{tag}

{/tag}

International Journal of Computer Applications

Volume 105 - Number 16

Year of Publication: 2014

Authors:

Nikita Somani

Dharmendra Mangal

10.5120/18461-9820

{bibtex}pxc3899820.bib{/bibtex}

Abstract

Paper introduced RSA cryptosystem and its security aspects. RSA is a public key algorithm that applied widely in the field of information security in the Internet-Banking and E-Commerce applications. The proposed scheme for RSA cryptosystem contains three prime numbers and overcome several attack possible on RSA. The proposed scheme has speed improvement on RSA decryption side by using the Chinese Reminder Theorem (CRT) and the scheme is semantically secure also.

References

- W. Diffie and M. Hellman, "New Direction in Cryptography," IEEE Transaction on Information Theory, vol. 22, pp. 644-654, 1976.
- R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public-key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
- R. C. Merkle, "Secure Communications over Insecure Channels," Communications of the ACM, vol. 21, no. 4, pp. 294-299, 1978.

- A. Al-Hasib and A. A. M. Mahmudul Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," in IEEE Third International Conference on Convergence and Hybrid Information Technology, 2008.
- S. B. Sasi, D. Dixon and J. Wilson, "A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security," IOSR Journal of Engineering, vol. 4, no. 3, 2014.
- G. R. Blakey, "A Computer Algorithm for Calculating the Product AB Modulo M," IEEE Transaction on Computers, vol. 32, no. 5, pp. 497-500, 1983.
- N. Pabhopote and V. Laohakosol, "Cobinatorial Aspects of the Generalized Euler's Totient," International Journal of Mathematics and Mathematical Science, pp. 1-15, 2010.
- L. Harn, "Public-Key Cryptosystem Design Based on Factoring and Discrete Logarithms," IEE Proceedings: Computers and Digital Techniques, vol. 144, no. 3, pp. 193-195, 1994.
- T. Beth and D. Gollmann, "Algorithm Engineering for Public Key Algorithms," IEEE Journal on selected areas in communications, vol. 7, no. 4, pp. 458-465, 1989.
- D. Boneh, "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, vol. 46, no. 2, pp. 203-213, 1999.
- J. J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," Electronic Letters, vol. 18, no. 21, pp. 905-907, 1982.
- A. Fait, "Batch RSA," Advance in Cryptology CRYPTO '89, vol. 435, pp. 175-185, 1989.
- D. Boneh and H. Shacham, "Fast Variants of RSA," CryptoBytes, vol. 5, no. 1, pp. 1-10, 2002.
- T. Collins, D. Hopkins, S. Langford and M. Sabin, "Public Key Cryptographic Apparatus and Method". US Patent #5848, 1997.
- [T. Takagi, "Fast RSA-type Cryptosystem Modulo pkq," Advances in Cryptology - CRYPTO '98, vol. 1462, pp. 318-326, 1998.
- C. A. M. Paixon, "An efficient variant of the RSA cryptosystem," Cryptology ePrint Archive, 2002.
- D. Garg and S. Verma, "Improvement over Public Key Cryptographic Algorithm," in IEEE International Advance Computing Conference, Patiala, 2009.
- A. H. Al-Hamami and I. A. Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm," IEEE International Conference on Advanced Computer Science Applications and Technologies, pp. 402-408, 2012.
- Y. Desmedt and A. M. Odlyzko, "A Chosentext Attack on RSA Cryptosystem and some Discrete Logarithm Schemes," Advances in Cryptology CRYPTO '85, vol. 218, pp. 5116-521, 1986.
- R. Kumar, "Security Analysis and Implementation of an Improved Cch2 Proxy Multi-Signature Scheme," International journal of computer network and Information security, vol. 4, pp. 46-54, 2014.
- P. C. Kocher, "Timing Attacks on Implementations of Dif?e-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology-CRYPTO '96, pp. 104-113, 1996.
- M. Wiener, "Cryptanalysis of Short RSA Secret Exponents," IEEE Transaction Information Theory, vol. 36, no. 3, pp. 553-558, 1990.

- D. Coppersmith, "Small Solutions to Polynomial Equations and Low Exponent RSA Vulnerabilities," Journal of Cryptology, vol. 10, pp. 233-260, 1997.
- D. Gordon, "Discrete Logarithms in GF(p) using the Number Field Sieve," SIAM J. Discrete Math, vol. 6, pp. 124-138, 1993.
- A. Shamir and E. Tromer, "Factoring Large Numbers with the TWIRL Device," Proceedings, CRYPTO, LNCS 2729, pp. 1-26, 2003.

Index Terms

Computer Science Security

Keywords

Cryptography Prime Numbers RSA Cryptosystem Security analysis