Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CRYPTANALYTIC ATTACKS ON RIVEST, SHAMIR, AND ADLEMAN (RSA) CRYPTOSYSTEM: ISSUES AND CHALLENGES

[1]ADAMU ABUBAKAR, [2]SHEHU JABAKA, [3]BELLO IDRITH TIJJANI, [1]AKRAM ZEKI, [4]HARUNA CHIROMA, [5]MOHAMMED JODA USMAN, [1]SHAKIRAT RAJI, [1]MURNI MAHMUD

[1]Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University; Malaysia
[2] Department of Computer Science, Federal College of Education(Technical)Gusau, Zamfara State Nigeria.
[3]Department of Physics, Faculty of Sciences, Bayero University Kano, Nigeria
[4]Department of Artificial Intelligence, Faculty of Computer Science and Information Technology, University Malaya, Malaysia
[5]School of Electronics and Information Engineering, Liaoning University of Technology, Jinzhou, China

E-mail: [1]100adamu@gmail.com, [2] smjabaka2@gmail.com, [3]idrithtijjani@gmail.com, [1]akramzeki@iium.edu.my , [4]freedonchi@yahoo.com , [5]usmanjoda1@yahoo.com, [1]peacefultosin@hotmail.com, [1]murni@iium.edu.my

ABSTRACT

RSA cryptosystem is an information security algorithm used for encrypting and decrypting of digital data in order to protect the content of the data and to ensure its privacy. Prior research studies have shown that RSA algorithm is very successful in protecting enterprises commercial services and systems as well as web servers and browsers to secure web traffic. In an email application, it's utilized to ensure the privacy and authenticity of email message. Some studies have also shown the efficiency of RSA algorithm in securing remote login sessions, and electronic credit-card payment systems. Generally RSA algorithm gain a security support because of it's frequently use in most applications where security of digital data is mostly a concern. Its strength lies with its ability of withstanding many forms of attacks. While many studies focus on proving that RSA algorithm is breakable under certain cryptanalytic attacks, yet there are some confrontations on the circumstances of applying those attacks. This paper presents the issues and challenges on some key aspects of cryptanalytic attacks on RSA algorithm. The paper also explores the perceived vulnerabilities of implementing RSA algorithm which can render a cryptanalyst easier means of attack.

Keywords: *RSA Cryptosystem, Cryptanalysis, Cryptanalytic Attacks*

1. INTRODUCTION

The onward increase in information and communication technology tools and services, drive enterprises to rely heavily on network applications and resources to conduct business and service. . Information security is very important in ensuring the success of businesses and the interconnected networks of that make business transaction possible. Here there are two security considerations in terms of the security of the connecting devices and the security of information that is required to be send through these connecting devices. The securities of these networks are closely tied to cryptography. Thus cryptography is a discipline that concerns the techniques of encryption and decryption of bits.

RSA is the first practical public-key cryptosystem named after its inventors Rivest, Shamir, and Adleman [1]. It allow for an encryption and decryption of data used mainly in during transmission over communication medium between two parties by the use of two keys, namely private key and the public key which lock and unlock data respectively. The source of the data used the receiver's public key to encrypt the data and send it over, and the receiver will have to use his private key to decrypt the data. Thus, only private key decrypt a data. RSA cryptosystem is widely used for both network and information security, where its implementation is seen in web

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

servers and browsers to secure web traffic [2], and ensure privacy and authenticity of Email, as well as providing secure remote login sessions. In online business the use of electronic credit-card payment systems is increasing, RSA cryptosystem is also applied to the electronic credit-card payment systems. Many applications that uses digital data requires tight security, RSA cryptosystem is used in most of these applications since the security of digital data considered to be very important. RSA cryptosystem gain a lot of trust from many enterprises and business, unfortunately, it suffers from some of cryptanalytic attacks [2-3]. Cryptanalysis is a terminology that indicates a way of unveiling the secret of a cryptographic algorithm. Thus in cryptography, particularly in encryption and decryption technique of plain text/cipher text, Cryptanalysts main concern is to reveal the plain text from the cipher text without prior knowledge of a decryption key [1-2] the plain text refer to the original text, while the cipher text is the encrypted text. Having the feelings that RSA cryptosystem is vulnerable to cryptanalytic attacks, researchers interest turn to find out the degree of weakness and strength of any attack on RSA cryptosystem. .

In the world of universal electronic connectivity, having protection and security are indeed a critical matter. Information and network security measures are required for the protection of data during their transmission as well as the transmission tools and resources.RSA cryptosystem has been analyzed for its possible weaknesses [2]. In some situation where there is an intension of attacking RSA cryptosystem will turn out to served as a prove of its strengths rather than weaknesses; however, there are records of other fascinating attacks on it. This paper aims at analyzing the different cryptanalytic attacks on RSA cryptosystem. Research into cryptanalysis attacks on the RSA system will be able to identify the complex ways in which attackers can break or compromise the implementation of the RSA system, and provide the necessary countermeasures for more secure design and the implementation of the RSA cryptosystem [2-3].

It is very important to the computing community to trace the existing prove that an encryption system is secure. It also critical to uncover the test available to see whether anyone can think of a way to break an encryption system In view of this statement, It is important to take any form cryptanalytic attack on RSA cryptosystem serious and identify its strength and weakness, this will no doubt identify the intricate ways in which attackers can break or compromise the implementation of the any encryption system. As a result, This paper review the issues and challenges on cryptanalytic attacks on RSA cryptosystem.

The remaining sections of this paper are 4. Section 2 present the RSA cryptosystem, section 3 discusses the evaluation of the strengths of cryptanalytic attacks on RSA cryptosystem, section 4. Section present the classification of cryptanalytic attacks on RSA cryptosystem, finally, Section 5 is the conclusion of the entire paper.

2. RSA CRYPTOSYSTEM

Rivest-Shamir-Adleman (RSA) is a special type of public key cryptography which over the year's has reigned supreme as the most widely accepted and implemented general-purpose approach public-key encryption techniques [4-7]. The RSA algorithm follows a block cipher encryption technique, in which the plaintext and the cipher are integers between 0 and n – 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 21024 [8].

The RSA cryptosystem (see Figure 1) is based on modular exponentiation modulo of the product of two large primes. Each individual has an encryption key consisting of a modulus n = pq where p and q are large prime numbers, with large digits each, and an exponent e that is relatively prime to (p - 1) (q - 1).

To produce a usable key, two large primes must be found. This can be done quickly on a computer using probabilistic primality tests. However, the product of these primes n= pq, with approximately 500 digits, cannot be factored in a reasonable length of time. In the RSA encryption method, messages are translated into sequences of integers. This can be done by translating each letter into an integer, as is done with the Caesar cipher [8].

Journal of Theoretical and Applied Information Technology
10th March 2014. Vol. 61 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

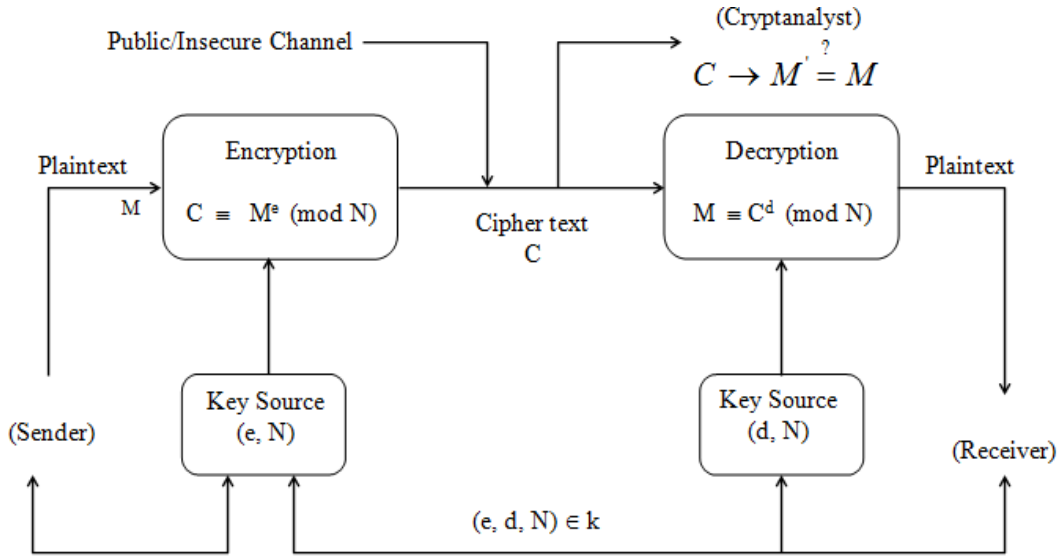

Figure 1. RSA Public Key Cryptography [8]

These integers are grouped together to form larger integers, each representing a block of letters. The encryption proceeds by transforming the integer M, representing the plain-text (the original message), to an integer C, representing the ciphertext (the encrypted message).

RSA algorithm that generate public-key/private-key pair are given by the following algorithm:

Input: A pair of prime number *p* and *q*
Output Public key (*n*, *e*) and private key (*n*, *d*).

Generate a pair of large, random prime number *p* and *q*.

for *n* = *pq*
Compute the modulus *n*
break
for e = odd public exponent
Select *e* between 3 and *n*-1 that is relatively prime to *p-1* and *q*-1.
break
for *d*= the private exponent
Compute *d* from *e*, *p* and *q*.
End

The encryption operation in the RSA cryptosystem is exponentiation to the eth power modulo n. The input m is the message; the output c is the resulting ciphertext. In practice, the message m is typically some kind of appropriately formatted key to be shared. The actual message is encrypted with the shared key using a traditional encryption algorithm. This construction makes it possible to encrypt a message of any length with only one exponentiation.

The decryption operation is exponentiation to the d^{th} power modulo n. The relationship between the exponent's e and d ensures that encryption and decryption are inverses, so that the decryption operation recovers the original message m. Without the private key (n, d) (or equivalently the prime factors p and q), it's difficult (by Conjecture 6) to recover m from c. Consequently, n and e can be made public without compromising security, which is the basic requirement for a public-key cryptosystem.

3. CRYPTANALYTIC ATTACKS ON RSA

Cryptanalysis is the science of devising techniques for revealing, or attempting to reveal, the cipher text into the original message without the right to do so. Cryptanalysis is a means of evaluating a cryptosystem's (such as the RSA cryptosystem) vulnerability [5-6].

The security of the RSA cryptosystem is based on the difficulty of factoring large prime numbers. Revealing the original message and private decryption key from the cipher text and public encryption key, has been conjectured to be as difficult as the factoring of the large number into prime p and q. However, the goal of an attacker (adversary) on the RSA cryptosystem is to reveal the original message M or to reveal the private decryption key d [6]. Prior research work has shown that no techniques exist to prove that an encryption scheme is secure, the only test available is to see whether anyone can think of a way to break It [7]. However, considering much dependent on, Factoring N, Computing φ (N) without

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

factoring N, and Determining d without factoring N or computing φ (N) and computing d in some other means in order enable cryptanalyst to compute φ (N), calculate d and hence break the RSA cryptosystem still seems much more difficult than determining its prime or composite. In a condition where Computing φ (N) without factoring N enables a cryptanalyst to directly calculate

$$d = 1/e \bmod \varphi(N) \quad (1)$$

is as difficult as the factoring of N, using φ (N). Furthermore, computing d without factoring N or computing φ (N) is not easier than factoring N into p and q for a cryptanalyst. However, a knowledge of d could enable a cryptanalyst to calculate d using e* d - 1 which appears to be a multiple of φ (N). But if N is sufficiently large a cryptanalyst would not be able to determine d more easily than factoring N [7]. A cryptanalyst in this situation may aim at d which is the equivalent to d if successful, and then a Brute-Force attack could break the RSA system. Computing d in some other means, Rivest, Shamir and Adleman held that even though "computing eth roots modulo N without factoring N" is less popular than a factoring problem but they were confident of its computational intractability. They further explained that it may be possible to prove that any general method of breaking their scheme yields an efficient factoring algorithm. These instances confirm that any method of breaking the RSA system is as difficult as factoring N.

Vendors and users are alerted about the use of timing attacks by cryptanalysts in breaking security systems [12]. A chosen cipher text attack against the RSA, common modulus attack, low encryption exponent attack and low decryption exponent attack, attack on encrypting and signing with the RSA has been explained by [6].

Kocher [12] further affirmed that a careful measuring of the amount of time needed for private exponent operations may lead attackers to factor the RSA keys. The algorithm for a chosen message attack was presented by [9] this their formulation allowed them to successfully mount the attack using only one message against the Lucas based systems and Demytko's system, which proved that the use of a non-homomorphic system is not necessarily the best way to foil chosen message attacks. The difficulty of reversing the computation of the RSA algorithm function without some knowledge of the trapdoor is major to break RSA cryptosystem [10].

[11] Presented a heuristic attack, which enabled them to recover the private key from the public key, thus demonstrating the breaking of a system. Under certain conditions cryptanalysis attacks can be exploited if the decryption exponent *d* length is approximately $n^{0.25}$ [12] an attack on the RSA algorithm can be mounted using Continuous fraction. [13] Categorized attacks on the RSA cryptosystem into attacks directed against the RSA algorithm, and attacks against the environment in which the RSA is used. A cryptanalyst is able to factor *n* into *p* and *q*, he/she can compute φ (*n*) = (p-1) (q-1) and then calculate the private decryption key *d* from the public encryption key *e* using extended Euclidean algorithm [17].

[7] explained the methods an adversary can use to crack the RSA cryptosystem, which includes: factoring *N*, if a cryptanalyst can manage to factor *N* he/she is able to compute φ *(n) = (p-1) (q-1)* and obtain the private decryption key *d*.

Cryptanalysis of the RSA algorithm basically used mathematical, brute-force and implementation attacks, A new approach in the cryptanalysis of the RSA by using mathematical and brute – force methods through mapping possible key space, and performing an exhaustive search for either private decryption exponent *d* or a value that is congruent to it is also feasible

[6]Categorized the attacks on the RSA cryptosystem into three categories which included [13]: factoring method attacks, attacks on the underlying mathematical function and attacks which exploit implementation details and flaws. [14] Held that the obvious way to attack the RSA system is by factoring the modulus *N* into *p* and *q*. He further explained a simple index calculus algorithm to factor *N*. [18] Argues that attacks which target insecure implementation should not be regarded as attacks that break the RSA system. Experts in RSA argue this because these attacks exploit weaknesses in the implementation rather than weaknesses in the algorithm. For example, the insecure storage of a decryption exponent, which a cryptanalyst might eventually discover and later use to decrypt any cipher text generated from the system. It is their view that the RSA cryptosystem requires both implementation and mathematical security of the decryption exponent, and not just long key size.

4. CLASSIFICATION OF CRYPTANALYTIC ATTACKS

4.1 Factorization Method Attacks

Integer factorisation is a well-known problem in number theory that involves finding non-trivial factors of a given composite number, say *N* (positive). There is no efficient algorithm for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

factoring large integers. It is important to note that not all integers are difficult to factor, when two primes, say *p* and *q*, are randomly chosen at a sufficiently large length at relatively the same size, Finding the factors *p* and *q* from their product by another person is extremely difficult [8].

Factorisation techniques can either be special purpose or general purpose. Special purpose techniques imply that the method is applicable to a certain class of numbers that has some special properties (such as small size factors and numbers having special mathematical form). According to [7] the Special purpose techniques usually fail. The general purpose factoring technique is a factoring method that is not restricted to factoring particular categories of numbers. The following are factoring techniques that can be a threat to RSA system.

4.1.1 The Pollard's $p-1$ Method.

Pollard's $p-1$ depends on the special properties of a nontrivial factor of *N* the algorithm utilizes a chosen value $a \in$ $_N$ at random by selecting a positive integer *K* that is divisible by many prime powers. It then Compute $a_k \equiv a^k \pmod N$ and find the greatest common divisor (gcd) of $f = \gcd(a_k - 1, N)$ where $f = 1 < f < N$ otherwise it repeats again until the factors are obtain [2], [8-9].

4.1.2 Number Field Sieve Attack.

The number field sieve is for the integers of the form $N = C_1 r^t + C_2 s^u$ where two irreducible polynomials $f(x)$ and $g(x)$ with small integer coefficients for which there exits an integer *m* such that $f(x) \equiv g(m) \equiv 0 \pmod N$ are formed. The polynomial should not have a common factor [10], [20-21].

4.1.3 Quadratic Sieve Factoring Method.

The quadratic sieve is based on Fermat's factorization method which attempts to find integers, say x and y such that $x^2 \equiv y^2 \bmod N$ And $x \neq \pm y \bmod N$, but N is not divisible by $x^2 - y^2 = (x-y)(x+y)$. However, N neither divides $x-1$ nor $x+1$ then $\gcd(x-y, N)$ is the nontrivial factor of N [8], [10].

The characteristics of cryptanalytic attacks by of factorization techniques are presented in table 1.

Table 1. Characteristics Of Cryptanalytic Attacks By Of Factorization Method Attacks

Algorithm	Complexity	Conditions
Pollard's $p-1$	$O\left(B \times \log B \times (\log N)^2\right)$	When B value is large it makes it run slowly, and it's more likely to produce a factor.
Number field sieve algorithm	$O\left(\exp\left((c+o(1))\sqrt[3]{\log N}\right)\sqrt[3]{(\log\log N)^2}\right)$	c could be in either $c = \left(32/9\right)^{1/3}$ for a special case when apply to a large number or $c = \left(64/9\right)^{1/3}$ for the a general case
Quadratic sieve algorithm	$O\left(\log^2 N^{(1+o(1))}\sqrt{\log N \log\log N}\right)$	Suitable when N is big, that is why is best for RSA

4.2 Attacks on the RSA Function.

These attacks exploit the special properties of the RSA function as a result of an improper selection of public encryption exponent *e*; private decryption exponent *d*, or both [9]. This is also due to poor padding of the messages and the relations that exist between encrypted messages and any misuse of the system. The attacks will be explained as follows:

4.2.1 Common Modulus Attack

When organisations share a common public modulus among their employees, and if the same plain text message is encrypted by, say two different encryption exponents that are relatively prime, the message can be revealed without either of the decryption exponents [9]. That is a cryptanalyst having the knowledge of modulus *n* can reveal the message *M*, using extended Euclidean algorithm, *x* and *y* values can be found

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

such that $xeA + yeB = 1$, *for* eA and eB are relatively prime.

4.2.2 Low Private Exponent Attack

In the RSA cryptosystem the private decryption exponent *d* is both used for decrypting cipher text and digital signature. These operations involve a considerable amount of time, proportional to the length of the decryption exponent. Devices require the private decryption exponent value to be small in order to accelerate decryption or signing operations [11]. However, an attack due to low key shows that a selection of a small value for the decryption exponent can result in breaking the entire system.

4.2.3 Guessing the Decryption Exponent value Attack

This attack involves attempting all the possible decryption exponent values on the cipher text until a right match for the key is found (a key value that reveals the plain text). Discovery of the private decryption exponent *d* can lead to the factorisation of modulus *n* into *p* and *q*, and as such, other cipher text can be decrypted, and therefore the entire system is broken [2].

4.3 Implementation Attacks

Implementation attacks (also termed side channel attacks) are based on the side channel information obtained from physical implementation details of the RSA function; or from the exploitation of the faults that leaked information in the implementation of the RSA system [2], [8-9]. These attacks target physical implementation faults rather weaknesses associated with the underlying mathematical algorithms implementation. The attacks are often applied against security tokens and smart cards. However, it is held that defence mechanisms against these attacks are difficult, but the amount of information leaked can be minimised or it can ensure that the observation of the physical implementation detail is made irrelevant to a cryptanalyst.

4.3.1 Timing Attack

The idea of timing attacks is concerned with the algorithms which have a public key dependent correlation between the input and the running of the cryptographic operations these attacks affect the implementation of the cryptosystems due to the optimisation for performance, and by monitoring the amount of time which can be correlated with input [12].

4.3.2 Power Analysis Attacks.

A power analysis attack involves monitoring the power consumption of cryptographic tokens. This attack takes advantage of the power consumption variation that occurs during different cryptographic operation steps [8], [15]. The information gained as a result of the power consumption variation can enable a cryptanalyst to discover the secret information.

4.3.3 Fault Analysis Attack

As the name implies, a fault analysis attack depends on the induced or implementation error on a key dependent cryptographic operation. Fault analysis attacks can be mounted against both the secret key and public key cryptographic devices. This attack exploits the likely errors on the RSA decryption or signing operations in cryptographic devices [20].

5. CONCLUSION

The strength of cryptanalysis attacks on the RSA cryptosystem has been studied; all possible known attacks on the system are overwhelming. However, these attacks demonstrated pitfalls in the implementation and obvious misuse of the RSA system. Most of the attacks cannot be avoided. The RSA system remains secure and can be trusted if a proper implementation of the system is adequately taken into consideration. The attacks have been classified into three categories which include: Attacks on the RSA function, Attacks based on the extraction of details in the implementation, and the Factorisation methods attacks. These attacks have demonstrated the dangers behind improper usage of the RSA system

The future of the RSA system will definitely come across continuing and greater challenges as the attacks on both algorithm and the underlying implementation of the system gain strength. Therefore it is imperative to improve the security provided by the algorithm. Without the attainment of an efficient factoring algorithm capable of factoring large integers such as the ones used as the modulus *n* of the RSA system, no viable alternative for the future system of the RSA system remains assured.

REFERENCES:

[1]. Rivest, R.L., Shamir, A., Adleman, L. A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, v.21 n.2, p.120-126, Feb. 1978

[2]. D. Boneh, Twenty years of attacks on the RSA acyptosystem, Notices of the AMS 46 (2) (February 1999) 203–213.

[3]. Kevin D. Bowers, Ari Juels, Ronald L. Rivest, Emily Shen: Drifting Keys: Impersonation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

detection for constrained devices. INFOCOM 2013: 1025-1033

[4]. Amr Youssef, An Attack Against the Revised Murthy–Swamy Cryptosystem, IEEE Transactions on Circuits and Systems—II: Express briefs, Vol . 55, No. 2, Feb2008

[5]. Stallings W. Cryptography and Network Security Principles and Practice. New Jersey: Pearson Education, Inc, Upper Saddle River 2006.

[6]. Loshin P. Personal Encryption Clearly Explained. USA: Academic Press. 1998.

[7]. Bruce, S. The psychology of security. In Communications of the ACM, 50 (5) p. 128 2007.

[8]. Yan S.Y. Cryptanalytic Attacks on RSA .Germany: Springer-Verlag, Heidelberg, 2008.

[9]. Bruce, S. Cryptography: The Importance of Not Being Different. In IEEE Computer, 32 (3) pp. 108-109. 1999.

[10]. Pomerance, C. "A Tale of Two Sieves." *Not. Amer. Math. Soc.* 43, 1473-1485, 1996

[11]. M. Wiener. Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, 36:553{558, 1990.

[12]. Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, 1999. Pages 104 – 113.

[13]. Bleichenbacher D., Joye M. and Quisquater J. J. A. New and Optimal Chosen-message Attack on RSA-type Cryptosystem" Information and Communication Technology of Lecture Notes in Computer Science (Volume 1334) pp. 302 – 313. 1997.

[14]. A.M. Youssef and G. Gong, "Cryptanalysis of a public key cryptosystem proposed at ACISP 2000," Proc. of the 6th Australian conference on information security and privacy, ACISP' 2001, Lectures Notes in Computer Science, LNCS2119, Springer-Verlag, pp. 15-20, 2001.

[15]. Chandra M. Kota and Cherif Aissi, Implementation of the RSA algorithm and its cryptanalysis" Proceedings of the 2002 ASEE Gulf Southwest Annual Conference, The University of Louisiana at Lafayette, March 20 – 22, 2002.

[16]. Delfs H. and Knebl (2002) Introduction to Cryptography: Principles and Applications. Germany: Springer- Verlag, Heidelberg

[17]. Koblitz N. and Menezes J. A. (2004) A Survey of Public- Key Cryptosystem

[18]. RSA Security (2004) what would it Take to Break the RSA Cryptosystem [online] Available from <http://www.rsasecurity.com/rsalabs/node.asp?id=2216 >.

[19]. Galbraith, Steven D. (2012), Mathematics of Public Key Cryptography, Cambridge University Press, pp. 272–273,

[20]. Coppersmith, D. "Modifications to the Number Field Sieve." *J. Cryptology* **6**, 169-180, 1993.

[21]. Elkenbracht-Huizing, R.-M. "An Implementation of the Number Field Sieve." *Experiment. Math.* **5**, 231-253, 1996.

[22]. Delfs H. and Knebl (2002) Introduction to Cryptography: Principles and Applications. Germany: Springer- Verlag, Heidelberg

[23]. Koblitz N. and Menezes J. A. (2004) A Survey of Public- Key Cryptosystem

[24]. RSA Security (2004) what would it Take to Break the RSA Cryptosystem [online] Available from <http://www.rsasecurity.com/rsalabs/node.asp?id=2216 >.

[25]. Galbraith, Steven D. (2012), Mathematics of Public Key Cryptography, Cambridge University Press, pp. 272–273.