):371, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865293~db=all~order=page`.

Kruh:1977:CC

[44] Louis Kruh. The churchyard ciphers. *Cryptologia*, 1(4):372–375, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865294~db=all~order=page`.

Highland:1977:CSE

[45] Harold Joseph Highland. CENSORED: a simulation exercise. *Cryptologia*, 1 (4):376–377, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865295~db=all~order=page`.

Kahn:1977:GME

[46] David Kahn. German military eavesdroppers. *Cryptologia*, 1(4):378–380, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865296~db=all~order=page`.

Deavours:1977:EPH

[47] Cipher A. Deavours and James A. Reeds. The Enigma: Part I: Historical perspectives. *Cryptologia*, 1(4):381–391, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865297~db=all~order=page`.

Winkel:1977:S

[48] Brian J. Winkel. Solution. *Cryptologia*, 1(4):391, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Fagone:1977:MCW

[49] Peter P. Fagone. A message in cipher written by General Cornwallis during the Revolutionary War. *Cryptologia*, 1(4):392–395, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865298~db=all~order=page`.

Winkel:1977:TTD

[50] Brian J. Winkel. There and there — a department. *Cryptologia*, 1(4):396–405, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865299~db=all~order=page`.

Unknown:1977:TSP

[51] Unknown. They should be paranoid. *Cryptologia*, 1(4):400–401, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). Originally published in *Datamation*, September 1977, pp. 29–30.

Simmons:1977:PCM

[52] Gustavus J. Simmons and Michael J. Norris. Preliminary comments on the M.I.T. public-key cryptosystem. *Cryptologia*, 1(4):406–414, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865300~db=all~order=page`.

Anonymous:1977:BCd

[53] Anonymous. Biographies of contributors. *Cryptologia*, 1(4):415–417, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865301~db=all~order=page`.

Unknown:1977:LE

[54] Unknown. Letter from the Editor. *Cryptologia*, 1(4):??, October 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Barker:1978:SHT

[55] Wayne G. Barker. Solving a Hagelin, type CD-57, cipher. *Cryptologia*, 2(1): 1–8, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865303~db=all~order=page`.

Wilson:1978:CCC

[56] David Wilson. Courses in cryptology — cryptanalysis course down under. *Cryptologia*, 2(1):9–11, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865304~db=all~order=page`.

Kahn:1978:FNG

[57] David Kahn. The Forschungsamt: Nazi Germany's most secret communications intelligence agency. *Cryptologia*, 2(1):12–19, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865305~db=all~order=page`.

Rohrbach:1978:MMMa

[58] Hans Rohrbach. Mathematical and mechanical methods in cryptography. I. *Cryptologia*, 2(1):20–37, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865306~db=all~order=page`.

Kruh:1978:IWF

[59] Louis Kruh. The inventions of William F. Friedman. *Cryptologia*, 2(1):38–

61, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865307~db=all~order=page.

Rivest:1978:RPC

[60] Ronald L. Rivest. Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem. *Cryptologia*, 2(1):62–65, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865308~db=all~order=page.

Deavours:1978:BRB

[61] Cipher A. Deavours. A book review: *Cryptanalysis of the Hagelin Cryptograph*, by Wayne G. Barker. *Cryptologia*, 2(1):66–67, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865309~db=all~order=page.

Knight:1978:CCa

[62] H. Gary Knight. Cryptanalyst's corner. *Cryptologia*, 2(1):68–74, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865310~db=all~order=page.

Weber:1978:JLS

[63] Ralph E. Weber. James Lovell and secret ciphers during the American Revolution. *Cryptologia*, 2(1):75–88, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865311~db=all~order=page.

Winkel:1978:TTDa

[64] Brian J. Winkel. There and there — a department. *Cryptologia*, 2(1):89–94, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865312~db=all~order=page.

Anonymous:1978:BCa

[65] Anonymous. Biographies of contributors. *Cryptologia*, 2(1):95–96, January 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865313~db=all~order=page.

Rohrbach:1978:MMMb

[66] Hans Rohrbach. Mathematical and mechanical methods in cryptography. II. *Cryptologia*, 2(2):101–121, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865315~db=all~order=page.

Kahn:1978:FLB

[67] David Kahn. Friedman's life: a book review. *Cryptologia*, 2(2):122–123, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865316~db=all~order=page.

Knight:1978:CCb

[68] H. Gary Knight. Cryptanalyst's corner. *Cryptologia*, 2(2):124–129, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865317~db=all~order=page`.

Kruh:1978:WWA

[69] Louis Kruh. Who wrote "The American Black Chamber"? *Cryptologia*, 2(2):130–133, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865318~db=all~order=page`.

Deavours:1978:CCC

[70] Cipher A. Deavours. Courses in cryptology — cryptology at Kean College. *Cryptologia*, 2(2):134–138, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865319~db=all~order=page`.

Kahn:1978:NAY

[71] David Kahn. Nuggets from the archives: Yardley tries again. *Cryptologia*, 2(2):139–143, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865320~db=all~order=page`.

Barker:1978:UDC

[72] Wayne G. Barker. The unsolved D'Agapeyeff cipher. *Cryptologia*, 2(2):144–147, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865321~db=all~order=page`.

Straight:1978:MMC

[73] David Straight. "Modern Methods for Computer Security and Privacy": a book review. *Cryptologia*, 2(2):148–150, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Straight:1978:OCS

[74] David Straight. "An Outline of Computer Security": a book review. *Cryptologia*, 2(2):148–150, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865322~db=all~order=page`.

Kahn:1978:PGB

[75] David Kahn. "Pictures Galore": a book review. *Cryptologia*, 2(2):151, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865323~db=all~order=page`.

Rubin:1978:CMDa

[76] Frank Rubin. Computer methods for decrypting multiplex ciphers. *Cryptologia*, 2(2):152–160, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865324~db=all~order=page`.

Winkel:1978:CBC

[77] Brian J. Winkel. Casanova and the Beaufort cipher. *Cryptologia*, 2(2):161–163, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865325~db=all~order=page`.

Kruh:1978:CC

[78] Louis Kruh. Cryptology as a career. *Cryptologia*, 2(2):164–167, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865326~db=all~order=page`.

Anonymous:1978:EC

[79] Anonymous. Encryption challenge. *Cryptologia*, 2(2):168–171, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Withheld:1978:EC

[80] Names Withheld. Encryption challenge. *Cryptologia*, 2(2):168–171, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865327~db=all~order=page`.

Kruh:1978:CED

[81] Louis Kruh. Cipher equipment: DH-26 handheld encryption unit. *Cryptologia*, 2(2):172–177, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865328~db=all~order=page`.

Winkel:1978:TAM

[82] Brian J. Winkel. A tribute to Alf Monge. *Cryptologia*, 2(2):178–185, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865329~db=all~order=page`.

Winkel:1978:TTDb

[83] Brian J. Winkel. There and there — a department. *Cryptologia*, 2(2):186–194, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865330~db=all~order=page`.

Anonymous:1978:BCb

[84] Anonymous. Biographies of contributors. *Cryptologia*, 2(2):195–197, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865331~db=all~order=page`.

Unknown:1978:CCB

[85] Unknown. "Codes and Ciphers" — a book review. *Cryptologia*, 2(2):??, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Unknown:1978:MWB

[86] Unknown. "The Man Who Broke Purple" — a book review. *Cryptologia*, 2(2):??, April 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Childs:1978:MRG

[87] J. Rives Childs. My recollections of G.2 A.6. *Cryptologia*, 2(3):201–214, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902659~db=all~order=page`.

Rubin:1978:CMDb

[88] Frank Rubin. Computer methods for decrypting random stream ciphers. *Cryptologia*, 2(3):215–231, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902660~db=all~order=page`. Reprinted in [1789, pp. 493–508].

Arnold:1978:FBC

[89] Philip M. Arnold. A forgotten book on ciphers. *Cryptologia*, 2(3):232–235, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902661~db=all~order=page`.

Foster:1978:CCC

[90] Caxton C. Foster. Courses in cryptology — cryptanalysis and computers. *Cryptologia*, 2(3):236–237, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902662~db=all~order=page`.

Knight:1978:CCc

[91] H. Gary Knight. Cryptanalysts' corner. *Cryptologia*, 2(3):238–241, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902663~db=all~order=page`.

Kruh:1978:CHIa

[92] Louis Kruh. A catalog of historical interest. *Cryptologia*, 2(3):242–253, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902664~db=all~order=page`.

Winkel:1978:ACS

[93] Brian J. Winkel. Astle cipher solved. *Cryptologia*, 2(3):254–256, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902665~db=all~order=page`.

Kahn:1978:FVB

[94] David Kahn. A famous variation — a book review. *Cryptologia*, 2(3):257, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902666~db=all~order=page`.

Kahn:1978:RDB

[95] David Kahn. Reveling in deception — a book review. *Cryptologia*, 2(3):258–259, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902667~db=all~order=page`.

Heitzenrater:1978:DWD

[96] Richard Heitzenrater. Decoding Wesley's diaries. *Cryptologia*, 2(3):260–264, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902668~db=all~order=page`.

Kahn:1978:SNR

[97] David Kahn. Short notices — reviews. *Cryptologia*, 2(3):265–266, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902669~db=all~order=page`.

Morris:1978:HCM

[98] Robert Morris. The Hagelin cipher machine (M-209): Reconstruction of the internal settings. *Cryptologia*, 2(3): 267–289, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902670~db=all~order=page`.

Kruh:1978:CRC

[99] Louis Kruh. Capsule reviews for crypto buffs. *Cryptologia*, 2(3):290–292, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902671~db=all~order=page`.

Winkel:1978:TTDc

[100] Brian J. Winkel. There and there — a department. *Cryptologia*, 2(3):293–298, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902672~db=all~order=page`.

Anonymous:1978:BCc

[101] Anonymous. Biographies of contributors. *Cryptologia*, 2(3):299–300, July 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902673~db=all~order=page`.

Blakley:1978:SNT

[102] Bob Blakley and G. R. Blakley. Security of number-theoretic public key cryptosystems against random attack. I. *Cryptologia*, 2(4):305–321, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902676~db=all~order=page`.

Kruh:1978:WNW

[103] Louis Kruh. What the Nazis were doing. *Cryptologia*, 2(4):322–323, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902677~db=all~order=page`.

Oakley:1978:RPC

[104] Howard T. Oakley. The Riverbank publications on cryptology. *Cryptologia*, 2(4):324–330, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902678~db=all~order=page`.

Kahn:1978:ECO

[105] David Kahn. Extraordinary codebreakers, outstanding family: a review. *Cryptologia*, 2(4):331–333, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902679~db=all~order=page`.

Kruh:1978:NCC

[106] Louis Kruh. A nineteenth century challenge cipher. *Cryptologia*, 2(4): 334, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902680~db=all~order=page`.

Knight:1978:CCd

[107] H. Gary Knight. Cryptanalysts' corner. *Cryptologia*, 2(4):335–337, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902681~db=all~order=page`.

Kruh:1978:CHIb

[108] Louis Kruh. A catalog of historical interest — Part II. *Cryptologia*, 2(4):338–349, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902682~db=all~order=page`.

Callas:1978:ACC

[109] Nicholas P. Callas. An application of computers to cryptology. *Cryptologia*, 2(4):350–364, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902683~db=all~order=page`.

Kahn:1978:OWB

[110] David Kahn. One of the worst — a book review. *Cryptologia*, 2(4):365, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902684~db=all~order=page`.

Kruh:1978:RC

[111] Louis Kruh. Rent a code. *Cryptologia*, 2(4):366–367, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902685~db=all~order=page`.

Winkel:1978:ALC

[112] Brian J. Winkel. "Action line" challenge. *Cryptologia*, 2(4):368–370, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902686~db=all~order=page`.

Kinnucan:1978:DEG

[113] Paul Kinnucan. Data encryption gurus: Tuchman and Meyer. *Cryptologia*, 2(4):371–381, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902687~db=all~order=page`.

Winkel:1978:TTDd

[114] Brian J. Winkel. There and there — a department. *Cryptologia*, 2(4):382–393, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902688~db=all~order=page`.

Anonymous:1978:BCd

[115] Anonymous. Biographies of contributors. *Cryptologia*, 2(4):394–395, October 1978. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902689~db=all~order=page`.

Kahn:1979:UC

[116] David Kahn. The Ultra conference. *Cryptologia*, 3(1):1–8, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902770~db=all~order=page`.

Hammer:1979:HDT

[117] Carl Hammer. How did TJB encode B2? *Cryptologia*, 3(1):9–15, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902771~db=all~order=page`.

Rohrbach:1979:RDA

[118] Hans Rohrbach. Report on the decipherment of the American strip cipher O-2 by the German Foreign Office. *Cryptologia*, 3(1):16–26, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902772~db=all~order=page`.

Makar:1979:CSP

[119] Boshra H. Makar. Cryptology at St. Peter's College. *Cryptologia*, 3(1):27–28, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902773~db=all~order=page`.

Blakley:1979:SNTa

[120] Bob Blakley and G. R. Blakley. Security of number theoretic public key cryptosystems against random attack. II. *Cryptologia*, 3(1):29–42, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902774~db=all~order=page`.

Ford:1979:HC

[121] James R. Ford. The HP-67/97 cryptograph. *Cryptologia*, 3(1):43–50, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1979:XC

[122] Louis Kruh. A xerograph of a classic. *Cryptologia*, 3(1):50, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902776~db=all~order=page`.

Sulzberger:1979:PDA

[123] A. O. Sulzberger, Jr. Papers disclose Allies' edge in knowing German codes. *Cryptologia*, 3(1):51–53, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902777~db=all~order=page`.

Winkel:1979:SC

[124] Brian J. Winkel. Studies on cryptology. *Cryptologia*, 3(1):52–53, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Shulman:1979:SC

[125] David Shulman. A Sherlockian cryptogram. *Cryptologia*, 3(1):54–56, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902778~db=all~order=page`.

Winkel:1979:TTa

[126] Brian J. Winkel. There and there. *Cryptologia*, 3(1):57–62, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902779~db=all~order=page`.

Anonymous:1979:BCa

[127] Anonymous. Biographies of contributors. *Cryptologia*, 3(1):63–64, January 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902780~db=all~order=page`.

Good:1979:EWC

[128] I. J. Good. Early work on computers at Bletchley Park. *Cryptologia*, 3(2):65–77, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902783~db=all~order=page`.

Kruh:1979:DMH

[129] Louis Kruh. Devices and machines: The Hagelin cryptographer, type C-52. *Cryptologia*, 3(2):78–82, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902784~db=all~order=page`.

Reeds:1979:SCC

[130] James A. Reeds. Solution of challenge cipher. *Cryptologia*, 3(2):83–95, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902785~db=all~order=page`.

Kahn:1979:ACB

[131] David Kahn. "American Codes": a book review. *Cryptologia*, 3(2):96–99, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902786~db=all~order=page`.

Shulman:1979:MTM

[132] David Shulman. The Macbeth test message. *Cryptologia*, 3(2):100–104, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a741902787~db=all~order=page.

Blakley:1979:SNTb

[133] Bob Blakley and G. R. Blakley. Security of number theoretic public key cryptosystems against random attack. III. *Cryptologia*, 3(2):105–118, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902788~db=all~order=page.

Kahn:1979:GCC

[134] David Kahn. A German consular cipher. *Cryptologia*, 3(2):119, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902789~db=all~order=page.

Wilson:1979:LCPa

[135] David Wilson. Littlewood's cipher: Part I: a challenge. *Cryptologia*, 3(2):120–121, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902790~db=all~order=page.

Hardie:1979:BRU

[136] Bradford Hardie. Book review: Ultra goes to war. *Cryptologia*, 3(2):122–126, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902791~db=all~order=page.

Anonymous:1979:BCb

[137] Anonymous. Biographies of contributors. *Cryptologia*, 3(2):127–128, April 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902792~db=all~order=page.

Inman:1979:NPT

[138] Bobby R. Inman. The NSA perspective on telecommunications protection in the nongovernmental sector. *Cryptologia*, 3(3):129–135, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902794~db=all~order=page.

Mellen:1979:JFB

[139] Greg Mellen. J. F. Byrne and the Chaocipher: Work in progress. *Cryptologia*, 3(3):136–154, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902795~db=all~order=page.

Rubin:1979:SCB

[140] Frank Rubin. Solving a cipher based on multiple random number streams. *Cryptologia*, 3(3):155–157, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902796~db=all~order=page.

Kahn:1979:FIA

[141] David Kahn. The futility of it all. *Cryptologia*, 3(3):158–165,

July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902797~db=all~order=page.

Kruh:1979:DDA

[142] Louis Kruh. The deadly double advertisements: Pearl Harbor warning or coincidence. *Cryptologia*, 3(3):166–171, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902798~db=all~order=page.

Wilson:1979:LCPb

[143] David Wilson. Littlewood's cipher: Part II: a method of solution. *Cryptologia*, 3(3):172–176, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902799~db=all~order=page.

Levine:1979:TMPa

[144] Jack Levine and Michael Willet. The two-message problem in cipher text Autokey. Part I. *Cryptologia*, 3(3):177–186, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902800~db=all~order=page.

Yuval:1979:HSR

[145] Gideon Yuval. How to swindle Rabin. *Cryptologia*, 3(3):187–189, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902801~db=all~order=page.

Kahn:1979:CRR

[146] David Kahn. Classic revive ??: a review. *Cryptologia*, 3(3):190–191, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:1979:SBC

[147] Anonymous. The Second Beale Cipher Symposium — call for papers. *Cryptologia*, 3(3):191, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902802~db=all~order=page.

Anonymous:1979:BCc

[148] Anonymous. Biographies of contributors. *Cryptologia*, 3(3):192, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902803~db=all~order=page.

Kahn:1979:SCI

[149] David Kahn. The significance of codebreaking and intelligence in Allied strategy and tactics. *Cryptologia*, 3(3):209–222, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865273~db=all~order=page.

Deavours:1979:KT

[150] C. A. Deavours. The kappa test. *Cryptologia*, 3(3):223–231, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a748865274~db=all~order=page.

Winkel:1979:WWJ

[151] Brian J. Winkel. Word ways, a journal worth going your way. *Cryptologia*, 3(3):232–234, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865275~db=all~order=page.

Reeds:1979:ECP

[152] James Reeds. Entropy calculations and particular methods of cryptanalysis. *Cryptologia*, 3(3):235–254, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865276~db=all~order=page.

Kruh:1979:CE

[153] Louis Kruh. Cipher equipment. *Cryptologia*, 3(3):255–260, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865277~db=all~order=page.

Leighton:1979:EUD

[154] Albert C. Leighton. "The earliest use of a dot cipher". *Cryptologia*, 3(3):261–274, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865278~db=all~order=page.

Mint:1979:DDC

[155] Royal Canadian Mint. DPEPE DPJO: a Canadian coin piece with a message. *Cryptologia*, 3(3):275–277, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865279~db=all~order=page.

Deavours:1979:KSM

[156] C. A. Deavours. Kullback's "Statistical Methods in Cryptanalysis" — book review. *Cryptologia*, 3(3):278–280, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865280~db=all~order=page. See [1661].

Morris:1979:ANB

[157] Robert Morris, N. J. A. Sloane, and A. D. Wyner. Assessment of the National Bureau of Standards proposed Federal Data Encryption Standard. *Cryptologia*, 3(3):281–291, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865281~db=all~order=page.

Anonymous:1979:PFI

[158] Anonymous. Proposed Federal Information Processing Data Encryption Standard. *Cryptologia*, 3(3):292–306, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865282~db=all~order=page.

Anonymous:1979:BCd

[159] Anonymous. Biographies of contributors. *Cryptologia*, 3(3):307–308, July 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865283~db=all~order=page`.

Sams:1979:MC

[160] Eric Sams. Musical cryptography. *Cryptologia*, 3(4):193–201, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902805~db=all~order=page`.

Rubin:1979:CAD

[161] Frank Rubin. Cryptographic aspects of data compression codes. *Cryptologia*, 3(4):202–205, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902806~db=all~order=page`. See also *Comm. ACM*, 19 (November 1976): 616–623.

Kruh:1979:CIO

[162] Louis Kruh. CP-III: One time cypher pad manual encryption device. *Cryptologia*, 3(4):206–209, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902807~db=all~order=page`.

Kahn:1979:G

[163] David Kahn. The Geheimschreiber. *Cryptologia*, 3(4):210–214, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902808~db=all~order=page`.

Unknown:1979:IGS

[164] Unknown. Interrogation on German secret teletypewriters. *Cryptologia*, 3 (4):211–214, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Arnold:1979:CEM

[165] Philip M. Arnold. Ciphers for the educated man. *Cryptologia*, 3(4):215–216, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902809~db=all~order=page`.

Kruh:1979:SN

[166] Louis Kruh. Short notices. *Cryptologia*, 3(4):217–219, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902810~db=all~order=page`.

Levine:1979:TMPb

[167] Jack Levine and Michael Willet. The two-message problem in cipher text Autokey. Part II. *Cryptologia*, 3(4): 220–231, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902811~db=all~order=page`.

Anonymous:1979:MC

[168] Anonymous. A musical cipher. *Cryptologia*, 3(4):232, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902812~db=all~order=page`.

Fischer:1979:LRC

[169] Elliot Fischer. Language redundancy and cryptanalysis. *Cryptologia*, 3 (4):233–235, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902813~db=all~order=page`.

Kruh:1979:DFT

[170] Louis Kruh. The day the Friedmans had a typo in their photo. *Cryptologia*, 3(4):236–241, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902814~db=all~order=page`.

Knight:1979:CC

[171] H. Gary Knight. Cryptanalysts' corner. *Cryptologia*, 3(4):242, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902815~db=all~order=page`.

Arnold:1979:GCB

[172] Philip M. Arnold. A German code book. *Cryptologia*, 3(4):243–245, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902816~db=all~order=page`. See Cryptologia **4**(1), 1980, pp. 54–55 for a picture of the code book.

Hardie:1979:TC

[173] Bradford Hardie. A theory of cryptography. *Cryptologia*, 3(4):246–247, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902817~db=all~order=page`.

Winkel:1979:TTb

[174] Brian J. Winkel. There and there. *Cryptologia*, 3(4):248–251, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902818~db=all~order=page`.

Anonymous:1979:BCe

[175] Anonymous. Biographies of contributors. *Cryptologia*, 3(4):252–253, October 1979. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902819~db=all~order=page`.

Lu:1980:SEP

[176] S. C. Lu and L. N. Lee. A simple and effective public-key cryptosystem. *Cryptologia*, 4(??):??, ???? 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See also *Comsat Technical Review,* **9**, 15–24 (1979).

Schuetz:1980:SSU

[177] Arthur Schuetz. Secret service unmasked. *Cryptologia*, 4(??):??, ???? 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Fagone:1980:SCE

[178] Peter P. Fagone. The solution of a Cromwellian era spy message (circa 1648). *Cryptologia*, 4(1):1–4, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902854~db=all~order=page`.

Kruh:1980:CDCa

[179] Louis Kruh. Cipher devices: The Cryptomatic HC-520. *Cryptologia*, 4(1):5–14, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902855~db=all~order=page`.

Golomb:1980:CRG

[180] Solomon W. Golomb. Cryptographic reflections on the genetic code. *Cryptologia*, 4(1):15–19, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902856~db=all~order=page`.

Richter:1980:NPK

[181] Michael Richter. A note on public-key cryptosystems. *Cryptologia*, 4(1):20–22, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902857~db=all~order=page`.

Kahn:1980:DTB

[182] David Kahn. "Deciphered Texts": a book review. *Cryptologia*, 4(1):22, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902858~db=all~order=page`.

Kruh:1980:MF

[183] Louis Kruh. Memories of Friedman. *Cryptologia*, 4(1):23–26, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902859~db=all~order=page`.

Knight:1980:CCa

[184] H. Gary Knight. Cryptanalysts' corner. *Cryptologia*, 4(1):27–29, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902860~db=all~order=page`.

Rivest:1980:FBE

[185] Ronald L. Rivest. "Forwards and backwards" encryption. *Cryptologia*, 4(1):30–33, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902861~db=all~order=page`. Reprinted in [1789, pp. 433–437].

Kruh:1980:CSC

[186] Louis Kruh. Ciphering system for a 19th Century challenge cipher. *Cryptologia*, 4(1):34–35, January 1980. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902862~db=all~order=page`.

Kahn:1980:PUC

[187] David Kahn. Problems of the unbreakable cipher. *Cryptologia*, 4(1):36–40, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902863~db=all~order=page`.

Shulman:1980:ASS

[188] David Shulman. Another solution to the Sherlockian cryptogram. *Cryptologia*, 4(1):41, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902864~db=all~order=page`.

Kahn:1980:ME

[189] David Kahn. The market for encryption. *Cryptologia*, 4(1):42–44, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902865~db=all~order=page`.

Ford:1980:HC

[190] James R. Ford. The HP-67/97 cryptograph. *Cryptologia*, 4(1):43–49, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902775~db=all~order=page`.

Kruh:1980:RMC

[191] Louis Kruh. Reminiscences of a master cryptologist. *Cryptologia*, 4(1):45–50, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902866~db=all~order=page`.

Eckler:1980:SCU

[192] A. Ross Eckler. Some comments on the use of the HP 67/97 as a cryptograph. *Cryptologia*, 4(1):51–53, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902867~db=all~order=page`.

Winkel:1980:TTa

[193] Brian J. Winkel. There and there. *Cryptologia*, 4(1):54–61, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902868~db=all~order=page`.

Anonymous:1980:BCa

[194] Anonymous. Biographies of contributors. *Cryptologia*, 4(1):62–63, January 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902869~db=all~order=page`.

Kahn:1980:IC

[195] David Kahn. Interviews with cryptologists. *Cryptologia*, 4(2):65–70, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a741902872~db=all~order=page.

Levine:1980:ADIa

[196] Jack Levine and Robert E. Hartwig. Applications of the Drazin inverse to the Hill cryptographic system. Part I. *Cryptologia*, 4(2):71–85, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902873~db=all~order=page.

Shulman:1980:CCC

[197] David Shulman. A curious cryptic composition. *Cryptologia*, 4(2):86–88, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902874~db=all~order=page.

Outerbridge:1980:SCC

[198] Richard Outerbridge. Some cryptographic and computing applications of the Toshiba LC-836MN Memo Note 30 pocket calculator. *Cryptologia*, 4(2): 89–94, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902875~db=all~order=page.

Anonymous:1980:RML

[199] Anonymous. Ready-made love letters. *Cryptologia*, 4(2):95, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902876~db=all~order=page.

Arnold:1980:AJS

[200] Philip M. Arnold. An apology for Jacopo Silvestri. *Cryptologia*, 4(2):96–103, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902877~db=all~order=page.

Raven:1980:MPB

[201] Francis A. Raven. "Memories of the Pacific": Book reviews. *Cryptologia*, 4(2):104–108, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902878~db=all~order=page.

Wall:1980:DSS

[202] Rajendra S. Wall. Decryption of simple substitution cyphers with word divisions using a content addressable memory. *Cryptologia*, 4(2):109–115, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902879~db=all~order=page.

Gillogly:1980:BCD

[203] James J. Gillogly. The Beale Cypher: a dissenting opinion. *Cryptologia*, 4 (2):116–119, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902880~db=all~order=page.

Kahn:1980:NAN

[204] David Kahn. Nuggets from the archives: a null code at the White

House. *Cryptologia*, 4(2):120–121, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902881~db=all~order=page`.

Anonymous:1980:S

[205] Anonymous. Solutions. *Cryptologia*, 4 (2):122, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902882~db=all~order=page`.

Winkel:1980:SCC

[206] Brian J. Winkel. Solution to cryptanalysts' corner Scotch homophonic. *Cryptologia*, 4(2):122, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Winkel:1980:TTb

[207] Brian J. Winkel. There and there. *Cryptologia*, 4(2):123–126, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902883~db=all~order=page`.

Anonymous:1980:BCb

[208] Anonymous. Biographies of contributors. *Cryptologia*, 4(2):127–128, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902884~db=all~order=page`.

Kruh:1980:CDT

[209] Louis Kruh. Cipher devices: TRS-80 data privacy system. *Cryptologia*, 4(2):181–183, April 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Deavours:1980:BCCa

[210] Cipher A. Deavours. The Black Chamber: a column. How the British broke Enigma. *Cryptologia*, 4(3):129–132, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902886~db=all~order=page`.

Bright:1980:HSI

[211] Herbert S. Bright. High-speed indirect cryption. *Cryptologia*, 4(3):133–139, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902887~db=all~order=page`.

Pady:1980:FCI

[212] Donald S. Pady and Laura S. Kline. Finger counting and the identification of James VI's secret agents. *Cryptologia*, 4(3):140–149, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902888~db=all~order=page`.

Levine:1980:ADIb

[213] Jack Levine and Robert E. Hartwig. Applications of the Drazin inverse to the Hill cryptographic system. Part II. *Cryptologia*, 4(3):150–168, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.`

informaworld.com/smpp/content~content=a741902889~db=all~order=page.

Barker:1980:OAC

[214] Wayne G. Barker. Opportunities for the amateur cryptanalyst can be anywhere. *Cryptologia*, 4(3):169–172, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902890~db=all~order=page.

Kruh:1980:WDB

[215] Louis Kruh. "The Work of a Diplomat": a book review. *Cryptologia*, 4(3):172, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1980:SCB

[216] David Kahn. Spy ciphers: a book review. *Cryptologia*, 4(3):173–176, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902891~db=all~order=page.

Knight:1980:CCb

[217] H. Gary Knight. Cryptanalysts' corner. *Cryptologia*, 4(3):177–180, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902892~db=all~order=page.

Kruh:1980:CDCb

[218] Louis Kruh. Cipher devices: a column cryptext TRS-80 data privacy system. *Cryptologia*, 4(3):181–183, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902893~db=all~order=page.

Cooper:1980:LTG

[219] R. H. Cooper. Linear transformations in Galois fields and their application to cryptography. *Cryptologia*, 4(3):184–188, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902894~db=all~order=page.

Anonymous:1980:BCc

[220] Anonymous. Biographies of contributors. *Cryptologia*, 4(3):189–190, July 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902895~db=all~order=page.

Ewing:1980:SSW

[221] Sir Alfred Ewing. Some special war work: Part I. *Cryptologia*, 4(4):193–203, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902897~db=all~order=page.

Kochanski:1980:RLL

[222] M. J. Kochanski. Remarks on Lu and Lee's proposals for a public-key cryptosystem. *Cryptologia*, 4(4):204–207, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902898~db=all~order=page.

Knight:1980:CCc

[223] H. Gary Knight. Cryptanalysts' corner. *Cryptologia*, 4(4):208–212, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902899~db=all~order=page`.

Nelson:1980:DCC

[224] Jim Nelson. The development of commercial cryptosystem standards. *Cryptologia*, 4(4):213–224, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902900~db=all~order=page`.

Kruh:1980:CET

[225] Louis Kruh. Cipher equipment: TST-1221. *Cryptologia*, 4(4):225–229, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902901~db=all~order=page`.

Makar:1980:TC

[226] Boshra H. Makar. Transfinite cryptography. *Cryptologia*, 4(4):230–237, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902902~db=all~order=page`.

Kruh:1980:PHR

[227] Louis Kruh. "Pearl Harbor Revisited": a book review. *Cryptologia*, 4(4): 237, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902903~db=all~order=page`. See [1792].

Kahn:1980:PC

[228] David Kahn. A professional's challenge. *Cryptologia*, 4(4):238–239, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902904~db=all~order=page`.

Deavours:1980:BCCb

[229] Cipher A. Deavours. The Black Chamber: a column — la méthode des bâtons. *Cryptologia*, 4(4):240–247, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902905~db=all~order=page`.

Kruh:1980:RVA

[230] Louis Kruh. A remarkable view of ancient America: a book review. *Cryptologia*, 4(4):248–249, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902906~db=all~order=page`.

Anonymous:1980:RRS

[231] Anonymous. Results of reader survey. *Cryptologia*, 4(4):250–251, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902907~db=all~order=page`.

Anonymous:1980:BCd

[232] Anonymous. Biographies of contributors. *Cryptologia*, 4(4):252–253, October 1980. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902908~db=all~order=page`.

Mellen:1981:GSL

[233] Greg Mellen. Graphic solution of a linear transformation cipher. *Cryptologia*, 5(1):1–19, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902952~db=all~order=page`.

Kahn:1981:PS

[234] David Kahn. The public's secrets. *Cryptologia*, 5(1):20–26, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902953~db=all~order=page`.

Rivest:1981:SAH

[235] Ronald L. Rivest. Statistical analysis of the Hagelin cryptograph. *Cryptologia*, 5(1):27–32, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902954~db=all~order=page`.

Ewing:1981:SSW

[236] Sir Alfred Ewing. Some special war work, Part II. *Cryptologia*, 5(1):33–39, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902955~db=all~order=page`.

Mellen:1981:CCa

[237] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 5(1):40–42, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902956~db=all~order=page`.

Deavours:1981:BCC

[238] Cipher A. Deavours. The Black Chamber: a column shutting off the spigot in 1981. *Cryptologia*, 5(1):43–45, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902957~db=all~order=page`.

Kruh:1981:CEC

[239] Louis Kruh. Cipher equipment: Collins CR-200/220 data security unit. *Cryptologia*, 5(1):46–50, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902958~db=all~order=page`.

Rubin:1981:DSC

[240] Frank Rubin. Decrypting a stream cipher based on J–K flip-flops. *Cryptologia*, 5(1):51–57, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902959~db=all~order=page`. Originally published in IEEE

Transactions on Computers. C-28(7): 483–487, 1979. Reprinted in [1789, 283–293].

Kruh:1981:UCB

[241] Louis Kruh. "From the Ultra Conference": a book review. *Cryptologia*, 5(1):58, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902960~db=all~order=page`.

Fischer:1981:TMC

[242] Elliot Fischer. A theoretical measure of cryptographic performance. *Cryptologia*, 5(1):59–62, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902961~db=all~order=page`. Reprinted in [1789, pp. 426–426].

Anonymous:1981:BCa

[243] Anonymous. Biographies of contributors. *Cryptologia*, 5(1):63, January 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902962~db=all~order=page`.

Kahn:1981:GSC

[244] David Kahn. German spy cryptograms. *Cryptologia*, 5(2):65–66, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902965~db=all~order=page`.

Hartwig:1981:ADIa

[245] Robert E. Hartwig and Jack Levine. Applications of the Drazin inverse to the Hill cryptographic system. Part III. *Cryptologia*, 5(2):67–77, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902966~db=all~order=page`.

Kallis:1981:CGC

[246] Stephen A. Kallis, Jr. The Code-O-Graph cipher disks. *Cryptologia*, 5(2): 78–83, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902967~db=all~order=page`.

Sturges:1981:HRP

[247] Gerald Sturges. The House Report on Public Cryptography. *Cryptologia*, 5(2):84–93, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902968~db=all~order=page`.

Costas:1981:HHC

[248] John P. Costas. The hand-held calculator as a cryptographic machine. *Cryptologia*, 5(2):94–117, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902969~db=all~order=page`.

Lembart:1981:PCS

[249] Lee Lembart. The Public Cryptography Study Group: U.S. and mathe-

maticians in code dispute. *Cryptologia*, 5(2):118–122, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902970~db=all~order=page.

Mellen:1981:CCb

[250] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 5(2):123, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902971~db=all~order=page.

Kruh:1981:CPB

[251] Louis Kruh. "A Code Problem": a book review. *Cryptologia*, 5(2):124–125, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902972~db=all~order=page.

Anonymous:1981:BCb

[252] Anonymous. Biographies of contributors. *Cryptologia*, 5(2):126, April 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902973~db=all~order=page.

Anonymous:1981:RPC

[253] Anonymous. Report of the Public Cryptography Study Group. *Cryptologia*, 5(3):130–142, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902975~db=all~order=page.

Davida:1981:CAR

[254] George I. Davida. The case against restraints on non-governmental research in cryptography. *Cryptologia*, 5(3):143–148, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902976~db=all~order=page.

Arnold:1981:PBC

[255] Philip M. Arnold. Palatino and Bibliander on ciphers. *Cryptologia*, 5(3):149–154, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902977~db=all~order=page.

Kruh:1981:RRD

[256] Louis Kruh. "Reward for Reading and Deciphering": a book review. *Cryptologia*, 5(3):155–157, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902978~db=all~order=page.

Fischer:1981:MCP

[257] Elliot Fischer. Measuring cryptographic performance with production processes. *Cryptologia*, 5(3):158–162, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902979~db=all~order=page.

Buck:1981:SHB

[258] R. Creighton Buck. Sherlock Holmes in Babylon. *Cryptologia*, 5(3):163–173, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902980~db=all~order=page.

Kruh:1981:CME

[259] Louis Kruh. Cipher machine exhibit at the Smithsonian Institution. *Cryptologia*, 5(3):174, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902981~db=all~order=page.

Stuerzinger:1981:C

[260] Oskar Stuerzinger. The A-22 cryptograph. *Cryptologia*, 5(3):175–183, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902982~db=all~order=page.

Winkel:1981:TT

[261] Brian J. Winkel. There and there. *Cryptologia*, 5(3):184–190, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902983~db=all~order=page.

Anonymous:1981:BCc

[262] Anonymous. Biographies of contributors. *Cryptologia*, 5(3):191, July 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902984~db=all~order=page.

Kahn:1981:GJB

[263] David Kahn. The genesis of the Jefferson/Bazeries cipher device. *Cryptologia*, 5(4):193–208, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1981:GJB

[264] Louis Kruh. The genesis of the Jefferson/Bazeries cipher device. *Cryptologia*, 5(4):193–208, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902986~db=all~order=page.

Kruh:1981:UGV

[265] Louis Kruh. "A User's Guide in Voice and Data Communications Protection": Book review. *Cryptologia*, 5(4):208–212, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902987~db=all~order=page.

Klingler:1981:LE

[266] L. Klingler. Letter to the Editor. *Cryptologia*, 5(4):209–210, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Costas:1981:LE

[267] J. Costas. Letter to the Editor. *Cryptologia*, 5(4):210–212, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hartwig:1981:ADIb

[268] Robert E. Hartwig and Jack Levine. Applications of the Drazin inverse to the Hill cryptographic system. Part IV. *Cryptologia*, 5(4):213–228, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902988~db=all~order=page`.

Groth:1981:SWE

[269] William Groth. Secret writing exhibit. *Cryptologia*, 5(4):229–230, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902989~db=all~order=page`.

Hammer:1981:HOH

[270] Carl Hammer. Higher-order homophonic ciphers. *Cryptologia*, 5(4):231–242, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902990~db=all~order=page`.

Wolf:1981:NTD

[271] Jack Keil Wolf. "Number Theory in Digital Signal Processing": a book review. *Cryptologia*, 5(4):243–246, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902991~db=all~order=page`. See [1667].

Deavours:1981:ISC

[272] C. A. Deavours. Interactive solution of columnar transposition ciphers. *Cryptologia*, 5(4):247–251, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902992~db=all~order=page`.

Anonymous:1981:BCd

[273] Anonymous. Biographies of contributors. *Cryptologia*, 5(4):252–253, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902993~db=all~order=page`.

Unknown:1981:LE

[274] Unknown. Letters to the Editor. *Cryptologia*, 5(4):??, October 1981. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rejewski:1982:MSE

[275] Marian Rejewski. Mathematical solution of the Enigma cipher. *Cryptologia*, 6(1):1–18, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903044~db=all~order=page`. Translated from the Polish by Christopher Kasparek.

Kasparek:1982:MMR

[276] Christopher Kasparek and Richard A. Woytak. In memoriam Marian Rejewski. *Cryptologia*, 6(1):19–25, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903045~db=all~order=page`.

Kahn:1982:WGL

[277] David Kahn. Why Germany lost the code war. *Cryptologia*, 6(1):26–31, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903046~db=all~order=page.

Kozaczuk:1982:ES

[278] Wldyslaw Kozaczuk. Enigma solved. *Cryptologia*, 6(1):32–33, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903047~db=all~order=page.

Deavours:1982:BC

[279] C. A. Deavours. The Black Chamber. *Cryptologia*, 6(1):34–37, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903048~db=all~order=page.

Kruh:1982:WMB

[280] Louis Kruh. 'Wilderness of Mirrors": a book review. *Cryptologia*, 6(1):38, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903049~db=all~order=page. See [1697].

Kruh:1982:BSM

[281] Louis Kruh. "Beale Society Material": Book reviews. *Cryptologia*, 6(1): 39, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903050~db=all~order=page.

Anderson:1982:IR

[282] Ralph V. Anderson. If I remember. *Cryptologia*, 6(1):40–44, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903051~db=all~order=page.

Mellen:1982:CCa

[283] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 6(1):45–46, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903052~db=all~order=page.

Kahn:1982:CPI

[284] David Kahn. Churchill pleads for the intercepts. *Cryptologia*, 6(1):47–49, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903053~db=all~order=page.

Woytak:1982:CMR

[285] Richard A. Woytak. A conversation with Marian Rejewski. *Cryptologia*, 6(1):50–60, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903054~db=all~order=page.

Hardie:1982:UES

[286] Bradford Hardie. "Unraveling the Enigma Story": a book review. *Cryptologia*, 6(1):61–64, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903055~db=all~order=page`.

Bundy:1982:DHB

[287] William P. Bundy. "From the Depths to the Heights": Book reviews. *Cryptologia*, 6(1):65–74, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903056~db=all~order=page`.

Rejewski:1982:RAB

[288] Marian Rejewski. Remarks on appendix 1 to "British Intelligence in the Second World War" by F. H. Hinsley. *Cryptologia*, 6(1):75–83, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903057~db=all~order=page`.

Kahn:1982:CCB

[289] David Kahn. "Computer Cryptography": a book review. *Cryptologia*, 6(1): 84, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903058~db=all~order=page`.

Kruh:1982:NCB

[290] Louis Kruh. The Navy cipher box Mark II. *Cryptologia*, 6(1):85–93, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903059~db=all~order=page`.

Anonymous:1982:BCa

[291] Anonymous. Biographies of contributors. *Cryptologia*, 6(1):94–95, January 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903060~db=all~order=page`.

Barclay:1982:UMS

[292] Mel L. Barclay and Joshua S. Barclay. Use of microcomputer system for medical record encryption and decryption using a sequential pseudorandom key. *Cryptologia*, 6(2):97–107, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903063~db=all~order=page`.

Fischer:1982:PHT

[293] Elliot Fischer. The performance of Hellman's time-memory trade-off against some rotor ciphers. *Cryptologia*, 6(2):108–114, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903064~db=all~order=page`.

Kahn:1982:NSH

[294] David Kahn. A new source for historians: Yardley's seized manuscript. *Cryptologia*, 6(2):115–119, April 1982. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903065~db=all~order=page.

Kahn:1982:MGJ

[295] David Kahn. In memoriam: Georges-Jean Painvin. *Cryptologia*, 6(2):120–127, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903066~db=all~order=page.

Sloane:1982:ECCa

[296] N. J. A. Sloane. Error-correcting codes and cryptography. Part I. *Cryptologia*, 6(2):128–153, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903067~db=all~order=page. Originally published in *The Mathematical Gardner*, D. A. Klarner (editor), Prindle, Weber & Schmidt, Boston, MA, 1981, pp. 346–382.

Kruh:1982:BRB

[297] Louis Kruh. Book reviews: a book with a book cipher. *Cryptologia*, 6(2):154–168, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903068~db=all~order=page.

Mellen:1982:CCb

[298] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 6(2):169–174, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903069~db=all~order=page.

Deavours:1982:KCP

[299] C. A. Deavours. Konheim's "Cryptography — A Primer": a book review. *Cryptologia*, 6(2):175–176, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903070~db=all~order=page. See [1668].

Kaiserling:1982:S

[300] M. C. W. Kaiserling. Sirius. *Cryptologia*, 6(2):177–178, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903071~db=all~order=page.

Winkel:1982:TTC

[301] Brian J. Winkel. There and there — a column. *Cryptologia*, 6(2):179–188, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903072~db=all~order=page.

Anonymous:1982:BCb

[302] Anonymous. Biographies of contributors. *Cryptologia*, 6(2):189–190, April 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903073~db=all~order=page.

Tucker:1982:RPNa

[303] Dundas P. Tucker. Rhapsody in Purple: a new history of Pearl Harbor — I. *Cryptologia*, 6(3):193–228, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903075~db=all~order=page`.

Berkovits:1982:FS

[304] Shimshon Berkovits. Factoring via superencryption. *Cryptologia*, 6(3):229–237, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903076~db=all~order=page`.

Kruh:1982:MCD

[305] Louis Kruh. The mystery of Colonel Decius Wadsworth's cipher device. *Cryptologia*, 6(3):238–247, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903077~db=all~order=page`.

Mellen:1982:CCc

[306] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 6(3):248–252, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903078~db=all~order=page`.

Morris:1982:CFU

[307] Robert H. Morris. Cryptographic features of the UNIX operating system. *Cryptologia*, 6(3):253–257, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.cs.bell-labs.com/~dmr/crypt.html; http://www.informaworld.com/smpp/content~content=a741903079~db=all~order=page`.

Sloane:1982:ECCb

[308] N. J. A. Sloane. Error-correcting codes and cryptography. Part II. *Cryptologia*, 6(3):258–278, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903080~db=all~order=page`. Originally published in *The Mathematical Gardner*, D. A. Klarner (editor), Prindle, Weber & Schmidt, Boston, MA, 1981, pp. 346–382.

Miller:1982:COA

[309] Donald V. Miller. Ciphertext only attack on the Merkle–Hellman public-key system under broadcast situations. *Cryptologia*, 6(3):279–281, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903081~db=all~order=page`.

Kaiserling:1982:SSM

[310] M. C. W. Kaiserling. Solution to Sirius music cipher. *Cryptologia*, 6(3): 282, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903082~db=all~order=page`.

Deavours:1982:HK

[311] C. A. Deavours. Helmich and the KL-7. *Cryptologia*, 6(3):283–284, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903083~db=all~order=page`.

Anonymous:1982:BCc

[312] Anonymous. Biographies of contributors. *Cryptologia*, 6(3):285–286, July 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903084~db=all~order=page`.

Davies:1982:SHT

[313] Donald W. Davies. The Siemens and Halske T52E cipher machine. *Cryptologia*, 6(4):289–308, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903086~db=all~order=page`.

Mellen:1982:CCd

[314] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 6(4):309–311, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903087~db=all~order=page`.

Akritas:1982:AVT

[315] Alkiviadis G. Akritas. Application of Vincent's Theorem in cryptography or one-time pads made practical. *Cryptologia*, 6(4):312–318, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903088~db=all~order=page`.

Vahle:1982:BPR

[316] M. O. Vahle and L. F. Tolendino. Breaking a pseudo random number based cryptographic algorithm. *Cryptologia*, 6(4):319–328, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903089~db=all~order=page`.

Meijer:1982:DSS

[317] Henk Meijer and Selim Akl. Digital signature schemes. *Cryptologia*, 6(4):329–338, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903090~db=all~order=page`.

Outerbridge:1982:PC

[318] Richard Outerbridge. A pedagogical cipher. *Cryptologia*, 6(4):339–345, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903091~db=all~order=page`. This paper is the winner of the Cryptologia First Annual Undergraduate Paper Competition in Cryptology.

Tucker:1982:RPNb

[319] Dundas P. Tucker. Rhapsody in Purple: a new history of Pearl Harbor: Part two of two. *Cryptologia*, 6(4):346–367, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a741903092~db=all~order=page.

Kallis:1982:CGC

[320] Stephen A. Kallis. A child's garden of cryptography. *Cryptologia*, 6(4):368–377, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a757776453~db=all~order=page.

Kruh:1982:BPB

[321] Louis Kruh. A basic probe of the Beale cipher as a bamboozlement. *Cryptologia*, 6(4):378–382, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903094~db=all~order=page.

Anonymous:1982:BCd

[322] Anonymous. Biographies of contributors. *Cryptologia*, 6(4):383–384, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903095~db=all~order=page.

Kahn:1983:CCR

[323] David Kahn. The Crypto '82 conference, a report on [the] conference. *Cryptologia*, 7(1):1–5, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902490~db=all~order=page.

Mellen:1983:CCa

[324] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 7(1):6–11, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902491~db=all~order=page.

Floyd:1983:ABC

[325] Denis R. Floyd. Annotated bibliography in conventional and public key cryptography. *Cryptologia*, 7(1):12–24, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902492~db=all~order=page.

Morris:1983:FCC

[326] S. Brent Morris. Fraternal cryptography: Cryptographic practices of American fraternal organizations. *Cryptologia*, 7(1):27–36, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902493~db=all~order=page.

Jurgensen:1983:LRU

[327] H. Jurgensen. Language redundancy and the unicity point. *Cryptologia*, 7(1):37–48, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902494~db=all~order=page.

Fak:1983:CPF

[328] Viiveke Fak. Cryptographic protection of files in an automated of-

fice system. *Cryptologia*, 7(1):49–62, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902495~db=all~order=page.

Makar:1983:ACC

[329] Boshra H. Makar. Application of a certain class of infinite matrices to the Hill cryptographic system. *Cryptologia*, 7(1):63–78, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902496~db=all~order=page.

Dyer:1983:PMB

[330] Thomas H. Dyer. "The Power of Magic": a book review. *Cryptologia*, 7(1):79–82, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902497~db=all~order=page.

Kruh:1983:CEC

[331] Louis Kruh. Cipher equipment: the cryptographic unit CSI-10. *Cryptologia*, 7(1):83–88, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902498~db=all~order=page.

Fischer:1983:UHC

[332] Elliot Fischer. Uncaging the Hagelin cryptograph. *Cryptologia*, 7(1):89–92, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902499~db=all~order=page.

Anonymous:1983:BCa

[333] Anonymous. Biographies of contributors. *Cryptologia*, 7(1):93–94, January 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902500~db=all~order=page.

Lundstrom:1983:FRI

[334] John B. Lundstrom. A failure of radio intelligence: An episode in the Battle of the Coral Sea. *Cryptologia*, 7(2):97–118, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902503~db=all~order=page.

Clarke:1983:ASR

[335] Brig. Gen. Carter W. Clarke. From the archives: Statement for record of participation of Brig. Gen. Carter W. Clarke, GSC in the transmittal of letters from Gen. George C. Marshall to Gov. Thomas E. Dewey, the latter part of September, 1944. *Cryptologia*, 7(2):119–131, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902504~db=all~order=page.

Bratzel:1983:ACL

[336] John F. Bratzel and Leslie B. Rout. Abwehr ciphers in Latin America. *Cryptologia*, 7(2):132–144, April 1983. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902505~db=all~order=page.

Kruh:1983:TC

[337] Louis Kruh and C. A. Deavours. The Typex cryptograph. *Cryptologia*, 7 (2):145–166, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902506~db=all~order=page.

Mellen:1983:CCb

[338] Greg Mellen. Cryptanalysis' corner. *Cryptologia*, 7(2):167–169, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902507~db=all~order=page.

Ndam:1983:PRD

[339] Babacar Alassane Ndam and Amadou Sarr. The problem of reciprocity in a Delastelle digraphic substitution. *Cryptologia*, 7(2):170–179, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902508~db=all~order=page.

Simmons:1983:WPP

[340] Gustavus J. Simmons. A "weak" privacy protocol using the RSA crypto algorithm. *Cryptologia*, 7(2):180–182, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902509~db=all~order=page.

Meijer:1983:RDS

[341] Henk Meijer and Selim Akl. Remarks on a digital signature scheme. *Cryptologia*, 7(2):183–186, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902510~db=all~order=page.

Deavours:1983:VAP

[342] C. A. Deavours. The view from across the pond: An interview with the Geneva Management Group. *Cryptologia*, 7(2):187–190, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902511~db=all~order=page.

Anonymous:1983:BCb

[343] Anonymous. Biographies of contributors. *Cryptologia*, 7(2):191–192, April 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902512~db=all~order=page.

Strasser:1983:NCD

[344] Gerhard F. Strasser. The noblest cryptologist: Duke August the Younger of Brunswick–Luneburg (Gustavus Selenus) and his cryptological activities. *Cryptologia*, 7(3):193–217, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.

informaworld.com/smpp/content~content=a741902514~db=all~order=page.

Bennett:1983:UPS

[345] Donald H. Bennett. An unsolved puzzle solved. *Cryptologia*, 7(3):218–234, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902515~db=all~order=page.

Davies:1983:EMS

[346] Donald W. Davies. The early models of the Siemens and Halske T52 cipher machine. *Cryptologia*, 7(3):235–253, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902516~db=all~order=page.

Kahn:1983:ER

[347] David Kahn. Eurocrypt 83: a report. *Cryptologia*, 7(3):254–256, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902517~db=all~order=page.

Mueller-Schloer:1983:GCE

[348] Christian Mueller-Schloer. DES-generated checksums for electronic signatures. *Cryptologia*, 7(3):257–273, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902518~db=all~order=page.

Mellen:1983:CCc

[349] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 7(3):274–277, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902519~db=all~order=page.

Kruh:1983:BMA

[350] Louis Kruh and Greg Mellen. Book, movie, article and game reviews. *Cryptologia*, 7(3):278–286, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902520~db=all~order=page.

Anonymous:1983:BCc

[351] Anonymous. Biographies of contributors. *Cryptologia*, 7(3):287–288, July 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902521~db=all~order=page.

Kruh:1983:HUG

[352] Louis Kruh. How to use the German Enigma cipher machine: a photographic essay. *Cryptologia*, 7(4):291–296, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902523~db=all~order=page.

Leighton:1983:SKB

[353] Albert C. Leighton and Stephen M. Matyas. The search for the key book to Nicholas Trist's book ciphers. *Cryptologia*, 7(4):297–314,

October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902524~db=all~order=page.

Anonymous:1983:AEI

[354] Anonymous. From the archives: Examples of intelligence obtained from cryptanalysis, 1 August 1946. *Cryptologia*, 7(4):315–326, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902525~db=all~order=page.

Winkler:1983:ACG

[355] Peter Winkler. The advent of cryptology in the game of bridge. *Cryptologia*, 7(4):327–332, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902526~db=all~order=page.

Stuerzinger:1983:BC

[356] Oskar Stuerzinger. The B-21 cryptograph. *Cryptologia*, 7(4):333–346, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902527~db=all~order=page.

Brandstrom:1983:PKC

[357] Hugo Brändström. A public-key cryptosystem based upon equations over a finite field. *Cryptologia*, 7(4):347–358, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902528~db=all~order=page.

Wolf:1983:RMB

[358] Daniel Wolf. ROTERM: a microprocessor based cipher terminal system. *Cryptologia*, 7(4):359–370, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902529~db=all~order=page.

Mellen:1983:CCd

[359] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 7(4):371–374, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902530~db=all~order=page.

Kruh:1983:BR

[360] Louis Kruh. Book reviews. *Cryptologia*, 7(4):375–379, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902531~db=all~order=page.

Anonymous:1983:BCd

[361] Anonymous. Biographies of contributors. *Cryptologia*, 7(4):380–381, October 1983. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902532~db=all~order=page.

Levine:1984:UCP

[362] J. Levine. U.S. cryptographic patents 1861–1981. *Cryptologia*, 8(??):??, ???? 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Simmons:1984:SVU

[363] Gustavus J. Simmons. A system for verifying user identity and authorization at the point-of sale or access. *Cryptologia*, 8(1):1–21, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902567~db=all~order=page`.

Sorkin:1984:LCA

[364] Arthur Sorkin. LUCIFER, a cryptographic algorithm. *Cryptologia*, 8 (1):22–42, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902568~db=all~order=page`. See also erratum, Cryptologia **7**, 1978, p. 118.

Kruh:1984:RTC

[365] Louis Kruh and Greg Mellen. Reviews of things cryptologic. *Cryptologia*, 8(1):43–53, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902569~db=all~order=page`.

Kruh:1984:WDI

[366] Louis Kruh. Who did it? *Cryptologia*, 8(1):54, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902570~db=all~order=page`.

Mellen:1984:CCa

[367] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 8(1):55–57, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902571~db=all~order=page`.

Kahn:1984:CMI

[368] David Kahn. Cipher machine inventor — Boris Hagelin dies. *Cryptologia*, 8(1):60–61, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902572~db=all~order=page`.

Yardley:1984:AAC

[369] Herbert O. Yardley. From the archives: Achievements of Cipher Bureau MI-8 during the First World War. documents by Major Herbert O. Yardley prepared under the direction of the Chief Signal Officer, 25 May 1945, SPSIS-1. Signal Security Agency. Washington, DC. *Cryptologia*, 8(1):62–74, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902573~db=all~order=page`.

Kruh:1984:BFI

[370] Louis Kruh. Because of the Freedom of Information Act (FOIA). *Cryptologia*, 8(1):75–77, January 1984. CODEN

CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902574~db=all~order=page.

Kruh:1984:CD

[371] Louis Kruh. Cipher devices. *Cryptologia*, 8(1):78–79, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902575~db=all~order=page.

Gillogly:1984:MA

[372] James J. Gillogly. The mysterious autocryptograph. *Cryptologia*, 8(1):79–81, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902576~db=all~order=page.

Davies:1984:A

[373] Donald W. Davies. The Autocryptograph. *Cryptologia*, 8(1):82–92, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902577~db=all~order=page.

Anonymous:1984:BCa

[374] Anonymous. Biographies of contributors. *Cryptologia*, 8(1):93–94, January 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902578~db=all~order=page.

Retter:1984:CMM

[375] Charles T. Retter. Cryptanalysis of a Maclaren–Marsaglia system. *Cryptologia*, 8(2):97–108, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902581~db=all~order=page. See also letters and responses, Cryptologia **8**, 1984, pp. 374–378.

Anonymous:1984:PSO

[376] Anonymous. Project on secrecy and openness in scientific and technical communication. *Cryptologia*, 8(2):109–111, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902582~db=all~order=page.

Kruh:1984:HHC

[377] Louis Kruh. Hand-held crypto device SEC-36. *Cryptologia*, 8(2):112–114, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902583~db=all~order=page.

Davies:1984:SHC

[378] Donald W. Davies. Sidney Hole's cryptographic machine. *Cryptologia*, 8(2):115–126, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902584~db=all~order=page.

Kruh:1984:LR

[379] Louis Kruh. Literature reviews. *Cryptologia*, 8(2):127–131, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902585~db=all~order=page.

Tilt:1984:KTM

[380] Borge Tilt. On Kullback's χ-tests for matching and non-matching multinomial distributions. *Cryptologia*, 8 (2):132–141, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902586~db=all~order=page; http://www.informaworld.com/smpp/content~content=a757776821~db=all~order=page.

Carroll:1984:SPM

[381] John M. Carroll and Pierre G. Laurin. Software protection for microcomputers. *Cryptologia*, 8(2):142–160, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902587~db=all~order=page.

Levine:1984:CPC

[382] Jack Levine. Corrections for published copy of United States cryptographic patents: 1861–1981. *Cryptologia*, 8(2):161–162, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902588~db=all~order=page.

Kruh:1984:SRC

[383] Louis Kruh. The Slidex RT code. *Cryptologia*, 8(2):163–172, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902589~db=all~order=page.

Erskine:1984:BIV

[384] Ralph Erskine. "British Intelligence — Volume II" — book review. *Cryptologia*, 8(2):173–180, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902590~db=all~order=page.

Anonymous:1984:ACC

[385] Anonymous. From the archives: Codes and ciphers for combined air-amphibian operations. *Cryptologia*, 8(2):181–186, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902591~db=all~order=page.

Shulman:1984:UCD

[386] David Shulman. An unknown cipher disk. *Cryptologia*, 8(2):187–190, April 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902592~db=all~order=page.

Anonymous:1984:BS

[387] Anonymous. Biographical sketches. *Cryptologia*, 8(2):191–192, April 1984.

CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902593~db=all~order=page.

Hammant:1984:ORN

[388] Thomas R. Hammant. The origins of Russian Navy communications intelligence. *Cryptologia*, 8(3):193–202, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902595~db=all~order=page.

Guelker:1984:CWM

[389] Francis Guelker. A cryptographer's war memories. *Cryptologia*, 8(3):203–207, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902596~db=all~order=page.

Weller:1984:RAJ

[390] Robert Weller. Rear Admiral Joseph N. Wenger USN (Ret) and the Naval Cryptologic Museum. *Cryptologia*, 8(3):208–234, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902597~db=all~order=page.

Arnold:1984:VRC

[391] Philip M. Arnold. "A View of Renaissance Cryptography" — a book review. *Cryptologia*, 8(3):235–241, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902598~db=all~order=page.

Deavours:1984:RSA

[392] C. A. Deavours. Reflections on the "state of the art". *Cryptologia*, 8(3):242–245, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902599~db=all~order=page.

Kruh:1984:CLa

[393] Louis Kruh. Cryptology and the law. *Cryptologia*, 8(3):246–248, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902600~db=all~order=page.

Kruh:1984:CE

[394] Louis Kruh. Cipher equipment. *Cryptologia*, 8(3):249, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902601~db=all~order=page.

Davies:1984:SPS

[395] Donald W. Davies. Sir Percy Scott's cypher. *Cryptologia*, 8(3):250–252, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902602~db=all~order=page.

Delaurentis:1984:FWC

[396] John M. Delaurentis. A further weakness in the Common Modu-

lus Protocol for the RSA cryptoalgorithm. *Cryptologia*, 8(3):253–259, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902603~db=all~order=page`.

Carroll:1984:RMK

[397] John M. Carroll. The resurrection of multiple-key ciphers. *Cryptologia*, 8(3):262–265, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902604~db=all~order=page`.

Blakley:1984:ACS

[398] G. R. Blakley. AAAS crypto sessions proceedings: Review. *Cryptologia*, 8(3):266–269, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902605~db=all~order=page`.

Mellen:1984:CCb

[399] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 8(3):270–275, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902606~db=all~order=page`.

Kruh:1984:CET

[400] Louis Kruh. Cipher equipment: Tst 3336 and Tst 9761. *Cryptologia*, 8(3):278–284, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902607~db=all~order=page`.

Jueneman:1984:IAB

[401] Robert R. Jueneman. IACR announces bulletin board service. *Cryptologia*, 8(3):285–286, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902608~db=all~order=page`.

Anonymous:1984:BCb

[402] Anonymous. Biographies of contributors. *Cryptologia*, 8(3):287–288, July 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902609~db=all~order=page`.

Kruh:1984:HC

[403] Louis Kruh. The heraldry of cryptology. *Cryptologia*, 8(4):289–301, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902611~db=all~order=page`.

Landsverk:1984:CRI

[404] O. G. Landsverk. Cryptography in runic inscriptions. *Cryptologia*, 8(4):302–319, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902612~db=all~order=page`. See remark [920].

Mellen:1984:CCc

[405] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 8(4):320–325, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902613~db=all~order=page.

Kruh:1984:CLb

[406] Louis Kruh. Cryptology and the law. *Cryptologia*, 8(4):326–331, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902614~db=all~order=page.

Erskine:1984:ATE

[407] Ralph Erskine. *Alan Turing: The Enigma* — book review. *Cryptologia*, 8(4):332–336, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902615~db=all~order=page.

Kullback:1984:LB

[408] Solomon Kullback. Looking back. *Cryptologia*, 8(4):337–342, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902616~db=all~order=page.

Cooper:1984:GKA

[409] Rodney Cooper and Wayne Patterson. A generalization of the knapsack algorithm using Galois fields. *Cryptologia*, 8(4):343–347, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902617~db=all~order=page.

Anderson:1984:FVS

[410] Roland Anderson. Finding vowels in simple substitution ciphers by computer. *Cryptologia*, 8(4):348–359, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902618~db=all~order=page.

Deavours:1984:CSS

[411] C. A. Deavours and Brian J. Winkel. "Cryptanalysis of Shift Stream Generated Stream Cipher Systems": Book review. *Cryptologia*, 8(4):360–363, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902619~db=all~order=page. See [1669].

Kruh:1984:TTR

[412] Louis Kruh. There and there — reviews and news. *Cryptologia*, 8(4):364–373, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902620~db=all~order=page.

Anonymous:1984:BCc

[413] Anonymous. Biographies of contributors. *Cryptologia*, 8(4):379–380, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a741902621~db=all~order=page.

Unknown:1984:ATE

[414] Unknown. Alan Turing: The Enigma. *Cryptologia*, 8(4):??, October 1984. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1985:AAB

[415] David Kahn. The annotated The American Black Chamber. *Cryptologia*, 9(1):1–37, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902691~db=all~order=page.

Kruh:1985:AVS

[416] Louis Kruh. An armchair view of the Smithsonian Institution cipher machine exhibit. *Cryptologia*, 9(1):38–51, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902692~db=all~order=page.

Erskine:1985:ESS

[417] Ralph Erskine. An early success story. *Cryptologia*, 9(1):52–54, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902693~db=all~order=page.

Gillogly:1985:FPM

[418] James J. Gillogly. Fast pattern matching for word lists. *Cryptologia*, 9(1):55–62, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902694~db=all~order=page.

Franksen:1985:EW

[419] Ole Immanuel Franksen. Expert witness. *Cryptologia*, 9(1):63–69, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902695~db=all~order=page.

Mellen:1985:CCa

[420] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 9(1):70–74, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902696~db=all~order=page.

Scott:1985:WOE

[421] Robert Scott. Wide-open encryption design offers flexible implementations. *Cryptologia*, 9(1):75–91, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902697~db=all~order=page.

Murray:1985:CB

[422] Master Sgt. Charles Murray. The crypt bug. *Cryptologia*, 9(1):92, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902698~db=all~order=page.

Anonymous:1985:BCa

[423] Anonymous. Biographies of contributors. *Cryptologia*, 9(1):95–96, January 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902699~db=all~order=page`.

Michener:1985:GRC

[424] John R. Michener. The "generalized rotor" cryptographic operator and some of its applications. *Cryptologia*, 9(2): 97–113, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902702~db=all~order=page`.

Retter:1985:KSA

[425] Charles T. Retter. A key-search attack on Maclaren–Marsaglia systems. *Cryptologia*, 9(2):114–130, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902703~db=all~order=page`.

Mitchell:1985:PSC

[426] Douglas W. Mitchell. A polygraphic substitution cipher based on multiple interlocking applications of Playfair. *Cryptologia*, 9(2):131–139, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902704~db=all~order=page`.

Varadharajan:1985:ERC

[427] V. Varadharajan and R. Odoni. Extension of RSA cryptosystems to matrix rings. *Cryptologia*, 9(2):140–153, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902705~db=all~order=page`.

Kruh:1985:CE

[428] Louis Kruh. Cipher equipment. *Cryptologia*, 9(2):154, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902706~db=all~order=page`.

Davies:1985:CWC

[429] Donald W. Davies. Charles Wheatstone's cryptograph and Pletts' cipher machine. *Cryptologia*, 9(2):155–160, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902707~db=all~order=page`.

Mellen:1985:CCb

[430] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 9(2):161–166, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902708~db=all~order=page`.

Price:1985:CCS

[431] Robert Price. A conversation with Claude Shannon: one man's approach to problem solving. *Cryptologia*, 9 (2):167–175, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~`

content=a741902709~db=all~order=page.

Kruh:1985:RL

[432] Louis Kruh. Reviews of the literature. *Cryptologia*, 9(2):176–186, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902710~db=all~order=page.

Anonymous:1985:BCb

[433] Anonymous. Biographies of contributors. *Cryptologia*, 9(2):188–189, April 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902711~db=all~order=page.

Michener:1985:AGR

[434] John R. Michener. Application of the generalized rotor cryptographic operator in the construction of substitution-permutation network block codes. *Cryptologia*, 9(3):193–201, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902713~db=all~order=page.

Kruskal:1985:TCS

[435] Joseph R. Kruskal. A trigraph cipher with a short key for hand use. *Cryptologia*, 9(3):202–222, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902714~db=all~order=page.

Williams:1985:SPK

[436] H. C. Williams. Some public-key crypto-functions as intractable as factorization. *Cryptologia*, 9(3):223–237, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902715~db=all~order=page.

Outerbridge:1985:DLA

[437] Richard Outerbridge. DEA and Lucifer available on Compuserve. *Cryptologia*, 9(3):238–239, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902716~db=all~order=page.

Kranz:1985:EHR

[438] Fred W. Kranz. Early history of Riverbank Acoustical Laboratories. *Cryptologia*, 9(3):240–246, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902717~db=all~order=page.

Winkel:1985:TTC

[439] Brian J. Winkel. There and there — a column of news. *Cryptologia*, 9(3):247–251, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902718~db=all~order=page.

Kruh:1985:KLC

[440] Louis Kruh. The Kryha Liliput ciphering machine. *Cryptologia*, 9(3):252–261, June 1985. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902719~db=all~order=page.

Erskine:1985:BIV

[441] Ralph Erskine. British Intelligence — Volume 3, Part 1 — book review. *Cryptologia*, 9(3):262–272, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902720~db=all~order=page.

Kruh:1985:CLIa

[442] Louis Kruh. Cryptology and the law — III. *Cryptologia*, 9(3):273–285, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902721~db=all~order=page.

Anonymous:1985:BCc

[443] Anonymous. Biographies of contributors. *Cryptologia*, 9(3):287–288, June 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902722~db=all~order=page.

Mellen:1985:CCc

[444] Greg Mellen. Cryptanalysts' corner. *Cryptologia*, 9(4):289–293, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902724~db=all~order=page.

Kruh:1985:RTC

[445] Louis Kruh and Ralph Erskine. Review of things cryptologic. *Cryptologia*, 9 (4):294–305, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902725~db=all~order=page.

Anonymous:1985:FOS

[446] Anonymous. Forty one and strong: Arlington Hall Station. *Cryptologia*, 9 (4):306–310, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902726~db=all~order=page.

Kruh:1985:ACS

[447] Louis Kruh. Automatic communications with the SIGABA and the M-294. *Cryptologia*, 9(4):311–315, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902727~db=all~order=page.

Erskine:1985:EPC

[448] Ralph Erskine. "Enigma and the Polish Contribution": Book review. *Cryptologia*, 9(4):316–323, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902728~db=all~order=page.

Kruh:1985:ECS

[449] Louis Kruh. Early communications security in the U.S. Navy.

Cryptologia, 9(4):324–331, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902729~db=all~order=page.

Atha:1985:BCH

[450] Robert I. Atha. Bombe! "I could hardly believe it!". *Cryptologia*, 9 (4):332–336, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902730~db=all~order=page.

Ephron:1985:ACA

[451] Henry D. Ephron. An American cryptanalyst in Australia. *Cryptologia*, 9 (4):337–340, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902731~db=all~order=page.

Kruh:1985:CLIb

[452] Louis Kruh. Cryptology and the law — IV. *Cryptologia*, 9(4):348–350, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902732~db=all~order=page.

August:1985:ITA

[453] David August. Information theoretic approach to secure LSFR ciphers. *Cryptologia*, 9(4):351–359, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902733~db=all~order=page.

Yagisawa:1985:NMR

[454] Masahiro Yagisawa. A new method for realizing public-key cryptosystem. *Cryptologia*, 9(4):360–371, 380, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902734~db=all~order=page.

Atkinson:1985:COL

[455] Russell Atkinson. Ciphers in oriental languages. *Cryptologia*, 9(4):373–380, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902735~db=all~order=page.

Anonymous:1985:BCd

[456] Anonymous. Biographies of contributors. *Cryptologia*, 9(4):381–382, October 1985. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902736~db=all~order=page.

Winkel:1986:LOE

[457] Brian J. Winkel. Letter from one of the Editors. *Cryptologia*, 10(1): 1, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902910~db=all~order=page.

Kruh:1986:CPC

[458] Louis Kruh. The control of public cryptography and freedom of speech — a review. *Cryptologia*, 10(1):2–9, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902911~db=all~order=page`.

Anonymous:1986:BCa

[459] Anonymous. Biographies of contributors. *Cryptologia*, 10(1):9, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902912~db=all~order=page`.

Anderson:1986:IMR

[460] Roland Anderson. Improving the machine recognition of vowels in simple substitution ciphers. *Cryptologia*, 10 (1):10–22, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902913~db=all~order=page`.

Barlow:1986:MSA

[461] Mike Barlow. A machine solution of the AMSCO cipher. *Cryptologia*, 10(1):23–33, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902914~db=all~order=page`.

Weierud:1986:MSB

[462] Frode Weierud. Machine secrets: a book review. *Cryptologia*, 10(1):34–37, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902915~db=all~order=page`.

Kahn:1986:SC

[463] David Kahn. Secrets of the code-breakers. *Cryptologia*, 10(1):38–41, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902916~db=all~order=page`.

Kruh:1986:ART

[464] Louis Kruh. Announcements and reviews of things cryptologic. *Cryptologia*, 10(1):42–45, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902917~db=all~order=page`.

Deavours:1986:EIC

[465] C. A. Deavours. Elle a de l'intelligence et de la conversation. *Cryptologia*, 10(1):47–49, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902918~db=all~order=page`.

Erskine:1986:AGC

[466] Ralph Erskine. From the archives: GC and CS mobilizes 'Men of the Professor Type'. *Cryptologia*, 10(1):50–59, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a782216711~db=all~order=page`.

Kruh:1986:CSEa

[467] Louis Kruh. 18th Century shorthand expert needed. *Cryptologia*, 10(1):60–62, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902920~db=all~order=page`.

Kruh:1986:CE

[468] Louis Kruh. Cipher equipment. *Cryptologia*, 10(1):63, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902921~db=all~order=page`.

Davies:1986:CEB

[469] Donald W. Davies. Cipher equipment: Bolton's cypher wheel. *Cryptologia*, 10(1):64, January 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902922~db=all~order=page`.

Kruh:1986:TM

[470] Louis Kruh. The Truman Memorandum. *Cryptologia*, 10(2):65–74, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902925~db=all~order=page`.

Desnoyers:1986:CEPa

[471] Charles-Hubert Desnoyers. Cryptanalytic essay — Part I: Solution of problem no. 166 published in elementary cryptanalysis. *Cryptologia*, 10(2):75–95, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902926~db=all~order=page`.

Roggeman:1986:RAC

[472] Yves Roggeman. Remarks on the auto-correlation function of binary periodic sequences. *Cryptologia*, 10(2):96–100, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902927~db=all~order=page`.

Kruh:1986:CLVa

[473] Louis Kruh. Cryptology and the law — V. *Cryptologia*, 10(2):101–107, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902928~db=all~order=page`.

Kruh:1986:RTCa

[474] Louis Kruh. Reviews of things cryptologic. *Cryptologia*, 10(2):110–122, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902929~db=all~order=page`.

Minow:1986:NT

[475] Martin Minow. No title. *Cryptologia*, 10(2):123–125, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902930~db=all~order=page`.

Kruh:1986:CSEb

[476] Louis Kruh. 18th Century shorthand expert needed (re-run). *Cryptologia*, 10(2):126–127, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902931~db=all~order=page`.

Anonymous:1986:BCb

[477] Anonymous. Biographies of contributors. *Cryptologia*, 10(2):128, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902932~db=all~order=page`.

Unknown:1986:DTS

[478] Unknown. Has Dr. Thouless survived death? *Cryptologia*, 10(2):??, April 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1986:CLVb

[479] Louis Kruh. Cryptology and the law — VI. *Cryptologia*, 10(3):129–133, July 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902934~db=all~order=page`.

Bloch:1986:EDD

[480] Gilbert Bloch and Ralph Erskine. Enigma: the dropping of the double encipherment. *Cryptologia*, 10(3):134–141, July 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902935~db=all~order=page`.

Outerbridge:1986:SDC

[481] Richard Outerbridge. Some design criteria for Feistel-cipher key schedules. *Cryptologia*, 10(3):142–156, July 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902936~db=all~order=page`.

Desnoyers:1986:CEPb

[482] Charles-Hubert Desnoyers. Cryptanalytic essay — Part II: Solution of problem no. 166 published in elementary cryptanalysis. *Cryptologia*, 10(3):158–183, July 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902937~db=all~order=page`.

Kruh:1986:RTCb

[483] Louis Kruh. Reviews of things cryptologic. *Cryptologia*, 10(3):184–191, July 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902938~db=all~order=page`.

Anonymous:1986:BCc

[484] Anonymous. Biographies of contributors. *Cryptologia*, 10(3):192, July 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902939~db=all~order=page`.

Carroll:1986:ACS

[485] John M. Carroll and Steve Martin. The automated cryptanalysis of substitu-

tion ciphers. *Cryptologia*, 10(4):193–209, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902941~db=all~order=page.

Barlow:1986:VMV

[486] Michael Barlow. The Voynich Manuscript — by Voynich? *Cryptologia*, 10(4):210–216, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902942~db=all~order=page.

Rubin:1986:FKP

[487] Frank Rubin. Foiling the known-plaintext attack. *Cryptologia*, 10(4):217–223, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902943~db=all~order=page.

Anonymous:1986:FIP

[488] Anonymous. Free IBM-PC encryption software. *Cryptologia*, 10(4):224, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902944~db=all~order=page.

Outerbridge:1986:CCC

[489] Richard Outerbridge. Cadbury code confidential. *Cryptologia*, 10(4):225–226, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902945~db=all~order=page.

Erskine:1986:LPH

[490] Ralph Erskine. "A Link With Pearl Harbor?" book review. *Cryptologia*, 10(4):227–229, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902946~db=all~order=page.

Mache:1986:G

[491] Wolfgang W. Mache. Geheimschreiber. *Cryptologia*, 10(4):230–242, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902947~db=all~order=page.

Deavours:1986:AMG

[492] Cipher A. Deavours and Louis Kruh. Appendix: Mechanics of the German telecipher machine. *Cryptologia*, 10(4):243–247, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902948~db=all~order=page.

Kruh:1986:CLVc

[493] Louis Kruh. Cryptology and the law — VII. *Cryptologia*, 10(4):248–253, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902949~db=all~order=page.

Anonymous:1986:BCd

[494] Anonymous. Biographies of contributors. *Cryptologia*, 10(4):254–255, October 1986. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902950~db=all~order=page.

Kochanski:1987:SDI

[495] Martin Kochanski. A survey of data insecurity packages. *Cryptologia*, 11 (1):1–15, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902995~db=all~order=page.

Winternitz:1987:CKA

[496] Robert Winternitz and Martin Hellman. Chosen-key attacks on a block cipher. *Cryptologia*, 11(1):16–20, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902996~db=all~order=page.

Levitin:1987:ECT

[497] Samuel M. Levitin. Equivalence classes: Toward more efficient search. *Cryptologia*, 11(1):21–28, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902997~db=all~order=page.

Schick:1987:S

[498] Joseph S. Schick. With the 849th SIS, 1942–45. *Cryptologia*, 11(1):29–39, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902998~db=all~order=page.

Hardie:1987:PPC

[499] Bradford Hardie. The POTUS-prime connection: Two notes (1) Roosevelt, Churchill, and me. *Cryptologia*, 11 (1):40–43, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902999~db=all~order=page.

Anonymous:1987:HCM

[500] Anonymous. (2) History of Converter M-134-C Top Secret Chapter XVIII. the Zero Machine. *Cryptologia*, 11 (1):44–46, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903000~db=all~order=page.

Deavours:1987:CCK

[501] C. A. Deavours. Cryptology courses at Kean College. *Cryptologia*, 11(1):47–50, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903001~db=all~order=page.

Kruh:1987:RTCa

[502] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 11(1):51–63, January 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.

informaworld.com/smpp/content~content=a741903002~db=all~order=page.

Bundy:1987:SMW

[503] William P. Bundy. Some of my wartime experiences. *Cryptologia*, 11(2):65–77, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903005~db=all~order=page.

Beesly:1987:WWT

[504] Patrick Beesly. Who was the third man at Pyry? *Cryptologia*, 11(2):78–80, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903006~db=all~order=page.

Kahn:1987:CBF

[505] David Kahn. The codebreaker behind the footlights. *Cryptologia*, 11(2):81–84, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903007~db=all~order=page.

Gouaz:1987:NHS

[506] Linda Y. Gouaz. Needles and haystacks: the search for Ultra in the 1930's (an excerpt). *Cryptologia*, 11(2):85–92, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903008~db=all~order=page.

Gillogly:1987:BEC

[507] James J. Gillogly. Breaking an Eighteenth Century shorthand system. *Cryptologia*, 11(2):93–98, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903009~db=all~order=page.

Anonymous:1987:CCC

[508] Anonymous. Cadbury caper or cipher? *Cryptologia*, 11(2):99–101, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903010~db=all~order=page.

Rubin:1987:FEK

[509] Frank Rubin. Foiling an exhaustive key-search attack. *Cryptologia*, 11(2):102–107, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903011~db=all~order=page.

Michener:1987:UCN

[510] John R. Michener. The use of complete, nonlinear, block codes for nonlinear, noninvertible mixing of pseudorandom sequences. *Cryptologia*, 11(2):108–111, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903012~db=all~order=page.

Richardson:1987:DES

[511] Robert M. Richardson. Digital Encryption Standard Users Group. *Cryptologia*, 11(2):112–114, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL

http://www.informaworld.com/smpp/content~content=a741903013~db=all~order=page.

Cheatham:1987:MDS

[512] Tom Cheatham. Message decryption and spelling checkers. *Cryptologia*, 11(2):115–118, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903014~db=all~order=page.

Kruh:1987:OCD

[513] Louis Kruh. An obscure cryptographic device. *Cryptologia*, 11(2):119–122, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903015~db=all~order=page.

Kruh:1987:RTCb

[514] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 11(2):123–128, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903016~db=all~order=page.

Whitaker:1987:BPB

[515] Paul Whitaker and Louis Kruh. From Bletchley Park to Berchtesgaden. *Cryptologia*, 11(3):129–141, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903018~db=all~order=page.

Bloch:1987:EBUa

[516] Gilbert Bloch and C. A. Deavours. ENIGMA before ULTRA: Polish work and the French contribution. *Cryptologia*, 11(3):142–155, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903019~db=all~order=page. Translated by C. A. Deavours. Reprinted in [1793, pp. 373–386].

Kruh:1987:SVF

[517] Louis Kruh. The shortsighted view of a foresighted Admiral. *Cryptologia*, 11(3):156–159, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903020~db=all~order=page.

Anonymous:1987:AMN

[518] Anonymous. From the archives: Memorandum on non-military codes and ciphers. *Cryptologia*, 11(3):160–161, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903021~db=all~order=page.

Deavours:1987:SBT

[519] C. A. Deavours. Sois belle et tais-toi. *Cryptologia*, 11(3):162–165, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903022~db=all~order=page.

Michener:1987:AKD

[520] John R. Michener. The application of key dependent and variable rotor sets to generalized rotor cryptographic systems. *Cryptologia*, 11(3): 166–171, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903023~db=all~order=page`.

Sancho:1987:EMD

[521] Justo Sancho. Enumeration of multivariable decipherable Boolean functions. *Cryptologia*, 11(3):172–181, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903024~db=all~order=page`.

Kak:1987:SIS

[522] Subhash C. Kak. The study of the Indus script general considerations. *Cryptologia*, 11(3):182–191, July 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903025~db=all~order=page`.

Carroll:1987:ACP

[523] John M. Carroll and Lynda Robbins. The automated cryptanalysis of polyalphabetic ciphers. *Cryptologia*, 11 (4):193–205, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903027~db=all~order=page`.

Bennett:1987:AEA

[524] John Bennett. Analysis of the encryption algorithm used in the WordPerfect word processing program. *Cryptologia*, 11(4):206–210, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903028~db=all~order=page`.

Levine:1987:SFC

[525] Jack Levine and Richard Chandler. Some further cryptographic applications of permutation polynomials. *Cryptologia*, 11(4):211–218, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903029~db=all~order=page`.

Clarke:1987:GCC

[526] William F. Clarke. Government Code and Cypher School: Its foundation and development with special reference to its Naval side. *Cryptologia*, 11(4):219–226, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903030~db=all~order=page`.

Bloch:1987:EBUb

[527] Gilbert Bloch and C. A. Deavours. Enigma before Ultra: the Polish success and check (1933–1939). *Cryptologia*, 11(4):227–234, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=`

a741903031~db=all~order=page. Translated by C. A. Deavours. Reprinted in [1793, pp. 387–394].

Erskine:1987:NEM

[528] Ralph Erskine and Frode Weierud. Naval Enigma: M4 and its rotors. *Cryptologia*, 11(4):235–244, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903032~db=all~order=page.

Kruh:1987:BRC

[529] Louis Kruh. British Rockex cipher machines. *Cryptologia*, 11(4):245–247, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903033~db=all~order=page.

Kruh:1987:RTCc

[530] Louis Kruh and Ralph Erskine. Reviews and things cryptologic. *Cryptologia*, 11(4):248–253, October 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903034~db=all~order=page.

Barlow:1988:VS

[531] Michael Barlow. Voynich solved? *Cryptologia*, 12(??):??, ???? 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Pearson:1988:CCC

[532] Peter K. Pearson. Cryptanalysis of the Ciarcia Circuit Cellar Data Encryptor. *Cryptologia*, 12(1):1–10, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903097~db=all~order=page.

Hammer:1988:SOH

[533] Carl Hammer. Second order homophonic ciphers. *Cryptologia*, 12(1):11–20, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903098~db=all~order=page.

Michener:1988:RDE

[534] John Michener. Recent developments in electronic circuitry and their effects on the implementation of substitution-permutation block codes. *Cryptologia*, 12(1):21–24, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903099~db=all~order=page.

Rubin:1988:CUP

[535] Frank Rubin. The cryptographic uses of Post tag systems. *Cryptologia*, 12 (1):25–33, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903100~db=all~order=page.

Kruh:1988:RTCa

[536] Louis Kruh, Ralph Erskine, and Michael Barlow. Reviews and things cryptologic. *Cryptologia*, 12(1):37–51, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a741903101~db=all~order=page.

Clarke:1988:YB

[537] William F. Clarke. The years between. *Cryptologia*, 12(1):52–58, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903102~db=all~order=page.

Erskine:1988:ATD

[538] Ralph Erskine. From the archives: Tunny decrypts. *Cryptologia*, 12(1):59–61, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903103~db=all~order=page.

Arnold:1988:HYG

[539] Jonathan P. Arnold. Herbert O. Yardley, gangbuster. *Cryptologia*, 12(1):62–64, January 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903104~db=all~order=page.

Kruh:1988:SBC

[540] Louis Kruh. Stimson, the Black Chamber, and the "Gentlemen's Mail" quote. *Cryptologia*, 12(2):65–89, April 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903107~db=all~order=page.

Clarke:1988:BP

[541] William F. Clarke. Bletchley Park 1941–1945. *Cryptologia*, 12(2):90–97, April 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903108~db=all~order=page. Reprinted in [1793, pp. 227–234].

Erskine:1988:AUB

[542] Ralph Erskine. From the archives: U-boat HF WT signalling. *Cryptologia*, 12(2):98–106, April 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903109~db=all~order=page.

Wayner:1988:RRC

[543] Peter Wayner. A redundancy reducing cipher. *Cryptologia*, 12(2):107–112, April 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903110~db=all~order=page.

Kak:1988:AC

[544] Subhash Kak. The Āryabhaṭa cipher. *Cryptologia*, 12(2):113–117, April 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903111~db=all~order=page.

Kruh:1988:RTCb

[545] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 12(2):118–127, April 1988. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903112~db=all~order=page.

Kak:1988:FAI

[546] Subhash C. Kak. A frequency analysis of the Indus script. *Cryptologia*, 12(3): 129–143, July 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903114~db=all~order=page.

Ellison:1988:SHM

[547] Carl M. Ellison. A solution of the Hebern messages. *Cryptologia*, 12(3): 144–158, July 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903115~db=all~order=page.

Jamnig:1988:SRC

[548] Peter Jamnig. Securing the RSA-cryptosystem against cycling attacks. *Cryptologia*, 12(3):159–164, July 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903116~db=all~order=page.

Kochanski:1988:ADI

[549] Martin Kochanski. Another data insecurity package. *Cryptologia*, 12(3):165–173 (or 165–177??), July 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903117~db=all~order=page.

Clarke:1988:PWO

[550] William F. Clarke. Post war organization. *Cryptologia*, 12(3):174–177, July 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903118~db=all~order=page.

Bloch:1988:EAU

[551] Gilbert Bloch and C. A. Deavours. Enigma avant Ultra, Enigma before Ultra. *Cryptologia*, 12(3):178–184, July 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903119~db=all~order=page. Translated by C. A. Deavours. Reprinted in [1793, pp. 395–401].

Kruh:1988:RTCc

[552] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 12(3):185–192, July 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741903120~db=all~order=page.

Carroll:1988:UBD

[553] John M. Carroll and Lynda E. Robbins. Using binary derivatives to test an enhancement of DES. *Cryptologia*, 12(4):193–208, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741908083~db=all~order=page.

Miller:1988:CTR

[554] Donald V. Miller. Cryptanalysis of a two round version of DES using index implications. *Cryptologia*, 12(4):209–219, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908084~db=all~order=page`.

Matthews:1988:EMF

[555] Robert Matthews. An empirical method for finding the keylength of periodic ciphers. *Cryptologia*, 12(4):220–224, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908085~db=all~order=page`.

Kurosawa:1988:PKC

[556] Kaoru Kurosawa, Toshiya Ito, and Masashi Takeuchi. Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number. *Cryptologia*, 12(4):225–233, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908086~db=all~order=page`.

Polis:1988:ENA

[557] Richard I. Polis. European needs and attitudes towards information security. *Cryptologia*, 12(4):234–239, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908087~db=all~order=page`.

Kruh:1988:PMC

[558] Louis Kruh and Johnnie Murray. A pulp magazine cipher. *Cryptologia*, 12(4):240, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908088~db=all~order=page`.

Kruh:1988:BCB

[559] Louis Kruh. The Beale Cipher as a bamboozlement — Part II. *Cryptologia*, 12(4):241–246, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908089~db=all~order=page`.

Deavours:1988:ISB

[560] C. A. Deavours. Interactive solution of Beaufort enciphered text with overlapping keys. *Cryptologia*, 12(4):247–255, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908090~db=all~order=page`.

Barlow:1988:MWB

[561] Mike Barlow. A mathematical word block cipher. *Cryptologia*, 12(4):256–264, October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741908091~db=all~order=page`.

Kruh:1988:RTCd

[562] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 12(4):265–269,

October 1988. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741908092~db=all~order=page.

Levine:1989:HCS

[563] Jack Levine and Richard Chandler. The Hill cryptographic system with unknown cipher alphabet but known plaintext. *Cryptologia*, 13(1):1–28, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902534~db=all~order=page.

Matthews:1989:DCE

[564] Robert Matthews. On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 13(1):29–42, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902535~db=all~order=page.

Belkora:1989:BHC

[565] Jeff Belkora. Belkoranic hill ciphering. *Cryptologia*, 13(1):43–49, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902536~db=all~order=page.

Greenfield:1989:CCU

[566] Gary R. Greenfield. A cryptography course for the University of Richmond. *Cryptologia*, 13(1):50–60, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902537~db=all~order=page.

Anderson:1989:CPS

[567] Roland Anderson. Cryptanalytic properties of short substitution ciphers. *Cryptologia*, 13(1):61–72, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902538~db=all~order=page.

Kak:1989:NMC

[568] Subhash C. Kak. A new method for coin flipping by telephone. *Cryptologia*, 13(1):73–78, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902539~db=all~order=page.

Kruh:1989:HCA

[569] Louis Kruh. The heraldry of cryptology — addendum. *Cryptologia*, 13(1):79–84, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902540~db=all~order=page.

Kruh:1989:RTCa

[570] Louis Kruh and Ralph Erskine. Reviews and things cryptologic. *Cryptologia*, 13(1):85–96, January 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902541~db=all~order=page.

Mache:1989:SCT

[571] Wolfgang W. Mache. The Siemens cipher teletype in the history of telecommunications. *Cryptologia*, 13(2):97–117, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902544~db=all~order=page. Reprinted in [1793, pp. 433–453].

Clarke:1989:PWO

[572] William F. Clarke. Post war organization. *Cryptologia*, 13(2):118–122, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902545~db=all~order=page.

Kruh:1989:BAC

[573] Louis Kruh. British–American cryptanalytic cooperation and an unprecedented admission by Winston Churchill. *Cryptologia*, 13(2):123–134, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902546~db=all~order=page.

Erskine:1989:ABP

[574] Ralph Erskine. From the archives: a Bletchley Park assessment of German intelligence on Torch. *Cryptologia*, 13(2):135–142, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902547~db=all~order=page.

Myer:1989:VCS

[575] Lt. Gen. Charles R. Myer. Viet Cong Sigint and U.S. Army COMSEC in Vietnam. *Cryptologia*, 13(2):143–150, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902548~db=all~order=page. Reprinted in [1793, pp. 301–308].

Georgiou:1989:MSC

[576] George Georgiou. A method to strengthen ciphers. *Cryptologia*, 13 (2):151–160, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902549~db=all~order=page.

Anderson:1989:RCP

[577] Roland Anderson. Recognizing complete and partial plaintext. *Cryptologia*, 13(2):161–166, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902550~db=all~order=page.

Guillou:1989:PKT

[578] Louis C. Guillou, Marc Davio, and Jean-Jacques Quisquater. Public-key techniques: Randomness and redundancy. *Cryptologia*, 13(2):167–189, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902551~db=all~order=page.

Kahn:1989:SWO

[579] David Kahn. A Soviet wiretapping office. *Cryptologia*, 13(2):190–191, April 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902552~db=all~order=page`.

Boyd:1989:AUS

[580] Carl Boyd. Anguish under siege: High-grade Japanese signal intelligence and the fall of Berlin. *Cryptologia*, 13(3):193–209, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902554~db=all~order=page`.

Deavours:1989:KKK

[581] C. A. Deavours. A Ku Klux Klan cipher. *Cryptologia*, 13(3):210–214, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902555~db=all~order=page`.

Kruh:1989:RTCb

[582] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 13(3):215–242, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902556~db=all~order=page`.

Wheeler:1989:PCC

[583] Daniel D. Wheeler. Problems with chaotic cryptosystems. *Cryptologia*, 13(3):243–250, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902557~db=all~order=page`.

Deavours:1989:SHC

[584] C. A. Deavours and Louis Kruh. The Swedish HC-9 ciphering machine. *Cryptologia*, 13(3):251–265, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902558~db=all~order=page`.

Matthews:1989:RDP

[585] Robert Matthews. A rotor device for periodic and random-key encryption. *Cryptologia*, 13(3):266–272, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902559~db=all~order=page`.

Blackman:1989:GCS

[586] Deane R. Blackman. The Gromark cipher, and some relatives. *Cryptologia*, 13(3):273–282, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902560~db=all~order=page`.

Unknown:1989:OCP

[587] Unknown. OSS cryptographic plan. *Cryptologia*, 13(3):283–287, July 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

August:1989:CEC

[588] David A. August. Cryptography and exploitation of Chinese manual cryptosystems: Part I: The encoding problem. *Cryptologia*, 13(4):289–302, October 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902562~db=all~order=page`.

Carroll:1989:CCP

[589] John M. Carroll and Lynda E. Robbins. Computer cryptanalysis of product ciphers. *Cryptologia*, 13(4):303–326, October 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902563~db=all~order=page`.

Kruh:1989:TYS

[590] Louis Kruh. Tales of Yardley: Some sidelights to his career. *Cryptologia*, 13 (4):327–358, October 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902564~db=all~order=page`.

August:1989:ITA

[591] David August. Information theoretic approach to secure LSFR ciphers. *Cryptologia*, 13(4):351–359, October 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1989:RTCc

[592] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 13(4):359–377, October 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902565~db=all~order=page`.

Unknown:1989:ACN

[593] Unknown. From the archives: Compromise of a Navy code. *Cryptologia*, 13(4):378–381, October 1989. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hinsley:1990:BIS

[594] F. H. Hinsley. British intelligence in the Second World War: An overview. *Cryptologia*, 14(1):1–10, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902623~db=all~order=page`.

Lewis:1990:DD

[595] Frank W. Lewis. The day of the dodo. *Cryptologia*, 14(1):11–27, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902624~db=all~order=page`.

Lipson:1990:MCC

[596] Stanley H. Lipson and Francine Abeles. The matrix cipher of C. L. Dodgson. *Cryptologia*, 14(1):28–36, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902625~db=all~order=page`.

Vogel:1990:IKC

[597] Daniel S. Vogel. Inside a KGB cipher. *Cryptologia*, 14(1):37–52, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902626~db=all~order=page`.

Rabson:1990:WOH

[598] John Rabson and Hugo Rabson. The War Office HK POW cypher system. *Cryptologia*, 14(1):53–60, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902627~db=all~order=page`.

August:1990:CEC

[599] David A. August. Cryptography and exploitation of Chinese manual cryptosystems. Part II: The encrypting problem. *Cryptologia*, 14(1):61–78, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902628~db=all~order=page`.

Kak:1990:VC

[600] Subhash C. Kak. The Vararuchi cipher. *Cryptologia*, 14(1):79–82, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902629~db=all~order=page`.

Kruh:1990:RTCa

[601] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 14(1):83–89, January 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902630~db=all~order=page`.

Donini:1990:CSR

[602] Rear Admiral (disch.) Luigi Donini and Augusto Buonafalce. The cryptographic services of the Royal British and Italian navies. *Cryptologia*, 14(2):97–127, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902633~db=all~order=page`. Translated by Augusto Buonafalce. Reprinted in [1793, pp. 3–33].

Abeles:1990:SVP

[603] Francine Abeles and Stanley H. Lipson. Some Victorian periodic polyalphabetic ciphers. *Cryptologia*, 14(2):128–134, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902634~db=all~order=page`. Reprinted in [1793, pp. 309–315].

Dunnigan:1990:NCPa

[604] Brian Leigh Dunnigan, Frank Lewis, and Mike Barlow. The Niagara cipher — Part I. *Cryptologia*, 14(2):135–138, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902635~db=all~order=page`.

Deavours:1990:SHC

[605] C. A. Deavours and Louis Kruh. The Swedish HC-9 ciphering machine

challenge. *Cryptologia*, 14(2):139–144, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902636~db=all~order=page`.

Greenough:1990:CUH

[606] H. Paul Greenough. Cryptanalysis of the uncaged Hagelin. *Cryptologia*, 14(2):145–161, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902637~db=all~order=page`.

Deavours:1990:SCT

[607] C. A. Deavours. Solution of C-35 texts with partial key overlaps. *Cryptologia*, 14(2):162–168, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902638~db=all~order=page`.

Kak:1990:IBF

[608] Subhash C. Kak. Indus and Brahmi — further connections. *Cryptologia*, 14(2):169–183, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902639~db=all~order=page`.

Kruh:1990:RTCb

[609] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 14(2):184–191, April 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902640~db=all~order=page`.

Byrne:1990:CEC

[610] John Byrne, Cipher A. Deavours, and Louis Kruh. Chaocipher enters the computer age when its method is disclosed to Cryptologia Editors. *Cryptologia*, 14(3):193–198, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902642~db=all~order=page`. Reprinted in [1793, pp. 317–322].

Dunnigan:1990:NCPb

[611] Brian Leigh Dunnigan, Frank Lewis, and Mike Barlow. The Niagara cipher — Part II. *Cryptologia*, 14(3):199–203, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902643~db=all~order=page`. Niagara cipher; British military cipher; polyalphabetic cipher.

Kozaczuk:1990:NCO

[612] Wladyslaw Kozaczuk. A new challenge for an old ENIGMA — Buster. *Cryptologia*, 14(3):204–216, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902644~db=all~order=page`. Marian Rejewski; mathematician-cryptologist; Enigma cipher; enciphered message; Russo-Japanese war; Polish Socialist Party; historical document.

Connell:1990:ANM

[613] Charles Connell. An analysis of NEWDES: a modified version of DES. *Cryptologia*, 14(3):217–224, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902645~db=all~order=page`. NEWDES; modified version; encryption algorithm; data encryption standard; secretness; S-boxes; microcomputer; bytes; entire f-function; key length.

Kiele:1990:TTE

[614] William A. Kiele. A tensor — theoretic enhancement to the Hill cipher system. *Cryptologia*, 14(3):225–233, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902646~db=all~order=page`. tensor-theoretic enhancement; Hill cipher system; Hill matrix algorithm; purely algebraic cryptographic system; algebraic cryptology; ring isomorphism theory; block size; invertible matrix; ciphertext blocks.

Kruh:1990:RTCc

[615] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 14(3):234–252, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902647~db=all~order=page`.

Kruh:1990:WWS

[616] Louis Kruh. Why was Safford pessimistic about breaking the German ENIGMA cipher machine in 1942? *Cryptologia*, 14(3):253–257, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902648~db=all~order=page`. Reprinted in [1793, pp. 235–239].

Baldwin:1990:HWS

[617] Robert W. Baldwin and Alan T. Sherman. How we solved the US$100,000 decipher puzzle (16 hours too late). *Cryptologia*, 14(3):258–284, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902649~db=all~order=page`. A preliminary version appears as Technical Report 89-3, Tufts University Department of Computer Science (July 1989), and in modified form as Technical Report UMIACS-TR-90-64/CS-TR-2468, University of Maryland, College Park (May 1990).

Anderson:1990:SCS

[618] Ross J. Anderson. Solving a class of stream ciphers. *Cryptologia*, 14(3):285–288, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902650~db=all~order=page`. keystream sequences; linear feedback shift registers; multiplexor; consistency check; observed keystream; address information.

Ritter:1990:SCP

[619] Terry Ritter. Substitution cipher with pseudo-random shuffling the dynamic substitution combiner.

Cryptologia, 14(4):289–303, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902652~db=all~order=page; http://www.io.com/~ritter/ARTS/DYNSUB2.HTM`. pseudo-random shuffling; dynamic substitution combiner; modified substitution cipher; translation table; plaintext symbols; ciphertext symbols; dynamic translation; symbol frequency statistics; cryptanalytic attacks; cryptographic combiner; exclusive-OR combining function; Vernam stream ciphers; one-way function; pseudo-random sequence; cryptanalysis.

Ephron:1990:C

[620] Henry D. Ephron. S. I. S./CB. *Cryptologia*, 14(4):304–330, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902653~db=all~order=page`. Reprinted in [1793, pp. 241–267].

Deavours:1990:TBW

[621] C. A. Deavours and Louis Kruh. The Turing0 bombe: Was it enough? *Cryptologia*, 14(4):331–349, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902654~db=all~order=page`. Reprinted in [1793, pp. 403–421].

Mitchell:1990:NKG

[622] Douglas W. Mitchell. Nonlinear key generators. *Cryptologia*, 14(4):350–354, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). key generators; nonlinear generation; key sequences; chaos-based approach; simulations; desirable properties.

Foster:1990:VDC

[623] Caxton C. Foster. Vowel distribution as a clue to vowel identification. *Cryptologia*, 14(4):355–362, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902655~db=all~order=page`. vowel identification; English; simple substitution cipher; equally distributed; text.

Kruh:1990:RTCd

[624] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 14(4):363–373, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902656~db=all~order=page`.

Weber:1990:MD

[625] Ralph E. Weber. A masked dispatch. *Cryptologia*, 14(4):374–380, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902657~db=all~order=page`.

Ritter:1991:TCP

[626] Terry Ritter. Transposition cipher with pseudo-random shuffling: The dynamic transposition combiner. *Cryptologia*, 15(1):1–17, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a741902738~db=all~order=page; http://www.io.com/~ritter/ARTS/DYNTRAN2.HTM. pseudorandom shuffling; dynamic transposition combiner; transposition cipher; cryptographic shuffling; bit-balancing data; usage-frequency statistics; exclusive-OR combining function; Vernam stream ciphers.

Lipson:1991:KVC

[627] Stanley H. Lipson and Francine Abeles. The key–vowel cipher of Charles S. Dodgson. *Cryptologia*, 15(1):18–24, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902739~db=all~order=page. Reprinted in [1793, pp. 323–329].

Kruh:1991:MIC

[628] Louis Kruh. Military Intelligence Corps Hall of Fame. *Cryptologia*, 15(1):25–28, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902740~db=all~order=page.

Kruh:1991:CCC

[629] Louis Kruh. Correspondence in cipher — a cipher typewriter catalogue. *Cryptologia*, 15(1):29–42, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902741~db=all~order=page.

Schwartz:1991:NGM

[630] Charles Schwartz. A new graphical method for encryption of computer data. *Cryptologia*, 15(1):43–46, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902742~db=all~order=page. pseudorandom number generator; decryption; graphical method; encryption; computer data; text; pictures; binary files; graphically generated inversions; bit pattern; uncrackability.

Lujan:1991:AMD

[631] Lt. Susan M. Lujan, USNR. Agnes Meyer Driscoll. *Cryptologia*, 15(1):47–56, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902743~db=all~order=page. Reprinted in [1793, pp. 269–278].

Bergen:1991:FSW

[632] H. A. Bergen and W. J. Caelli. File security in WordPerfect 5.0. *Cryptologia*, 15(1):57–66, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://catless.ncl.ac.uk/Risks/12.01.html; http://www.informaworld.com/smpp/content~content=a741902744~db=all~order=page. file security; files cryptanalysis; locked document option; word processing package WordPerfect V5.0; encryption key; ciphertext.

Kruh:1991:RTCa

[633] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 15(1):67–80, January 1991. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902745~db=all~order=page.

Ritter:1991:EGC

[634] Terry Ritter. The efficient generation of cryptographic confusion sequences. *Cryptologia*, 15(2):81–139, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://fizz.sys.uea.ac.uk/~rs/ritter.html; http://www.ciphersbyritter.com/ARTS/CRNG2ART.HTM; http://www.informaworld.com/smpp/content~content=a741902748~db=all~order=page. cryptographic confusion sequences; pseudorandom sequence; random number generators; cryptographic applications; random sequences; incompleteness theorem; deterministic implementation; external analysis; RNG comparison; chaos; Cebysev mixing; cellular automata; linear congruential; linear feedback shift register; nonlinear shift register; generalized feedback shift register; additive types; isolator mechanisms; one-way functions; combined sequences; random permutations; primitive mod 2 polynomials; empirical state-trajectory approach; RNG design analysis; GFSR.

Wheeler:1991:SIC

[635] Daniel D. Wheeler and Robert A. J. Matthews. Supercomputer investigations of a chaotic encryption algorithm. *Cryptologia*, 15(2):140–152, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902749~db=all~order=page. chaotic encryption algorithm; nonlinear pseudorandom number generator; chaos theory; cycling keys; low-precision arithmetic; numerical investigation; Cray Y-MP machine; cycling problem.

Burke:1991:LER

[636] Colin Burke and Ralph Erskine. Letters to the Editor: Re: Safford article. *Cryptologia*, 15(2):153–160, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). Reprinted in [1793, pp. 279–286].

Guy:1991:LER

[637] Jacques B. M. Guy. Letter to the Editor: Re: Voynich Manuscript. *Cryptologia*, 15(2):161–166, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1991:RTCb

[638] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 15(2):167–176, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902750~db=all~order=page.

Garon:1991:WES

[639] Gilles Garon and Richard Outerbridge. DES watch: An examination of the sufficiency of the Data Encryption Standard for financial institution information security in the 1990's. *Cryptologia*, 15(3):177–193, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902752~db=all~order=page. data

encryption standard; financial institution information security; FIs; unmodified single-key DES; financial systems; key management security; double-length keys; financial systems.

Anderson:1991:TFC

[640] Ross J. Anderson. Tree functions and cipher systems. *Cryptologia*, 15(3):194–202, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902753~db=all~order=page`. encryption systems; plaintext bit; hash function; ciphertext errors; error extension; tree function; ciphertext attack; computable attack; connectivity; DES; RSA key selection; algorithm design.

Desmedt:1991:CDN

[641] Yvo G. Desmedt. The "*A*" cipher does not necessarily strengthen security. *Cryptologia*, 15(3):203–206, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902754~db=all~order=page`. enciphering transformation; multiplication; homomorphism; A cipher; cryptanalyst.

Guy:1991:SPT

[642] Jacques B. M. Guy. Statistical properties of the two folios of the Voynich Manuscript. *Cryptologia*, 15(3):207–218, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902755~db=all~order=page`.

Callimahos:1991:LWF

[643] Lambros D. Callimahos. The legendary William F. Friedman. *Cryptologia*, 15(3):219–236, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902756~db=all~order=page`.

Kruh:1991:SET

[644] Louis Kruh and Paul Edden. Seizing the ENIGMA: Two reviews of one book. *Cryptologia*, 15(3):237–240, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902757~db=all~order=page`.

Kruh:1991:RTCc

[645] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 15(3):241–246, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902758~db=all~order=page`.

Friedman:1991:IRC

[646] William F. Friedman. Information regarding cryptographic systems submitted for use by the military service and forms to be used. *Cryptologia*, 15(3):247–257, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902759~db=all~order=page`.

Guy:1991:VIO

[647] Jacques B. M. Guy. Vowel identification: An old (but good) al-

gorithm. *Cryptologia*, 15(3):258–262, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902760~db=all~order=page`. vowel identification; accurate algorithm; plaintext; simple substitution cipher; very fast algorithm; Soviet researcher.

Friedman:1991:BHS

[648] William F. Friedman. A brief history of the Signal Intelligence Service by the Military Service and forms to be used. *Cryptologia*, 15(3):263–272, July 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902761~db=all~order=page`.

Kahn:1991:PHI

[649] David Kahn. Pearl Harbor and the inadequacy of cryptanalysis. *Cryptologia*, 15(4):273–294, October 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902763~db=all~order=page`. Reprinted in [1793, pp. 35–56].

Parker:1991:UMP

[650] Frederick D. Parker. The unsolved messages of Pearl Harbor. *Cryptologia*, 15(4):295–313, October 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902764~db=all~order=page`. Reprinted in [1793, pp. 57–75].

Anderson:1991:ECI

[651] Roland Anderson. Extending the concept of interval. *Cryptologia*, 15(4):314–324, October 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902765~db=all~order=page`. interval concept; cryptography; identity information.

Kruh:1991:RTCd

[652] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 15(4):325–334, October 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902766~db=all~order=page`.

Anonymous:1991:ASU

[653] Anonymous. From the archives: Security of Ultra Dexter and Rabid Intelligence War Department. *Cryptologia*, 15(4):341–354, October 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902767~db=all~order=page`.

Wheeler:1991:PMN

[654] Daniel D. Wheeler. Problems with Mitchell's nonlinear key generators. *Cryptologia*, 15(4):355–363, October 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902768~db=all~order=page`. pseudo random numbers; successive differences; nonlinear key generators; probable-word attack.

Kruh:1992:RTCa

[655] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 16(1):1–22, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902821~db=all~order=page`.

Robinson:1992:FRC

[656] Bill Robinson. The fall and rise of cryptanalysis in Canada. *Cryptologia*, 16(1):23–38, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902822~db=all~order=page`. Reprinted in [1793, pp. 77–92].

Erskine:1992:GNG

[657] Ralph Erskine. The German Naval grid in World War II. *Cryptologia*, 16(1):39–51, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902823~db=all~order=page`.

Carroll:1992:CCE

[658] John M. Carroll, Jeff Verhagen, and Perry T. Wong. Chaos in cryptography: The escape from the strange attractor. *Cryptologia*, 16(1):52–72, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902824~db=all~order=page`. cryptography; random characteristics; cipher system; pseudo-random number generators; random generators; Lorenz attractor; chaotic nature; strange attractor; key management; authentication protocols.

Gaj:1992:PCM

[659] Krzysztof Gaj. Polish cipher machine — LUCIDA. *Cryptologia*, 16(1):73–80, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902825~db=all~order=page`.

Kruh:1992:BPH

[660] Louis Kruh. "Betrayal at Pearl Harbor": Book review. *Cryptologia*, 16 (1):81–85, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902826~db=all~order=page`. See [1675].

Kruh:1992:SCD

[661] Louis Kruh. Sliding code device of unknown origin. *Cryptologia*, 16(1):86–88, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902827~db=all~order=page`.

Al-Kadit:1992:OCA

[662] Ibrahim A. Al-Kadit. Origins of cryptology: The Arab contributions. *Cryptologia*, 16(2):97–126, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902830~db=all~order=page`. Reprinted in [1793, pp. 93–122].

Rabson:1992:AWB

[663] John Rabson. All are well at Boldon: a mid-Victorian code system. *Cryptologia*, 16(2):127–135, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902831~db=all~order=page`.

McLaughlin:1992:YAM

[664] Robert McLaughlin. Yet another machine to break DES. *Cryptologia*, 16(2):136–144, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902832~db=all~order=page`. data encryption standard; DES; current high-speed encryption chips; hardware fuzzy comparers; breaking process.

Kruh:1992:ANC

[665] Louis Kruh. Army–Navy collaboration for cryptanalysis of enemy systems. *Cryptologia*, 16(2):145–164, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902833~db=all~order=page`.

Sassoon:1992:ASA

[666] George T. Sassoon. The application of Sukhotin's algorithm to certain non-English languages. *Cryptologia*, 16(2):165–173, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902834~db=all~order=page`. Sukhotin algorithm; vowel-finding algorithm; simple-substitution ciphertext; foreign languages; computer program VOWEL1; compiled BASIC; English; Georgian; Croatian; Scottish Gaelic; Hungarian; Hebrew languages.

Alvarez:1992:PDC

[667] David Alvarez. A Papal diplomatic code. *Cryptologia*, 16(2):174–176, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902835~db=all~order=page`.

Webb:1992:PKC

[668] William A. Webb. A public-key cryptosystem based on complementing sets. *Cryptologia*, 16(2):177–181, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902836~db=all~order=page`. public key cryptosystem; complementing sets; integers.

Kruh:1992:RTCb

[669] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 16(2):182–190, April 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902837~db=all~order=page`.

Wayner:1992:MF

[670] Peter Wayner. Mimic functions. *Cryptologia*, 16(3):193–214, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL

http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1029.html; http://www.informaworld.com/smpp/content~content=a741902839~db=all~order=page. data compression; encryption; mimic function; Huffman coding; context-free grammars.

King:1992:IPR

[671] John C. King and Dennis R. Bahler. An implementation of probabilistic relaxation in the cryptanalysis of simple substitution ciphers. *Cryptologia*, 16(3): 215–225, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902840~db=all~order=page. trigram statistics generation; probabilistic relaxation; cryptanalysis; Pascal; adjustment formula; simple substitution ciphers; homophonic ciphers.

Anderson:1992:CRN

[672] Ross Anderson. Chaos and random numbers. *Cryptologia*, 16(3):226, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Shirriff:1992:DVC

[673] Ken Shirriff, Curt Welch, and Andrew Kinsman. Decoding a VCR controller code. *Cryptologia*, 16(3):227–234, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902841~db=all~order=page; http://www.righto.com/papers/vcr.html. video cassette recorder programming; encryption; encoding; VCR Plus+; remote control; decoding.

Kruh:1992:RTCc

[674] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 16(3):235–249, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902842~db=all~order=page.

Mitchell:1992:RCT

[675] Douglas W. Mitchell. "Rubik's Cube" as a transposition device. *Cryptologia*, 16(3):250–256, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902843~db=all~order=page. data security; cryptography; Rubik's Cube; transposition cipher; multiple anagramming.

Oswald:1992:WFF

[676] Alison L. Oswald. William Frederick Friedman: a pictorial essay. *Cryptologia*, 16(3):257–264, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902844~db=all~order=page.

Safford:1992:AFD

[677] Lieutenant L. F. Safford. From the archives: The functions and duties of the Cryptography Section, Naval Communications. *Cryptologia*, 16(3):265–281, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902845~db=all~order=page.

Foster:1992:CVI

[678] Caxton C. Foster. A comparison of vowel identification methods. *Cryptologia*, 16(3):282–286, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902846~db=all~order=page`. cryptoanalysis; simple substitution cipher; vowel identification methods; consonant line; vowel distribution; machine readable computer program manual.

Kahn:1992:RMU

[679] David Kahn. Roosevelt, MAGIC, and ULTRA. *Cryptologia*, 16(4):289–319, October 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902848~db=all~order=page`. Reprinted in [1793, pp. 123–153].

Anonymous:1992:ASU

[680] Anonymous. From the archives: Strategic use of communications during the World War. *Cryptologia*, 16(4):320–326, October 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902849~db=all~order=page`.

Fagone:1992:PSS

[681] Peter P. Fagone. Partial solutions of Swift's 18th Century Mock Latin passages. *Cryptologia*, 16(4):327–338, October 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902850~db=all~order=page`.

Kruh:1992:RTCd

[682] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 16(4):339–346, October 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902851~db=all~order=page`.

Gaddy:1992:RCD

[683] David W. Gaddy. Rochford's cipher: a discovery in Confederate cryptography. *Cryptologia*, 16(4):347–362, October 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902852~db=all~order=page`. Rochfort cipher; Confederated States Navy cipher; American Civil War cryptography; Rochford's cipher; historical background; Confederate message; grille cipher system.

Levine:1993:TMP

[684] Jack Levine and Richard Chandler. The two-message problem in the Hill cryptographic system with unknown cipher alphabet. *Cryptologia*, 17(1):1–30, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639218~db=all~order=page`. Hill cryptographic system; Hill two-message problem; ciphertexts; encipherment; single plaintext; key matrices; cipher alphabet; row-reduced echelon form; linear equations; unknown elements.

Spillman:1993:UGA

[685] Richard Spillman, Mark Janssen, Bob Nelson, and Martin Kepner. Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers. *Cryptologia*, 17(1):31–44, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639212~db=all~order=page; http://www.plu.edu/~janssema/abstract.html; http://www.plu.edu/~janssema/ga_solve.zip`. cryptanalysis; directed random search algorithm; genetic algorithm; simple substitution cipher.

King:1993:FSH

[686] John C. King and Dennis R. Bahler. A framework for the study of homophonic ciphers in classical encryption and genetic systems. *Cryptologia*, 17(1):45–54, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639213~db=all~order=page`. classical encryption; genetic systems; multiplicity; real number; unicity distances; historical homophonic ciphers; genes.

Mitchell:1993:NRN

[687] Douglas W. Mitchell. A nonlinear random number generator with known, long cycle length. *Cryptologia*, 17 (1):55–62, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639214~db=all~order=page`. random number generator; cryptographic keystreams; division algorithm; seed values; long cycle length; keystream generation.

OConnor:1993:IEP

[688] Luke O'Connor. The inclusion–exclusion principle and its applications to cryptography. *Cryptologia*, 17(1):63–79, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639215~db=all~order=page; http://www.zurich.ibm.com/~oco/pub/iep.html; http://www.zurich.ibm.com/~oco/pub/iep.ps.Z`. inclusion-exclusion principle; combinatorial method; cardinality; cryptography; Boolean functions; permutations; cryptographic mapping; nonlinearity; nondegeneracy; confusion; diffusion.

Kruh:1993:CTR

[689] Louis Kruh. A cryptological travelogue: Riverbank — 1992. *Cryptologia*, 17(1):80–94, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639216~db=all~order=page`.

Kruh:1993:RTCa

[690] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 17(1):95–110, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639217~db=all~order=page`.

Burke:1993:IHC

[691] Colin Burke. An introduction to an historic computer document: The 1946

Pendergass Report cryptanalysis and the digital computer. *Cryptologia*, 17(2):113–123, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639221~db=all~order=page`. Reprinted in [1793, pp. 361–371].

Burke:1993:CUH

[692] C. Burke. Cryptanalytic use of high-speed digital computing machines. *Cryptologia*, 17(2):124–147, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639222~db=all~order=page`. OP20G; special purpose devices; Atlas; general purpose mathematical computer; general purpose cryptanalytic machine.

King:1993:ASS

[693] John C. King and Dennis R. Bahler. An algorithmic solution of sequential homophonic ciphers. *Cryptologia*, 17(2):148–165, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639223~db=all~order=page`. algorithmic solution; cryptanalytic algorithm; sequential homophonic cipher; word divisions; simple substitution cipher; probabilistic relaxation.

Kruh:1993:RTCb

[694] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 17(2):166–171, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639224~db=all~order=page`.

Kruh:1993:YOC

[695] Louis Kruh. A 77-year old challenge cipher known, long cycle length. *Cryptologia*, 17(2):172–174, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639225~db=all~order=page`. simple substitution cipher; cryptosystem; Cipher Disk; Playfair Cipher.

Chang:1993:MKC

[696] Chin-Chen Chang and Ren-Junn Hwang. Master keys for an M^3 cryptoscheme. *Cryptologia*, 17(2):175–186, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639226~db=all~order=page`. M/sup 3/; public-key cryptoscheme; master keys.

Matthews:1993:UGA

[697] Robert A. J. Matthews. The use of genetic algorithms in cryptanalysis. *Cryptologia*, 17(2):187–201, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639227~db=all~order=page`. cryptanalysis; genetic algorithms; cryptographic systems; keyspaces; GENALYST.

Ramesh:1993:AAS

[698] R. S. Ramesh, G. Athithan, and K. Thiruvengadam. An automated

approach to solve simple substitution ciphers. *Cryptologia*, 17(2):202–218, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639228~db=all~order=page`. simple substitution cipher solving; tuple generator; message length; encryption; dictionary system; decoding; personal computer.

Alvarez:1993:PCS

[699] David Alvarez. The Papal cipher section in the early Nineteenth Century. *Cryptologia*, 17(2):219–224, April 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639229~db=all~order=page`. Reprinted in [1793, pp. 155–160].

DeLeeuw:1993:HSA

[700] Karl De Leeuw and Hans Van Der Meer. A homophonic substitution in the archives of the Last Great Pensionary of Holland. *Cryptologia*, 17(3):225–236, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639231~db=all~order=page`.

Kahn:1993:EC

[701] David Kahn. An Enigma chronology. *Cryptologia*, 17(3):237–246, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639232~db=all~order=page`. Reprinted in [1793, pp. 423–432].

Kahn:1993:ACN

[702] David Kahn. From the archives: Compromise of Naval code F-3. *Cryptologia*, 17(3):247–250, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639233~db=all~order=page`.

Kruh:1993:RTCc

[703] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 17(3):251–263, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639234~db=all~order=page`.

Shepherd:1993:QRC

[704] S. J. Shepherd, P. W. Sanders, and C. T. Stockel. The quadratic residue cipher and some notes on implementation. *Cryptologia*, 17(3):264–282, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639235~db=all~order=page`. quadratic residue cipher; implementation; public key cryptosystems; RSA algorithm; Rivest-Shamir-Adleman cipher; number theory; prime numbers; factorization; QRC.

Nenninger:1993:AJC

[705] Timothy K. Nenninger. From the archives: Japanese codebook found. *Cryptologia*, 17(3):283–284, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.`

informaworld.com/smpp/content~content=a748639236~db=all~order=page.

Ruland:1993:RDS

[706] Christoph Ruland. Realizing digital signatures with one-way hash functions. *Cryptologia*, 17(3):285–300, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639237~db=all~order=page. digital signatures; one-way hash functions; asymmetric cryptographic systems; smart cards; one-time signatures; optimally implemented hash functions; asymmetric algorithms; one-bit signatures; N-bit signatures; infinite signature trees; performance.

Chin:1993:CSG

[707] Yuan-Chung Chin, PeCheng Wang, and Jing-Jang Hwang. Cryptanalysis on Schwartz graphical encryption method. *Cryptologia*, 17(3):301–304, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639238~db=all~order=page. cryptanalysis; Schwartz graphical encryption method; chosen-plaintext attack; known-plaintext attack; mask approach; exclusive-or operations; XOR operations; plaintext-independent process.

King:1993:RKB

[708] John C. King. A reconstruction of the key to Beale cipher number two. *Cryptologia*, 17(3):305–317, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639239~db=all~order=page. Beale cipher number two; cryptographic key reconstruction; encryption; B1; B2; statistical anomalies; artificial intelligence techniques; automated cryptanalysis; 1885 pamphlet versions; book ciphers; heuristic search; homophonic ciphers; probabilistic relaxation.

Editor:1993:SQ

[709] Editor. Stimson quote. *Cryptologia*, 17(3):318–??, July 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ganesan:1993:STL

[710] Ravi Ganesan and Alan T. Sherman. Statistical techniques for language recognition: An introduction and guide for cryptanalysts. *Cryptologia*, 17(4):321–366, October 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639241~db=all~order=page. Preliminary version available as Technical Report CS-TR-3036/UMIACS-TR-93-16, University of Maryland College Park (February 1993), and as Technical Report TR CS-93-02, University of Maryland Baltimore County (February 28, 1993).

Spillman:1993:CKC

[711] Richard Spillman. Cryptanalysis of knapsack ciphers using genetic algorithms. *Cryptologia*, 17(4):367–377, October 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.

informaworld.com/smpp/content~content=a748639242~db=all~order=page. See comments [726].

Kruh:1993:RTCd

[712] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 17(4):378–394, October 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639243~db=all~order=page.

Leighton:1993:SWC

[713] Albert C. Leighton. The statesman who could not read his own mail. *Cryptologia*, 17(4):395–402, October 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639244~db=all~order=page.

Anonymous:1993:RCC

[714] Anonymous. Riverbank's 1917 cryptologic contributions to the United States officially recognized as National Security Agency adopts Editor's suggestion. *Cryptologia*, 17(4):403–406, October 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639245~db=all~order=page.

Forsyth:1993:ACS

[715] W. S. Forsyth and R. Safavi-Naini. Automated cryptanalysis of substitution ciphers. *Cryptologia*, 17(4):407–418, October 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639246~db=all~order=page. automated cryptanalysis; substitution ciphers; simulated annealing; monoalphabetic substitution ciphers; convergence; cooling schedule; performance; block ciphers.

Kruh:1994:RTCa

[716] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 18(1):1–21, January 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639248~db=all~order=page.

Deavours:1994:BBB

[717] C. A. Deavours. "Those Brilliant Brits": Book review. *Cryptologia*, 18(1):22–24, January 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639249~db=all~order=page.

Dawson:1994:DCA

[718] Ed Dawson and Andrew Clark. Divide and conquer attacks on certain classes of stream ciphers. *Cryptologia*, 18(1):25–40, January 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639250~db=all~order=page. stream ciphers; keystream generators; plaintext attack; divide and conquer method; summation generator; universal logic sequence; cryptanalysis.

Greenfield:1994:YAM

[719] Gary R. Greenfield. Yet another matrix cryptosystem. *Cryptologia*, 18(1):41–

51, January 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639251~db=all~order=page. matrix cryptosystem; nonlinear autokey matrix system; plaintext; Hill system; matrix trace; chosen plaintext attack.

Halligan:1994:ARI

[720] J. Halligan. From the archives: Radio intelligence and communication security. *Cryptologia*, 18(1):52–79, January 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639252~db=all~order=page.

Denniston:1994:YDS

[721] Robin Denniston. Yardley's diplomatic secrets. *Cryptologia*, 18(2):81–127, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639255~db=all~order=page.

Kruh:1994:RTCb

[722] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 18(2):128–140, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639256~db=all~order=page.

Davies:1994:NIH

[723] D. W. Davies. New information on the history of the Siemens and Halske T52 cipher machines. *Cryptologia*, 18(2):141–146, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639257~db=all~order=page. Reprinted in [1793, pp. 455–460].

Selmer:1994:NMS

[724] Ernst S. Selmer. The Norwegian modifications of the Siemens and Halske T52e cipher machines. *Cryptologia*, 18(2):147–149, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639258~db=all~order=page. Reprinted in [1793, pp. 461–463].

Kahn:1994:ARF

[725] David Kahn. From the archives: a real fake message. *Cryptologia*, 18(2):150–152, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639259~db=all~order=page.

Rubin:1994:CCK

[726] Frank Rubin. Comments on "Cryptanalysis of Knapsack Ciphers Using Genetic Algorithms". *Cryptologia*, 18 (2):153–154, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639260~db=all~order=page. See [711].

Ritter:1994:EPR

[727] Terry Ritter. Estimating population from repetitions in accumulated random samples. *Cryptologia*, 18(2):155–190, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a748639261~db=all~order=page.

Mead:1994:BJA

[728] David Mead. The breaking of the Japanese Army administrative code. *Cryptologia*, 18(3):193–203, July 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639263~db=all~order=page. Reprinted in [1793, pp. 465–475].

Hagelin:1994:SHC

[729] Boris C. W. Hagelin and David Kahn. The story of the Hagelin cryptos. *Cryptologia*, 18(3):204–242, July 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639264~db=all~order=page. Edited by David Kahn. Reprinted in [1793, pp. 477–515].

McKay:1994:AAD

[730] C. G. McKay. From the archives: Arvid Damm makes an offer. *Cryptologia*, 18(3):243–249, July 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639265~db=all~order=page. Arvid Damm; cipher device; cryptograms.

Kruh:1994:PSF

[731] Louis Kruh. The Postal Service fails to deliver the goods. *Cryptologia*, 18(3):250–252, July 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639266~db=all~order=page.

Carroll:1994:WKW

[732] John M. Carroll and Sri Nurdiati. On weak keys and weak data: Foiling the two nemeses. *Cryptologia*, 18(3):253–280, July 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639267~db=all~order=page. weak data; cryptographic keys; plain text; predictable regularities; crypto text; encryption; key space; alphabet length; PN string; interlocutory role; DES keys; Vernam-type cipher; block cipher.

Kruh:1994:RTCc

[733] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 18(3):281–287, July 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639268~db=all~order=page.

Ganesan:1994:STL

[734] Ravi Ganesan and Alan T. Sherman. Statistical techniques for language recognition: An empirical study using real and simulated English. *Cryptologia*, 18(4):289–331, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639270~db=all~order=page. A preliminary version appears as Technical Report CS-TR-3036/UMIACS-TR-93-16, University of Maryland Col-

lege Park (July 1993), and a complete version (with supplement) appears as Technical Report TR CS-93-03, University of Maryland Baltimore County (September 28, 1993) [48 pages].

King:1994:ACA

[735] John C. King. An algorithm for the complete automated cryptanalysis of periodic polyalphabetic substitution ciphers. *Cryptologia*, 18(4):332–355, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639271~db=all~order=page`. automated cryptanalysis; periodic polyalphabetic substitution ciphers; cryptanalytic algorithm; monoalphabetic ciphers; probabilistic alphabets; probabilistic relaxation; primary alphabet; polyalphabetic ciphers; word divisions; ciphertext-only attack; Vigenére ciphers; Variant Beaufort ciphers; Beaufort ciphers.

Corcoran:1994:MVC

[736] William J. Corcoran. A multiloop Vigenère cipher with exceptionally long component series. *Cryptologia*, 18(4):356–371, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639272~db=all~order=page`. multiloop Vigenére cipher; exceptionally long component series; computer generation; polyalphabetic cryptographic system; character set; linear congruential generating function; component series; cryptanalysis; multiloop system; computationally secure; personal computers; Spectra Publishing; Power Basic; BASIC.

Li:1994:CAT

[737] Chuan-Ming Li, Tzonelih Hwang, and Narn-Yih Lee. Conspiracy attacks on the threshold RSA signature scheme. *Cryptologia*, 18(4):372–380, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639273~db=all~order=page`. conspiracy attacks; threshold RSA signature scheme; shared generation; secure signatures; digital signature scheme; greatest common divisor; Desmedt-Frankel scheme; secure threshold signature schemes; Lagrange interpolating polynomial.

Kruh:1994:PTN

[738] Louis Kruh. A pictorial tour of the National Cryptologic Museum. *Cryptologia*, 18(4):381–389, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639274~db=all~order=page`.

Kruh:1994:RTCd

[739] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 18(4):390–398, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639275~db=all~order=page`.

Reeds:1995:WFF

[740] Jim Reeds. William F. Friedman's transcription of the Voynich

Manuscript. *Cryptologia*, 19(1):1–23, January 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639277~db=all~order=page`.

Kruh:1995:WCR

[741] Louis Kruh. When a court ruled for Bacon instead of Shakespeare — temporarily. *Cryptologia*, 19(1):24–38, January 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639278~db=all~order=page`.

Davies:1995:LCM

[742] Donald W. Davies. The Lorenz cipher machine SZ42. *Cryptologia*, 19(1):39–61, January 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639279~db=all~order=page`. Reprinted in [1793, pp. 517–539].

Denniston:1995:F

[743] Robin Denniston. Fetterlein and others. *Cryptologia*, 19(1):62–64, January 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639280~db=all~order=page`.

Miller:1995:CME

[744] A. Ray Miller. The cryptographic mathematics of Enigma. *Cryptologia*, 19(1):65–80, January 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639281~db=all~order=page`.

Erskine:1995:USU

[745] Ralph Erskine. Ultra and some U. S. Navy carrier operations. *Cryptologia*, 19(1):81–96, January 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639282~db=all~order=page`.

Drea:1995:WJA

[746] Edward J. Drea. Were the Japanese Army codes secure? *Cryptologia*, 19(2):113–136, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Deavours:1995:A

[747] C. A. Deavours. The Autoscritcher. *Cryptologia*, 19(2):137–148, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:1995:MSK

[748] Anonymous. In memoriam: Solomon Kullback. *Cryptologia*, 19(2):149–150, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1995:COB

[749] David Kahn. The cryptologic origin of Braille. *Cryptologia*, 19(2):151–152, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

deLeeuw:1995:TGA

[750] Karl de Leeuw and Hans van der Meer. A turning grille from the ancestral castle of the Dutch stadtholders. *Cryptologia*, 19(2):153–165, 1995. CODEN

CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1995:ECT

[751] David Kahn. Enemy codes and their solution. *Cryptologia*, 19(2):166–197, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Liaw:1995:EPA

[752] Horng-Twu Liaw and Chin-Laung Lei. An efficient password authentication scheme based on a unit circle. *Cryptologia*, 19(2):198–208, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1995:RTCa

[753] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 19(2):209–215, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schlesinger:1995:CPC

[754] Stephen Schlesinger. Cryptanalysis for peacetime: Codebreaking and the birth and structure of the United Nations. *Cryptologia*, 19(3):217–235, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruth:1995:RLC

[755] Louis Kruth. Riverbank Laboratory correspondence, 1919 (SRH-50). *Cryptologia*, 19(3):236–246, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1995:BCS

[756] Michael van der Meulen. The book cipher system of the *Wehrmacht*. *Cryptologia*, 19(3):247–260, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Alvarez:1995:DEC

[757] David Alvarez. A Dutch enciphered code. *Cryptologia*, 19(3):261–264, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Jakobsen:1995:FMC

[758] Thomas Jakobsen. A fast method for cryptanalysis of substitution ciphers. *Cryptologia*, 19(3):265–274, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rubin:1995:QDQ

[759] Frank Rubin. The quadratic and double quadratic residue ciphers. *Cryptologia*, 19(3):275–284, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wayner:1995:STS

[760] Peter Wayner. Strong theoretical steganography. *Cryptologia*, 19(3):285–299, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruth:1995:RTC

[761] Louis Kruth. Reviews and things cryptologic. *Cryptologia*, 19(3):300–318, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:1995:CS

[762] Anonymous. Change and structure. *Cryptologia*, 19(3):319–320, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Weber:1995:SOF

[763] Ralph E. Weber. Seward's other folly: the fight over America's first encrypted cable. *Cryptologia*, 19(4):321–348, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1995:WGN

[764] Michael van der Meulen. Werftschlüssel: a German Navy hand cipher system Part I. *Cryptologia*, 19(4):349–364, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1995:RTCb

[765] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 19(4):365–374, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Johnson:1995:MOJ

[766] Tom Johnson. The mystery of an old Japanese codebook. *Cryptologia*, 19(4):380–384, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gaddy:1995:CC

[767] David W. Gaddy. The cylinder-cipher. *Cryptologia*, 19(4):385–391, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Johnson:1995:CC

[768] Mike Johnson. Cryptology in cyberspace. *Cryptologia*, 19(4):392–396, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rubin:1995:MAU

[769] Frank Rubin. Message authentication using quadratic residues. *Cryptologia*, 19(4):397–404, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gillogly:1995:COC

[770] James J. Gillogly. Ciphertext-only cryptanalysis of Enigma. *Cryptologia*, 19(4):405–413, 1995. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Alvarez:1996:IDC

[771] David Alvarez. Italian diplomatic cryptanalysis in World War I. *Cryptologia*, 20(1):1–10, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bauer:1996:CDM

[772] Friedrich L. Bauer. Cryptological devices and machines in the Deutsches Museum, Munich. *Cryptologia*, 20(1): 11–13, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1996:RTCa

[773] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 20(1):14–36, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1996:WGN

[774] Michael van der Meulen. Werftschlüssel: a German Navy hand cipher system Part II. *Cryptologia*, 20(1):37–54, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

David:1996:WWI

[775] Charles David. A World War II German Army field cipher and how we

broke it. *Cryptologia*, 20(1):55–76, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schaefer:1996:SDE

[776] Edward F. Schaefer. A simplified Data Encryption Standard algorithm. *Cryptologia*, 20(1):77–84, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Clark:1996:COK

[777] Andrew Clark, Ed Dawson, and Helen Bergen. Combinatorial optimization and the knapsack cipher. *Cryptologia*, 20(1):85–93, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Alvarez:1996:FLV

[778] David Alvarez. Faded lustre: Vatican cryptography, 1815–1920. *Cryptologia*, 20(2):97–131, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Buonafalce:1996:AE

[779] Augusto Buonafalce. The Alberti Exhibition. *Cryptologia*, 20(2):132–134, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ratcliff:1996:CWW

[780] Rebecca Ratcliff. Cryptology and World War II: NSA's 1995 History Symposium. *Cryptologia*, 20(2):135–140, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1996:R

[781] Michael van der Meulen. Reihenschieber. *Cryptologia*, 20(2):141–154, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Mellen:1996:SAC

[782] Greg Mellen. Some adventures in Cryptoland. *Cryptologia*, 20(2):155–164, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dawson:1996:ACX

[783] E. Dawson and L. Nielsen. Automated cryptanalysis of XOR plaintext strings. *Cryptologia*, 20(2):165–181, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1996:RTCb

[784] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 20(2):183–191, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Currier:1996:MPT

[785] Prescott Currier. My "Purple" trip to England in 1941. *Cryptologia*, 20 (3):193–201, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1996:CEB

[786] Michael van der Meulen. Cryptology in the early Bundesrepublik. *Cryptologia*, 20(3):202–222, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Leary:1996:CC

[787] Thomas (Penn) Leary. Cryptology in the 15th and 16th Century. *Cryptologia*, 20(3):223–242, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Golomb:1996:FJN

[788] Solomon W. Golomb. On factoring Jevons' Number. *Cryptologia*, 20(3): 243–246, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rubin:1996:DHS

[789] Frank Rubin. Designing a high-security cipher. *Cryptologia*, 20(3):247–257, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Heys:1996:CSP

[790] Howard M. Heys and Stafford E. Tavares. Cryptanalysis of substitution-permutation networks using key-dependent degeneracy. *Cryptologia*, 20 (3):258–274, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kak:1996:ISS

[791] Subhash C. Kak. An Indus–Sarasvatī signboard. *Cryptologia*, 20(3):275–279, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1996:RTCc

[792] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 20(3):280–288, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Whitehead:1996:COB

[793] David Whitehead. Cobra and other bombes. *Cryptologia*, 20(4):289–307, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hinsley:1996:CHN

[794] Harry Hinsley. The counterfactual history of no Ultra. *Cryptologia*, 20(4): 308–324, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gillogly:1996:CC

[795] James J. Gillogly and Larry Harnisch. Cryptograms from the crypt. *Cryptologia*, 20(4):325–329, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:1996:KSI

[796] Ralph Erskine. Kriegsmarine signal indicators. *Cryptologia*, 20(4):330–340, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1996:SEH

[797] David Kahn. Some early Hungarian Communist ciphers. *Cryptologia*, 20(4):347–358, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rubin:1996:OTP

[798] Frank Rubin. One-time pad cryptography. *Cryptologia*, 20(4):359–364, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1996:RTCd

[799] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 20(4):365–380, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Pesic:1997:FVF

[800] Peter Pesic. François Viète, father of modern cryptanalysis — two new

manuscripts. *Cryptologia*, 21(1):1–29, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sims:1997:BAM

[801] John Cary Sims. The Brusa Agreement of May 17, 1943. *Cryptologia*, 21(1): 30–38, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderOye:1997:FLR

[802] David Schimmelpenninck van der Oye. A first look at Russia's codebreakers: a book review. *Cryptologia*, 21(1):39–41, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:1997:FNE

[803] Ralph Erskine. The first Naval Enigma decrypts of World War II. *Cryptologia*, 21(1):42–46, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:1997:EAI

[804] David H. Hamer. Enigma: Actions involved in the 'double stepping' of the middle rotor. *Cryptologia*, 21(1):47–50, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Guy:1997:DSC

[805] Jacques B. M. Guy. The distribution of signs *c* and *o* in the Voynich Manuscript: Evidence for a real language? *Cryptologia*, 21(1):51–54, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Chang:1997:DSS

[806] C. C. Chang, J. K. Jan, and H. C. Kowng. A digital signature scheme based upon the theory of quadratic residues. *Cryptologia*, 21(1):55–70, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Constance:1997:HJB

[807] Paul Constance. How Jim Bamford probed the NSA. *Cryptologia*, 21(1): 71–74, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1997:RTCa

[808] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 21(1):75–92, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sassoon:1997:BCM

[809] George Sassoon. British company makes PGP easier to use. *Cryptologia*, 21(1):93–94, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rubin:1997:ETG

[810] Aviel D. Rubin. An experience teaching a graduate course in cryptography. *Cryptologia*, 21(2):97–109, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1997:RTCb

[811] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 21(2):110–128, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Clark:1997:PGA

[812] Andrew Clark and Ed Dawson. A parallel genetic algorithm for cryptanalysis of the polyalphabetic substitution cipher. *Cryptologia*, 21(2):129–138, 1997.

CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Chau:1997:OWF

[813] H. F. Chau and H.-K. Lo. One-way functions in reversible computations. *Cryptologia*, 21(2):139–148, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Scott:1997:SJN

[814] Norman Scott. Solving Japanese Naval ciphers 1943–45. *Cryptologia*, 21(2): 149–157, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1997:BEE

[815] David Kahn. British economic espionage. *Cryptologia*, 21(2):158–164, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:1997:GWI

[816] Anonymous. German wireless intercept organization. *Cryptologia*, 21(2):165–190, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Deavours:1997:LCA

[817] C. A. Deavours. Lobsters, crabs, and the Abwehr Enigma. *Cryptologia*, 21(3):193–199, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1997:B

[818] Michael van der Meulen. Bundeswehrtarnverfahren. *Cryptologia*, 21 (3):200–217, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1997:RTCc

[819] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 21(3):218–236, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Cain:1997:HBG

[820] Thomas R. Cain and Alan T. Sherman. How to break Gifford's Cipher. *Cryptologia*, 21(3):237–286, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kelley:1997:SSC

[821] Stephen J. Kelley. The SIGCUM Story: Cryptographic failure, cryptologic success. *Cryptologia*, 21(4):289–316, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Koblitz:1997:CTT

[822] Neal Koblitz. Cryptography as a teaching tool. *Cryptologia*, 21(4):317–326, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lee:1997:SPA

[823] Nara-Yih Lee and Tzonelih Hwang. On the security of Park et al.'s key distribution protocol for digital mobile communications. *Cryptologia*, 21(4):327–334, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1997:RTCd

[824] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 21(4):335–349, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Foster:1997:DOT

[825] Caxton C. Foster. Drawbacks of the one-time pad. *Cryptologia*, 21(4):350–352, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Greenough:1997:CSH

[826] H. Paul Greenough. Cryptanalysis of the Swedish HC-9: a known-plaintext approach. *Cryptologia*, 21(4):353–367, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Comstock:1997:RIS

[827] Lieutenant Commander I. W. Comstock. Radio intelligence and security. *Cryptologia*, 21(4):368–377, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1998:SCC

[828] David Kahn. Soviet Comint in the Cold War. *Cryptologia*, 22(1):1–24, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Weierud:1998:SCS

[829] Frode Weierud. Sweden cryptographic superpower: a book review. *Cryptologia*, 22(1):25–28, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Burke:1998:GTS

[830] Colin Burke. A gracious but tragic special Ultra message. *Cryptologia*, 22(1): 29–32, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1998:FGC

[831] Michael van der Meulen. A first German Cryptologic Exhibition. *Cryptologia*, 22(1):33–48, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1998:RTCa

[832] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 22(1):49–55, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Moldovyan:1998:SEA

[833] A. A. Moldovyan and N. A. Moldovyan. Software encryption algorithms for transparent protection technology. *Cryptologia*, 22(1):56–68, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Heider:1998:CF

[834] Franz-Peter Heider. A colossal fish. *Cryptologia*, 22(1):69–95, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1998:SWS

[835] Louis Kruh. Still waiting to be solved: Elgar's 1897 cipher message. *Cryptologia*, 22(2):97–98, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lewis:1998:SRS

[836] Graydon A. Lewis. Setting the record straight on Midway. *Cryptologia*, 22(2): 99–101, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:1998:ECS

[837] Anonymous. Elementary cipher solution. *Cryptologia*, 22(2):102–120, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Nichols:1998:BC

[838] Randall K. Nichols. The Bible Code. *Cryptologia*, 22(2):121–133, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Moldovyan:1998:FBC

[839] A. A. Moldovyan and N. A. Moldovyan. Flexible block cipher with provably inequivalent cryptalgorithm modifications. *Cryptologia*, 22(2):134–140, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1998:RGD

[840] Michael van der Meulen. The road to German diplomatic ciphers — 1919 to 1945. *Cryptologia*, 22(2):141–166, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1998:RTCb

[841] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 22(2):167–191, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Mendelson:1998:ERC

[842] Kenneth A. Mendelson, Stephen T. Walker, and Joan D. Winston. The evolution of recent cryptographic policy in the United States. *Cryptologia*, 22(3):193–210, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:1998:EVE

[843] David H. Hamer, Geoff Sullivan, and Frode Weierud. Enigma variations: an extended family of machines. *Cryptologia*, 22(3):211–229, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Viterbo:1998:CAC

[844] Emanuele Viterbo. The ciphered autobiography of a 19th Century Egyptologist. *Cryptologia*, 22(3):231–243, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kelly:1998:MS

[845] Thomas Kelly. The myth of the Skytale. *Cryptologia*, 22(3):244–260, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1998:RTCc

[846] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 22(3):261–265, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Coppersmith:1998:AFR

[847] Don Coppersmith. Attacking four-round Luby–Rackoff ciphers. *Cryptologia*, 22(3):266–278, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kourtis:1998:SDD

[848] A. Kourtis and Ch. Mantakas. Statistical distribution of delta modulated speech signals as a means for cryptanalysis in voice encryption systems. *Cryptologia*, 22(3):279–287, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Reeds:1998:SCB

[849] Jim Reeds. Solved: the ciphers in Book III of Trithemius's Steganographia. *Cryptologia*, 22(4):291–317, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ernst:1998:NAC

[850] Thomas Ernst. The numerical–astrological ciphers in the Third Book of Trithemius's Steganographia. *Cryptologia*, 22(4):318–341, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderOye:1998:TCS

[851] David Schimmelpenninck van der Oye. Tsarist codebreaking: Some background and some examples. *Cryptologia*, 22(4):342–353, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Pfeiffer:1998:BGW

[852] Paul N. Pfeiffer. Breaking the German weather ciphers in the Mediterranean Detachment G, 849th Signal Intelligence Service. *Cryptologia*, 22(4):354–369, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1998:AHY

[853] Louis Kruh. Another Herbert O. Yardley mystery? *Cryptologia*, 22(4):370–375, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1998:RTCd

[854] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 22(4):376–379, 1998. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lomonaco:1999:QGQ

[855] Samuel J. Lomonaco. A quick glance at quantum cryptography. *Cryptologia*, 23(1):1–41, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1999:RTCa

[856] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 23(1):42–54, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Reeds:1999:BRC

[857] Jim Reeds. Breakthrough in Renaissance cryptography: a book review. *Cryptologia*, 23(1):59–62, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:1999:SBT

[858] David Kahn. Students better than a pro (Bazeries) and an author (Candela). *Cryptologia*, 23(1):63–64, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:1999:KSS

[859] Ralph Erskine. Kriegsmarine short signal systems — and how Bletchley Park exploited them. *Cryptologia*, 23(1):65–92, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Budiansky:1999:TCP

[860] Stephen Budiansky. A tribute to Cecil Phillips—and Arlington Hall's "Meritocracy". *Cryptologia*, 23(2):97–107,

1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Davies:1999:BRL

[861] Donald W. Davies. The bombe: a remarkable logic machine. *Cryptologia*, 23(2):108–138, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Greenough:1999:CHC

[862] H. Paul Greenough. Cryptanalysis of the Hagelin C-52 and similar machines a known plaintext attack. *Cryptologia*, 23(2):139–156, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Walker:1999:CPUa

[863] Stephen T. Walker and Joan D. Winston. Cryptography policy update. *Cryptologia*, 23(2):157–163, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1999:RTCb

[864] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 23(2):171–188, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ulbricht:1999:EU

[865] Heinz Ulbricht. Enigma-Uhr. *Cryptologia*, 23(3):193–205, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bauer:1999:EHR

[866] Friedrich L. Bauer. An error in the history of rotor encryption devices. *Cryptologia*, 23(3):206–210, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Savard:1999:EMI

[867] John J. G. Savard and Richard S. Pekelney. The ECM Mark II: Design, history, and cryptology. *Cryptologia*, 23(3):211–228, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Davies:1999:EDB

[868] Donald W. Davies. Effectiveness of the diagonal board. *Cryptologia*, 23 (3):229–239, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vanderMeulen:1999:GAF

[869] Michael van der Meulen. German Air Force Signal Intelligence 1956: a museum of comint and sigint. *Cryptologia*, 23(3):240–256, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

McKay:1999:SCS

[870] Craig Graham McKay. Swedish cryptanalysis and the saga of Arne Beurling: a book review. *Cryptologia*, 23(3):257–258, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1999:VHF

[871] Louis Kruh. Vint Hill Farms Station. *Cryptologia*, 23(3):259–260, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Roch:1999:BIA

[872] Axel Roch. Biopolitics and intuitive algebra in the mathematization of cryptology? a review of Shannon's "A Mathematical Theory of

Cryptography" from 1945. *Cryptologia*, 23(3):261–266, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ellis:1999:HNS

[873] J. H. Ellis. The history of non-secret encryption. *Cryptologia*, 23(3):267–273, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1999:RTCc

[874] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 23(3):274–286, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hagerty:1999:UYM

[875] Alexander Hagerty. An unpublished Yardley manuscript. *Cryptologia*, 23 (4):289–297, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Smith:1999:UDG

[876] David M. Smith. The use of decrypted German weather reports in the operations of the Fifteenth Air Force over Europe. *Cryptologia*, 23(4):298–304, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Williams:1999:NVM

[877] Robert L. Williams. A note on the Voynich Manuscript. *Cryptologia*, 23(4):305–309, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sullivan:1999:SNC

[878] Geoff Sullivan and Frode Weierud. The Swiss NEMA cipher machine. *Cryptologia*, 23(4):310–328, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Walker:1999:CPUb

[879] Stephen T. Walker and Joan D. Winston. Cryptography policy update. *Cryptologia*, 23(4):329–342, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:1999:RTCd

[880] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 23(4):343–352, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Mclean:1999:NC

[881] Ridley Mclean. Naval communications. *Cryptologia*, 23(4):353–379, 1999. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Winkel:2000:AGM

[882] Brian J. Winkel. Annual Greg Mellen Memorial Cryptology Scholarship Prize. *Cryptologia*, 24(1):1–3, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Williams:2000:ASL

[883] Heidi Williams. Applying statistical language recognition techniques in the ciphertext-only cryptanalysis of Enigma. *Cryptologia*, 24(1):4–17, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schneier:2000:SSC

[884] Bruce Schneier. A self-study course in block-cipher cryptanalysis. *Cryptologia*, 24(1):18–33, 2000. CODEN

CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sawada:2000:GRC

[885] Hideki Sawada and Takahiro Abe. Groups and RSA cryptosystems. *Cryptologia*, 24(1):34–40, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2000:GAE

[886] David H. Hamer. G-312: an Abwehr Enigma. *Cryptologia*, 24(1):41–54, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Marks:2000:RWE

[887] Philip Marks and Frode Weierud. Recovering the wiring of Enigma's Umkehrwalze A. *Cryptologia*, 24(1):55–66, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2000:RTCa

[888] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 24(1):67–93, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:2000:WDS

[889] Ralph Erskine. What did the Sinkov Mission receive from Bletchley Park? *Cryptologia*, 24(2):97–109, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Jacobsen:2000:CVA

[890] Philip H. Jacobsen. A cryptologic veteran's analysis of "Day of Deceit" — a book review. *Cryptologia*, 24(2):110–118, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1689].

Budiansky:2000:CBP

[891] Stephen Budiansky. Closing the book on Pearl Harbor. *Cryptologia*, 24(2):119–130, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Davies:2000:UCD

[892] Donald W. Davies. An unidentified cipher device. *Cryptologia*, 24(2):131–134, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Knudsen:2000:COA

[893] Lars R. Knudsen and Vincent Rijmen. Ciphertext-only attack on Akelarre. *Cryptologia*, 24(2):135–147, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wang:2000:TGI

[894] Chih-Hung Wang and Tzonelih Hwang. (t, m) threshold and generalized ID-based conference key distribution system. *Cryptologia*, 24(2):148–159, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ratcliff:2000:CTC

[895] Rebecca A. Ratcliff. Cryptology through the centuries: NSA's 1999 History Symposium. *Cryptologia*, 24(2):160–167, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2000:RTCb

[896] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 24(2):168–189,

2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Pesic:2000:CLF

[897] Peter Pesic. The clue to the labyrinth: Francis Bacon and the decryption of nature. *Cryptologia*, 24(3):193–211, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Parker:2000:HOG

[898] Frederick D. Parker. How OP-20-G got rid of Joe Rochefort. *Cryptologia*, 24(3):212–234, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hammant:2000:RSC

[899] Thomas R. Hammant. Russian and Soviet cryptology I — some communications intelligence in Tsarist Russia. *Cryptologia*, 24(3):235–249, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Li:2000:TMS

[900] Chuan-Ming Li, Tzonelih Hwang, Narn-Yih Lee, and Juin-Jang Tsai. (t, n) threshold-multisignature scheme and generalized-multisignature scheme where suspected forgery implies traceability of adversarial shareholders. *Cryptologia*, 24(3):250–268, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2000:RTCc

[901] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 24(3):269–286, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Huffman:2000:NCT

[902] Stephen Huffman. The Navajo Code Talkers: a cryptologic and linguistic perspective. *Cryptologia*, 24(4):289–320, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

McKay:2000:AJF

[903] Craig McKay. From the archives: Japanese fears and the ironies of interception. *Cryptologia*, 24(4):321–323, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Phillips:2000:ASG

[904] Cecil Phillips. The American solution of a German one-time-pad cryptographic system (G-OTP). *Cryptologia*, 24(4):324–332, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hammant:2000:IMI

[905] Thomas R. Hammant. II — the Magdeburg Incident: the Russian view. *Cryptologia*, 24(4):333–338, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schindler:2000:HSA

[906] John R. Schindler. A hopeless struggle: Austro-Hungarian cryptology during World War I. *Cryptologia*, 24(4):339–350, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Burke:2000:LE

[907] Colin Burke. Letter to the editor. *Cryptologia*, 24(4):351–352, 2000. CODEN

CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Saeednia:2000:HMH

[908] Shahrokh Saeednia. How to make the Hill Cipherh secure. *Cryptologia*, 24(4):353–360, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Atkinson:2000:DBK

[909] Russell Atkinson. David Brian Kern: Theft of trade secrets. *Cryptologia*, 24(4):361–369, 2000. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Turing:2001:VNC

[910] Alan M. Turing. Visit to National Cash Register Corporation of Dayton, Ohio. *Cryptologia*, 25(1):1–10, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gladwin:2001:ATV

[911] Lee A. Gladwin. Alan Turing's visit to Dayton. *Cryptologia*, 25(1):11–17, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rubin:2001:TEC

[912] Michael Rubin. The telegraph, espionage, and cryptology in Nineteenth Century Iran. *Cryptologia*, 25(1):18–36, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Risca:2001:DBS

[913] Viviana I. Risca. DNA-based steganography. *Cryptologia*, 25(1):37–49, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hammant:2001:RSCa

[914] Thomas R. Hammant. Russian and Soviet cryptology III — Soviet Comint and the Civil War, 1918–1921. *Cryptologia*, 25(1):50–60, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hammant:2001:RSCb

[915] Thomas R. Hammant. Russian and Soviet cryptology IV — some incidents in the 1930's. *Cryptologia*, 25(1):61–63, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2001:RTCa

[916] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 25(1):64–79, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ibbotson:2001:SC

[917] Peter Ibbotson. Sayers and ciphers. *Cryptologia*, 25(2):81–87, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Burke:2001:KPA

[918] Colin Burke. Kim Philby, the American intelligence community, and OP-20-G: the fox built the hen-house and took the keys. *Cryptologia*, 25(2):88–90, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Winkler:2001:AEC

[919] Jonathan Winkler. From the archives: Early corporate espionage amid World War I censorship. *Cryptologia*, 25(2): 91–94, 2001. CODEN CRYPE6. ISSN

0161-1194 (print), 1558-1586 (electronic).

Johnsen:2001:CRI

[920] Ben Johnsen. Cryptography in runic inscriptions: a remark on the article, "Cryptography in Runic Inscriptions," by O. G. Landsverk. *Cryptologia*, 25(2):95–100, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Marks:2001:UDEa

[921] Philip Marks. Umkehrwalze D: Enigma's rewirable reflector — Part I. *Cryptologia*, 25(2):101–141, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2001:RTCb

[922] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 25(2):142–159, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2001:GLC

[923] Anonymous. The glow-lamp ciphering and deciphering machine: Enigma. *Cryptologia*, 25(3):161–173, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2001:NHC

[924] Anonymous. The noncryptanalytic headaches of cryptanalysts. *Cryptologia*, 25(3):174–176, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Marks:2001:UDEb

[925] Philip C. Marks. Umkehrwalze D: Enigma's rewirable reflector — Part II. *Cryptologia*, 25(3):177–212, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hernandez:2001:GAC

[926] J. C. Hernández, A. Ribagorda, P. Isasi, and J. M. Sierra. Genetic algorithms can be used to obtain good linear congruential generators. *Cryptologia*, 25(3):213–229, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2001:RTCc

[927] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 25(3):230–239, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Budiansky:2001:CIM

[928] Stephen Budiansky. Codebreaking with IBM machines in World War II. *Cryptologia*, 25(4):241–255, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

deLeeuw:2001:JFE

[929] Karl de Leeuw. Johann Friedrich Euler (1741–1800): Mathematician and cryptologist at the court of the Dutch Stadholder William V. *Cryptologia*, 25(4):256–274, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Landini:2001:ELS

[930] Gabriel Landini. Evidence of linguistic structure in the Voynich Manuscript using spectral analysis. *Cryptologia*, 25(4):275–295, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Marks:2001:UDEc

[931] Philip C. Marks. Umkehrwalze D: Enigma's rewirable reflector — Part III. *Cryptologia*, 25(4):296–310, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2001:RTCd

[932] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 25(4):311–317, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2002:CEB

[933] Louis Kruh and Cipher Deavours. The commercial Enigma: Beginnings of machine cryptography. *Cryptologia*, 26(1): 1–16, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Michie:2002:CBW

[934] Donald Michie. Colossus and the breaking of the wartime "fish" codes. *Cryptologia*, 26(1):17–58, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2002:WCC

[935] Louis Kruh. The world of codes and ciphers at the Heinz Nixdorf Museumsforum. *Cryptologia*, 26(1):59–67, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gnanaguruparan:2002:RHS

[936] Meenakshi Gnanaguruparan and Subhash Kak. Recursive hiding of secrets in visual cryptography. *Cryptologia*, 26(1):68–76, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2002:RTCa

[937] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 26(1):77–79, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Glunder:2002:WGO

[938] Georg Glünder and Paul Whitaker. Wireless and "Geheimschreiber" operator in the war, 1941–1945. *Cryptologia*, 26(2):81–96, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sullivan:2002:EMI

[939] Geoff Sullivan. The ECM Mark II: Some observations on the rotor stepping. *Cryptologia*, 26(2):97–100, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Koot:2002:EOE

[940] H. Koot. Expert's opinion on the Enigma ciphering machine. *Cryptologia*, 26(2):101–102, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Clive:2002:BS

[941] Keith P. Clive. The battle of the seals. *Cryptologia*, 26(2):103–112, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Beckman:2002:ECD

[942] Bengt Beckman. An early cipher device: Fredrik Gripenstierna's machine. *Cryptologia*, 26(2):113–123, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2002:BRB

[943] Anonymous. Britain reveals its bombe to America from the archives. *Cryptologia*, 26(2):124–128, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Phan:2002:FNS

[944] Raphael Chung-Wei Phan. Further notes for a self-study course in block-cipher cryptanalysis. *Cryptologia*, 26 (2):129–137, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2002:RTCb

[945] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 26(2):138–158, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:2002:RT

[946] David Kahn. A riverbank trove. *Cryptologia*, 26(3):161–164, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Stallings:2002:AES

[947] William Stallings. The Advanced Encryption Standard. *Cryptologia*, 26 (3):165–188, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Heys:2002:TLD

[948] Howard M. Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wolfe:2002:NCA

[949] Henry B. Wolfe. Non-cryptanalytic attacks. *Cryptologia*, 26(3):222–234, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2002:RTCc

[950] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 26(3):235–239, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2002:CRJ

[951] Anonymous. Codetalkers recognition not just the Navajos. *Cryptologia*, 26(4):241–256, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sullivan:2002:CHM

[952] Geoff Sullivan. Cryptanalysis of Hagelin machine pin wheels. *Cryptologia*, 26(4):257–273, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bauer:2002:SAR

[953] Craig Bauer and Christian N. S. Tate. A statistical attack on the running key cipher. *Cryptologia*, 26(4):274–282, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Phan:2002:MAE

[954] Raphael Chung-Wei Phan. Mini Advanced Encryption Standard (Mini-AES): a testbed for cryptanalysis students. *Cryptologia*, 26(4):283–306, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2002:RTCd

[955] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 26(4):307–317, 2002. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Freeman:2003:PRS

[956] Wes Freeman, Geoff Sullivan, and Frode Weierud. Purple revealed: Simulation and computer-aided cryptanalysis of Angooki Taipu B. *Cryptologia*, 27(1):1–43, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Turing:2003:CRS

[957] Alan M. Turing. Critique of "Running Short Cribs on the U. S. Navy Bombe". *Cryptologia*, 27(1):44–49, January 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gladwin:2003:AMT

[958] Lee A. Gladwin. Alan M. Turing's critique of running short cribs on the US Navy bombe. *Cryptologia*, 27(1):50–54, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2003:RTCa

[959] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 27(1):55–72, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

deLeeuw:2003:DIR

[960] Karl de Leeuw. The Dutch invention of the rotor machine, 1915–1923. *Cryptologia*, 27(1):73–94, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2003:EOR

[961] David H. Hamer. The Enigmas — and other recovered artefacts — of U-85. *Cryptologia*, 27(2):97–110, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:2003:AWS

[962] Ralph Erskine. From the archives: What the Sinkov Mission brought to Bletchley Park. *Cryptologia*, 27(2):111–118, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ratcliff:2003:HSL

[963] R. A. Ratcliff. How statistics led the Germans to believe Enigma secure and why they were wrong: Neglecting the practical mathematics of cipher machines. *Cryptologia*, 27(2):119–131, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Buonafalce:2003:SEB

[964] Augusto Buonafalce. From the Skytale to the Enigma: Book review. *Cryptologia*, 27(2):132–134, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

David:2003:SSE

[965] James David. Soviet secrets in the ether — clandestine radio stations at the New York and San Francisco Consulates in World War II. *Cryptologia*, 27(2):135–147, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Musa:2003:SAA

[966] Mohammad A. Musa, Edward F. Schaefer, and Stephen Wedig. A simplified AES algorithm and its linear and differential cryptanalyses. *Cryptologia*, 27(2):148–177, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Winkel:2003:ECC

[967] Brian J. Winkel. Extraordinary cryptology collection. *Cryptologia*, 27(2): 180–181, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2003:RTCb

[968] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 27(2):182–191, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Jacobsen:2003:FPH

[969] Philip H. Jacobsen. Foreknowledge of Pearl Harbor? No!: the story of the US Navy's efforts on JN-25B. *Cryptologia*, 27(3):193–205, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1689].

Faurholt:2003:UCC

[970] Niels Faurholt. Urkryptografen ("the clock cryptograph"). *Cryptologia*, 27 (3):206–208, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Clarkson:2003:CMM

[971] Dorothy Clarkson. Cypher machines maintenance and restoration spanning sixty years. *Cryptologia*, 27(3):209–216, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Abeles:2003:MTC

[972] Francine F. Abeles. The Memoria Technica cipher. *Cryptologia*, 27(3): 217–229, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2003:RTCc

[973] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 27(3):230–232, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sheldon:2003:SRU

[974] Rose Mary Sheldon. The Sator Rebus: an unsolved cryptogram? *Cryptologia*, 27(3):233–287, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:2003:BJT

[975] Ralph Erskine and Peter Freeman. Brigadier John Tiltman: One of Britain's finest cryptologists. *Cryptologia*, 27(4):289–318, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Fabris:2003:NUP

[976] Francesco Fabris and Myron Curtis. A nomenclator used by propaganda fide during the Chinese Rites Controversy. *Cryptologia*, 27(4):319–338, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

vonzurGathen:2003:CCF

[977] Joachim von zur Gathen. Claude Comiers: the first arithmetical cryptography. *Cryptologia*, 27(4):339–349,

2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anderson:2003:NSG

[978] Bob Anderson and George McGinnis. Naval Security Group Command display. *Cryptologia*, 27(4):350–360, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Phan:2003:IDC

[979] Raphael Chung-Wei Phan. Impossible differential cryptanalysis of Mini-AES. *Cryptologia*, 27(4):361–374, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2003:RTCd

[980] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 27(4):375–378, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kruh:2003:SBC

[981] Louis Kruh. The Shakespeare–Bacon controversy continues on the stage. *Cryptologia*, 27(4):379–380, 2003. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:2004:CJM

[982] David Kahn. Charles J. Mendelsohn and why I envy him. *Cryptologia*, 28(1):1–17, January 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639548~db=all~order=page`.

Zetterstrom:2004:SST

[983] Urban Zetterström. Swedish SA teleprinter cipher system. *Cryptologia*, 28(1):18–30, January 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639549~db=all~order=page`.

Rugg:2004:EHP

[984] Gordon Rugg. An elegant hoax? A possible solution to the Voynich manuscript. *Cryptologia*, 28(1):31–46, January 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639550~db=all~order=page`.

Anonymous:2004:EFE

[985] Anonymous. Enigma and friends exhibit: Bletchley Park exhibit opens. *Cryptologia*, 28(1):47–49, January 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639551~db=all~order=page`.

Kochanski:2004:CCE

[986] Martin Kochanski. The comedy of commercial encryption software. *Cryptologia*, 28(1):50–54, January 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639552~db=all~order=page`.

Savory:2004:PER

[987] Stuart Savory. Pocket Enigma: The review. *Cryptologia*, 28(1):55–59, January 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a748639553~db=all~order=page.

Kruh:2004:RTCa

[988] Louis Kruh. Reviews and things cryptologic: Kruh, David. Riverbank: The Trial of William Shakespeare, a play. Eldridge Publishing Co., P. O. Box 14367, Tallahassee FL 32317 USA. 2003. 70 pp. $6.50; Jackson, John, Ed. *The secret War of Hut 3: The First Story of How Intelligence from Enigma Signals Decoded at Bletchley Park Was Used During World War II*. The Military Press, 1 Gallagher Close, Milton Keynes MK8 01Q UK. 2002. 115 pp. 8 1/2in by 11 3/4in. Hardback 25.00/839.30; Paperback £15.00/ $23.60.0 pp. $24.95; Kennedy, Shawn. *Funny Cryptograms*. Sterling Publishing Co., 387 Park Ave. South, New York NY 10016-8810 USA. 2003. 96 pp. $6.95; Petitcolas, Fabien A. P., Editor. *Information Hiding. 5th International Workshop, Noordwijkerhout, The Netherlands, Oct., 2000*. Springer-Verlag, 175 Fifth Ave., New York NY 10010 USA. 2003. 427 pp. $69.00; Boyd, Colin and Anish Mathuria. *Protocols for Authentication and Key Establishment*. Springer-Verlag, 175 Fifth Avenue, New York, NY 10010 USA. 2003. 321 pp. $54.95; Smith, Sarah. *Chasing Shakespeare*. Atria Books, 1230 Avenue of the America, New York NY 10020 USA. 2003. 337 pp. $24.00; Farago, Ladislas. *Burn After Reading: The Espionage History of World War II*. Naval Institute Press, 291 Wood Road, Annapolis MD 21402 USA. 2003 reprint. 319 pp. $18.95. *Cryptologia*, 28(1):60–95, January 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639554~db=all~order=page.

Holden:2004:CCC

[989] Joshua Holden. A comparison of cryptography courses. *Cryptologia*, 28(2): 97–111, April 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639556~db=all~order=page.

Kruh:2004:UGW

[990] Louis Kruh. Unknown German World War II cipher device. *Cryptologia*, 28(2):112–114, April 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639557~db=all~order=page.

Cowan:2004:REH

[991] Michael J. Cowan. Rasterschlüssel 44 — the epitome of hand field ciphers. *Cryptologia*, 28(2):115–148, April 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639558~db=all~order=page. See correction [1010].

Lawrence:2004:VRM

[992] John Lawrence. The versatility of Rejewski's method: Solving for the wiring of the second rotor. *Cryptologia*, 28(2):149–152, April 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a748639559~db=all~order=page.

Quirantes:2004:MZN

[993] Arturo Quirantes. Model Z: a numbers-only Enigma version. *Cryptologia*, 28(2):153–156, April 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639560~db=all~order=page. See correction [1003].

Driskell:2004:WBS

[994] Lisa Driskell. Wavelet-based steganography. *Cryptologia*, 28(2):157–174, April 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639561~db=all~order=page.

Kruh:2004:RTCb

[995] Louis Kruh. Reviews and things cryptologic: Jackson, John, Ed. *The Secret War of Hut 3: The First Story of How Intelligence from Enigma Signals Decoded at Bletchley Park Was Used During World War II*. The Military Press, 1 Gallagher Close, Milton Keynes MK8 01Q, United Kingdom. 2002, 115 pp., 8 1/2in by 11 3/4in. Hardback £25.00/$39.30; Paperback £15.00/$23.60; Carter, Philip and Ken Russell. *Brain Sizzlers*. Sterling Publishing Co., Inc., 387 Park Avenue South, New York NY 10016-8810 USA. 2003. 304 p. $5.95; Jenkins, Gerald and Magdalen Bear. *Codes and Ciphers: Clever Devices for Coding and Decoding to cut out and make*. Parkwest Publications Inc., P. O. Box 20261, New York NY 10025 USA. 2003. 32 pp. $12.00; Jenkins, Gerald and Anne Wild. *Be a Codebreaker! Mystery messages to puzzle over and decipher*. Parkwest Publications Inc., P. O. Box 20261, New York NY 10025 USA. 2003. 32 pp. $10.00; Praham, Jill. *So Power Can Be Brought into Play: SIGINT and the Pusan Perimeter*. Center for Cryptologic History, National Security Agency, 9800 Savage Road, Fort Meade MD 20755-6886 USA. 2000. 18 pp; Nickles, David Paull. *Under the Wire: How the Telegraph Changed Diplomacy*. Harvard University Press, Cambridge MA 02138 USA. 2003. 265 pp. $30.95; Mowry, David P. *German Cipher Machines of World War II*. Center for Cryptologic History, National Security Agency, 9800 Savage Road, Fort Meade MD 20755-6886 USA. 2003. 32 pp; Myers, Katherine. *Codebreaker*. Salvo Press, 61428 Elder Ridge Street, Bend OR 97702 USA. 2000. 289 pp. $16.95 paperback; Mao, Wenbo. *Modern Cryptography: Theory and Practice*. Pearson Education, Prentice Hall Professional Technical Reference, Upper Saddle River NJ 07458 USA. 2004. 707 pp. $54.99. *Cryptologia*, 28(2):175–190, April 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639562~db=all~order=page.

Bury:2004:PCD

[996] Jan Bury. Polish codebreaking during the Russo–Polish war of 1919–1920. *Cryptologia*, 28(3):193–203, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.

informaworld.com/smpp/content~content=a748639564~db=all~order=page.

Koss:2004:PEM

[997] Mike Koss. The paper Enigma Machine. *Cryptologia*, 28(3):204–210, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://mckoss.com/crypto/enigma.htm; http://www.findarticles.com/p/articles/mi_qa3926/is_200407/ai_n9458626; http://www.informaworld.com/smpp/content~content=a748639565~db=all~order=page.

Erskine:2004:NES

[998] Ralph Erskine and Philip Marks. Naval Enigma: Seahorse and other Kriegsmarine cipher blunders. *Cryptologia*, 28(3):211–241, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639566~db=all~order=page.

Kruh:2004:RTCc

[999] Louis Kruh. Reviews and things cryptologic: Mohamad Mrayati, Yahya Meer Alain, and M. Hassan al-Tayyan, Eds. *Ibn Adlan's Treatise: A Manual on Cryptanalysis written for King alAsraf*. Volume Two of Series, Arabic Origins of Cryptology. King Faisal Center for Research and Islamic Studies, P. O. Box 51049, Riyadh 11543, SAUDI ARABIA. 2003. 113 pp. $15.00. *Cryptologia*, 28(3):242–252, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639567~db=all~order=page.

Buonafalce:2004:SSM

[1000] Augusto Buonafalce. Sir Samuel Morland's Machina Cyclologica Cryptographica. *Cryptologia*, 28(3):253–264, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639568~db=all~order=page.

SolerFuensanta:2004:MCS

[1001] José Ramón Soler Fuensanta. Mechanical cipher systems in the Spanish Civil War. *Cryptologia*, 28(3):265–276, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639569~db=all~order=page.

Niblo:2004:USN

[1002] Graham A. Niblo. The University of Southampton National Cipher Challenge. *Cryptologia*, 28(3):277–286, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639570~db=all~order=page.

Anonymous:2004:CMZ

[1003] Anonymous. Correction: *Model Z: A Numbers-Only Enigma Version*, Arturo Quirantes, Volume XXVII, Number 2, pp. 153–156, April 2004. *Cryptologia*, 28(3):??, July 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [993].

Richard:2004:BJA

[1004] Joseph E. Richard. The breaking of the Japanese Army's codes. *Cryptologia*, 28(4):289–308, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639572~db=all~order=page.

vonzurGathen:2004:FJB

[1005] Joachim von zur Gathen. Friederich Johann Buck: Arithmetic puzzles in cryptography. *Cryptologia*, 28(4):309–324, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.findarticles.com/p/articles/mi_qa3926/is_200410/ai_n9464432; http://www.informaworld.com/smpp/content~content=a748639573~db=all~order=page.

Donovan:2004:FJS

[1006] Peter Donovan. The flaw in the JN25 series of ciphers. *Cryptologia*, 28 (4):325–340, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639574~db=all~order=page.

Stehle:2004:BLC

[1007] Damien Stehlé. Breaking Littlewood's cipher. *Cryptologia*, 28(4):341–357, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639575~db=all~order=page.

Al-Ubaidy:2004:BBA

[1008] Mahmood Khalel Ibrahem Al-Ubaidy. Black-box attack using neuro-identifier. *Cryptologia*, 28(4):358–372, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639576~db=all~order=page.

Kruh:2004:RTCd

[1009] Louis Kruh. Reviews and things cryptologic: Young, Adam L. and Moti Yung. Malicious Cryptography: Exposing Cryptovirology. Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis IN 46256 USA. 2004, 392 pp. $45.00. *Cryptologia*, 28(4):373–379, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.findarticles.com/p/articles/mi_qa3926/is_200410/ai_n9464431; http://www.informaworld.com/smpp/content~content=a748639577~db=all~order=page.

Anonymous:2004:CRE

[1010] Anonymous. Corrections: *Rasterschlüssel 44 — The Epitome of Hand Field Ciphers*, Cryptologia XXVIII(2): 115–149, April 2004. *Cryptologia*, 28(4):??, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [991].

Gaddy:2004:LEV

[1011] David Gaddy. Letter to the editor: Vigenère decryption. *Cryptologia*, 28(4):??, October 2004. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bruckner:2005:GFC

[1012] Hilmar-Detlef Brückner. Germany's first cryptanalysis on the Western Front: Decrypting British and French naval ciphers in World War I. *Cryptologia*, 29(1):1–22, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244764; http://www.informaworld.com/smpp/content~content=a748639579~db=all~order=page.

Gladwin:2005:DSB

[1013] Lee A. Gladwin. The diplomacy of security: Behind the negotiations of Article 18 of the Sino-American Cooperative Agreement. *Cryptologia*, 29(1):23–42, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244701; http://www.informaworld.com/smpp/content~content=a748639580~db=all~order=page.

Kahn:2005:MIM

[1014] David Kahn. The Man in the Iron Mask — encore et enfin, cryptologically. *Cryptologia*, 29(1):43–49, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244754; http://www.informaworld.com/smpp/content~content=a748639581~db=all~order=page.

Mandhani:2005:WUD

[1015] Navneet Mandhani and Subhash Kak. Watermarking using decimal sequences. *Cryptologia*, 29(1):50–58, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639582~db=all~order=page.

Overbey:2005:KHC

[1016] Jeffrey Overbey, William Traves, and Jerzy Wojdylo. On the keyspace of the Hill cipher. *Cryptologia*, 29(1):59–72, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639583~db=all~order=page.

Cooper:2005:PKC

[1017] Rodney H. Cooper and Christopher G. Andrews. The public key covert channel. *Cryptologia*, 29(1):73–75, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639584~db=all~order=page.

Kahn:2005:ACW

[1018] David Kahn. From the archives: Codetalkers not wanted. *Cryptologia*, 29(1):76–87, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244789; http://www.informaworld.com/smpp/content~content=a748639585~db=all~order=page.

Kruh:2005:RTCa

[1019] Louis Kruh. Reviews and things cryptologic: Bamford, James. *A Pretext For War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies*. Doubleday. 2004. 420 pp. $26.95; Goldreich, Oded. Foundations of Cryptography: Volume II: Basic Applications. Cambridge University Press, 40 West 20th Street, New York NY 10011-4211 USA. 2004. 798 pp. $75.00; McBain. Ed. *Hark!*. Simon & Schuster, 1230 Avenue of the Americas, New York NY 10020 USA. 2004. 293 pp. $24.95; Spillman, Richard J. Classical and Contemporary Cryptology. Pearson Prentice Hall, Pearson Education, Inc., Upper Saddle River NJ 07458 USA. 2005. 285 pp. $54.00; Teuscher, Christof (Ed.) Alan Turing: Life and Legacy of a Great Thinker. Springer-Verlag, 175 Fifth Ave., New York NY 10010 USA. 2004. 542 pp. $69.95; Balliett, Blue and Brett Helquist, Illustrator. *Chasing Vermeer*. Scholastic Press, 557 Broadway, New York NY 10012 USA. 2004. 254 pp. $16.96; Caldwell, Ian and Dustin Thomason. *The Rule of Four*. The Dial Press/Random House, Inc., 1745 Broadway NY 10019 USA. 2004. 372 pp. $24.00/$34 Canada. *Cryptologia*, 29(1):88–93, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244737; http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244743; http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244747; http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244749; http://www.findarticles.com/p/articles/mi_qa3926/is_200501/ai_n13244806; http://www.informaworld.com/smpp/content~content=a748639586~db=all~order=page.

Kahn:2005:DSD

[1020] David Kahn. David Shulman dies — the bibliographer of cryptology. *Cryptologia*, 29(1):94–95, January 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639587~db=all~order=page.

Jacobsen:2005:PHR

[1021] Philip H. Jacobsen. Pearl Harbor: Radio officer Leslie Grogan of the SS Lurline and his misidentified signals. *Cryptologia*, 29(2):97–120, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639589~db=all~order=page.

Kahn:2005:PEC

[1022] David Kahn. The Polish Enigma Conference and some excursions. *Cryptologia*, 29(2):121–126, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639590~db=all~order=page.

Ingerman:2005:THC

[1023] Peter Zilahy Ingerman. Two Hebern cryptographic machines. *Cryptologia*, 29(2):127–147, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print),

1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639591~db=all~order=page.

Phan:2005:HEB

[1024] Raphael C.-W. Phan. How to explain block cipher cryptanalysis to your kids. *Cryptologia*, 29(2):148–158, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639592~db=all~order=page.

Bauer:2005:CYP

[1025] Craig Bauer and Suzanne E. Gladfelter. Cryptology in York, Pennsylvania. *Cryptologia*, 29(2):159–175, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639593~db=all~order=page.

Kruh:2005:RTCb

[1026] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 29(2):176–187, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639594~db=all~order=page.

Kruh:2005:UMC

[1027] Louis Kruh. Unknown military coding device: Can you identify it? *Cryptologia*, 29(2):190–191, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639595~db=all~order=page.

Anonymous:2005:LEa

[1028] Anonymous. Letter to the Editor. *Cryptologia*, 29(2):??, April 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sullivan:2005:BGA

[1029] Geoff Sullivan and Frode Weierud. Breaking German Army ciphers. *Cryptologia*, 29(3):193–232, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.hut-six.co.uk/bgac/; http://www.informaworld.com/smpp/content~content=a778118429~db=all~order=page.

Lawrence:2005:SRE

[1030] John Lawrence. A study of Rejewski's equations. *Cryptologia*, 29(3):233–247, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118430~db=all~order=page.

Bauer:2005:RAA

[1031] Craig Bauer and Elliott J. Gottloeb. Results of an automated attack on the running key cipher. *Cryptologia*, 29(3):248–254, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118431~db=all~order=page.

Pekelney:2005:EEE

[1032] Richard Pekelney. Excellent, exceptional, enormous crypto source. *Cryptologia*, 29(3):255–256, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL

http://www.informaworld.com/smpp/content~content=a778118649~db=all~order=page.

Cordery:2005:HRI

[1033] Robert Cordery and Leon Pintsov. History and role of information security in postage evidencing and payment. *Cryptologia*, 29(3):257–271, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118650~db=all~order=page.

Kruh:2005:EAC

[1034] Louis Kruh. Enigma articles from Cryptologia. *Cryptologia*, 29(3):272–273, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118651~db=all~order=page.

Kruh:2005:CUG

[1035] Louis Kruh. Crypto user's guide. *Cryptologia*, 29(3):273, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118652~db=all~order=page.

Kruh:2005:CTI

[1036] Louis Kruh. Confederate treasure issues. *Cryptologia*, 29(3):274, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118653~db=all~order=page.

Kruh:2005:DNY

[1037] Louis Kruh. Detective notebook for young adults. *Cryptologia*, 29(3):274–275, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118654~db=all~order=page.

Kruh:2005:CLM

[1038] Louis Kruh. College-level math crypto text. *Cryptologia*, 29(3):275, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118655~db=all~order=page.

Kruh:2005:CNP

[1039] Louis Kruh. Code names post 9/11. *Cryptologia*, 29(3):276, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118656~db=all~order=page.

Kruh:2005:CSM

[1040] Louis Kruh. Coral Sea, Midway, and Aleutians naval intelligence. *Cryptologia*, 29(3):276–277, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118657~db=all~order=page.

Kruh:2005:BVP

[1041] Louis Kruh. Broad view of power of mathematics. *Cryptologia*, 29(3):277–278, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a778118658~db=all~order=page.

Kruh:2005:FL

[1042] Louis Kruh. Friedman legacy. *Cryptologia*, 29(3):278, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118659~db=all~order=page.

Kruh:2005:PHR

[1043] Louis Kruh. Pearl Harbor revisited. *Cryptologia*, 29(3):278–279, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118660~db=all~order=page.

Kruh:2005:GE

[1044] Louis Kruh. Global eavesdropping. *Cryptologia*, 29(3):279–280, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118661~db=all~order=page.

Kruh:2005:CAH

[1045] Louis Kruh. Cryptology in American history. *Cryptologia*, 29(3): 280, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118662~db=all~order=page.

Kruh:2005:HDA

[1046] Louis Kruh. HMS Dunedin acts on Enigma material. *Cryptologia*, 29(3): 280–281, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118663~db=all~order=page.

Kruh:2005:NS

[1047] Louis Kruh. Novel secrets. *Cryptologia*, 29(3):281–282, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a778118664~db=all~order=page.

Kruh:2005:RTCc

[1048] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 29(3):??, July 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2005:CCF

[1049] John F. Dooley. Codes and ciphers in fiction: An overview. *Cryptologia*, 29(4):290–328, October 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639597~db=all~order=page.

Kahn:2005:HGT

[1050] David Kahn. How garbles tickled history. *Cryptologia*, 29(4):329–336, October 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639598~db=all~order=page.

Rocca:2005:CGE

[1051] Charles F. Rocca. Cryptology in general education. *Cryptologia*, 29(4):337–

342, October 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639600~db=all~order=page.

Lawrence:2005:FPW

[1052] John Lawrence. Factoring for the plugboard — was Rejewski's proposed solution for breaking the Enigma feasible? *Cryptologia*, 29(4):343–366, October 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639601~db=all~order=page.

Thilaka:2005:EHC

[1053] B. Thilaka and K. Rajalakshmi. An extension of Hill Cipher using generalised inverses and m th residue modulo n. *Cryptologia*, 29(4):367–376, October 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639602~db=all~order=page.

Kruh:2005:RTCd

[1054] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 29(4):377–380, October 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639603~db=all~order=page.

Anonymous:2005:LEb

[1055] Anonymous. Letter from the Editor. *Cryptologia*, 29(4):??, October 2005. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:2006:NBA

[1056] Ralph Erskine. The 1944 Naval BRUSA Agreement and its aftermath. *Cryptologia*, 30(1):1–22, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992010~db=all~order=page.

Faurholt:2006:AKD

[1057] Niels Faurholt. Alexis Køhl: a Danish inventor of cryptosystems. *Cryptologia*, 30(1):23–29, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992008~db=all~order=page.

Bury:2006:TPW

[1058] Jan Bury. TELMA — a Polish wireless communications security machine of World War II. *Cryptologia*, 30(1):31–38, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992011~db=all~order=page.

Buonafalce:2006:BRC

[1059] Augusto Buonafalce. Bellaso's reciprocal ciphers. *Cryptologia*, 30(1):39–51, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992006~db=all~order=page.

Blackman:2006:NGC

[1060] Deane R. Blackman. Note on Geheimschreiber cam wheels. *Cryptologia*,

30(1):53–54, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992007~db=all~order=page.

Stallings:2006:WSH

[1061] William Stallings. The Whirlpool secure hash function. *Cryptologia*, 30 (1):55–67, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992009~db=all~order=page.

Holden:2006:UHM

[1062] Joshua Holden, Richard Layton, Laurence Merkle, and Tina Hudson. Underwater hacker missile wars: a cryptography and engineering contest. *Cryptologia*, 30(1):69–77, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992012~db=all~order=page.

Kruh:2006:RTCc

[1063] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 30(1):79–81, January 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992005~db=all~order=page.

Brawley:2006:MJL

[1064] Joel V. Brawley. In memory of Jack Levine (1907–2005). *Cryptologia*, 30(2):83–97, April 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992343~db=all~order=page.

Freeman:2006:ZTR

[1065] Peter Freeman. The Zimmermann Telegram revisited: a reconciliation of the primary sources. *Cryptologia*, 30(2):98–150, April 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992342~db=all~order=page.

Biard:2006:BJN

[1066] Forrest R. Biard. Breaking of Japanese Naval codes: Pre-Pearl Harbor to Midway. *Cryptologia*, 30(2):151–158, April 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992344~db=all~order=page.

Talbert:2006:CSO

[1067] Robert Talbert. The cycle structure and order of the rail fence cipher. *Cryptologia*, 30(2):159–172, April 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992345~db=all~order=page.

Penumarthi:2006:AW

[1068] Kiranmayi Penumarthi and Subhash Kak. Augmented watermarking. *Cryptologia*, 30(2):173–180, April 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a741992341~db=all~order=page.

Kruh:2006:RTCa

[1069] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 30(2):181–192, April 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741992346~db=all~order=page.

Gallehawk:2006:TPS

[1070] John Gallehawk. Third person singular (Warsaw, 1939). *Cryptologia*, 30(3):193–198, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865337~db=all~order=page.

Gladwin:2006:DSS

[1071] Lee A. Gladwin. Did sigint seal the fates of 19,000 POWs? *Cryptologia*, 30(3):199–211, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865338~db=all~order=page.

Donovan:2006:IJC

[1072] Peter W. Donovan. The indicators of Japanese ciphers 2468, 7890, and JN-25A1. *Cryptologia*, 30(3):212–235, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865340~db=all~order=page.

Joyner:2006:ETI

[1073] David Joyner and David Kahn. Edited transcript of interview with Peter Hilton for "Secrets of War". *Cryptologia*, 30(3):236–250, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865341~db=all~order=page.

Schmeh:2006:EGE

[1074] Klaus Schmeh. The East German encryption machine T-310 and the algorithm it used. *Cryptologia*, 30(3):251–257, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865339~db=all~order=page.

Griffing:2006:SXP

[1075] Alexander Griffing. Solving XOR plaintext strings with the Viterbi algorithm. *Cryptologia*, 30(3):258–265, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865333~db=all~order=page.

Oliveira:2006:CCA

[1076] Claudia Oliveira, José António Xexéo, and Carlos André Carvalho. Clustering and categorization applied to cryptanalysis. *Cryptologia*, 30(3):266–280, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748865334~db=all~order=page.

Simons:2006:BCF

[1077] John L. Simons. Bridge cryptography fundamentals. *Cryptologia*, 30(3):281–286, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865336~db=all~order=page`.

Kruh:2006:RTCb

[1078] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 30(3):287–291, July 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748865335~db=all~order=page`.

Winkel:2006:LE

[1079] Brian J. Winkel. Letter from the editor. *Cryptologia*, 30(4):293, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a759130010~db=all~order=page`.

Erskine:2006:PRT

[1080] Ralph Erskine. The Poles reveal their secrets: Alastair Denniston's account of the July 1939 meeting at Pyry. *Cryptologia*, 30(4):294–305, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a759130005~db=all~order=page`.

Bauer:2006:CCD

[1081] Craig Bauer and John Ulrich. The cryptologic contributions of Dr. Donald Menzel. *Cryptologia*, 30(4):306–339, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a759130006~db=all~order=page`.

Boklan:2006:HBC

[1082] Kent D. Boklan. How I broke the Confederate code (137 years too late). *Cryptologia*, 30(4):340–345, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a759130004~db=all~order=page`.

Pommerening:2006:KTC

[1083] Klaus Pommerening. Kasiski's test: Couldn't the repetitions be by accident? *Cryptologia*, 30(4):346–352, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a759130003~db=all~order=page`.

Buonafalce:2006:JPD

[1084] Augusto Buonafalce, Niels Faurholt, and Bjarne Toft. Julius Petersen—Danish mathematician and cryptologist. *Cryptologia*, 30(4):353–360, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a759130007~db=all~order=page`.

Griffing:2006:SRK

[1085] Alexander Griffing. Solving the running key cipher with the Viterbi algorithm. *Cryptologia*, 30(4):361–367, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content~content=a759130002~db=all~order=page.

Mills:2006:RIC

[1086] Donald Mills. Review of "Introduction to Coding Theory" by Ron M. Roth. *Cryptologia*, 30(4):368–369, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a759130008~db=all~order=page. See [1705].

Kruh:2006:RTCd

[1087] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 30(4):370–374, October 2006. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a759130009~db=all~order=page.

Bauer:2007:LE

[1088] Craig Bauer. Letter from the editor. *Cryptologia*, 31(1):1, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432778.

vonzurGathen:2007:ZTO

[1089] Joachim von zur Gathen. Zimmermann Telegram: The original draft. *Cryptologia*, 31(1):2–37, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432771.

Hatch:2007:PEM

[1090] David A. Hatch. The punitive expedition military reform and communications intelligence. *Cryptologia*, 31 (1):38–45, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432775.

Fuensanta:2007:SCS

[1091] José Ramón Soler Fuensanta and Francisco Javier López-Brea Espiau. The strip cipher—the Spanish official method. *Cryptologia*, 31(1):46–56, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432773.

Jacobsen:2007:SAG

[1092] Philip H. Jacobsen. Station AL—Guadalcanal: a full service WWII cryptologic unit. *Cryptologia*, 31(1):57–75, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432770.

Bauer:2007:CME

[1093] Craig Bauer and Katherine Millward. Cracking matrix encryption row by row. *Cryptologia*, 31(1):76–83, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432772.

Burke:2007:ACS

[1094] Colin Burke. From the archives: Codebreaking (or not) in Shang-

hai. *Cryptologia*, 31(1):84–86, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432777.

Mills:2007:RCT

[1095] Donald Mills. Review of "Cryptography: Theory and Practice" by D. R. Stinson. *Cryptologia*, 31(1):87–88, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432776. See [1706].

Joyner:2007:RAC

[1096] David Joyner. Review of "Authentication Codes and Combinatorial Designs" by Dingyi Pei. *Cryptologia*, 31(1):89–91, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432774. See [1702].

Kruh:2007:RTCc

[1097] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 31(1):92–94, January 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a769432780.

Schinner:2007:VME

[1098] Andreas Schinner. The Voynich Manuscript: Evidence of the hoax hypothesis. *Cryptologia*, 31(2):95–107, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a773638459.

Lewand:2007:CCB

[1099] Robert Lewand. A cryptology course at Bletchley Park. *Cryptologia*, 31(2):108–111, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a773635820.

Machiavelo:2007:ACO

[1100] António Machiavelo and Rogério Reis. Automated ciphertext—only cryptanalysis of the Bifid cipher. *Cryptologia*, 31(2):112–124, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a773636204.

Parakh:2007:OTU

[1101] Abhishek Parakh. Oblivious transfer using elliptic curves. *Cryptologia*, 31(2):125–132, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a773638593.

Marnas:2007:AQA

[1102] Stelios I. Marnas, Lefteris Angelis, and George L. Bleris. An application of quasigroups in all-or-nothing transform. *Cryptologia*, 31(2):133–142, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a773634430.

Hoffman:2007:SIA

[1103] Nick Hoffman. A simplified IDEA algorithm. *Cryptologia*, 31(2):143–151, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773639295`.

Alvarez:2007:WFD

[1104] David Alvarez. Wilhelm Fenner and the development of the German Cipher Bureau, 1922–1939. *Cryptologia*, 31(2):152–163, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773637955`.

Paulis:2007:SA

[1105] Herbert Paulis. The Scheuble apparatus. *Cryptologia*, 31(2):164–178, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773637535`.

Bauer:2007:ARS

[1106] Craig Bauer and Joel Burkholder. From the archives: Reading Stimson's mail. *Cryptologia*, 31(2):179–184, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773639872`.

Christensen:2007:RMC

[1107] Chris Christensen. Review of "Mathematical Ciphers from Caesar to RSA" by Anne L. Young. *Cryptologia*, 31(2):185–187, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773638579`. See [1709].

Kahn:2007:OMA

[1108] David Kahn. The Old Master of Austrian cryptology. *Cryptologia*, 31(2):188–191, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773639319`.

Dooley:2007:RCFa

[1109] John F. Dooley. Reviews of cryptologic fiction. *Cryptologia*, 31(2):192–195, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773634531`.

Kruh:2007:RTCb

[1110] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 31(2):196–200, April 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a773634010`.

Stamp:2007:SCF

[1111] Mark Stamp and Wing On Chan. SIGABA: Cryptanalysis of the full keyspace. *Cryptologia*, 31(3):201–222, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779880103`.

Jacobsen:2007:RSP

[1112] Philip H. Jacobsen. Radio silence of the Pearl Harbor Strike Force confirmed again: The saga of Secret Message Serial (SMS) numbers. *Cryptologia*, 31(3):223–232, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779873253`.

Shepherd:2007:TEA

[1113] Simon J. Shepherd. The Tiny Encryption Algorithm. *Cryptologia*, 31(3): 233–245, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779872422`.

Gupta:2007:CEH

[1114] Indivar Gupta, Jasbir Singh, and Roopika Chaudhary. Cryptanalysis of an extension of the Hill Cipher. *Cryptologia*, 31(3):246–253, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779877634`.

David:2007:BOC

[1115] James David. Bourbon operations in China following World War II. *Cryptologia*, 31(3):254–262, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779875758`.

Rislakki:2007:SCG

[1116] Jukka Rislakki. Searching for cryptology's great wreck. *Cryptologia*, 31(3): 263–267, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779873135`.

Bury:2007:API

[1117] Jan Bury. From the archives: Polish interwar MFA's cipher compromised? *Cryptologia*, 31(3):268–277, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779875386`.

Kahn:2007:HCB

[1118] David Kahn. "Histoire cryptologique" — a book review. *Cryptologia*, 31(3): 278–280, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779875934`.

Christensen:2007:RDS

[1119] Chris Christensen. Review of "Decrypted Secrets: Methods and Maxims of Cryptology", Fourth Edition by F. L. Bauer. *Cryptologia*, 31(3):281–283, July 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a779878432`. See [1710].

Kruh:2007:RTCa

[1120] Louis Kruh. Reviews and things cryptologic. *Cryptologia*, 31(3):284–287, July 2007. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a779870303.

Sibert:2007:RWB

[1121] Olin Sibert. Robert W. Baldwin, 1957–2007. *Cryptologia*, 31(4):289–291, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876843.

Sibert:2007:ME

[1122] W. Olin Sibert and Robert W. Baldwin. The Multics encipher_Algorithm. *Cryptologia*, 31(4):292–304, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876569.

Gladwin:2007:BCR

[1123] Lee A. Gladwin. Bulldozer: a cribless Rapid Analytical Machine (RAM) solution to Enigma and its variations. *Cryptologia*, 31(4):305–315, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876731.

Holdener:2007:CSH

[1124] Judy A. Holdener and Eric J. Holdener. A cryptographic scavenger hunt. *Cryptologia*, 31(4):316–323, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876689.

Zhong:2007:AZF

[1125] Cheng Zhong. An attack on the Zhou–Fan–Li Authenticated Multiple-Key Agreement Protocol. *Cryptologia*, 31(4):324–325, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876831.

Kuhl:2007:RC

[1126] Alex Kuhl. Rejewski's catalog. *Cryptologia*, 31(4):326–331, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876516.

Olson:2007:RDA

[1127] Edwin Olson. Robust dictionary attack of short simple substitution ciphers. *Cryptologia*, 31(4):332–342, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876776.

Bury:2007:AUW

[1128] Jan Bury. From the archives: The U.S. and West German agent radio ciphers. *Cryptologia*, 31(4):343–357, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876754.

Hamer:2007:RTS

[1129] David Hamer. Review of "Thirty Secret Years: A. G. Denniston's Work in Signals Intelligence: 1914–1944" by Robin

Denniston. *Cryptologia*, 31(4):358–360, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876554. See [1711].

Buonafalce:2007:RCV

[1130] Augusto Buonafalce. Review of "The Curse of the Voynich. The Secret History of the World's Most Mysterious Manuscript" by Nicholas Pelling. *Cryptologia*, 31(4):361–362, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876510. See [1703].

Dooley:2007:RCFb

[1131] John F. Dooley. Reviews of cryptologic fiction. *Cryptologia*, 31(4):363–366, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876730.

Christensen:2007:JMM

[1132] Chris Christensen and Robert E. Lewand. 2008 Joint Mathematics Meetings contributed paper session: Cryptology for undergraduates. *Cryptologia*, 31(4):367, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876805.

Bauer:2007:NT

[1133] Craig Bauer. A note of thanks. *Cryptologia*, 31(4):368, October 2007. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a782876564.

Adler:2008:RED

[1134] Jeffrey D. Adler, Ryan W. Fuoss, Michael J. Levin, and Amanda R. Youell. Reading encrypted diplomatic correspondence: An undergraduate research project. *Cryptologia*, 32(1):1–12, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789465815.

Phan:2008:IRK

[1135] Raphael C.-W. Phan and Adi Shamir. Improved related-key attacks on DESX and DESX+. *Cryptologia*, 32(1):13–22, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466282.

Christensen:2008:TCC

[1136] Chris Christensen and Suzanne Gladfelter. Taking a cryptology class to Bletchley Park. *Cryptologia*, 32(1):23–32, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466622.

Chan:2008:KEE

[1137] Wayne S. Chan. Key enclosed: Examining the evidence for the missing key letter of the Beale Cipher. *Cryptologia*, 32(1):33–36, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586

(electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466178.

Parakh:2008:OTB

[1138] Abhishek Parakh. Oblivious transfer based on key exchange. *Cryptologia*, 32(1):37–44, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789467129.

Winkel:2008:LLM

[1139] Brian Winkel. Lessons learned from a mathematical cryptology course. *Cryptologia*, 32(1):45–55, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466057.

Kahn:2008:FPQ

[1140] David Kahn. The future of the past—questions in cryptologic history. *Cryptologia*, 32(1):56–61, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789467313.

Buonafalce:2008:CSC

[1141] Augusto Buonafalce. Cicco Simonetta's cipher-breaking rules. *Cryptologia*, 32 (1):62–70, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466556.

Cowan:2008:BSP

[1142] Michael J. Cowan. Breaking short Playfair ciphers with the simulated annealing algorithm. *Cryptologia*, 32 (1):71–83, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466907.

Bury:2008:AIB

[1143] Jan Bury. From the archives: Intercepting best friend? *Cryptologia*, 32(1):84–87, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466336.

Christensen:2008:RCW

[1144] Chris Christensen. Review of "The Collective Works of Captain George P. McGinnis" by George P. McGinnis. *Cryptologia*, 32(1):88–89, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466109.

Christensen:2008:RHT

[1145] Chris Christensen. Review of "How to Tell a Secret: Tips, Tricks & Techniques for Breaking Codes & Conveying Covert Information" by P. J. Huff and J. G. Lewin. *Cryptologia*, 32(1):90–91, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466389. See [1712].

Holden:2008:RCC

[1146] Joshua Holden. Review of "Complexity and Cryptography: An Introduction" by John Talbot and Dominic Welsh. *Cryptologia*, 32(1):92–

97, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789465840. See [1707].

Gallehawk:2008:RDI

[1147] John C. Gallehawk. Review of "Delusions of Intelligence" by R. A. Ratcliff. *Cryptologia*, 32(1):98–100, January 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a789466541. See [1704].

Grajek:2008:MMM

[1148] Marek Grajek. Monument in memoriam of Marian Rejewski, Jerzy Różycki and Henryk Zygalski unveiled in Poznań. *Cryptologia*, 32(2):101–103, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a793248099.

Batey:2008:DKR

[1149] Mavis Batey. Dilly Knox — a reminiscence of this pioneer Enigma cryptanalyst. *Cryptologia*, 32(2):104–130, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a793244738.

Yang:2008:SAA

[1150] Ching-Nung Yang and Tse-Shih Chen. Security analysis of authentication of images using recursive visual cryptography. *Cryptologia*, 32(2):131–136, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a793245470.

Srikwan:2008:UCT

[1151] Sukamol Srikwan and Markus Jakobsson. Using cartoons to teach Internet security. *Cryptologia*, 32(2):137–154, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a793246797.

Melka:2008:SOR

[1152] Tomi S. Melka. Structural observations regarding RongoRongo tablet 'Keiti'. *Cryptologia*, 32(2):155–179, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a793241365.

Hatch:2008:AFT

[1153] David A. Hatch. From the archives: Friedman takes the stand. *Cryptologia*, 32(2):180–183, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a793241354.

Kruh:2008:RFI

[1154] Louis Kruh. Review of "Figuring It Out At Bletchley Park 1939–1945" by John Gallehawk and Kerry Johnson. *Cryptologia*, 32(2):184–185, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content%7Econtent=a793242145. See [1713].

Christensen:2008:RVC

[1155] Chris Christensen. Review of "Voices of the Code Breakers: Personal Accounts of the Secret Heroes of World War II" by Michael Paterson. *Cryptologia*, 32(2):186–188, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a793248678`. See [1714].

Christensen:2008:RHA

[1156] Chris Christensen. Review of "A^3 and His Algebra" by Nancy E. Albert. *Cryptologia*, 32(2):189–196, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a793242250`. See [1699].

Anonymous:2008:CYB

[1157] Anonymous. Can you break the NKU monopoly? *Cryptologia*, 32(2): 197, ???? 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content%7Econtent=a793241249`.

Erskine:2008:CKE

[1158] Ralph Erskine. Captured *Kriegsmarine* Enigma documents at Bletchley Park. *Cryptologia*, 32(3):199–219, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Albrecht:2008:AAC

[1159] Martin Albrecht. Algebraic attacks on the Courtois toy cipher. *Cryptologia*, 32(3):220–276, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Burke:2008:ALB

[1160] Colin Burke. From the archives: The last Bombe run, 1955. *Cryptologia*, 32(3):277–278, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Massey:2008:RSA

[1161] James L. Massey. Review of series on Arabic origins of cryptology. *Cryptologia*, 32(3):280–283, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2008:RBH

[1162] Chris Christensen. Review of *The History of Information Security: A Comprehensive Handbook* edited by Karl de Leeuw and Jan Bergstra. *Cryptologia*, 32(3):284–294, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1795].

Dooley:2008:RCF

[1163] John F. Dooley. Reviews of cryptologic fiction. *Cryptologia*, 32(3):295–298, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Boklan:2008:HBE

[1164] Kent D. Boklan. How I broke an encrypted diary from the War of 1812. *Cryptologia*, 32(4):299–310, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Grey:2008:RGC

[1165] Christopher Grey and Andrew Sturdy. The 1942 reorganization of the Govern-

ment Code and Cypher School. *Cryptologia*, 32(4):311–333, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schrodel:2008:BSV

[1166] Tobias Schrödel. Breaking short Vigenère ciphers. *Cryptologia*, 32(4):334–347, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Jaworski:2008:RRZ

[1167] Jerzy Jaworski. Rejewski–Różycki–Zygalski lectures in computer science. *Cryptologia*, 32(4):348–350, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2008:AIC

[1168] Jan Bury. From the archives: Inside a Cold War crypto cell. Polish Cipher Bureau in the 1980s. *Cryptologia*, 32(4):351–367, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Diffie:2008:WDW

[1169] Whitfield Diffie. What did we do before biometric passports? A review of *Who Are You? Identification, Deception, and Surveillance in Early Modern Europe* by Valentin Groebner. *Cryptologia*, 32(4):368–369, 2008. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Esq:2009:BTR

[1170] Louis Kruh Esq. A belated tribute to Rosario Candela. *Cryptologia*, 33(1): 1–11, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Aumasson:2009:CHF

[1171] Jean-Philippe Aumasson. Cryptanalysis of a hash function based on norm form equations. *Cryptologia*, 33(1):12–15, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Beaver:2009:CCA

[1172] Cheryl Beaver. Cryptology in the classroom: Analyzing a zero-knowledge protocol. *Cryptologia*, 33(1):16–23, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Melka:2009:SCA

[1173] Tomi S. Melka. Some considerations about the *Kohau Rongorongo* script in the light of a statistical analysis of the 'Santiago Staff'. *Cryptologia*, 33(1):24–73, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2009:BUC

[1174] Jan Bury. Breaking unbreakable ciphers. the Asen Georgiyev spy case. *Cryptologia*, 33(1):74–88, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2009:RBCa

[1175] Chris Christensen. Review of *Modern Cryptanalysis: Techniques for Advanced Code Breaking* by Christopher Swenson. *Cryptologia*, 33(1):89–94, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1728].

Hamer:2009:RBG

[1176] David H. Hamer. Review of *Herivelismus and the German Military Enigma* by John Herivel. *Cryptologia*, 33(1):95–97, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1720].

David:2009:RBU

[1177] James David. Review of *The U.S. Intelligence Community* (Fifth Edition) by Jeffrey T. Richelson. *Cryptologia*, 33(1):99–101, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1671, 1672, 1680, 1685, 1726].

Phan:2009:RBE

[1178] Raphael C.-W. Phan. Review of *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition by Ross J. Anderson. *Cryptologia*, 33(1):102–103, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1716].

Kruh:2009:RBB

[1179] David Kruh. Review of *Spies of the Bible: Espionage in Israel from the Exodus to the Bar Kokhba Revolt* by Rose Mary Sheldon. *Cryptologia*, 33(1):104–105, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1715].

Dooley:2009:WWB

[1180] John F. Dooley and Yvonne I. Ramirez. Who wrote *The Blonde Countess*? A stylometric analysis of Herbert O. Yardley's fiction. *Cryptologia*, 33(2):108–117, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1659].

Fuensanta:2009:BCJ

[1181] José Ramón Soler Fuensanta. *Treaty of Cryptography* by Joaquín García Carmona? *Cryptologia*, 33(2):118–124, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rice:2009:ECC

[1182] Blake Rice and Bill Yankosky. Elliptic curve cryptography with the TI-83. *Cryptologia*, 33(2):125–141, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

McDevitt:2009:MC

[1183] Tim McDevitt and Tom Leap. Multimedia cryptology. *Cryptologia*, 33 (2):142–150, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

May:2009:UMW

[1184] Mike May, S. J. Using Maple worksheets to enable student explorations of cryptography. *Cryptologia*, 33(2):151–157, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Boliver:2009:CCO

[1185] David E. Boliver. Cryptology as college outreach to young teens. *Cryptologia*, 33(2):158–165, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Link:2009:RBK

[1186] David Link. Resurrecting *Bomba Kryptologiczna*: Archaeology of algorithmic artefacts, I. *Cryptologia*, 33(2):166–182, 2009. CODEN CRYPE6. ISSN

0161-1194 (print), 1558-1586 (electronic).

Liu:2009:AKJ

[1187] Jiqiang Liu and Sheng Zhong. Analysis of Kim-Jeon-Yoo password authentication schemes. *Cryptologia*, 33(2):183–187, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Angel:2009:CMD

[1188] José de Jesús Angel Angel and Guillermo Morales-Luna. Cryptographic methods during the Mexican Revolution. *Cryptologia*, 33(2):188–196, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Burke:2009:RBC

[1189] Colin Burke. Review of *American Cryptology during the Cold War, 1945–1989* by Thomas R. Johnson. *Cryptologia*, 33(2):197–200, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1679].

Christensen:2009:RBI

[1190] Chris Christensen. Review of *An Introduction to Mathematical Cryptography* by Hoffstein, Pipher, and Silverman. *Cryptologia*, 33(2):201–204, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1721].

Brandt:2009:RBI

[1191] Howard E. Brandt. Review of *Protecting Information: From Classical Error Correction to Quantum Cryptography* by Susan Loepp and William K. Wootters. *Cryptologia*, 33(2):205–207, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1701].

Joyner:2009:RBN

[1192] David Joyner. Review of *Algorithmic Number Theory: Lattices, Curves and Cryptography*, Edited by J. P. Buhler and P. Stevenhagen. *Cryptologia*, 33(2):208–211, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1796].

Dooley:2009:RCF

[1193] John F. Dooley. Reviews of cryptologic fiction. *Cryptologia*, 33(2):212–215, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gallery:2009:TCS

[1194] Eimear Gallery and Chris J. Mitchell. Trusted computing: Security and applications. *Cryptologia*, 33(3):217–245, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kim:2009:ADS

[1195] Jongsung Kim and Raphael C.-W. Phan. Advanced differential-style cryptanalysis of the NSA's Skipjack block cipher. *Cryptologia*, 33(3):246–270, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2009:RTP

[1196] Chris Christensen. Reviews of two *Post-Quantum Cryptography* books. *Cryptologia*, 33(3):271–273, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2009:RBB

[1197] David H. Hamer. Review of *From Bletchley with Love* by Mavis Batey. *Cryptologia*, 33(3):274–275, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1718].

Dooley:2009:AYM

[1198] John F. Dooley. Another Yardley mystery. *Cryptologia*, 33(3):276–282, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Chaum:2009:AVV

[1199] David Chaum, Ben Hosp, Stefan Popoveniuc, and Poorvi L. Vora. Accessible voter-verifiability. *Cryptologia*, 33(3):283–291, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Budiansky:2009:RBI

[1200] Stephen Budiansky. Review of *Decoding the IRA* by Tom Mahon and James J. Gillogly. *Cryptologia*, 33(3):292–294, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1723].

Schwartz:2009:CAC

[1201] Kathryn A. Schwartz. Charting Arabic cryptology's evolution. *Cryptologia*, 33(4):297–304, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Simmons:2009:ACS

[1202] Sean Simmons. Algebraic cryptanalysis of simplified AES. *Cryptologia*, 33(4):305–314, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gu:2009:SDB

[1203] Haihua Gu and Dawu Gu. Speeding up the double-base recoding algorithm of scalar multiplication. *Cryptologia*, 33(4):315–320, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ravi:2009:ALS

[1204] Sujith Ravi and Kevin Knight. Attacking letter substitution ciphers with integer programming. *Cryptologia*, 33 (4):321–334, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Yum:2009:CHC

[1205] Dae Hyun Yum and Pil Joong Lee. Cracking Hill ciphers with goodness-of-fit statistics. *Cryptologia*, 33(4):335–342, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schmeh:2009:ECW

[1206] Klaus Schmeh. Enigma's contemporary witness: Gisbert Hasenjaeger. *Cryptologia*, 33(4):343–346, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2009:ACM

[1207] Jan Bury. From the archives: CX–52 messages read by Red Poles? *Cryptologia*, 33(4):347–352, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wolfe:2009:RBH

[1208] Henry B. Wolfe. Review of *Eavesdropping on Hell: Historical Guide to Western Communications Intelligence and Holocaust, 1939–1945* by Robert J. Hanyok. *Cryptologia*, 33(4):353–355, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1700].

Christensen:2009:RBS

[1209] Chris Christensen. Review of *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* by James Bamford. *Cryptologia*, 33(4):356–358, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1717].

Christensen:2009:RBCb

[1210] Chris Christensen. Review of *Random Curves* by Neal Koblitz. *Cryptologia*, 33(4):359–365, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1722].

Christensen:2009:RBV

[1211] Chris Christensen. Review of *Ultra Versus U-Boats: Enigma Decrypts in The National Archives* by Roy Conyers Nesbit. *Cryptologia*, 33(4):366–369, 2009. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1725].

Anonymous:2010:TDK

[1212] Anonymous. A tribute to David Kahn. *Cryptologia*, 34(1):1–11, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:2010:HDW

[1213] David Kahn. How I discovered World War II's greatest spy. *Cryptologia*, 34 (1):12–21, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Strasser:2010:NCF

[1214] Gerhard F. Strasser. Ninth-Century figural poetry and medieval Easter tables—possible inspirations for the square tables of Trithemius and Vigenère? *Cryptologia*, 34(1):22–26, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2010:ATF

[1215] Chris Christensen. Alan Turing's first cryptology textbook and Sinkov's revision of it. *Cryptologia*, 34(1):27–43, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Faurholt:2010:SGC

[1216] Niels Faurholt. E. S. Schieber German code device from WWII. *Cryptologia*, 34(1):44–51, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Holbl:2010:AIE

[1217] Marko Hölbl, Tatjana Welzer, and Boštjan Brumen. Attacks and improvement of an efficient remote mutual authentication and key agreement scheme. *Cryptologia*, 34(1):52–59, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2010:OLU

[1218] Jan Bury. Operation Lotos: An unsuccessful attempt on U.S. Government

communications. *Cryptologia*, 34(1): 60–87, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2010:RBP

[1219] Chris Christensen. Review of *Bletchley Park: An Inmate's Story* by James Thirsk. *Cryptologia*, 34(1):88–89, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1729].

Booker:2010:RBW

[1220] Clyde G. Booker. Review of *West Wind Clear: Cryptology and the Winds Message Controversy – A Documentary History*. *Cryptologia*, 34(1):90–95, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1719].

Dooley:2010:RCFa

[1221] John F. Dooley. Reviews of cryptologic fiction. *Cryptologia*, 34(1):96–100, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Winkel:2010:DCS

[1222] Brian Winkel. David, calm down! on second and more reflective thought, don't! *Cryptologia*, 34(2):101–103, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Patarin:2010:SLY

[1223] Jacques Patarin and Valérie Nachef. "I shall love you until death" (Marie-Antoinette to Axel von Fersen). *Cryptologia*, 34(2):104–114, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lang:2010:WDW

[1224] Benedek Láng. Why don't we decipher an outdated cipher system? the codex of Rohonc. *Cryptologia*, 34(2):115–144, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Koblitz:2010:SCO

[1225] Neal Koblitz. Secret codes and online security: a seminar for entering students. *Cryptologia*, 34(2):145–154, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kurt:2010:DUC

[1226] Yesem Kurt. Deciphering an undergraduate cryptology course. *Cryptologia*, 34(2):155–162, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Stallings:2010:NBCa

[1227] William Stallings. NIST block cipher modes of operation for confidentiality. *Cryptologia*, 34(2):163–175, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2010:RCH

[1228] Chris Christensen. Review of the 2009 Cryptologic History Symposium: *Global Perspectives on Cryptologic History*. *Cryptologia*, 34(2):176–179, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2010:RCFb

[1229] John F. Dooley. Reviews of cryptologic fiction. *Cryptologia*, 34(2):180–185, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Booker:2010:RBA

[1230] Clyde G. Booker. Review of *The Attack on the Liberty: The Untold Story of Israel's Deadly 1967 Assault on a U.S. Spy Ship* by James Scott. *Cryptologia*, 34(2):186–189, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1737]. See also [1666, 1693].

Burke:2010:RBS

[1231] Colin Burke. Review of *The Secret Sentry: The Untold Story of the National Security Agency* by Matthew M. Aid. *Cryptologia*, 34(2):190–193, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1730].

Levine:2010:RBR

[1232] Emil H. Levine. Review of *Deciphering the Rising Sun: Navy and Marine Corps Codebreakers, Translators, and Interpreters in the Pacific War* by Roger Dingman. *Cryptologia*, 34(2):194–196, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1733].

Kahn:2010:LKC

[1233] David Kahn. Louis Kruh, cryptologist, editor, activist. *Cryptologia*, 34(3):197–199, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Assarpour:2010:HWB

[1234] Ali Assarpour and Kent D. Boklan. How we broke the Union Code (148 years too late). *Cryptologia*, 34(3):200–210, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Konikoff:2010:ASA

[1235] Jacob Konikoff and Seth Toplosky. Analysis of simplified DES algorithms. *Cryptologia*, 34(3):211–224, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Stallings:2010:NBCb

[1236] William Stallings. NIST block cipher modes of operation for authentication and combined confidentiality and authentication. *Cryptologia*, 34(3):225–235, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Popoveniuc:2010:SEV

[1237] Stefan Popoveniuc and Poorvi L. Vora. Secure electronic voting — a framework. *Cryptologia*, 34(3):236–257, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Parakh:2010:IVP

[1238] Abhishek Parakh and Subhash Kak. Internet voting protocol based on improved implicit security. *Cryptologia*, 34(3):258–268, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2010:RBC

[1239] Chris Christensen. Review of *Elementary Cryptanalysis: A Mathematical Approach*, Second Edition, by Abraham Sinkov, revised and updated by Todd Feil. *Cryptologia*, 34(3):269–272, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1660, 1738].

Christensen:2010:RBR

[1240] Chris Christensen. Review of *The Real Enigma Heroes* by Phil Shanahan. *Cryptologia*, 34(3):273–277, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1727].

Christensen:2010:RTG

[1241] Chris Christensen. Review of two "gift books" about cryptology. *Cryptologia*, 34(3):278–279, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Jain:2010:NEP

[1242] Ashwin Jain and C. Hari. A new efficient protocol for k-out-of-n oblivious transfer. *Cryptologia*, 34(4):282–290, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schmeh:2010:AKH

[1243] Klaus Schmeh. Alexander von Kryha and his encryption machines. *Cryptologia*, 34(4):291–300, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Fuensanta:2010:SEH

[1244] José Ramón Soler Fuensanta, Francisco Javier López-Brea Espiau, and Frode Weierud. Spanish Enigma: a history of the Enigma in Spain. *Cryptologia*, 34(4):301–328, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rijmenants:2010:EMP

[1245] Dirk Rijmenants. Enigma message procedures used by the Heer, Luftwaffe and Kriegsmarine. *Cryptologia*, 34(4):329–339, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:2010:URL

[1246] Ralph Erskine. Ultra reveals a late *B-Dienst* success in the Atlantic. *Cryptologia*, 34(4):340–358, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Burke:2010:ALC

[1247] Colin Burke. From the archives: a lady codebreaker speaks: Joan Murray, the Bombes and the perils of writing crypto-history from participants' accounts. *Cryptologia*, 34(4):359–370, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Strasser:2010:RBB

[1248] Gerhard F. Strasser. Review of *Versteckte Botschaften. Die faszinierende Geschichte der Steganografie* (Hidden Messages. The Fascinating Story of Steganography). *Cryptologia*, 34(4): 371–380, 2010. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2011:WHY

[1249] John F. Dooley. Was Herbert O. Yardley a traitor? *Cryptologia*, 35(1):1–15, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ertel:2011:ERB

[1250] Wolfgang Ertel, Lucia Jans, Walter Herzhauser, and Joachim Fessler. An Enigma replica and its blueprints. *Cryptologia*, 35(1):16–21, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Reeds:2011:AD

[1251] Jim Reeds. American Dragon. *Cryptologia*, 35(1):22–41, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lewand:2011:SKD

[1252] Robert Edward Lewand. Secret keeping 101—Dr. Janice Martin Benario and the Women's College connection to ULTRA. *Cryptologia*, 35(1):42–46, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Azizi:2011:IAC

[1253] Abdelmalek Azizi and Mostafa Azizi. Instances of Arabic cryptography in Morocco. *Cryptologia*, 35(1):47–57, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Das:2011:KEF

[1254] Manik Lal Das. A key escrow-free identity-based signature scheme without using secure channel. *Cryptologia*, 35(1):58–72, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:WDW

[1255] Chris Christensen and David Agard. William Dean Wray (1910–1962): the evolution of a cryptanalyst. *Cryptologia*, 35(1):73–96, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:RBN

[1256] Chris Christensen. Review of *Cryptography and Network Security: Principles and Practice*, fifth edition. *Cryptologia*, 35(1):97–99, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:RBCa

[1257] Chris Christensen. Review of *Algebraic Cryptanalysis*. *Cryptologia*, 35(1):100–105, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:RBCb

[1258] Chris Christensen. Review of *Understanding Cryptography*. *Cryptologia*, 35(1):106–107, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:2011:LE

[1259] David Kahn. Letter to the editor. *Cryptologia*, 35(2):109, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2011:DKC

[1260] David H. Hamer. The David Kahn Collection at NSA's National Cryptologic Museum. *Cryptologia*, 35(2):110–113, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Marks:2011:OUC

[1261] Philip Marks. Operational use and cryptanalysis of the Kryha cipher machine. *Cryptologia*, 35(2):114–155, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Patterson:2011:CB

[1262] Wayne Patterson. The cryptology of baseball. *Cryptologia*, 35(2):156–163, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Smoot:2011:ACB

[1263] Betsy Rohaly Smoot. An accidental cryptologist: The brief career of Genevieve Young Hitt. *Cryptologia*, 35(2):164–175, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2011:ABO

[1264] Jan Bury. From the archives: Breaking OTP ciphers. *Cryptologia*, 35(2):176–188, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:RBS

[1265] Chris Christensen. Review of *The Secret Life of Bletchley Park: The World War II Codebreaking Centre and the Men and Women Who Were There*. *Cryptologia*, 35(2):189–191, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:RBPa

[1266] Chris Christensen. Review of Bletchley Park Trust Reports by Frank Carter. *Cryptologia*, 35(2):192–195, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2011:RBM

[1267] David H. Hamer. Review of *Dilly—The Man Who Broke Enigmas* by Mavis Batey. *Cryptologia*, 35(2):196–197, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Budiansky:2011:LE

[1268] Stephen Budiansky. Letter to the Editor. *Cryptologia*, 35(3):199–202, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bellovin:2011:FMI

[1269] Steven M. Bellovin. Frank Miller: Inventor of the one-time pad. *Cryptologia*, 35(3):203–222, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Preparata:2011:STU

[1270] Franco P. Preparata. Steps toward unraveling a Vatican cipher of the 1930s. *Cryptologia*, 35(3):223–234, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hajny:2011:AAS

[1271] Jan Hajny and Vaclav Zeman. Anonymous authentication with spread revelation. *Cryptologia*, 35(3):235–246, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kapera:2011:SRS

[1272] Zdzis aw J. Kapera. Summary report of the state of the Soviet Military Sigint in November 1942 noticing "ENIGMA". *Cryptologia*, 35(3):247–256, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Child:2011:CAC

[1273] Paul W. Child. Cipher against ciphers: Jonathan Swift's Latino–Anglicus satire of medicine. *Cryptologia*, 35(3):257–266, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:UNC

[1274] Chris Christensen. US Navy cryptologic mathematicians during World War II. *Cryptologia*, 35(3):267–276, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Carter:2011:KBJ

[1275] Frank Carter. Keith Batey and John Herivel: Two distinguished Bletchley Park cryptographers. *Cryptologia*, 35(3):277–281, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2011:RBR

[1276] Chris Christensen. Review of *Inside Room 40: The Codebreakers of World War I* by Paul Grannon. *Cryptologia*, 35(3):282–288, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1741].

Glees:2011:RBU

[1277] Anthony Glees. Review of *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* by Richard J. Aldrich. *Cryptologia*, 35(3):289–292, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1739].

Christensen:2011:RBB

[1278] Chris Christensen. Review of *The Bletchley Park Codebreakers* by Ralph Erskine and Michael Smith. *Cryptologia*, 35(3):293–296, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1746].

Bury:2011:OSU

[1279] Jan Bury. Operation *Stonka*. an ultimate deception spy game. *Cryptologia*, 35(4):297–327, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rubin:2011:JFB

[1280] Moshe Rubin. John F. Byrne's Chaocipher revealed: An historical and technical appraisal. *Cryptologia*, 35(4):328–379, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2011:EBE

[1281] Anonymous. Editorial Board EOV. *Cryptologia*, 35(4):ebi, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bauer:2012:SCG

[1282] Craig Bauer. Space crunchers and GOST busters! *Cryptologia*, 36(1):1, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Courtois:2012:SEG

[1283] Nicolas T. Courtois. Security evaluation of GOST 28147-89 in view of international standardisation. *Cryptologia*, 36(1):2–13, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schmeh:2012:PCC

[1284] Klaus Schmeh. The pathology of cryptology — a current survey. *Cryptologia*, 36(1):14–45, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Brier:2012:HSS

[1285] Eric Brier, Wenjie Fang, and David Naccache. How to scatter a secret? *Cryptologia*, 36(1):46–54, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Donovan:2012:FJS

[1286] Peter Donovan. The flaw in the JN-25 series of ciphers, II. *Cryptologia*, 36(1):55–61, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Shim:2012:SFT

[1287] Kyung-Ah Shim. Security flaws in three password-based remote user authentication schemes with smart cards. *Cryptologia*, 36(1):62–69, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ball:2012:XAD

[1288] Matthew V. Ball, Cyril Guyot, James P. Hughes, Luther Martin, and Landon Curt Noll. The XTS–AES disk encryption algorithm and the security of ciphertext stealing. *Cryptologia*, 36(1):70–79, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2012:RBM

[1289] John F. Dooley. Review of *The Mystic Cipher* by Dennis L. Mangrum. *Cryptologia*, 36(1):80–83, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1724].

Bauer:2012:YTT

[1290] Craig Bauer. 100 years times two: Alan Turing and the Voynich Manuscript. *Cryptologia*, 36(2):85–87, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2012:LHE

[1291] Chris Christensen, David Joyner, and Jenna Torres. Lester Hill's error-detecting codes. *Cryptologia*, 36(2):88–103, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Minier:2012:IDR

[1292] Marine Minier, Raphael C.-W. Phan, and Benjamin Pousse. On integral distinguishers of Rijndael family of ciphers. *Cryptologia*, 36(2):104–118, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2012:PKL

[1293] Jan Bury. Project Kalina: The lotos operation conundrum. *Cryptologia*, 36(2):119–128, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sherman:2012:LAT

[1294] Alan T. Sherman, Dhananjay Phatak, Vivek G. Relan, and Bhushan Sonawane. Location authentication, tracking, and emergency signaling through power line communication: Designs and protocols for new out-of-band strategies. *Cryptologia*, 36(2):129–148, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Beaver:2012:KPN

[1295] Cheryl Beaver and Stuart Boersma. KRYPTOS: a Pacific Northwest cryptanalysis contest for undergraduates.

Cryptologia, 36(2):149–156, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2012:RCH

[1296] Chris Christensen. Review of the 2011 Cryptologic History Symposium *Cryptology in War and Peace: Crisis Points in History*. *Cryptologia*, 36(2):157–160, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2012:RBR

[1297] John F. Dooley. Review of *Joe Rochefort's War* by Elliot Carlson. *Cryptologia*, 36(2):161–163, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1745].

Hamer:2012:RBS

[1298] David H. Hamer. Review of *The Secrets of Station X — How the Bletchley Park Codebreakers Helped Win the War* by Michael Smith. *Cryptologia*, 36(2):164–166, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1752].

Christensen:2012:RBD

[1299] Chris Christensen. Review of *Secret Days: Code-Breaking in Bletchley Park* by Asa Briggs. *Cryptologia*, 36(2):167–172, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1744].

Christensen:2012:RBW

[1300] Chris Christensen. Review of *Neil Webster's Cribs for Victory* edited by Joss Pearson. *Cryptologia*, 36(2):173–175, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1750].

Christensen:2012:RBS

[1301] Chris Christensen. Review of *In the Shadow of Pont du Gard: The Polish Enigma in Vichy France (June 1940 to November 1942)* by Zdzislaw J. Kapera. *Cryptologia*, 36(2):176–178, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1747].

Christensen:2012:RBE

[1302] Chris Christensen. Review of *Inside Enigma: The Secrets of the Enigma Machine and Other Historic Cipher Machines* by Tom Perera. *Cryptologia*, 36(2):179–180, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1743].

Christensen:2012:RBI

[1303] Chris Christensen. Review of *The Information: A History, A Theory, A Flood* by James Gleick. *Cryptologia*, 36(2):181–182, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1757].

Agard:2012:RBT

[1304] David Agard and Chris Christensen. Review of *The Theory That Would Not Die* by Sharon McGrayne. *Cryptologia*, 36(2):183–190, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1748].

Zabell:2012:CAM

[1305] Sandy Zabell. Commentary on Alan M. Turing: The applications of probability to cryptography. *Cryptologia*, 36(3):191–214, 2012. CODEN

CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2012:APG

[1306] Jan Bury. Assembling the puzzle game: The Jacek Jurzak spy case. *Cryptologia*, 36(3):215–229, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Strasser:2012:LCF

[1307] Gerhard F. Strasser. Late 18th-century French encrypted diplomatic "Letters of Recommendation" — or, how to unwittingly carry your own warrant. *Cryptologia*, 36(3):230–239, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bard:2012:SRP

[1308] Gregory V. Bard, Shaun V. Ault, and Nicolas T. Courtois. Statistics of random permutations and the cryptanalysis of periodic block ciphers. *Cryptologia*, 36(3):240–262, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Fuensanta:2012:CSD

[1309] J. Ramón Soler Fuensanta, Francisco Javier López-Brea Espiau, and Diego Navarro Bonilla. A cryptanalysis service during the Spanish Civil War. *Cryptologia*, 36(3):263–289, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2012:FCI

[1310] David H. Hamer. First Charlotte International Cryptologic Symposium and Exhibit. *Cryptologia*, 36(3):290–294, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Turing:2012:RSS

[1311] Alan M. Turing and D. Bayley. Report on speech secrecy system DELILAH, a technical description compiled by A. M. Turing and Lieutenant D. Bayley REME, 1945–1946. *Cryptologia*, 36(4):295–340, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2012:PCW

[1312] Jan Bury. Polish cold war codebreaking of 1959–1989: a preliminary assessment. *Cryptologia*, 36(4):341–379, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2012:EBE

[1313] Anonymous. Editorial Board EOV. *Cryptologia*, 36(4):ebi, 2012. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Courtois:2013:LCK

[1314] Nicolas T. Courtois. Low-complexity key recovery attacks on GOST block cipher. *Cryptologia*, 37(1):1–10, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kelly:2013:RPP

[1315] Saul Kelly. Room 47: The Persian prelude to the Zimmermann telegram. *Cryptologia*, 37(1):11–50, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Campos:2013:GAM

[1316] Fco. Alberto Campos, Alberto Gascón, Jesús María Latorre, and J. Ramón Soler. Genetic algorithms and mathematical programming to crack the

Spanish strip cipher. *Cryptologia*, 37 (1):51–68, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dang:2013:CFI

[1317] Quynh Dang. Changes in Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard. *Cryptologia*, 37(1):69–73, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Holden:2013:DSV

[1318] Joshua Holden. Demitasse: a 'small' version of the Tiny Encryption Algorithm and its use in a classroom setting. *Cryptologia*, 37(1):74–83, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2013:TPU

[1319] John F. Dooley. 1929–1931: a transition period in U.S. cryptologic history. *Cryptologia*, 37(1):84–98, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:RSP

[1320] Chris Christensen. Review of *Secret Postings: Bletchley Park to the Pentagon* by Charlotte Webb. Book Tower Publishing, Redditch, Worcestershire, UK, 2011. 72 pages, Paperback, £6.99. ISBN 978-0-9557164-1-6. *Cryptologia*, 37(1):99–101, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:RIC

[1321] Chris Christensen. Review of *Introduction to Cryptography with Mathematical Foundations and Computer Implementation* by Alexander Stanoyevitch. Chapman and Hall/CRC, Boca Raton, FL, 2010. 699 pages, Hardcover, $89.95. ISBN 1-4398-1763-4. *Cryptologia*, 37(1):102–104, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:ACH

[1322] Chris Christensen. Announcement of the 2013 Cryptologic History Symposium "Technological Change and Cryptology: Meeting the Historical Challenges" 17-18 October 2013. *Cryptologia*, 37(2):105–106, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Holden:2013:GHF

[1323] Joshua Holden. A good hash function is hard to find, and vice versa. *Cryptologia*, 37(2):107–119, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Campbell:2013:LCS

[1324] Samantha Campbell, Max Grinchenko, and William Smith. Linear cryptanalysis of simplified AES under change of S-box. *Cryptologia*, 37(2):120–138, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rezabek:2013:TSO

[1325] Randy Rezabek. TICOM and the search for OKW / *Chi*. *Cryptologia*, 37(2):139–153, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kumar:2013:RIH

[1326] Sachin Kumar and R. K. Sharma. Recursive information hiding of se-

crets by random grids. *Cryptologia*, 37(2):154–161, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

deLeeuw:2013:RFL

[1327] Karl de Leeuw. Review of *Forschungsstelle Langeveld: Duits Afluisterstation in bezet Nederland* by Hans Knap. *Cryptologia*, 37(2):162–166, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:RMM

[1328] Chris Christensen. Review of *Memories of My Work at the Cipher Bureau of the General Staff Second Department 1930–1945* by Marian Rejewski. *Cryptologia*, 37(2):167–174, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Joyner:2013:RAS

[1329] David Joyner. Review of *Algebraic Shift Register Sequences* by Mark Goresky and Andrew Klapper. *Cryptologia*, 37 (2):175–183, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:RDO

[1330] Chris Christensen. Review of *Decoding Organization: Bletchley Park, Codebreaking and Organization Studies* by Christopher Grey. *Cryptologia*, 37(2):184–188, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Joyner:2013:RCB

[1331] David Joyner. Review of *Cryptographic Boolean Functions and Applications* by Thomas Cusick and Pantelimon Stanica. *Cryptologia*, 37(2):189–192, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schmeh:2013:MVM

[1332] Klaus Schmeh. A milestone in Voynich manuscript research: Voynich 100 Conference in Monte Porzio Catone, Italy. *Cryptologia*, 37(3):193–203, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anderson:2013:BBK

[1333] Jeanne Anderson. Breaking the BTK Killer's cipher. *Cryptologia*, 37(3):204–209, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Flynn:2013:JBC

[1334] William G. Flynn and Sharon Maneki. The Jack Butcher Case: A story of courage, commitment, and concern. *Cryptologia*, 37(3):210–214, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Mateer:2013:CBC

[1335] Todd D. Mateer. Cryptanalysis of Beale Cipher Number Two. *Cryptologia*, 37(3):215–232, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Fuensanta:2013:RST

[1336] José Ramón Soler Fuensanta, Francisco Javier López-Brea Espiau, and Diego Navarro Bonilla. Revealing secrets in two wars: The Spanish codebreakers at PC Bruno and PC Cadix. *Cryptologia*, 37(3):233–249,

2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dhavare:2013:ECH

[1337] Amrapali Dhavare, Richard M. Low, and Mark Stamp. Efficient cryptanalysis of homophonic substitution ciphers. *Cryptologia*, 37(3):250–281, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:RBT

[1338] Chris Christensen. Review of *Code Talker* by C. Nez (with J. S. Avila). *Cryptologia*, 37(3):282–284, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:RTS

[1339] Chris Christensen. Review of two software-based textbooks. *Cryptologia*, 37(3):285–288, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Alexander:2013:WCC

[1340] John Alexander, Kevin Coleman, David White, Nick Miers, and John Gallehawk. Whittingham–Collingwood cipher machine. *Cryptologia*, 37(4): 289–304, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Glass:2013:FYS

[1341] Darren Glass. A first-year seminar on cryptography. *Cryptologia*, 37(4):305–310, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Stallings:2013:DSA

[1342] William Stallings. Digital signature algorithms. *Cryptologia*, 37(4):311–327, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Azizi:2013:IAC

[1343] Abdelmalek Azizi and Mostafa Azizi. Instances of Arabic cryptography in Morocco II. *Cryptologia*, 37(4):328–337, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Fronczak:2013:ATC

[1344] Maria Fronczak. Atbah-type ciphers in the Christian Orient and numerical rules in the construction of Christian substitution ciphers. *Cryptologia*, 37(4):338–344, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sun:2013:PKA

[1345] Da-Zhi Sun and Zhen-Fu Cao. On the privacy of Khan et al.'s dynamic ID-based remote authentication scheme with user anonymity. *Cryptologia*, 37(4):345–355, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2013:RBA

[1346] Chris Christensen. Review of biographies of Alan Turing. *Cryptologia*, 37(4):356–367, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2013:RBC

[1347] David H. Hamer. Review of *Hitler's Codebreakers — German Signals Intel-*

ligence in World War 2 by John Jackson. *Cryptologia*, 37(4):368–370, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2013:EBE

[1348] Anonymous. Editorial Board EOV. *Cryptologia*, 37(4):ebi, 2013. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Calof:2014:CEH

[1349] Jeff Calof, Jeff Hill, and Moshe Rubin. Chaocipher exhibit 5: History, analysis, and solution of *Cryptologia*'s 1990 challenge. *Cryptologia*, 38(1):1–25, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bertoni:2014:MKE

[1350] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The making of KECCAK. *Cryptologia*, 38 (1):26–60, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rezabek:2014:RFC

[1351] Randy Rezabek. The Russian fish with caviar. *Cryptologia*, 38(1):61–76, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2014:JMM

[1352] John F. Dooley and Elizabeth Anne King. John Matthews Manly: The *Collier*'s articles. *Cryptologia*, 38(1):77–88, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2014:RID

[1353] John F. Dooley. Review of *Inferno* by Dan Brown. *Cryptologia*, 38(1):89–92, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2014:RMP

[1354] John F. Dooley. Review of *Mr. Penumbra's 24-Hour Bookstore* by Robin Sloan. *Cryptologia*, 38(1):93–95, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Strasser:2014:RMM

[1355] Gerhard F. Strasser. Review of *Mechanisches Memorieren und Chiffrieren um 1430: Johannes Fontanas Tractatus de instrumentis artis memorie* by Horst Kranz and Walter Oberschelp. *Cryptologia*, 38(1):96–101, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rescher:2014:LMD

[1356] Nicholas Rescher. Leibniz's *Machina Deciphratoria*: A Seventeenth-Century proto-Enigma. *Cryptologia*, 38(2):103–115, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Chang:2014:CT

[1357] Kelly Chang, Richard M. Low, and Mark Stamp. Cryptanalysis of Typex. *Cryptologia*, 38(2):116–132, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schwartz:2014:TTC

[1358] Kathryn A. Schwartz. From text to technological context: Medieval Arabic cryptology's relation to paper, numbers, and the post. *Cryptologia*, 38(2):133–146, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2014:PMC

[1359] Jan Bury. Pinpointing the mark: On the Cold War SIGINT capability. *Cryptologia*, 38(2):147–151, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2014:NCR

[1360] Chris Christensen. The National Cash Register Company additive recovery machine. *Cryptologia*, 38(2):152–177, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Jung:2014:TDD

[1361] Ki-Hyun Jung and Kee-Young Yoo. Three-directional data hiding method for digital images. *Cryptologia*, 38 (2):178–191, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2014:RSH

[1362] Chris Christensen. Review of *Secret History: The Story of Cryptology* by Craig P. Bauer. *Cryptologia*, 38(2):192–193, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Smoot:2014:RWW

[1363] Betsy Rohaly Smoot. Review of *World War I and the Origins of U.S. Military Intelligence* by James L. Gilbert. *Cryptologia*, 38(2):194–196, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lasry:2014:SDT

[1364] George Lasry, Nils Kopal, and Arno Wacker. Solving the double transposition challenge with a divide-and-conquer approach. *Cryptologia*, 38(3): 197–214, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kak:2014:CAP

[1365] Subhash Kak and Monisha Prabhu. Cryptographic applications of primitive Pythagorean triples. *Cryptologia*, 38(3):215–222, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Koss:2014:WIL

[1366] Lorelei Koss. Writing and information literacy in a cryptology first-year seminar. *Cryptologia*, 38(3):223–231, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rocca:2014:MHC

[1367] Charles F. Rocca Jr. Mathematics in the history of cryptography. *Cryptologia*, 38(3):232–243, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kahn:2014:NIS

[1368] David Kahn. The Naval intercept station at Bainbridge Island, Washington. *Cryptologia*, 38(3):244–247, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

List:2014:RC

[1369] David List and John Gallehawk. Revelation for Cilli's. *Cryptologia*, 38(3): 248–265, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Grey:2014:ACB

[1370] Christopher Grey. From the archives: Colonel Butler's satire of Bletchley Park. *Cryptologia*, 38(3):266–275, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2014:RCH

[1371] Chris Christensen. Review of the 2013 Cryptologic History Symposium, *Technological Change and Cryptology: Meeting the Historical Challenge*. *Cryptologia*, 38(3):276–281, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2014:BRB

[1372] David H. Hamer. Book review: *Dönitz, U-Boats, Convoys* by Jak P. Mallmann Showell. *Cryptologia*, 38(3):282–284, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2014:BRBa

[1373] Chris Christensen. Book review: *A Brief History of Cryptology and Cryptographic Algorithms* by John F. Dooley. *Cryptologia*, 38(3):285–286, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2014:BRBb

[1374] Chris Christensen. Book review: *The History of Traffic Analysis: World War I–Vietnam* by Donald A. Borrmann et al. *Cryptologia*, 38(3):287–290, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2014:BRBc

[1375] Chris Christensen. Book review: *Bletchley Park: The Code-Breakers of Station X* by Michael Smith. *Cryptologia*, 38(3):291–292, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2014:LHR

[1376] Chris Christensen. Lester Hill revisited. *Cryptologia*, 38(4):293–332, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Boklan:2014:HDC

[1377] Kent D. Boklan. How I decrypted a Confederate diary — and the question of the race of Mrs. Jefferson Davis. *Cryptologia*, 38(4):333–347, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Courtois:2014:CTG

[1378] Nicolas T. Courtois. Cryptanalysis of two GOST variants with 128-bit keys. *Cryptologia*, 38(4):348–361, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Rojas:2014:KZP

[1379] Raul Rojas. Konrad Zuse's proposal for a cipher machine. *Cryptologia*, 38(4):362–369, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wang:2014:CIK

[1380] Qinglong Wang and Jintai Ding. Cryptanalysis and improvement of a k-out-of-n oblivious transfer protocol. *Cryptologia*, 38(4):370–376, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2014:EBE

[1381] Anonymous. Editorial board EOV. *Cryptologia*, 38(4):ebi, 2014. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Smoot:2015:NRT

[1382] Betsy Rohaly Smoot. NSA release and transfer of records related to William F. Friedman. *Cryptologia*, 39(1):1–2, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Babinkostova:2015:SGT

[1383] L. Babinkostova, A. M. Bowden, A. M. Kimball, and K. J. Williams. A simplified and generalized treatment of DES-related ciphers. *Cryptologia*, 39(1):3–24, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Marks:2015:EWD

[1384] Philip Marks. Enigma wiring data: Interpreting Allied conventions from World War II. *Cryptologia*, 39(1):25–65, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Narvaez:2015:SDC

[1385] Roberto Narváez. Some diplomatic ciphers of the First Mexican Federal Republic (1824–1830). *Cryptologia*, 39(1):66–83, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schmeh:2015:SCI

[1386] Klaus Schmeh. Second Charlotte International Cryptologic Symposium. *Cryptologia*, 39(1):84–91, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2015:BRB

[1387] John F. Dooley. Book review: *George Fabyan* by Richard Munson. *Cryptologia*, 39(1):92–98, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2015:BRBa

[1388] Chris Christensen. Book review: *The Lost World of Bletchley Park* by Sinclair McKay. *Cryptologia*, 39(1):99–100, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2015:BRB

[1389] David H. Hamer. Book review: *Gordon Welchman: Bletchley Park's Architect of Ultra Intelligence* by Joel Greenberg. *Cryptologia*, 39(1):101–103, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ciungu:2015:HSR

[1390] Lavinia Corina Ciungu and David Kahn. A historical survey of Romanian intelligence. *Cryptologia*, 39(2):105–120, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Horng:2015:ADS

[1391] Gwoboa Horng. Accelerating DSA signature generation. *Cryptologia*, 39(2):121–125, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Antal:2015:KSP

[1392] Eugen Antal and Pavol Zajac. Key space and period of Fialka M-125 cipher machine. *Cryptologia*, 39(2):126–144, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Courtois:2015:CGM

[1393] Nicolas T. Courtois, Theodosis Mourouzis, Michal Misztal, Jean-Jacques Quisquater, and Guangyan Song. Can GOST be made secure against differential cryptanalysis? *Cryptologia*, 39(2):145–156, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

deLeeuw:2015:JFW

[1394] Karl de Leeuw. J. F. W. Nuboer and the reintroduction of machine cryptography by the Royal Netherlands Navy, 1915–1940. *Cryptologia*, 39(2):157–172, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bauer:2015:FAT

[1395] Craig Bauer. Friedman Auditorium times two. *Cryptologia*, 39(2):173–177, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2015:RIM

[1396] Chris Christensen. Review of IEEE Milestone Award to the Polish Cipher Bureau for "The First Breaking of Enigma Code". *Cryptologia*, 39(2):178–193, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2015:BRBb

[1397] Chris Christensen. Book review: *Marian Rejewski: The Man Who Defeated Enigma* by Zdzisław Jan Kapera. *Cryptologia*, 39(2):194–197, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2015:BRA

[1398] Chris Christensen. Book review: *Alan Turing: His Work and Impact*, edited by S. Barry Cooper and Jan van Leeuwen. *Cryptologia*, 39(2):198–202, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anderson:2015:KC

[1399] Jeanne Anderson. Kaczynski's ciphers. *Cryptologia*, 39(3):203–209, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2015:SMA

[1400] Chris Christensen and Jared Antrobus. The story of Mamba: Aligning messages against recovered additives. *Cryptologia*, 39(3):210–243, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Martinez:2015:SPC

[1401] V. Gayoso Martínez, L. Hernández Encinas, and A. Queiruga Dios. Security and practical considerations when implementing the elliptic curve integrated encryption scheme. *Cryptologia*, 39(3):244–269, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gu:2015:EPC

[1402] Haihua Gu, Dawu Gu, Wenlu Xie, and Ray C. C. Cheung. Efficient pairing computation on Huff curves. *Cryptologia*, 39(3):270–275, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lang:2015:SLA

[1403] Benedek Láng. Shame, love, and alcohol: Private ciphers in early modern Hungary. *Cryptologia*, 39(3):276–287, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2015:BRBd

[1404] Chris Christensen. Book review: *Blackett's War* by Stephen Budiansky. *Cryptologia*, 39(3):288–290, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Konheim:2015:ICT

[1405] Alan G. Konheim. The impetus to creativity in technology. *Cryptologia*, 39(4):291–314, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2015.1044816`.

Smoot:2015:PHF

[1406] Betsy Rohaly Smoot. Parker Hitt's first cylinder device and the Genesis of U.S. Army cylinder and strip devices. *Cryptologia*, 39(4):315–321, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2014.988371`.

Courtois:2015:MSF

[1407] Nicolas Courtois. On multiple symmetric fixed points in GOST. *Cryptologia*, 39(4):322–334, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2014.988362`.

Barr:2015:TKL

[1408] Thomas H. Barr and Andrew J. Simoson. Twisting the keyword length from a Vigenère cipher. *Cryptologia*, 39(4):335–341, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2014.988365`.

Schmeh:2015:EBM

[1409] Klaus Schmeh. Encrypted books: Mysteries that fill hundreds of pages. *Cryptologia*, 39(4):342–361, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2014.988369`.

Christensen:2015:BRBe

[1410] Chris Christensen. Book review: *Act of War: Lyndon Johnson, North Korea, and the Capture of the Spy Ship Pueblo* by Jack Cheevers. *Cryptologia*, 39(4):362–372, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2015.1009756`.

Christensen:2015:BRBf

[1411] Chris Christensen. Book review: *The Riddle of the Labyrinth* by Margalit Fox. *Cryptologia*, 39(4):

373–375, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2014.915693`.

Anonymous:2015:EBE

[1412] Anonymous. Editorial board EOV. *Cryptologia*, 39(4):ebi, 2015. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2015.1086600`.

Hwang:2016:ROR

[1413] Tzonelih Hwang and Prosanta Gope. RT-OCFB: Real-time based optimized cipher feedback mode. *Cryptologia*, 40(1):1–14, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Goodman:2016:BIF

[1414] Michael Goodman and Huw Dylan. British intelligence and the fear of a Soviet attack on Allied communications. *Cryptologia*, 40(1):15–32, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kollar:2016:SVC

[1415] Jozef Kollár. Soviet VIC cipher: No respector of Kerckoff's principles. *Cryptologia*, 40(1):33–48, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lasry:2016:AKP

[1416] George Lasry, Nils Kopal, and Arno Wacker. Automated known-plaintext cryptanalysis of short Hagelin M-209 messages. *Cryptologia*, 40(1):49–69, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Ostwald:2016:HMC

[1417] Olaf Ostwald and Frode Weierud. History and modern cryptanalysis of Enigma's pluggable reflector. *Cryptologia*, 40(1):70–91, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wright:2016:RTM

[1418] John Wright. Rejewski's test message as a crib. *Cryptologia*, 40(1):92–106, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2016:RPL

[1419] John F. Dooley. Review of *Prisoners, Lovers, & Spies*, by Kristie Macrakis. *Cryptologia*, 40(1):107–112, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bury:2016:O

[1420] Jan Bury. Operation "Zachod": Sex, lies, and ciphers. *Cryptologia*, 40(2):113–140, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2015.1113830`.

Lasry:2016:COC

[1421] George Lasry, Nils Kopal, and Arno Wacker. Ciphertext-only cryptanalysis of Hagelin M-209 pins and lugs. *Cryptologia*, 40(2):141–176, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2015.1028683`.

Thimbleby:2016:HFM

[1422] Harold Thimbleby. Human factors and missed solutions to Enigma de-

sign weaknesses. *Cryptologia*, 40(2): 177–202, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2015.1028680`.

Fuensanta:2016:SSC

[1423] José Ramón Soler Fuensanta and Vicente Guasch Portas. States by secrecy: Cryptography and guerrillas in the Spanish Civil War. *Cryptologia*, 40(2):203–214, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/01611194.2015.1028687`.

Wik:2016:EZR

[1424] Anders Wik. Enigma Z30 retrieved. *Cryptologia*, 40(3):215–220, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Loebenberger:2016:DPL

[1425] Daniel Loebenberger and Michael Nüsken. Design principles of DES-like ciphers: A historical overview. *Cryptologia*, 40(3):221–239, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Strasser:2016:SZG

[1426] Gerhard F. Strasser. Samuel Zimmermann's *gehaimnussen:* the earliest cryptological book in German. *Cryptologia*, 40(3):240–260, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sanguino:2016:ASS

[1427] Luis Alberto Benthin Sanguino, Gregor Leander, Christof Paar, Bernhard Esslinger, and Ingo Niebel. Analyzing the Spanish strip cipher by combining combinatorial and statistical methods. *Cryptologia*, 40(3):261–284, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hwang:2016:PCP

[1428] Tzonelih Hwang and Prosanta Gope. PFC-CTR, PFC-OCB: Efficient stream cipher modes of authencryption. *Cryptologia*, 40(3):285–302, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Pommerening:2016:CNF

[1429] Klaus Pommerening. Cryptanalysis of nonlinear feedback shift registers. *Cryptologia*, 40(4):303–315, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Narvxeez:2016:CJL

[1430] Roberto Narváez. On the cryptography of James Leander Cathcart (1767–1843). *Cryptologia*, 40(4):316–326, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wright:2016:RST

[1431] John Wright. A recursive solution for Turing's *H-M* factor. *Cryptologia*, 40(4):327–347, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kak:2016:SEC

[1432] Subhash Kak. Simulating entanglement in classical computing for cryptographic applications. *Cryptologia*, 40 (4):348–354, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Samuels:2016:LFP

[1433] Martin Samuels. Ludwig Föppl: A Bavarian cryptanalyst on the Western front. *Cryptologia*, 40(4):355–373, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lasry:2016:CCT

[1434] George Lasry, Nils Kopal, and Arno Wacker. Cryptanalysis of columnar transposition cipher with long keys. *Cryptologia*, 40(4):374–398, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bauer:2016:RUM

[1435] Craig Bauer. Review of *Unveiling the Mystic Ciphers* by Dave Ramsden. *Cryptologia*, 40(4):399–401, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Smoot:2016:AZC

[1436] Betsy Rohaly Smoot and David Hatch. Ann Zeilinger Caracristi (1 February 1921–10 January 2016). *Cryptologia*, 40(5):403–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Boklan:2016:HDR

[1437] Kent D. Boklan. How I deciphered a Robert E. Lee letter — and a note on the power of context in short polyalphabetic ciphers. *Cryptologia*, 40(5): 406–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bonavoglia:2016:LPP

[1438] Paolo Bonavoglia and Consolato Pellegrino. The last poem of Pietro Giannone — finally decrypted. *Cryptologia*, 40(5):411–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Girard:2016:BTC

[1439] Daniel J. Girard. Breaking "Tirpitz": Cryptanalysis of the Japanese–German joint naval cipher. *Cryptologia*, 40(5):428–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Leap:2016:FIB

[1440] Tom Leap, Tim McDevitt, Kayla Novak, and Nicolette Siermine. Further improvements to the Bauer–Millward attack on the Hill cipher. *Cryptologia*, 40(5):452–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2016:RTB

[1441] Chris Christensen. A review of three books about the women of Bletchley Park. *Cryptologia*, 40(5):469–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hoffman:2016:RIS

[1442] Nick Hoffman. Review of *Intercept: The Secret History of Computers and Spies* by Gordon Corera. *Cryptologia*, 40(5):477–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Visco:2016:SMT

[1443] David Visco. Somerton man times two. *Cryptologia*, 40(5):481–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Smoot:2016:CPS

[1444] Betsy Rohaly Smoot. Call for papers: 2017 Symposium on Cryptologic History. *Cryptologia*, 40(5):484–??, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Lasry:2016:CCS

[1445] George Lasry, Moshe Rubin, Nils Kopal, and Arno Wacker. Cryptanalysis of Chaocipher and solution of Exhibit 6. *Cryptologia*, 40(6):487–514, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kepley:2016:CMR

[1446] Shane Kepley, David Russo, and Rainer Steinwandt. Cryptanalysis of a modern rotor machine in a multicast setting. *Cryptologia*, 40(6):515–521, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Yu:2016:NFC

[1447] Qian Yu and Chang N. Zhang. A new and fast cryptographic hash function based on RC4. *Cryptologia*, 40(6):522–540, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bauer:2016:JSK

[1448] Craig Bauer, Gregory Link, and Dante Molle. James Sanborn's *Kryptos* and the matrix encryption conjecture. *Cryptologia*, 40(6):541–552, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Hamer:2016:RPA

[1449] David H. Hamer. Review of *Prof: Alan Turing Decoded* by Dermot Turing. *Cryptologia*, 40(6):553–555, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2016:CRP

[1450] Chris Christensen. Companion review of *Prof: Alan Turing Decoded* by Dermot Turing. *Cryptologia*, 40(6):556–562, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2016:RCC

[1451] Chris Christensen. Review of *Codes, Ciphers and Spies: Tales of Military Intelligence in World War I* by John F. Dooley. *Cryptologia*, 40(6):563–566, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2016:RUN

[1452] Chris Christensen. Review of *U.S. Navy Codebreakers, Linguists, and Intelligence Officers against Japan, 1910–1941* by Steven E. Maffeo. *Cryptologia*, 40(6):567–569, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2016:EB

[1453] Anonymous. Editorial board. *Cryptologia*, 40(6):ebi, 2016. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Vobbilisetty:2017:CCU

[1454] Rohit Vobbilisetty, Fabio Di Troia, Richard M. Low, Corrado Aaron Visaggio, and Mark Stamp. Classic cryptanalysis using hidden Markov models. *Cryptologia*, 41(1):1–28, 2017. CODEN CRYPE6. ISSN 0161-1194 (print),

1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2015.1126660.

Sherman:2017:CPD

[1455] Alan T. Sherman, John Seymour, Akshayraj Kore, and William Newton. Chaum's protocol for detecting man-in-the-middle: Explanation, demonstration, and timing studies for a text-messaging scenario. *Cryptologia*, 41(1):29–54, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2015.1135487.

Wieczorek:2017:PDG

[1456] Rafal Wieczorek. Putative duplication glyph in the Rongorongo script. *Cryptologia*, 41(1):55–72, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1196052.

Schmeh:2017:RNC

[1457] Klaus Schmeh. Review of the 15th NSA Cryptologic History Symposium. *Cryptologia*, 41(1):73–80, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1169460.

Christensen:2017:RSE

[1458] Chris Christensen. Review of *The SIGABA/ECM II Cipher Machine: "A Beautiful Idea"* by Timothy J. Mucklow. *Cryptologia*, 41(1):81–84, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236634.

Christensen:2017:RNG

[1459] Chris Christensen. Review of *The Neglected Giant: Agnes Meyer Driscoll* by K. Johnson. *Cryptologia*, 41(1):85–89, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236643.

Christensen:2017:RIN

[1460] Chris Christensen. Review of *An Introduction to Number Theory with Cryptography* by James S. Kraft and Lawrence Washington. *Cryptologia*, 41(1):90–91, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236629.

Landwehr:2017:RSS

[1461] Dominik Landwehr. Review of *Simpliciana: Schriften der Grimmelshausen Gesellschaft 2014*. *Cryptologia*, 41(1):92–96, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236628.

Ehme:2017:JRT

[1462] Jeffrey Ehme. A joy to review: Two books about primes and factoring: [Rempe-Gillen, Lasse, and Rebecca Waldecker. *Primality Testing for Beginners*. Student Mathematical Library, American Mathematical Society, 2013, 244 pages, Paperback, $39. ISBN 978-0-8218-9883-3. Wagstaff, Jr.,

Samuel. *The Joy of Factoring*, Student Mathematical Library, American Mathematical Society, 2013. 293 pages. Paperback, $43.39. ISBN 978-1-4704-1048-3]. *Cryptologia*, 41(1):97–100, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236625`.

Lasry:2017:DAM

[1463] George Lasry, Ingo Niebel, Nils Kopal, and Arno Wacker. Deciphering ADFGVX messages from the Eastern Front of World War I. *Cryptologia*, 41(2):101–136, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1169461`.

Stallings:2017:FPE

[1464] William Stallings. Format-preserving encryption: Overview and NIST specification. *Cryptologia*, 41(2):137–152, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1169457`.

Meyer:2017:BG

[1465] Lauren De Meyer and Serge Vaudenay. DES S-box generator. *Cryptologia*, 41(2):153–171, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1169456`.

Schmeh:2017:RHC

[1466] Klaus Schmeh. Review of the 2nd Historical Ciphers Colloquium in Kassel, Germany. *Cryptologia*, 41(2):172–177, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1219787`.

Christensen:2017:RIG

[1467] Chris Christensen. Review of *The Imitation Game*. *Cryptologia*, 41(2):178–181, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236639`.

Christensen:2017:RDB

[1468] Chris Christensen. Review of *Demystifying the Bombe* by Dermot Turing. *Cryptologia*, 41(2):182–183, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236632`.

Hamer:2017:RSW

[1469] David H. Hamer. Review of *The Secret World* by Hugh Trevor-Roper. *Cryptologia*, 41(2):184–185, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236623`.

Hamer:2017:RSE

[1470] David H. Hamer. Review of *Solving Enigma's Secrets* by John Jackson. *Cryptologia*, 41(2):186–189, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236619`.

Christensen:2017:RME

[1471] Chris Christensen. Review of *The Mathematics of Encryption: An Elementary Introduction* by M. Cozzens and S. Miller. *Cryptologia*, 41(2):190–194, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236642`.

Sherman:2017:NSA

[1472] David Sherman. The National Security Agency and the William F. Friedman Collection. *Cryptologia*, 41(3):195–238, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1169458`.

Smith:2017:EFS

[1473] G. Stuart Smith. Elizebeth Friedman's security and career concerns prior to World War II. *Cryptologia*, 41(3):239–246, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1257523`.

Rugg:2017:HSF

[1474] Gordon Rugg and Gavin Taylor. Hoaxing statistical features of the Voynich Manuscript. *Cryptologia*, 41(3):247–268, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1206753`.

Alexander:2017:GMD

[1475] John Alexander, John Gallehawk, John Jackson, Allen Pearce, and Edward Simpson. A German machine for differencing and testing additives. *Cryptologia*, 41(3):269–280, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1289718`.

Christensen:2017:CBR

[1476] Chris Christensen. A comment on a book review. *Cryptologia*, 41(3):281–282, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236627`.

Christensen:2017:RTZ

[1477] Chris Christensen. Review of *The Triumph of Zygalski's Sheets: The Polish Enigma in the Early 1940* by Zdzisław J. Kapera. *Cryptologia*, 41(3):283–285, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236646`. See corrections [1508].

Christensen:2017:RSS

[1478] Chris Christensen. Review of *SIGINT: The Secret History of Signals Intelligence 1914–1945* by Peter Matthews. *Cryptologia*, 41(3):286–287, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236637`.

Christensen:2017:RBP

[1479] Chris Christensen. Review of *Bletchley Park: The Secret Archives* by Sinclair McKay. *Cryptologia*, 41(3):288, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1236644`.

Anonymous:2017:DHF

[1480] Anonymous. David Hamer, family man and Enigma expert, remembered and missed. *Cryptologia*, 41(4):289–294, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1343556`.

Wright:2017:TBV

[1481] John Wright. The Turing bombe *victory* and the first naval Enigma decrypts. *Cryptologia*, 41(4):295–328, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1219786`.

Christensen:2017:ERB

[1482] Chris Christensen. The evolving relationship between mathematics and cryptology, 1951–1952: SCAG and the beginnings of SCAMP and NSASAB. *Cryptologia*, 41(4):329–387, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1219788`.

Varga:2017:ZIP

[1483] Charles Varga. Is Zendia the Isle of Pines? *Cryptologia*, 41(4):388–394, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1327698`.

Ostwald:2017:MBE

[1484] Olaf Ostwald and Frode Weierud. Modern breaking of Enigma ciphertexts. *Cryptologia*, 41(5):395–421, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1238423`.

Bultel:2017:HEM

[1485] Xavier Bultel, Jannik Dreier, Pascal Lafourcade, and Malika More. How to explain modern security concepts to your children. *Cryptologia*, 41(5):422–447, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1238422`.

Echard:2017:HEI

[1486] Jean-Philippe Échard and Pierrick Gaudry. A harmonious encoding of instrument values by a nineteenth-century Parisian violin dealer. *Cryptologia*, 41(5):448–458, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1257524`.

Wolf:2017:SCW

[1487] Gunnar E. Wolf and Gina Gallegos-García. Strengthening a curated web of trust in a geographically distributed project. *Cryptologia*, 41(5):459–475, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1238421`.

Smoot:2017:NSA

[1488] Betsy Rohaly Smoot. National Security Agency releases Army Security Agency histories covering 1945–1963. *Cryptologia*, 41(5):476–478, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1325789`.

Christensen:2017:RSM

[1489] Chris Christensen. Review of *Silence Means Security: Secrets of a WWII Code-Breaking WAC* by B. Nicodemus. *Cryptologia*, 41(5):479–480, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1326272`.

Christensen:2017:RCW

[1490] Chris Christensen. Review of *Code Warriors: NSA's Codebreakers and the Secret Intelligence War against the Soviet Union* by S. Budiansky. *Cryptologia*, 41(5):481–484, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1326794`.

Schmeh:2017:RUH

[1491] Klaus Schmeh. Review of *Unsolved: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies* by Craig Bauer. *Cryptologia*, 41(5):485–490, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1346339`.

Hieu:2017:CDF

[1492] Phan Du'o'ng Hiệu and Neal Koblitz. Cryptography during the French and American wars in Vietnam. *Cryptologia*, 41(6):491–511, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1292825`.

Bury:2017:LCW

[1493] Jan Bury. Lambda: A cold war Polish line encryptor and the networks it served. *Cryptologia*, 41(6):512–533, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1357983`.

Agievich:2017:MPS

[1494] S. Agievich, A. Gorodilova, V. Idrisova, N. Kolomeec, G. Shushuev, and N. Tokareva. Mathematical problems of the Second International Students' Olympiad in Cryptography. *Cryptologia*, 41(6):534–565, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2016.1260666`.

Anonymous:2017:EBE

[1495] Anonymous. Editorial board EOV. *Cryptologia*, 41(6):??, 2017. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1403537`.

Marks:2018:MTB

[1496] Philip Marks. Mr. Twinn's bombes. *Cryptologia*, 42(1):1–80, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Mishra:2018:NLA

[1497] P. R. Mishra, Yogesh Kumar, N. R. Pillai, and R. K. Sharma. On nonlinearity and affine equivalence of permutations over an arbitrary finite commutative ring with unity. *Cryptologia*, 42(1):81–94, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Nedved:2018:SJW

[1498] Gregory J. Nedved. The Sino–Japanese war of 1894–1895: Partially decrypted. *Cryptologia*, 42(2):95–105, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Vazquez:2018:RME

[1499] Manuel Vázquez and Paz Jiménez-Seral. Recovering the military Enigma using permutations — filling in the details of Rejewski's solution. *Cryptologia*, 42(2):106–134, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Stallings:2018:OCO

[1500] William Stallings. The offset codebook (OCB) block cipher mode of operation for authenticated encryption. *Cryptologia*, 42(2):135–145, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Mishra:2018:EST

[1501] Dheerendra Mishra. Efficient and secure two-factor dynamic ID-based password authentication scheme with provable security. *Cryptologia*, 42(2):146–175, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schmeh:2018:REH

[1502] Klaus Schmeh. Review of the 3rd European Historical Ciphers Colloquium in Smolenice, Slovakia. *Cryptologia*, 42(2):176–182, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Dooley:2018:RMP

[1503] John F. Dooley. Review of *A Mind at Play* by Jimmy Soni and Rob Goodman. *Cryptologia*, 42(2):183–190, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Courtois:2018:DOS

[1504] Nicolas Courtois. Decryption oracle slide attacks on T-310. *Cryptologia*, 42(3):191–204, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bonavoglia:2018:WWN

[1505] Paolo Bonavoglia. A 1916 World War I notebook of Luigi Sacco. *Cryptologia*, 42(3):205–221, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Wright:2018:RES

[1506] John Wright. Rejewski's equations: Solving for the entry permutation. *Cryptologia*, 42(3):222–226, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Moufek:2018:NVM

[1507] Hamza Moufek and Kenza Guenda. A new variant of the McEliece cryptosystem based on the Smith form of convolutional codes. *Cryptologia*, 42(3):227–239, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anonymous:2018:CRT

[1508] Anonymous. Corrections to "Review of *The Triumph of Zygalski's Sheets: The Polish Enigma in the Early 1940s*" 2017. *Cryptologia* **41(3)**: 283–285. *Cryptologia*, 42(3):240, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). See [1477].

Shaffer:2018:SSI

[1509] Ryan Shaffer. Spies and signals intelligence in the early Cold War. *Cryptologia*, 42(3):241–253, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Joyner:2018:RLC

[1510] David Joyner. Review of *A Life in Code* by Stuart G. Smith and *The Woman Who Smashed Codes* by Jason Fagone. *Cryptologia*, 42(3):254–257, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Anderson:2018:RCG

[1511] Deborah Anderson. Review of *Code Girls: The untold story of the American women code breakers of World War II* by Liza Mundy. *Cryptologia*, 42(3):258–261, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Erskine:2018:RHH

[1512] Ralph Erskine. Review of *The Hidden History of Bletchley Park: A Social and Organisational History, 1939–1945* by Christopher Smith. *Cryptologia*, 42(3):262–264, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Schmeh:2018:RVM

[1513] Klaus Schmeh. Review of *The Voynich Manuscript* by Raymond Clemens and *The Voynich Manuscript: The world's most Mysterious and Esoteric Codex* by Stephen Skinner. *Cryptologia*, 42(3):265–270, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2018:RCB

[1514] Chris Christensen. Review of *Code Breaking in the Pacific* by Peter Donovan and John Mack. *Cryptologia*, 42 (3):271–273, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2018:RMS

[1515] Chris Christensen. Review of *The Mathematics of Secrets* by Joshua Holden. *Cryptologia*, 42(3):274–277, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Christensen:2018:RNC

[1516] Chris Christensen. Review of *The New Codebreakers* edited by P. Ryan, D. Naccache, and J.-J. Quisquater. *Cryptologia*, 42(3):278–283, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Kiraly:2018:CCR

[1517] Levente Zoltán Király and Gábor Tokai. Cracking the code of the Rohonc Codex. *Cryptologia*, 42(4):285–315, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1449147`.

Courtois:2018:COA

[1518] Nicolas T. Courtois and Maria-Bristena Oprisanu. Ciphertext-only attacks and weak long-term keys in T-310. *Cryptologia*, 42(4):316–336, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1362065`.

Sherman:2018:CEC

[1519] Alan T. Sherman, David DeLatte, Michael Neary, Linda Oliva, Dhananjay Phatak, Travis Scheponik, Geoffrey L. Herman, and Julia Thompson. Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia*, 42(4):337–377, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1362063`.

Christensen:2018:RWD

[1520] Chris Christensen. Review of *Working on the Dark Side of the Moon: Life Inside the National Security Agency* by Thomas Reed Willemain. *Cryptologia*, 42(4):378–380, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1449148`.

Biermann:2018:AGB

[1521] Norbert Biermann. Analysis of Giouan Battista Bellaso's cipher challenges of 1555. *Cryptologia*, 42(5):381–407, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1422050`.

McDevitt:2018:PTM

[1522] Tim McDevitt, Jessica Lehr, and Ting Gu. A parallel time–memory trade-off attack on the Hill cipher. *Cryptologia*, 42(5):408–426, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1422051`.

Courtois:2018:FCE

[1523] Nicolas Courtois, Jörg Drobick, and Klaus Schmeh. Feistel ciphers in East Germany in the communist era. *Cryptologia*, 42(5):427–444, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1428835`.

Christensen:2018:RLC

[1524] Chris Christensen. Review of *Lorenz* and comments on the work of William Tutte: Roberts, Captain Jerry. *Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park*. The History Press, Stroud, Gloucestershire UK, 2017. 240 pages, Hardcover, £20. ISBN 978-0-7509-7885-9. *Cryptologia*, 42(5):445–466, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1435216`.

Strasser:2018:RVB

[1525] Gerhard F. Strasser. Review of *Versteckte Botschaften. Die faszinierende Geschichte der Steganografie*. 2., aktualisierte und erweiterte Auflage (*Hidden Messages. The Fascinating Story of Steganography*. 2nd, updated and expanded edition) by Klaus Schmeh. *Cryptologia*, 42(5):467–475, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1435207`.

Tomokiyo:2018:HRS

[1526] Satoshi Tomokiyo. How I reconstructed a Spanish cipher from 1591. *Cryptologia*, 42(6):477–484, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2017.1370038`.

Lasry:2018:COC

[1527] George Lasry, Nils Kopal, and Arno Wacker. Ciphertext-only cryptanalysis of short Hagelin M-209 ciphertexts. *Cryptologia*, 42(6):485–513, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1428836`.

Kuzuoglu:2018:CCC

[1528] Ulug Kuzuoglu. Chinese cryptography: The Chinese Nationalist Party and intelligence management, 1927–1949. *Cryptologia*, 42(6):514–539, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1449146`.

Christensen:2018:RGG

[1529] Chris Christensen. Review of *A Grand Gossip: The Bletchley Park Diary of Basil Cottle* edited by James and Judith Hodsdon. *Cryptologia*, 42(6):540–543, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1449149`.

Christensen:2018:RTH

[1530] Chris Christensen. Review of *TICOM: The Hunt for Hitler's Codebreakers* by Randy Rezabek. *Cryptologia*, 42(6):544–547, 2018. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1449150`.

Anonymous:2018:EBE

[1531] Anonymous. Editorial Board EOV. *Cryptologia*, 42(6):??, 2018. CODEN CRYPE6. ISSN 0161-1194 (print),

1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1472455.

Anonymous:2019:SCH

[1532] Anonymous. 2019 Symposium on Cryptologic History. *Cryptologia*, 43(1):1, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1531593.

Courtois:2019:LCB

[1533] Nicolas T. Courtois, Maria-Bristena Oprisanu, and Klaus Schmeh. Linear cryptanalysis and block cipher design in East Germany in the 1970s. *Cryptologia*, 43(1):2–22, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1483981.

Tomokiyo:2019:IIC

[1534] Satoshi Tomokiyo. Identifying Italian ciphers from continuous-figure ciphertexts (1593). *Cryptologia*, 43(1):23–46, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1503207.

Peinado:2019:RSS

[1535] Alberto Peinado. Reconstruction of a 1940 Spanish strip cipher by means of a cyclic rotation model applied to encrypted telegrams. *Cryptologia*, 43(1):47–64, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1522678.

Christensen:2019:RSW

[1536] Chris Christensen. Review of *The Spy Who Couldn't Spell* by Yudhijit Bhattacharjee. *Cryptologia*, 43(1):65–68, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1471429.

Christensen:2019:RSJ

[1537] Chris Christensen. Review of *Stanley Johnston's Blunder: the Reporter Who Spilled the Secret Behind the U.S. Navy's Victory at Midway* by Elliot Carlson. *Cryptologia*, 43(1):69–76, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1503208.

Christensen:2019:RAD

[1538] Chris Christensen. Review of *Alastair Denniston: Code-Breaking from Room 40 to Berkeley Street and the Birth of GCHQ* by Joel Greenberg. *Cryptologia*, 43(1):77–80, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1503209.

Christensen:2019:EHS

[1539] Chris Christensen. Edward Hugh Simpson CB (10 December 1922–5 February 2019). *Cryptologia*, 43 (2):81–83, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1583823.

Christensen:2019:AJM

[1540] Chris Christensen, Jared Antrobus, and Edward Simpson. Aligning JN-25 messages in depth using weights when the code groups scan. *Cryptologia*, 43(2):84–137, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1528311`.

Gorodilova:2019:PSF

[1541] A. Gorodilova, S. Agievich, C. Carlet, E. Gorkunov, V. Idrisova, N. Kolomeec, A. Kutsenko, S. Nikova, A. Oblaukhov, S. Picek, B. Preneel, V. Rijmen, and N. Tokareva. Problems and solutions from the fourth International Students' Olympiad in Cryptography (NSUCRYPTO). *Cryptologia*, 43(2):138–174, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1517834`.

Courtois:2019:SAL

[1542] Nicolas T. Courtois, Marios Georgiou, and Matteo Scarlata. Slide attacks and LC-weak keys in T-310. *Cryptologia*, 43(3):175–189, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1548392`.

Alhadawi:2019:DPB

[1543] Hussam S. Alhadawi, Mohamad Fadli Zolkipli, Saba M. Ismail, and Dragan Lambić. Designing a pseudorandom bit generator based on LFSRs and a discrete chaotic map. *Cryptologia*, 43(3):190–211, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1548390`.

Maitra:2019:SSS

[1544] Tanmoy Maitra, Debasis Giri, and Ram N. Mohapatra. SAS-SIP: A secure authentication scheme based on ECC and a fuzzy extractor for session initiation protocol. *Cryptologia*, 43(3):212–232, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1548391`.

Mathivanan:2019:QCB

[1545] P. Mathivanan, A. Balaji Ganesh, and R. Venkatesan. QR code-based ECG signal encryption/decryption algorithm. *Cryptologia*, 43(3):233–253, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1549122`.

Bentajer:2019:IBD

[1546] Ahmed Bentajer, Mustapha Hedabou, Karim Abouelmehdi, Zakaria Igarramen, and Said El Fezazi. An IBE-based design for assured deletion in cloud storage. *Cryptologia*, 43(3):254–265, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1549123`.

Lasry:2019:CED

[1547] George Lasry, Nils Kopal, and Arno Wacker. Cryptanalysis of Enigma double indicators with hill climbing. *Cryp-*

tologia, 43(4):267–292, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1551253`.

Sherman:2019:SSR

[1548] Alan Sherman, Enis Golaszewski, Edward LaFemina, Ethan Goldschen, Mohammed Khan, Lauren Mundy, Mykah Rather, Bryan Solis, Wubnyonga Tete, Edwin Valdez, Brian Weber, Damian Doyle, Casey O'Brien, Linda Oliva, Joseph Roundy, and Jack Suess. The SFS summer research study at UMBC: Project-based learning inspires cybersecurity students. *Cryptologia*, 43(4):293–312, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1557298`.

Omrani:2019:LLI

[1549] Tasnime Omrani, Rhouma Rhouma, and Rabei Becheikh. LICID: a lightweight image cryptosystem for IoT devices. *Cryptologia*, 43(4):313–343, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1563009`.

Dooley:2019:BCF

[1550] John F. Dooley. The Beale ciphers in fiction. *Cryptologia*, 43(4):344–358, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1550691`.

Bouchaudy:2019:GFW

[1551] Jean-François Bouchaudy. Genuine French WWII M-209 cryptograms. *Cryptologia*, 43(5):359–371, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596180`.

Bussi:2019:MHF

[1552] Khushboo Bussi, Dhananjoy Dey, P. R. Mishra, and B. K. Dass. MGR hash functions. *Cryptologia*, 43(5):372–390, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596995`.

Tuncer:2019:BBF

[1553] Türker Tuncer. Block-based fuzzy-image authentication method. *Cryptologia*, 43(5):391–413, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1582117`.

Kalita:2019:ACI

[1554] Manashee Kalita, Themrichon Tuithung, and Swanirbhar Majumder. An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. *Cryptologia*, 43(5):414–437, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1579122`.

Clayton:2019:LRE

[1555] Mike Clayton and John Gallehawk. Letter repeats in Enigma ciphertext produced by same-letter keying. *Cryptologia*, 43(5):438–457, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1565108`.

Bonavoglia:2019:BCR

[1556] Paolo Bonavoglia. Bellaso's 1552 cipher recovered in Venice. *Cryptologia*, 43(6):459–465, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596181`.

Smith:2019:GCA

[1557] Emma May Smith and Marco Ponzi. Glyph combinations across word breaks in the Voynich manuscript. *Cryptologia*, 43(6):466–485, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596998`.

Grosek:2019:RBV

[1558] Otokar Grosek, Eugen Antal, and Tomás Fabsic. Remarks on breaking the Vigenère autokey cipher. *Cryptologia*, 43(6):486–496, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596997`.

Ayat:2019:RAS

[1559] S. Masih Ayat and Meysam Ghahramani. A recursive algorithm for solving "a secret sharing" problem. *Cryptologia*, 43(6):497–503, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596996`.

Kishore:2019:PCH

[1560] Neha Kishore and Priya Raina. Parallel cryptographic hashing: Developments in the last 25 years. *Cryptologia*, 43(6):504–535, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1609130`.

Christensen:2019:RHC

[1561] Chris Christensen. Review of *History of Cryptography and Cryptanalysis* by John Dooley. *Cryptologia*, 43(6):536–538, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1623344`.

Christensen:2019:RCB

[1562] Chris Christensen. Review of *The Cypher Bureau* by Eilidh McGinness. *Cryptologia*, 43(6):539–541, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1623937`.

Christensen:2019:RXZ

[1563] Chris Christensen. Review of *X, Y & Z* by Dermot Turing. *Cryptologia*, 43(6):542–544, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1623938`.

Roberto:2019:RMS

[1564] R. Narváez Roberto. Review of *Mensajes secretos. La historia de la criptografía Española desde sus inicios hasta los años 50 (Secret Messages. The History of Spanish Cryptography from its beginnings until the 1950s)* by Soler Fuensanta, José Ramón, and Francisco Javier López-Brea Eespiau. *Cryptologia*, 43(6):545–550, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1609131`.

Dooley:2019:RCC

[1565] John F. Dooley. Review of *3 Ciphers* by Carol Ritz. *Cryptologia*, 43(6):551–552, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1629676`.

Timm:2020:PGA

[1566] Torsten Timm and Andreas Schinner. A possible generating algorithm of the Voynich manuscript. *Cryptologia*, 44(1):1–19, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1596999`.

Courtois:2020:VES

[1567] Nicolas T. Courtois and Marios Georgiou. Variable elimination strategies and construction of nonlinear polynomial invariant attacks on T-310. *Cryptologia*, 44(1):20–38, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1650845`.

Bonavoglia:2020:CDC

[1568] Paolo Bonavoglia. The cifra delle caselle: a XVI Century superencrypted cipher. *Cryptologia*, 44(1):39–52, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1609132`.

Diaz:2020:PAC

[1569] Alejandra Diaz, Alan T. Sherman, and Anupam Joshi. Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1):53–67, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1623343`.

Kumar:2020:ODT

[1570] Manoj Kumar, T. S. Suresh, Saibal K. Pal, and Anupama Panigrahi. Optimal differential trails in lightweight block ciphers ANU and PICO. *Cryptologia*, 44(1):68–78, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1650844`.

Sherman:2020:INC

[1571] David Sherman, Betsy Rohaly Smoot, and Robert J. Hanyok. Introducing a new *Cryptologia* series: Sources and methods for cryptologic history. *Cryptologia*, 44(1):79–81, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://`

www.tandfonline.com/doi/full/10.1080/01611194.2019.1670284.

Anonymous:2020:RTC

[1572] Anonymous. Review of two collections of essays about Alan Turing: Copeland, Jack, Jonathan Bowen, Mark Sprevak, Robin Wilson, and others, *The Turing Guide*, Oxford University Press, Oxford, 2017. 546 pages, Paperback, $29.95. ISBN 978-0-19-874783-3. Floyd, Juliet and Alisa Bokulich (eds.), *Philosophical Explorations of the Legacy of Alan Turing: Turing 100*, Springer International Publishing, Cham, Switzerland, 2017. 361 pages, Hardcover, $139.99. ISBN 978-3-319-53278-3. *Cryptologia*, 44(1):82–86, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1650846.

Anonymous:2020:RRL

[1573] Anonymous. Review of *Real Life Cryptology* by Benedek Láng. *Cryptologia*, 44(1):87–90, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1650847.

Dooley:2020:RTR

[1574] John F. Dooley. Review of *The Third Reich is Listening* by Christian Jennings. *Cryptologia*, 44(1):91–95, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1655505.

Weierud:2020:GMC

[1575] Frode Weierud and Sandy Zabell. German mathematicians and cryptology in WWII. *Cryptologia*, 44(2):97–171, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1600076.

Smoot:2020:SMC

[1576] Betsy Rohaly Smoot and Robert J. Hanyok. Sources and methods for cryptologic history: Research at the US National Archives — the "Big Two" record groups. *Cryptologia*, 44(2):172–196, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706066.

Park:2020:FKL

[1577] Seongmin Park, Juneyeun Kim, Kookrae Cho, and Dae Hyun Yum. Finding the key length of a Vigenère cipher: How to improve the twist algorithm. *Cryptologia*, 44(3):197–204, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1657202.

Kaeding:2020:SHC

[1578] Thomas Kaeding. Slippery hill-climbing technique for ciphertext-only cryptanalysis of periodic polyalphabetic substitution ciphers. *Cryptologia*, 44(3):205–222, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://

www.tandfonline.com/doi/full/10.1080/01611194.2019.1655504.

Gorodilova:2020:FIS

[1579] Anastasiya Gorodilova, Sergey Agievich, Claude Carlet, Xiang dong Hou, Valeria Idrisova, Nikolay Kolomeec, Alexandr Kutsenko, Luca Mariot, Alexey Oblaukhov, Stjepan Picek, Bart Preneel, Razvan Rosie, and Natalia Tokareva. The Fifth International Students' Olympiad in cryptography — NSUCRYPTO: Problems and their solutions. *Cryptologia*, 44(3):223–256, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1670282.

Beaver:2020:CTY

[1580] Cheryl Beaver and Stuart Boersma. Celebrating ten years of KRYPTOS: a series of cryptanalysis. *Cryptologia*, 44(3):257–266, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1670283.

Sherman:2020:SMC

[1581] David Sherman. Sources and methods for cryptologic history: the William and Elizebeth Smith Friedman collections. *Cryptologia*, 44(3):267–279, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1733134.

Dooley:2020:RSW

[1582] John F. Dooley. Review of *The Secret World* by Christopher Andrew. *Cryptologia*, 44(3):280–284, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706210.

McCarthy:2020:RIC

[1583] Jerry McCarthy. Review of the 2nd International Conference on Historical Cryptology in Mons, Belgium. *Cryptologia*, 44(3):285–288, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1659447.

Courtois:2020:CPI

[1584] Nicolas T. Courtois, Aidan Patrick, and Matteo Abbondati. Construction of a polynomial invariant annihilation attack of degree 7 for T-310. *Cryptologia*, 44(4):289–314, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706062.

Khatoon:2020:CIA

[1585] Shaheena Khatoon and Balwant Singh Thakur. Cryptanalysis and improvement of authentication scheme for roaming service in ubiquitous network. *Cryptologia*, 44(4):315–340, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706061.

Pandey:2020:SAH

[1586] Prateek Pandey and Ratnesh Litoriya. Securing and authenticating healthcare records through blockchain technology. *Cryptologia*, 44(4):341–356,

2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706060.

Biswas:2020:TPB

[1587] Anindya Kumar Biswas and Mou Dasgupta. Two polynomials based (t, n) threshold secret sharing scheme with cheating detection. *Cryptologia*, 44(4):357–370, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1717676.

Parsons:2020:SMC

[1588] Sarah Parsons. Sources and methods for cryptologic history: NSA.gov — a tour through its history and resources. *Cryptologia*, 44(4):371–382, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1753264.

Christensen:2020:RCC

[1589] Chris Christensen. Review of *Code Cracking for Kids*, by Jean Daigneau. *Cryptologia*, 44(4):383–384, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1754965.

Kenyon:2020:EGC

[1590] David Kenyon and Frode Weierud. Enigma G: The counter Enigma. *Cryptologia*, 44(5):385–420, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1661134.

Alin:2020:PCA

[1591] Jonas Alin. Principal component analysis of characters in the Voynich manuscript and their classifications based on comparative analysis of writings in known languages. *Cryptologia*, 44(5):421–437, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1688203.

BoppreNiehues:2020:SSS

[1592] Lucas Boppré Niehues, Joachim von zur Gathen, Lucas Pandolfo Perin, and Ana Zumalacárregui. Sidon sets and statistics of the ElGamal function. *Cryptologia*, 44(5):438–450, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1790128.

Saikia:2020:EDE

[1593] Monjul Saikia and Md. Anwar Hussain. Efficient data encryption technique using quaternions for wireless sensor network. *Cryptologia*, 44(5):451–471, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1755745.

Hanyok:2020:SMS

[1594] Robert J. Hanyok and Betsy Rohaly Smoot. Sources and methods series: considering other record groups in Nara holding cryptologic and

cryptologic-related records. *Cryptologia*, 44(5):472–476, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1792003`.

Dooley:2020:RME

[1595] John F. Dooley. Review of *A Most Enigmatic War*, by James Goodchild. *Cryptologia*, 44(5):477–480, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1688204`.

Melka:2020:EMT

[1596] Tomi S. Melka and Robert M. Schoch. Exploring a mysterious tablet from Easter Island: the issues of authenticity and falsifiability in *rongorongo* studies. *Cryptologia*, 44(6):481–544, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706065`.

Megyesi:2020:DHM

[1597] Beáta Megyesi, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker, and Michelle Waldispühl. Decryption of historical manuscripts: the DECRYPT project. *Cryptologia*, 44(6):545–559, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1716410`.

Hanyok:2020:SMC

[1598] Robert J. Hanyok and Betsy Rohaly Smoot. Sources and methods: contingency and its role in researching records of cryptologic history — a discussion and some lessons to apply for future research. *Cryptologia*, 44(6):560–568, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1834989`.

Christensen:2020:REB

[1599] Chris Christensen. Review of *The Enigma Bulletin* edited by Zdzisław J. Kapera. *Cryptologia*, 44(6):569–572, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1732497`.

Christensen:2020:RBP

[1600] Chris Christensen. Review of *Bletchley Park and D-Day* by David Kenyon. *Cryptologia*, 44(6):573–576, 2020. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1732498`.

Bures:2021:CPC

[1601] Kenneth J. Bures. Cracking PURPLE: cryptanalysis of the *Angooki Taipu B* switch tables. *Cryptologia*, 45(1):1–43, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706064`.

Daruka:2021:VM

[1602] István Daruka. On the Voynich manuscript. *Cryptologia*, 45(1):44–80, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2019.1706063`.

Smoot:2021:SMU

[1603] Betsy Rohaly Smoot. Sources and methods: uncovering the story of American cryptology in World War I. *Cryptologia*, 45(1):81–87, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1858371`.

Christensen:2021:RBT

[1604] Chris Christensen. Review of *Breaking Teleprinter Ciphers at Bletchley Park* by James A. Reeds, Whitfield Diffie, and J. V. Field. *Cryptologia*, 45(1):88–93, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1804484`.

Bonavoglia:2021:RCC

[1605] Paolo Bonavoglia. Review of *Classical cryptology at play* by Silvio Coccaro. *Cryptologia*, 45(1):94–96, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1793824`.

Tokar:2021:NHT

[1606] John A. Tokar. NSA honors two *Cryptologia* board members. *Cryptologia*, 45(2):97–101, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/07352689.2021.1891679`.

Nedved:2021:HYR

[1607] Gregory J. Nedved. Herbert O. Yardley revisited: what does the new evidence say? *Cryptologia*, 45(2):102–128, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1767706`.

Fuensanta:2021:HMC

[1608] José Ramón Soler Fuensanta, Héctor Soler Bonet, and Diego Navarro Bonilla. How to make a codebook versatile. The example of the ASLET code. *Cryptologia*, 45(2):129–166, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1718800`.

Tate:2021:ICM

[1609] Kirsten Tate. Identifying concealed messages using authorship attribution. *Cryptologia*, 45(2):167–177, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1736206`.

Courtois:2021:NIA

[1610] Nicolas T. Courtois. A nonlinear invariant attack on T-310 with the original Boolean function. *Cryptologia*, 45(2):178–192, 2021. CODEN CRYPE6. ISSN 0161-1194 (print),

1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1736207.

Anonymous:2021:CHS

[1611] Anonymous. 18th Cryptologic History Symposium. *Cryptologia*, 45(3):193, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1915382.

Sommervoll:2021:GAA

[1612] Åvald Åslaugson Sommervoll and Leif Nilsen. Genetic algorithm attack on Enigma's plugboard. *Cryptologia*, 45(3):194–226, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1721617.

Chauhan:2021:QTA

[1613] Dimpy Chauhan, Indivar Gupta, and Rashmi Verma. Quasigroups and their applications in cryptography. *Cryptologia*, 45(3):227–265, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1721615.

Teseleanu:2021:QSP

[1614] George Teseleanu. Quasigroups and substitution permutation networks: a failed experiment. *Cryptologia*, 45(3):266–281, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1750506.

Wase:2021:BLB

[1615] Viktor Wase. Benford's Law in the Beale ciphers. *Cryptologia*, 45(3):282–286, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1821409.

Dooley:2021:RFF

[1616] John Dooley. Review of *Flight of the Fox* by Gray Basnight. *Cryptologia*, 45(3):287–288, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1829182.

Weierud:2021:MTR

[1617] Frode Weierud. In memoriam: Thomas Ralph Erskine CB (1933–2021). *Cryptologia*, 45(4):289–308, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1935363.

Bouchaudy:2021:ESG

[1618] Jean-François Bouchaudy. Enigma: the spoils of Gustave Bertrand, or "par où tout a commencé". *Cryptologia*, 45(4):309–341, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1736205.

Geraud-Stewart:2021:FCL

[1619] Rémi Géraud-Stewart and David Naccache. A French cipher from the late 19^{th} century. *Cryptologia*, 45(4):342–370, 2021. CODEN CRYPE6. ISSN 0161-1194 (print),

1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1753265.

Hanyok:2021:SMS

[1620] Robert Hanyok. Sources and methods: Searching for cryptologic records in the findings of post-World War II allied technical surveys and commissions. *Cryptologia*, 45(4):371–378, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1921072.

Erskine:2021:RNS

[1621] Ralph Erskine. Review of *The Nazi Spy Ring in America* by Rhodri Jeffreys-Jones. *Cryptologia*, 45(4):379–382, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1878308.

Lasry:2021:DGD

[1622] George Lasry, Ingo Niebel, and Torbjörn Andersson. Deciphering German diplomatic and naval attaché messages from 1900–1915. *Cryptologia*, 45(5):383–425, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1755914.

Phelan:2021:LAF

[1623] Ronald Phelan and David Simpson. Ludlings: not all fun and games. *Cryptologia*, 45(5):426–433, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1761482.

Timm:2021:RLV

[1624] Torsten Timm and Andreas Schinner. Review of *The linguistics of the Voynich manuscript* by Claire Bowern and Luke Lindemann. *Cryptologia*, 45(5):434–438, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1911875.

Patterson:2021:ASU

[1625] Blain Patterson. Analyzing student understanding of cryptography using the SOLO taxonomy. *Cryptologia*, 45(5):439–449, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1755746.

Bashir:2021:CIB

[1626] Malik Zia Ullah Bashir and Rashid Ali. Cryptanalysis and improvement of a blind multi-document signcryption scheme. *Cryptologia*, 45(5):450–464, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1755913.

Smoot:2021:SMC

[1627] Betsy Rohaly Smoot. Sources and methods for cryptologic history: researching individuals (and the biography boom). *Cryptologia*, 45(5):465–473, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://

www.tandfonline.com/doi/full/10.1080/01611194.2021.1929567.

Christensen:2021:ROV

[1628] Chris Christensen. Review of *Operation Vengeance: The Astonishing Aerial Ambush That Changed World War II* by Dan Hampton. *Cryptologia*, 45(5):474–477, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1839816.

Lasry:2021:DPC

[1629] George Lasry, Beáta Megyesi, and Nils Kopal. Deciphering papal ciphers from the 16th to the 18th Century. *Cryptologia*, 45(6):479–540, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1755915.

Mastan:2021:CTS

[1630] J. Mohamedmoideen Kader Mastan and R. Pandian. Cryptanalysis of two similar chaos-based image encryption schemes. *Cryptologia*, 45(6):541–552, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1814447.

Griffiths:2021:CUE

[1631] Barry J. Griffiths. Cryptography in undergraduate education: perceptions of postgraduate students. *Cryptologia*, 45(6):553–562, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1804482.

Christensen:2021:RCB

[1632] Chris Christensen. Review of *The Codebreakers of Bletchley Park* by Dermot Turing. *Cryptologia*, 45(6):563–564, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1839814.

Christensen:2021:RCC

[1633] Chris Christensen. Review of *A Course in Cryptography* by Heiko Knospe. *Cryptologia*, 45(6):565–568, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1804483.

Christensen:2021:RUN

[1634] Chris Christensen. Review of *The U.S. Navy's On-the-Roof Gang, Volume Two, War in the Pacific* by Matt Zullo. *Cryptologia*, 45(6):569–570, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1878307.

Christensen:2021:RCP

[1635] Chris Christensen. Review of *Codebreaking: A Practical Guide* by Elonka Dunin and Klaus Schmeh. *Cryptologia*, 45(6):571–572, 2021. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1873207.

Bean:2022:EBL

[1636] Richard W. Bean, George Lasry, and Frode Weierud. Eavesdropping on the Biafra–Lisbon link — breaking historical ciphers from the Biafran war. *Cryptologia*, 46(1):1–66, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1762261`.

Blanchard:2022:PVV

[1637] Enka Blanchard, Ryan Robucci, Ted Selker, and Alan T. Sherman. Phrase-verified voting: Verifiable low-tech remote boardroom voting. *Cryptologia*, 46(1):67–101, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1975324`.

Kopal:2022:DTD

[1638] Nils Kopal and Michelle Waldispühl. Deciphering three diplomatic letters sent by Maximilian II in 1575. *Cryptologia*, 46(2):103–127, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1858370`.

Tuncer:2022:NCC

[1639] Türker Tuncer and Huseyin Yuce Kurum. A novel Collatz conjecture-based digital image watermarking method. *Cryptologia*, 46(2):128–147, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1821408`.

Edemskiy:2022:IEL

[1640] Vladimir Edemskiy, Chenhuang Wu, and Chunxiang Xu. Improvements on k-error linear complexity of q-ary sequences derived from Euler quotients. *Cryptologia*, 46(2):148–166, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1827312`.

Kalachi:2022:FSA

[1641] Hervé Talé Kalachi. On the failure of the smart approach of the GPT cryptosystem. *Cryptologia*, 46(2):167–182, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1829181`.

Christensen:2022:RUN

[1642] Chris Christensen. Review of *The U.S. Navy's On-the-Roof Gang, Volume One, Prelude to War* by Matt Zullo. *Cryptologia*, 46(2):183–184, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1839815`.

Christensen:2022:ROD

[1643] Chris Christensen. Review of *One Day in August* by David O'Keefe. *Cryptologia*, 46(2):185–192, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1901798`.

Christensen:2022:RGW

[1644] Chris Christensen. Review of *Geniuses at War: Bletchley Park, Colossus, and the Dawn of the Digital Age* by David A. Price. *Cryptologia*, 46(2):193–194, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1969702`.

Bouchaudy:2022:EXP

[1645] Jean-François Bouchaudy. Enigma, the XYZ period (1939–1940). *Cryptologia*, 46(3):195–271, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2020.1864681`.

Christensen:2022:RBBa

[1646] Chris Christensen. Review of *Before Bletchley Park: The Codebreakers of the First World War* by Paul Gannon. *Cryptologia*, 46(3):272–276, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1949760`.

Christensen:2022:RBBb

[1647] Chris Christensen. Review of *Backing Bletchley: The Codebreaking Outstations from Eastcote to GCHQ* by Ronald Koorm. *Cryptologia*, 46(3):277–279, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1969705`.

Christensen:2022:RMX

[1648] Chris Christensen. Review of *Madame X: The Story of '003', the U.S. Army Cryptologic Bombe in World War II* by Michael Barbakoff. *Cryptologia*, 46(3):280–283, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1949761`.

Christensen:2022:RIN

[1649] Chris Christensen. Review of *Images of the National Archives Codebreakers* by Stephen Twigge. *Cryptologia*, 46(3):284–286, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1950077`.

Christensen:2022:RRA

[1650] Chris Christensen. Review of *Reflections of Alan Turing: a Relative Story* by Dermot Turing. *Cryptologia*, 46(3):287–289, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1969703`.

Anonymous:2022:C

[1651] Anonymous. Correction. *Cryptologia*, 46(3):290, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2022.2061772`.

Relkin:2022:SOC

[1652] Paul W. Relkin. Solving the Olum 1 cipher. *Cryptologia*, 46(4):291–301,

2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1974124`.

Dunin:2022:HWS

[1653] Elonka Dunin, Magnus Ekhall, Konstantin Hamidullin, Nils Kopal, George Lasry, and Klaus Schmeh. How we set new world records in breaking Playfair ciphertexts. *Cryptologia*, 46(4):302–322, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1905734`.

Bonavoglia:2022:CRV

[1654] Paolo Bonavoglia. The ciphers of the Republic of Venice: an overview. *Cryptologia*, 46(4):323–346, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1901797`.

Chaum:2022:UPU

[1655] David Chaum, Mario Yaksetig, Alan T. Sherman, and Joeri de Ruiter. UDM: Private user discovery with minimal information disclosure. *Cryptologia*, 46(4):347–379, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1911876`.

Christensen:2022:RUU

[1656] Chris Christensen. Review of *USN & USMC WW II Cryptologists' Oral Histories; Voices from the past*, Volumes 1 and 2 by U.S. Naval Cryptologic Veterans Association. Volume 1 of 2 (A–L). 2019. 450 + vi pages, Softcover, \$16.95. ISBN 978-1-7988-8747-9. Volume 2 of 2 (M–Z). 2019. 365 + iv pages, Softcover, \$16.95. ISBN 978-1-7988-8811-7. *Cryptologia*, 46(4):380–381, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1969704`.

Christensen:2022:RRW

[1657] Chris Christensen. Review of *Radio War: The Secret Espionage War of the Radio Security Service 1938–1946* by David Abrutat. Fonthill Media, Stroud, Gloucestershire, UK. 2019. 192 pages, Hardcover, £25.00 (\$38.00). ISBN 978-1-78155-759-4. *Cryptologia*, 46(4):382–384, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2021.1969706`.

Christensen:2022:RBM

[1658] Chris Christensen. Review of *The Bombe: The Machine that Defeated Enigma* by Dermot Turing. Arcturus Publishing Limited, London, 2021. 64 pages, Trade paperback A-5, £11.20. ISBN 978-1-3988-1244-4. *Cryptologia*, 46(4):385–386, 2022. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/01611194.2022.2026840`.

Yardley:1934:BC

[1659] Herbert O. (Herbert Osborn) Yardley. *The Blonde Countess*. Longmans, Green and Co., New York, NY, USA, 1934. 3 + 314 pp. LCCN PZ3.Y20 Bl.

Sinkov:1968:ECM

[1660] Abraham Sinkov. *Elementary Cryptanalysis; a Mathematical Approach*, volume 22 of *New mathematical library*. Random House, New York, NY, USA, 1968. ix + 189 pp. LCCN Z104 .S47; Z104 .S617.

Kullback:1976:SMC

[1661] Solomon Kullback. *Statistical Methods in Cryptanalysis*, volume C-4 of *Cryptographic Series*. Aegean Park Press, Laguna Hills, CA, USA, 1976. ISBN 0-89412-006-9. vi + 206 pp. US$.

Hoffman:1977:MMC

[1662] Lance J. Hoffman. *Modern methods for computer security and privacy*. Prentice-Hall, Upper Saddle River, NJ 07458, USA, 1977. ISBN 0-13-595207-7. xiii + 255 pp. LCCN QA76.9.A25 H63.

Lewin:1978:UGWa

[1663] Ronald Lewin. *Ultra goes to war: the secret story*. Hutchinson, London, UK, 1978. ISBN 0-09-134420-4. 397 + 6 pp. LCCN D810.S7 L43 1978b. US$6.95.

Lewin:1978:UGWb

[1664] Ronald Lewin. *Ultra goes to war: the first account of World War II's greatest secret based on official documents*. McGraw-Hill, New York, NY, USA, 1978. ISBN 0-07-037453-8. 397 + 6 pp. LCCN D810.S7 L43 1978. US$12.95.

Reeds:1978:HCM

[1665] J. Reeds, D. Ritchie, and R. Morris. The Hagelin cypher machine (M-209): Cryptanalysis from ciphertext alone. Submitted to the journal Cryptologia, but never published. For the story behind the suppression of publication, see [1686]. Internal technical memoranda TM 78-1271-10, TM 78-1273-2., 1978.

Ennes:1979:ALT

[1666] James M. Ennes. *Assault on the Liberty: the true story of the Israeli attack on an American Intelligence ship*. Random House, New York, NY, USA, 1979. ISBN 0-394-50512-3. 299 + 8 pp. LCCN DS127.6.N3 E56; DS127.6.N3.E56.

McClellan:1979:NTD

[1667] James H. McClellan and Charles M. Rader. *Number theory in digital signal processing*. Prentice-Hall signal processing series. Prentice-Hall, Upper Saddle River, NJ 07458, USA, 1979. ISBN 0-13-627349-1. xii + 276 pp. LCCN TK5102.5 .M216 1979.

Konheim:1981:CP

[1668] Alan G. Konheim. *Cryptography, a primer*. John Wiley, New York, NY, USA, 1981. ISBN 0-471-08132-9. xiv + 432 pp. LCCN Z103 .K66.

Barker:1984:CSR

[1669] Wayne G. Barker. *Cryptanalysis of Shift Register Generated Stream Cipher Systems*, volume 39 of *Cryptographic Series*. Aegean Park Press, Laguna Hills, CA, USA, 1984. ISBN 0-89412-087-5. ???? pp. LCCN ????

Deavours:1985:MCM

[1670] Cipher A. Deavours and Louis Kruh. *Machine Cryptography and Modern Cryptanalysis*. The Artech House telecom library. Artech House Inc., Norwood, MA, USA, 1985. ISBN 0-89006-

161-0. xiv + 258 pp. LCCN Z103 .D43 1985.

Richelson:1985:UIC

[1671] Jeffrey Richelson. *The U.S. intelligence community*. Ballinger Pub. Co., Cambridge, MA, USA, 1985. ISBN 0-88730-024-3, 0-88730-025-1 (paperback). xxv + 358 pp. LCCN JK468.I6 R53 1985.

Richelson:1989:UIC

[1672] Jeffrey Richelson. *The U.S. intelligence community*. Ballinger Pub. Co., Cambridge, MA, USA, second edition, 1989. ISBN 0-88730-245-9, 0-88730-226-2 (paperback). xxvi + 485 pp. LCCN JK468.I6 R53 1989.

Lindstrom:1990:IEB

[1673] Lamont Lindstrom and Geoffrey M. (Geoffrey Miles) White. *Island encounters: black and white memories of the Pacific War*. Smithsonian Institution Press, Washington, DC, USA, 1990. ISBN 0-87474-457-1. viii + 194 pp. LCCN D769.9 .L56 1990.

Kahn:1991:SER

[1674] David Kahn. *Seizing the enigma: the race to break the German U-boat codes, 1939–1943*. Houghton-Mifflin, Boston, 1991. ISBN 0-395-42739-8. xii + 336 + 16 pp. LCCN D810.C88 K34 1991. US$24.95.

Rusbridger:1991:BPH

[1675] James Rusbridger and Eric Nave. *Betrayal at Pearl Harbor: how Churchill lured Roosevelt into World War II*. Summit Books, New York, NY, USA, 1991. ISBN 0-671-70805-8. 302 + 16 pp. LCCN D767.92 .R87 1991.

Hinsley:1993:CIS

[1676] F. H. (Francis Harry) Hinsley and Alan Stripp, editors. *Codebreakers: the inside story of Bletchley Park*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1993. ISBN 0-19-820327-6, 0-19-285304-X (paperback). xxi + 321 + 8 pp. LCCN D810.C88 M46 1993.

Kahn:1994:CBA

[1677] David Kahn. *Codebreaking and the Battle of the Atlantic*, volume 36 of *The Harmon memorial lectures in military history*. United States Air Force Academy, Colorado Springs, CO, USA, 1994. 16 pp. LCCN D770 .K26 1994.

Parker:1994:PHR

[1678] Frederick D. Parker. *Pearl Harbor revisited: United States Navy communications intelligence, 1924–1941*, volume 6 of *United States cryptologic history. Series 4, World War II*. National Security Agency, Center for Cryptologic History, Fort George G. Meade, MD, USA, 1994. v + 98 pp. LCCN D767.92 .P27 1994.

Johnson:1995:ACD

[1679] Thomas R. Johnson. *American Cryptology During the Cold War, 1945–1989. Book 1: The Struggle for Centralization, 1945–1960*. Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD, USA, 1995. iii + 59 pp. LCCN JZ5630 .J64 1995. URL `http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/nsa-1.pdf`.

Richelson:1995:UIC

[1680] Jeffrey Richelson. *The U.S. intelligence community*. Westview Press, Boulder, CO, USA, third edition, 1995. ISBN 0-8133-2355-6 , 0-8133-2376-2 (paperback). xix + 524 pp. LCCN JK468.I6 R53 1995. URL `http://www.loc.gov/catdir/enhancements/fy0832/94048474-b.html`.

Anonymous:1996:TAI

[1681] Anonymous. *The Twentieth Anniversary Index, 1977–1996*. Cryptologia, Department of Mathematical Sciences, United States Military Academy, West Point, NY 10996, USA, 1996. ISBN ???? ???? pp. LCCN ???? US$20.00.

Knap:1998:FLD

[1682] Hans Knap. *Forschungsstelle Langeveld: Duits afluisterstation in bezet Nederland. (Dutch) [Langeveld Research Center: German listening post in occupied Netherlands]*. Bataafsche Leeuw, Amsterdam, The Netherlands, 1998. ISBN 90-6707-467-5. 352 pp. LCCN D810.C7.

Erskine:1999:CDD

[1683] R. Erskine. Cipher A. Deavours, David Kahn, Louis Kruh, Greg Mellen, Brian J. Winkel (eds.), Selections from Cryptologia: History, People and Technology. *Intelligence and national security*, 14(3):247–??, 1999. CODEN ???? ISSN 0268-4527 (print), 1743-9019 (electronic).

Kidwell:1999:DRE

[1684] Peggy Aldrich Kidwell. Departments — reviews — electronic genie rescuing Prometheus; Forbes' greatest technology stories; information ages; the mathematical theory of communication; LEO: The incredible story of the world's first business; computer architects of the information society; Cryptologia; the supply of information technology workers in the US. *IEEE Annals of the History of Computing*, 21(4):81–84, October/December 1999. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic). URL `http://ieeexplore.ieee.org/iel5/85/17389/00801538.pdf`.

Richelson:1999:UIC

[1685] Jeffrey Richelson. *The U.S. intelligence community*. Westview Press, Boulder, CO, USA, fourth edition, 1999. ISBN 0-8133-6893-6 (paperback). xvi + 526 pp. LCCN JK468.I6 R53 1999. URL `http://www.loc.gov/catdir/enhancements/fy0831/98052830-b.html; http://www.loc.gov/catdir/enhancements/fy0831/98052830-d.html`.

Ritchie:19xx:DCW

[1686] Dennis M. Ritchie. Dabbling in the cryptographic world — a story. This undated note describes the interesting history behind the nonpublication of a paper [1665] on the Hagelin cypher machine (M-209), submitted to the journal Cryptologia, because of shadowy suggestions of a "retired gentleman from Virginia"., 19xx. URL `http://www.cs.bell-labs.com/~dmr/crypt.html`.

Freedman:2000:CBP

[1687] Maurice Freedman. *The Codebreakers, 1901–1945: Bletchley Park and the Second World War*. Leo Cooper, Lon-

don, UK, 2000. ISBN 0-85052-747-3. x + 190 pp. LCCN 940.548641.

Smith:2000:ECB

[1688] Michael Smith. *The Emperor's Codes: Bletchley Park and the breaking of Japan's secret ciphers*. Bantam, London, UK, 2000. ISBN 0-553-81320-x. 410 + 16 pp. LCCN 940.548641.

Stinnett:2000:DDT

[1689] Robert B. Stinnett. *Day of deceit: the truth about FDR and Pearl Harbor*. Free Press, New York, NY, USA, 2000. ISBN 0-684-85339-6 (hardcover). xiv + 386 pp. LCCN D767.92 .S837 2000.

Winterbotham:2000:USI

[1690] F. W. (Frederick William) Winterbotham. *The Ultra secret: the inside story of Operation Ultra, Bletchley Park and Enigma*. Orion, London, UK, 2000. ISBN 0-7528-3751-6. xv + 199 pp. LCCN 940.548641; M02.G00738.

Young:2000:EVL

[1691] Irene Young. *Enigma variations: love, war and Bletchley Park*. Mainstream Publishers, Edinburgh, Scotland, 2000. ISBN 1-84018-377-2 (paperback). 191 pp. LCCN D810.C88. URL `http://www.loc.gov/catdir/enhancements/fy0801/00456800-d.html`.

Anonymous:2001:DYI

[1692] Anonymous. Departments: For your information: Proof playright wins Pulitzer; call for mathematician mentors; 45th reunion conference for Ross program; undergraduate paper competitions in Cryptologia; volunteers sought for AWM essay contest; corrections. *Notices of the American Mathematical Society*, 48(6):607–608, 2001. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic).

Cristol:2002:LII

[1693] A. Jay Cristol. *The Liberty incident: the 1967 Israeli attack on the U.S. Navy spy ship*. Brassey's Inc., Washington, DC, USA, 2002. ISBN 1-57488-414-X. xx + 295 + 8 pp. LCCN DS127.6.N3.C74; DS127.6.N3.C74 2002.

Anonymous:2003:ADC

[1694] Anonymous. Alec Dakin: codebreaker who was among the first at Bletchley Park to see the news that Hitler was dead. *The Times [London, UK]*, page 1, 2003. ISSN 0140-0460, 0956-1382. URL `http://www.thetimes.co.uk/tto/archive/`.

Keen:2003:HDK

[1695] John Keen. *Harold 'Doc' Keen and the Bletchley Park bombe*. M and M Baldwin, Cleobury Mortimer, Kidderminster, England, 2003. ISBN 0-947712-42-9 (paperback). 89 pp. LCCN X07.F02423.

Luke:2003:MRB

[1696] Doreen Luke. *My road to Bletchley Park*. M and M Baldwin, Cleobury Mortimer, Kidderminster, England, 2003. ISBN 0-947712-44-5. 53 pp. LCCN X03.F01112.

Martin:2003:WMI

[1697] David C. Martin. *Wilderness of Mirrors: Intrigue, Deception, and the Secrets that Destroyed Two of the Cold War's Most Important Agents*. The Lyons Press, ????, 2003. ISBN 1-58574-824-2. 256 (est.) pp.

DeBrosse:2004:SBU

[1698] Jim DeBrosse and Colin B. Burke. *The secret in Building 26: the untold story of America's ultra war against the U-boat Enigma codes*. Random House, New York, NY, USA, 2004. ISBN 0-375-50807-4, 1-58836-353-8, 0-375-75995-6. xxix + 272 pp. LCCN D810.C88 D43 2004. URL http://www.loc.gov/catdir/samples/random045/2003058494.html; http://www.randomhouse.com/catalog/display.pperl?isbn=9781588363534.

Albert:2005:HAH

[1699] Nancy E. Albert. *A^3 and his algebra: how a boy from Chicago's West Side became a force in American mathematics*. iUniverse, New York, NY, USA, 2005. ISBN 0-595-32817-2. xiv + 349 pp. LCCN 01.50.

Hanyok:2005:EHH

[1700] Robert J. Hanyok. *Eavesdropping on Hell: Historical Guide to Western Communications Intelligence and the Holocaust, 1939–1945*, volume 9 of *United States cryptologic history. Series IV*. Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD, USA, second edition, 2005. v + 167 pp. LCCN D810.C88. URL http://purl.access.gpo.gov/GPO/LPS92209.

Loepp:2006:PIC

[1701] Susan Loepp and William Kent Wootters. *Protecting Information: From Classical Error Correction to Quantum Cryptography*. Cambridge University Press, Cambridge, UK, 2006. ISBN 0-521-82740-X (hardback), 0-521-53476-3 (paperback). xv + 287 pp. LCCN QA76.889.L64 2006; QA76.889.L64. URL http://www.loc.gov/catdir/enhancements/fy0632/2006002404-d.html; http://www.loc.gov/catdir/toc/ecip067/2006002404.html.

Pei:2006:ACC

[1702] Dingyi Pei. *Authentication codes and combinatorial designs*. Discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, 2006. ISBN 1-58488-473-8. viii + 244 pp. LCCN QA76.9.A25 P42 2006. URL http://www.loc.gov/catdir/enhancements/fy0647/2005026036-d.html; http://www.loc.gov/catdir/toc/ecip0518/2005026036.html.

Pelling:2006:CVS

[1703] Nick Pelling. *The curse of the Voynich: the secret history of the world's most mysterious manuscript*. Compelling Press, Surbiton, Surrey, UK, 2006. ISBN 0-9553160-0-6 (paperback). 230 pp. LCCN Z105.5.V65 P45 2006. URL http://www.loc.gov/catdir/toc/fy0711/2007386907.html.

Ratcliff:2006:DIE

[1704] R. A. Ratcliff. *Delusions of intelligence: Enigma, Ultra and the end of secure ciphers*. Cambridge University Press, Cambridge, UK, 2006. ISBN 0-521-85522-5. xvii + 314 pp. LCCN ????

Roth:2006:ICT

[1705] Ron M. Roth. *Introduction to coding theory*. Cambridge University Press, Cambridge, UK, 2006. ISBN 0-521-84504-1 (hardcover). xi + 566 pp. LCCN QA268 .R67 2006. URL http://www.loc.gov/catdir/

enhancements/fy0665/2006280936-d.html; http://www.loc.gov/catdir/enhancements/fy0665/2006280936-t.html; http://www.loc.gov/catdir/enhancements/fy0733/2006280936-b.html.

Stinson:2006:CTP

[1706] Douglas R. Stinson. *Cryptography: theory and practice*. Discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, third edition, 2006. ISBN 1-58488-508-4. 593 pp. LCCN ????

Talbot:2006:CCI

[1707] John Talbot and D. J. A. Welsh. *Complexity and cryptography: an introduction*. Cambridge University Press, Cambridge, UK, 2006. ISBN 0-521-85231-5, 0-521-61771-5. xii + 292 pp. LCCN Z103 .T35 2006. URL http://www.loc.gov/catdir/enhancements/fy0659/2006296276-d.html; http://www.loc.gov/catdir/enhancements/fy0659/2006296276-t.html; http://www.loc.gov/catdir/enhancements/fy0733/2006296276-b.html.

Watkins:2006:CLC

[1708] Gwen Watkins. *Cracking the Luftwaffe codes: the secrets of Bletchley Park*. Greenhill, London, UK, 2006. ISBN 1-85367-687-X (hardcover). 231 pp. LCCN M06.G01845.

Young:2006:MCC

[1709] Anne L. Young. *Mathematical ciphers: from Caesar to RSA*, volume 25 of *Mathematical world*. American Mathematical Society, Providence, RI, USA, 2006. ISBN 0-8218-3730-3. viii + 159 pp. LCCN ????

Bauer:2007:DSM

[1710] Friedrich Ludwig Bauer. *Decrypted secrets: methods and maxims of cryptology*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., fourth edition, 2007. ISBN 3-540-24502-2 (Springer Berlin). xii + 524 + 16 pp. LCCN ????

Denniston:2007:TSY

[1711] Robin Denniston and Alastair Guthrie Denniston. *Thirty secret years: A. G. Denniston's work in signals intelligence, 1914–1944*. Polperro Heritage Press, Clifton-upon-Teme, Worcestershire, UK, 2007. ISBN 0-9553648-0-9 (paperback). 172 pp. LCCN Z103.4.G7 D46 2007.

Huff:2007:HTS

[1712] P. J. Huff and J. G. Lewin. *How to tell a secret: tips, tricks, and techniques for breaking codes and conveying covert information*. Collins, London, UK, 2007. ISBN 0-06-113794-4. xi + 258 pp. LCCN UB247 .H84 2007. URL http://www.loc.gov/catdir/toc/fy0712/2006053036.html.

Johnson:2007:FIB

[1713] Kerry Johnson and John Gallehawk. *Figuring It Out at Bletchley Park 1939–1945*. BookTowerPublishing, ????, 2007. ISBN 0-9557164-0-3. 208 (est.) pp. LCCN M09.C03399.

Paterson:2007:VCB

[1714] Michael Paterson. *Voices from the Code Breakers: Personal Accounts of the Secret Heroes of World War II*. David & Charles, ????, 2007. ISBN 0-7153-2280-X. 288 (est.) pp.

Sheldon:2007:SBE

[1715] Rose Mary Sheldon. *Spies of the Bible: espionage in Israel from the Exodus to the Bar Kokhba revolt*. Greenhill Books, London, UK, 2007. ISBN 1-85367-636-5. 304 pp. LCCN DS121 .S54 2007.

Anderson:2008:SEG

[1716] Ross Anderson. *Security Engineering: a Guide to Building Dependable Distributed Systems*. John Wiley, New York, NY, USA, second edition, 2008. ISBN (cloth), 0-470-06852-3 (cloth). xl + 1040 pp. LCCN QA76.9.A25; QA76.9.A25 A54 2008. URL `http://www.loc.gov/catdir/enhancements/fy0827/2008006392-d.html`; `http://www.loc.gov/catdir/enhancements/fy0827/2008006392-t.html`.

Bamford:2008:SFU

[1717] James Bamford. *The Shadow Factory: the Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. Doubleday, New York, NY, USA, 2008. ISBN 0-385-52132-4. ix + 395 pp. LCCN UB256.U6.B38 2008; UB256.U6.B38.

Batey:2008:BL

[1718] Mavis Batey. *From Bletchley with love*. Bletchley Park Trust, Milton Keynes, UK, 2008. ISBN 1-906723-04-4. 39 pp. LCCN D810.C88 B372 2008.

Hanyok:2008:WWC

[1719] Robert J. Hanyok and David P. Mowry. *West Wind clear: cryptology and the Winds message controversy: a documentary history*, volume 10 of *United States cryptologic history. Series IV, World War II*. Center for Cryptologic History, National Security Agency, Fort Meade, MD, USA, 2008. xxi + 327 pp. LCCN D767.92 .H36 2008. URL `http://proquest.safaribooksonline.com/?uiCode=yaleu&xmlId=01120090001SI`.

Herivel:2008:HGM

[1720] John Herivel. *Herivelismus and the German military Enigma: Warsaw, May 1928 to Bletchley Park, May 1940*. M and M Baldwin, Cleobury Mortimer, Kidderminster, England, 2008. ISBN 0-947712-46-1. 144 pp. LCCN D810.C88 H47 2008.

Hoffstein:2008:IMC

[1721] Jeffrey Hoffstein, Jill Catherine Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Undergraduate texts in mathematics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 0-387-77993-0 (hardcover). xv + 523 pp. LCCN QA268 .H64 2008.

Koblitz:2008:RCJ

[1722] Neal Koblitz. *Random Curves: Journeys of a Mathematician*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-74077-5, 3-540-74078-3. 392 pp. LCCN QA29.K57.A3 2008.

Mahon:2008:DI

[1723] Tom (Thomas G.) Mahon and James Gillogly. *Decoding the IRA*. Mercier Press, Cork, Ireland, 2008. ISBN 1-85635-604-3. 348 pp. LCCN DA914 .M34 2008.

Mangrum:2008:MCS

[1724] Dennis L. Mangrum. *The mystic cipher: a story of the lost Rhoade's gold mine*. CFI, Springville, Utah, 2008. ISBN 1-59955-219-1. viii + 247 pp. LCCN PS3613.A537 M97 2008.

Nesbit:2008:UVU

[1725] Roy Conyers Nesbit. *Ultra versus U-Boats: Enigma decrypts in the National Archives*. Pen and Sword Military, Barnsley, UK, 2008. ISBN 1-84415-874-8 (hardcover). viii + 248 pp. LCCN D810.C88 N49 2008.

Richelson:2008:UIC

[1726] Jeffrey Richelson. *The U.S. intelligence community*. Westview Press, Boulder, CO, USA, fifth edition, 2008. ISBN 0-8133-4362-3. xvi + 592 pp. LCCN JK468.I6 R53 1999.

Shanahan:2008:REH

[1727] Phil Shanahan, Colin Grazier, Tony Fasson, and Tommy Brown. *The real Enigma heroes*. Tempus, Stroud, Gloucestershire, UK, 2008. ISBN 0-7524-4472-7. 223 pp. LCCN D810.C88 S53 2008.

Swenson:2008:MCT

[1728] Christopher Swenson. *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. John Wiley, New York, NY, USA, 2008. ISBN (cloth), 0-470-13593-X (cloth). xxviii + 236 pp. LCCN QA76.9.A25 S932 2008. URL `http://www.loc.gov/catdir/enhancements/fy0806/2007051636-d.html; http://www.loc.gov/catdir/enhancements/fy0808/2007051636-t.html; http://www.loc.gov/catdir/enhancements/fy0810/2007051636-b.html`.

Thirsk:2008:BPI

[1729] James W. Thirsk. *Bletchley Park: an inmate's story*. Galago, Bromley, UK, 2008. ISBN 0-946995-88-5 (paperback). 192 + 8 pp. LCCN ????

Aid:2009:SSU

[1730] Matthew M. Aid. *The Secret Sentry: the Untold History of the National Security Agency*. Bloomsbury Press, New York, NY, USA, 2009. ISBN 1-59691-515-3. viii + 423 + 8 pp. LCCN UB256.U6 2009. URL `04; 2; http://www.gbv.de/dms/bowker/toc/9781596915152.; http://www.loc.gov/catdir/toc/ecip0826/2008037442.; only`.

Bard:2009:AC

[1731] Gregory V. Bard. *Algebraic cryptanalysis*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-88757-1 (ebook), 0-387-88756-3. xxxiii + 356 pp. LCCN Z103 .B37 2009eb. URL `http://link.library.utoronto.ca/eir/EIRdetail.cfm?Resources__ID=896123&T=F`.

Cusick:2009:CBF

[1732] Thomas W. Cusick and Pantelimon Stănică. *Cryptographic Boolean Functions and Applications*. Elsevier Academic Press, Amsterdam, The Netherlands, 2009. ISBN 0-12-374890-9 (hardcover). xii + 232 pp. LCCN QA10.3 .C87 2009.

Dingman:2009:DRS

[1733] Roger Dingman. *Deciphering the Rising Sun: Navy and Marine Corps Codebreakers, Translators, and Interpreters in the Pacific War*. Naval In-

stitute Press, Annapolis, MD, USA, 2009. ISBN 1-59114-211-3. xx + 340 + 16 pp. LCCN D810.S7 2009. URL http://www.gbv.de/dms/bowker/toc/9781591142119.

Kranz:2009:MMC

[1734] Horst Kranz and Walter Oberschelp. *Mechanisches Memorieren und Chiffrieren um 1430: Johannes Fontanas Tractatus de instrumentis artis memorie*, volume 59 of *Boethius (Series); Wissenschaftsgeschichte*. Steiner, Stuttgart, Germany, 2009. ISBN 3-515-09296-X. 167 pp. LCCN BF383 .K77 2009.

Paar:2009:UCT

[1735] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-642-04100-0 (hardcover), 3-642-04101-9 (paperback). xviii + 372 pp. LCCN A76.9.A25 P437 2009.

Schmeh:2009:VBF

[1736] Klaus Schmeh. *Versteckte Botschaften: die faszinierende Geschichte der Steganografie. (German) [Hidden Messages. The Fascinating Story of Steganography]*. Telepolis. Heise, Hannover, Germany, 2009. ISBN 3-936931-54-2 (paperback). xi + 234 pp. LCCN ???? SFR 32.00; EUR 18.00.

Scott:2009:ALU

[1737] James (James M.) Scott. *The attack on the Liberty: the untold story of Israel's deadly 1967 assault on a U.S. spy ship*. Simon and Schuster, New York, NY, USA, 2009. ISBN 1-4165-5482-3. 374 pp. LCCN DS127.6.N3 S368 2009. URL http://www.loc.gov/catdir/enhancements/fy0908/2009015338-d.html; http://www.loc.gov/catdir/enhancements/fy0909/2009015338-s.html.

Sinkov:2009:ECM

[1738] Abraham Sinkov and Todd Feil. *Elementary Cryptanalysis: a Mathematical Approach*, volume 22 of *Anneli lax new mathematical library*. Mathematical Association of America, Washington, DC, USA, second edition, 2009. ISBN 0-88385-647-6. xiv + 212 pp. LCCN Z104 SIN 2009. URL http://www.loc.gov/catdir/enhancements/fy0914/2009927623-d.html; http://www.loc.gov/catdir/enhancements/fy0914/2009927623-t.html.

Aldrich:2010:GUS

[1739] Richard J. (Richard James) Aldrich. *GCHQ: the uncensored story of Britain's most secret intelligence agency*. Harper Press, London, UK, 2010. ISBN 0-00-727847-0 (hardcover), 0-00-731265-2 (paperback). xxi + 666 + 16 pp. LCCN UB251.G7 A53 2010.

Batey:2010:DMW

[1740] Mavis Batey. *Dilly: the man who broke Enigmas*. Biteback, London, UK, 2010. ISBN 1-906447-15-2 (paperback). 256 (est.) pp. LCCN ???? US$9.99.

Gannon:2010:IRC

[1741] Paul Gannon. *Inside Room 40: the codebreakers of World War I*. Ian Allen Publishers, Hersham, Surrey, UK, 2010. ISBN 0-7110-3408-7. 287 + 8 pp. LCCN D639.S7 G36 2010x.

McKay:2010:SLB

[1742] Sinclair McKay. *The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there*. Aurum, London, UK, 2010. ISBN 1-84513-539-3 (hardcover). vi + 336 + 8 pp. LCCN D810.C88 M35 2010x.

Perera:2010:IES

[1743] Tom Perera. *Inside Enigma: The Secrets of the Enigma Machine and Other Historic Cipher Machines*. Radio Society of Great Britain, Bedford, UK, 2010. ISBN 1-905086-64-4. 206 (est.) pp. LCCN ????

Briggs:2011:SDC

[1744] Asa Briggs. *Secret days: code-breaking in Bletchley Park*. Frontline Books, London, UK, 2011. ISBN 1-84832-615-7. xix + 202 + 26 pp. LCCN D810.C88 B75 2011.

Carlson:2011:JRW

[1745] Elliot Carlson. *Joe Rochefort's war: the odyssey of the codebreaker who outwitted Yamamoto at Midway*. Naval Institute Press, Annapolis, MD, US, 2011. ISBN 1-61251-060-4 (hardcover). ???? pp. LCCN D774.M5 C28 2011.

Erskine:2011:BPC

[1746] Ralph Erskine and Michael Smith. *The Bletchley Park codebreakers*. Biteback, London, UK, 2011. ISBN 1-84954-078-0. xvi + 495 pp. LCCN ????

Kapera:2011:SPD

[1747] Zdzisław Jan Kapera. *In the Shadow of Pont du Gard: the Polish Enigma in Vichy France (June 1940 to November 1942)*, volume 7 of *The Enigma Bulletin*. The Enigma Press, Kraków, Poland, 2011. ISBN 83-86110-72-4. ISSN 0867-8693. 111 + 1 + 16 pp. LCCN ????

McGrayne:2011:TWH

[1748] Sharon Bertsch McGrayne. *The theory that would not die: how Bayes' rule cracked the Enigma code, hunted down Russian submarines, and emerged triumphant from two centuries of controversy*. Yale University Press, New Haven, CT, USA, 2011. ISBN 0-300-16969-8. xiii + 320 pp. LCCN QA279.5 .M415 2011.

McKay:2011:SLB

[1749] Sinclair McKay. *The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there*. Gardners Books, 2011. ISBN 1-84513-633-0. ???? pp. LCCN ????

Pearson:2011:NWC

[1750] Joss Pearson, editor. *Neil Webster's cribs for victory: the untold story of Bletchley Park's secret room*. Polperro Heritage, Clifton-upon-Teme, UK, 2011. ISBN 0-9559541-8-5 (paperback). ???? pp. LCCN ????

Rejewski:2011:WZM

[1751] Marian Rejewski. *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego w latach 1930–1945. (Polish) [Memories of my work at the Cipher Bureau of the General Staff Second Department 1930–1945]*. Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań, Poland, 2011. ISBN 83-232-2237-1. 160 + 18 + 157 + 1 pp. LCCN Z103.4.P7 R45 2011.

Smith:2011:SSX

[1752] Michael Smith. *The secrets of Station X: how the Bletchley Park codebreakers helped win the war*. Biteback Pub., London, UK, 2011. ISBN 1-84954-095-0 (paperback). 328 + 16 pp. LCCN D810.C88 S659 2011.

Stallings:2011:CNS

[1753] William Stallings. *Cryptography and network security: principles and practice*. Prentice-Hall, Upper Saddle River, NJ 07458, USA, fifth edition, 2011. ISBN 0-13-609704-9. xxiii + 719 pp. LCCN TK5105.59 .S713 2011.

Stanoyevitch:2011:ICM

[1754] Alexander Stanoyevitch. *Introduction to Cryptography: with Mathematical Foundations and Computer Implementations*. Discrete mathematics and its applications. Chapman and Hall/CRC, Boca Raton, FL, USA, 2011. ISBN 1-4398-1763-4 (hardcover). xix + 649 pp. LCCN QA268 .S693 2010.

Webb:2011:SPB

[1755] Charlotte Webb. *Secret Postings: Bletchley Park to the Pentagon*. BookTower, Redditch, Worcestershire, UK, 2011. ISBN 0-9557164-1-1 (paperback). 71 pp. LCCN ???? £6.99.

Gilbert:2012:WWO

[1756] James L. (James Leslie) Gilbert. *World War I and the origins of U.S. military intelligence*. Scarecrow Press, Lanham, MD, USA, 2012. ISBN 0-8108-8459-3 (hardcover), 0-8108-8460-7 (e-book). x + 245 pp. LCCN UB251.U5 G55 2012.

Gleick:2012:IHT

[1757] James Gleick. *The information: a history, a theory, a flood*. Fourth Estate, London, UK, 2012. ISBN 0-00-722574-1 (paperback). 526 pp. LCCN ????

Goresky:2012:ASR

[1758] Mark Goresky and Andrew Klapper. *Algebraic Shift Register Sequences*. Cambridge University Press, Cambridge, UK, 2012. ISBN 1-107-01499-9 (hardcover). xv + 498 pp. LCCN QA267.5.S4 G64 2012.

Grey:2012:DOB

[1759] Christopher Grey. *Decoding organization: Bletchley Park, codebreaking and organization studies*. Cambridge University Press, Cambridge, UK, 2012. ISBN 1-107-00545-0 (hardcover). xviii + 322 pp. LCCN D810.C88 G74 2012. URL `http://assets.cambridge.org/97811070/05457/cover/9781107005457.jpg`.

Sloan:2012:MPH

[1760] Robin Sloan. *Mr. Penumbra's 24-hour bookstore: a novel*. Farrar, Straus and Giroux, New York, NY, USA, 2012. ISBN 0-374-21491-3, 0-374-70883-5 (e-book). 288 pp. LCCN PS3619.L6278 M77 2012.

Bauer:2013:SHS

[1761] Craig P. Bauer. *Secret history: the story of cryptology*, volume 76 of *Discrete mathematics and its applications*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 2013. ISBN 1-4665-6186-6 (hardback). xxv + 594 pp. LCCN QA76.9.A25 B384 2013.

Borrmann:2013:HTA

[1762] Donald A. Borrmann et al. *The History of Traffic Analysis: World War I–Vietnam*. Penny Hill Press Inc., ????, 2013. ISBN ???? 48 (est.) pp. LCCN ????

Brown:2013:I

[1763] Dan Brown. *Inferno*. Bantam Press, London, UK, 2013. ISBN 0-593-07249-9. x + 461 pp. LCCN ????

Brown:2013:IN

[1764] Dan Brown. *Inferno: a novel*. Doubleday, New York, NY, USA, 2013. ISBN 0-385-53785-9 (hardback). x + 461 pp. LCCN PS3552.R685434 I54 2013.

Budiansky:2013:BW

[1765] Stephen Budiansky. *Blackett's war*. Alfred A. Knopf, New York, NY, USA, 2013. ISBN 0-307-59596-X. 306 pp. LCCN D810.R33 B79 2013.

Cheevers:2013:AWL

[1766] Jack Cheevers. *Act of war: Lyndon Johnson, North Korea, and the capture of the spy ship Pueblo*. NAL Caliber, New York, NY, USA, 2013. ISBN 0-451-46619-5 (hardcover). xiv + 431 + 16 pp. LCCN VB230 .C44 2013.

Dooley:2013:BHC

[1767] John F. Dooley. *A brief history of cryptology and cryptographic algorithms*. SpringerBriefs in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2013. ISBN 3-319-01628-8 (ebook). ISSN 2191-5768. xii + 99 pp. LCCN QA76.9.A25.

Fox:2013:RLQ

[1768] Margalit Fox. *The riddle of the labyrinth: the quest to crack an ancient code*. Ecco, An imprint of HarperCollins Publishers, New York, NY, USA, 2013. ISBN 0-06-222883-8 (hardcover), 0-06-222888-9 (e-book). xx + 363 pp. LCCN P1038 .F69 2013. URL `http://www.loc.gov/catdir/enhancements/fy1406/2013404394-b.html`.

Kapera:2013:MRM

[1769] Zdzisław Jan Kapera. *Marian Rejewski: the man who defeated "Enigma"*, volume 8 of *The Enigma bulletin*. The Enigma Press, Kraków, Poland, 2013. ISBN 83-86110-72-4. 111 pp. LCCN ????

McKay:2013:LWB

[1770] Sinclair McKay. *The lost world of Bletchley Park: the official illustrated history of the wartime codebreaking centre*. Aurum Press, London, UK, 2013. ISBN 1-78131-191-9 (hardcover), 1-78131-279-6 (e-book). 192 pp. LCCN D810.C88 M39 2013.

Munson:2013:GFT

[1771] Richard Munson. *George Fabyan: the tycoon who broke ciphers, ended wars, manipulated sound, built a levitation machine, and organized the modern research center*. Porter Books, ????, 2013. ISBN 1-4903-4562-0 (paperback). iii + 185 pp. LCCN ????

Showell:2013:DUB

[1772] Jak P. Mallmann Showell. *Dönitz, U-boats, convoys: the British version of his memoirs from the Admiralty's secret anti-submarine reports*. Frontline

Books, London, UK, 2013. ISBN 1-84832-701-3 (hardcover). xvi + 208 + 16 pp. LCCN D781 .S536 2013.

Sloan:2013:MPH

[1773] Robin Sloan. *Mr. Penumbra's 24-hour bookstore*. Atlantic Books, London, UK, 2013. ISBN 1-78239-119-3, 1-78239-120-7 (e-book). 291 pp. LCCN ????

Wagstaff:2013:JF

[1774] Samuel S. Wagstaff, Jr. *The joy of factoring*, volume 68 of *Student mathematical library*. American Mathematical Society, Providence, RI, USA, 2013. ISBN 1-4704-1048-6 (paperback). xiv + 293 pp. LCCN QA241 .W29 2013.

Greenberg:2014:GWB

[1775] Joel Greenberg. *Gordon Welchman: Bletchley Park's architect of ultra intelligence*. Frontline Books, Barnsley, UK, 2014. ISBN 1-84832-752-8 (hardcover). xvi + 286 + 16 pp. LCCN TK5102.94 .G744 2014x.

Kraft:2014:INT

[1776] James S. Kraft and Lawrence C. Washington. *An introduction to number theory with cryptography*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 2014. ISBN 1-4822-1441-5 (hardcover). xviii + 554 pp. LCCN QA241 .K73 2014.

Macrakis:2014:PLS

[1777] Kristie Macrakis. *Prisoners, lovers, and spies: the story of invisible ink from Herodotus to al-Qaeda*. Yale University Press, New Haven, CT, USA, 2014. ISBN 0-300-17925-1 (hardcover). xiv + 377 pp. LCCN Z104.5 .M33 2014.

Ramsden:2014:UMC

[1778] Dave Ramsden. *Unveiling the Mystic Ciphers: Thomas Anson and the Shepherd's Monument Inscription*. CreateSpace Independent Publishing, ????, 2014. ISBN 1-5031-1988-2. 128 [est.] pp. LCCN ????

Rempe-Gillen:2014:PTB

[1779] Lasse Rempe-Gillen and Rebecca Waldecker. *Primality testing for beginners*, volume 70 of *Student mathematical library*. American Mathematical Society, Providence, RI, USA, 2014. ISBN 0-8218-9883-3. xii + 244 pp. LCCN QA241 .R45813 2014.

Corera:2015:ISH

[1780] Gordon Corera. *Intercept: the secret history of computers and spies*. Weidenfeld and Nicolson, London, UK, 2015. ISBN 1-78022-784-1 (paperback), 0-297-87173-0 (hardcover), 0-297-87174-9 (e-pub). xiv + 431 pp. LCCN JN329.I6 C67 2015.

Hesselmann:2015:SSG

[1781] Peter Hesselmann. *Simpliciana: Schriften der Grimmelshausen-Gesellschaft XXXVI (2014)*, volume 36 of *Simpliciana*. Peter Lang, Bern, Switzerland, 2015. ISBN 3-0343-1667-4, 3-0351-0831-5 (e-book). LCCN PT1732. URL `http://alltitles.ebrary.com/Doc?id=11054400; http://lib.myilibrary.com?id=783274; http://public.eblib.com/choice/PublicFullRecord.aspx?p=2049038`.

Johnson:2015:NGA

[1782] Kevin Wade Johnson. *The neglected giant: Agnes Meyer Driscoll*, volume Volume 10 of *Center for Crypto-*

logic History special series. National Security Agency, Center for Cryptologic History, Fort George G. Meade, MD, USA, 2015. 66 pp. LCCN Z103. URL `http://purl.fdlp.gov/GPO/gpo73633`.

Kapera:2015:TZS

[1783] Zdzisław Jan Kapera. *The triumph of Zygalski's sheets: the Polish Enigma in the early 1940*, volume 9 of *The Enigma bulletin*. Enigma Press, Kraków, Poland, 2015. ISBN 83-86110-79-1 (paperback). ISSN 0867-8693. 221 + xvi pp. LCCN D810.C88 K374 2015. URL `http://scans.hebis.de/35/63/02/35630244_toc.pdf`.

Maffeo:2015:UNC

[1784] Steven E. Maffeo. *U.S. Navy codebreakers, linguists, and intelligence officers against Japan, 1910–1941: a biographical dictionary*. Rowan and Littlefield, Lanham, MD, USA, 2015. ISBN 1-4422-5563-3 (hardcover), 1-4422-5564-1. xxxiii + 540 pp. LCCN D810.S7 M2535 2015.

Mucklow:2015:SEI

[1785] Timothy J. (Timothy Jones) Mucklow. *The SIGABA/ECM II Cipher Machine: "a beautiful idea"*. National Security Agency, Center for Cryptologic History, Fort George G. Meade, MD, USA, 2015. 44 pp. LCCN ???? URL `http://purl.fdlp.gov/GPO/gpo58671`.

Turing:2015:PAT

[1786] Dermot Turing. *Prof: Alan Turing decoded: a biography*. The History Press, Stroud, Gloucestershire, UK, 2015. ISBN 1-84165-643-7 (print), 0-7509-6524-X (e-book). 319 pp. LCCN QA29.T8 T78 2015.

Dooley:2016:CCS

[1787] John F. Dooley. *Codes, ciphers and spies: tales of military intelligence in World War I*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2016. ISBN 3-319-29414-8 (paperback), 3-319-29415-6 (e-book). xvii + 280 + 39 pp. LCCN D639.C75 D66 2016.

McKay:2016:BPS

[1788] Sinclair McKay. *Bletchley Park: the Secret Archives*. Aurum Press, produced in association with Bletchley Park, London, UK, 2016. ISBN 1-78131-534-5 (hardcover). 176 pp. LCCN D810.C88 M388 2016.

Deavours:1987:CYT

[1789] Cipher A. Deavours, David Kahn, Louis Kruh, and Greg Mellen, editors. *Cryptology yesterday, today, and tomorrow*. The Artech House communication and electronic defense library. Artech House Inc., Norwood, MA, USA, 1987. ISBN 0-89006-253-6. xi + 519 pp. LCCN Z103.C76 1987. US$60.00. First volume of selected papers from issues of Cryptologia.

Deavours:1989:CMH

[1790] Cipher A. Deavours, David Kahn, et al., editors. *Cryptology: machines, history, & methods*. Artech House Inc., Norwood, MA, USA, 1989. ISBN 0-89006-399-0. x + 508 pp. LCCN Z103 .C75 1989. Second volume of selected papers from issues of Cryptologia.

Richelson:1990:UIC

[1791] Jeffrey Richelson, editor. *The U.S. intelligence community: organization, operations, and management, 1947–1989*. Chadwyck-Healey, Alexandria, VA, USA, 1990. 266 pp. LCCN JK468.I6 1990.

Love:1995:PHR

[1792] Robert William Love, editor. *Pearl Harbor revisited*. The Franklin and Eleanor Roosevelt Institute series on diplomatic and economic history. St. Martin's Press, New York, NY, USA, 1995. ISBN 0-312-09593-7. viii + 200 pp. LCCN D767.92 .P3985 1995.

Deavours:1998:SCH

[1793] Cipher A. Deavours, David Kahn, Louis Kruh, Greg Mellen, and Brian J. Winkel, editors. *Selections From Cryptologia: History, People, And Technology*. The Artech House telecommunications library. Artech House Inc., Norwood, MA, USA, February 1998. ISBN 0-89006-862-3. vii + 552 pp. LCCN Z103.S45 1998. US$78.20. URL `http://www.opengroup.com/open/cbbooks/089/0890068623.shtml`. Third volume of selected papers from issues of Cryptologia.

Winkel:2005:GEC

[1794] Brian J. Winkel, Cipher A. Deavours, David Kahn, and Louis Kruh, editors. *The German Enigma cipher machine: Beginnings, Success, and Ultimate Failure*. Artech House computer security series. Artech House Inc., Norwood, MA, USA, 2005. ISBN 1-58053-996-3. x + 439 pp. LCCN D810.C88 G47 2005. US$95.00.

deLeeuw:2007:HIS

[1795] Karl de Leeuw and J. A. Bergstra, editors. *The History of Information Security: a Comprehensive Handbook*. Elsevier, Amsterdam, The Netherlands, 2007. ISBN 0-444-51608-5 (hardcover). xi + 887 pp. LCCN Z103 .H63 2007. URL `http://www.sciencedirect.com/science/book/9780444516084`.

Buhler:2008:ANT

[1796] Joe P. Buhler and P. Stevenhagen, editors. *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Mathematical Sciences Research Institute publications*. Cambridge University Press, Cambridge, UK, 2008. ISBN 0-521-80854-5 (hardback). x + 652 pp. LCCN QA241.A426; QA241.A426 2008.

Cooper:2013:ATH

[1797] S. Barry Cooper and Jan van Leeuwen, editors. *Alan Turing — His Work and Impact*. Elsevier Science, Inc., Amsterdam, The Netherlands, 2013. ISBN 0-12-386980-3 (hardcover). xxi + 914 pp. LCCN QA29.T8 C65 2013. URL `http://amzn.to/VS1tdc; http://store.elsevier.com/product.jsp?isbn=9780123869807; http://www.mathcomp.leeds.ac.uk/turing2012/give-page.php?300`.

Turing:2021:RAT

[1798] Dermot Turing. *Reflections of Alan Turing: a relative story*. The History Press, Gloucestershire, UK, 2021. ISBN 0-7509-9609-9 (hardcover), 0-7509-9707-9 (ePub e-book). 207 pp. LCCN QA29.T8 T87 2021.