IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-7 E-ISSN: 2347-2693

Simulation Survey of RSA and Its Variants

R. Kumar[1*], A.K. Jain[2]

[1*]Sagar Institute of Science, Technology and Engineering (SISTec-E), Bhopal, India
[2]Sagar Institute of Science, Technology and Engineering (SISTec-E), Bhopal, India

[*]*Corresponding Author: errajeshkumarcs@gmail.com*

Available online at: www.ijcseonline.org

Received: 21/May/2017, Revised: 12/Jun/2017, Accepted: 09/Jul/2017, Published: 30/Jul/2017

***Abstract*—** Cryptography is used in securing data transmission over insecure networks. The selection of algorithm requires the condition of fulfillment of authentication, confidentiality, integrity and non-repudiation. Among all public key encryption algorithms, RSA is globally accepted encryption algorithm due to its hardness against various possible attacks. In this paper, we studied RSA, enhanced RSA, Elgamal, chinese remainder theorem (CRT) based RSA, multi-power RSA, three-prime RSA and Elgamal-RSA cryptosystem.

***Keywords*—**CRT, Elgamal, Multi-prime RSA, Security, Three-prime RSA

I. INTRODUCTION

In symmetric key cryptography, same key is used for encryption and decryption operations. It is shared only between the communicating parties and it is known as shared secret key. The sender uses it to encrypt the plaintext before the transmission and the receiver uses the same key to decrypt the received ciphertext. Public key cryptography involves two separate keys maintained by each communicating party: a public key and a private key. The public key is available globally i.e. it is broadcasted to all the communicating parties and its equivalent private key is kept undisclosed. Whenever sender wants to send the information secretly, the plaintext is encrypted by the sender with the receiver's public key before its transmission. The received ciphertext is decrypted by the receiver using its own corresponding private key.

Examples of public key encryption algorithms are: ElGamal, RSA, Rabin, and many more.

Among these public key encryption algorithms, RSA is the extensively deployed public key cryptosystem. It is utilized in securing e-mail, web traffic, wireless devices and many more. It can be slow in constrained environments because of the fact that it is relies on arithmetic modulo large numbers. One of the well known methods to fasten the decryption of RSA is the use of the famous Chinese Remainder Theorem (CRT) [1]. In this paper, we studied the CRT-RSA [2, 3], Multi-Power RSA [4], Three-Prime RSA [5, 6] and Elgamal-RSA cryptosystem [7]. The comparison has been done among traditional RSA, Enhanced RSA, Elgamal and RSA-Elgamal encryption algorithms. The decryption exponent d, two large primes p and q are required for CRT based fast decryption. Due to this, there is an added source of insecurity. Nevertheless, if the decryption component d is given then it is effortless to factor the modulus n. Therefore, no security is lost in using this method.

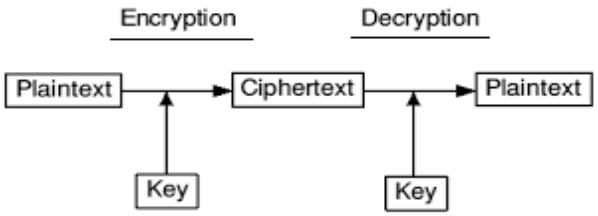

Figure.1: Cryptography

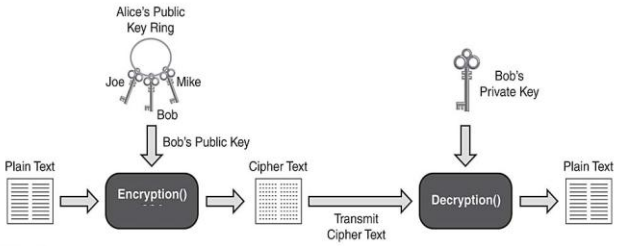

Figure.2: RSA algorithm

This paper is structured in five sections. Section II describes the basic RSA algorithm. Section III discusses variants of RSA. Section IV will describe the comparison among these variants. Finally, section V will conclude the article and future work.

II. TRADITIONAL RSA

The traditional RSA algorithm is deployed for both digital signatures as well as public key encryption (see Figure 2). Its

security relies on the complex factorization of large integers. Its steps are as follows.

- Choose two large prime integers p and q.
- Compute the product n = pq.
- Select e (e<n) which has no common factors with either p-1 or q-1.
- Calculate the decryption exponent by following ed mod (p-1) (q-1) = 1.
- The encryption is done by using $E(m) = m^c \bmod n$, where m is any message.
- The decryption is done by using $D(c) = c^d \bmod n$, where c is any ciphertext.
- The public key (which is globally available) is the pair of integers (n,e).
- The private key (which is kept undisclosed) is the group of integers (p,q,d).

III. VARIANTS OF RSA

In order to increase the execution speed of traditional RSA decryption, numerous authors have given their valuable contribution in the field. In order to speed up RSA decryption, one interesting approach is given using the Chinese Remainder Theorem (CRT) [2, 3]. One can further speed up RSA decryption using moduli of the form $N = p^{b-1}q$ where q and q are n/b bits each [4]. A different approach is provided by [5, 6]. In these articles, they are using multi - prime RSA or three-prime RSA to speed up the decryption of the RSA cryptosystem.

Enhanced RSA is based on the RSA algorithm. In order to generate the value of N, the enhanced RSA uses an additional third prime number. Due to this, the encryption and the decryption process become faster. Moreover, it generates the public and private keys faster than the traditional RSA [7]. Taher has proposed an asymmetric key algorithm using Diffie-Hellman key exchange algorithm and it is named as "Elgamal" [8]. Its working is over finite fields [9]. The security of Elgamal cryptosystem relies on the hardness of breaking famous Discrete Logarithm Problem (DLP).

Another efficient method has been proposed and the authors proved that their method is faster than the original RSA and

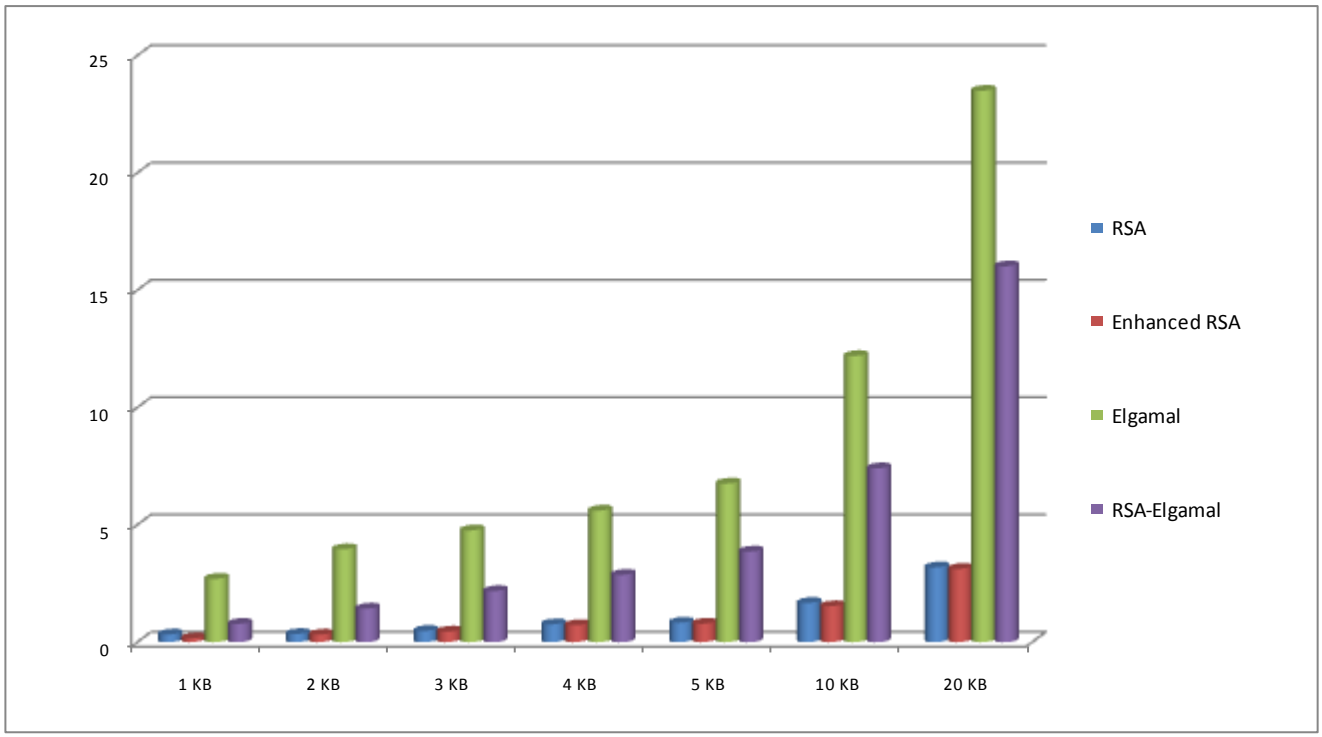

Figure 1. Comparison of RSA variants based on their total execution time

Elgamal cryptosystems [10]. In order to generate the public and private keys, a new encryption scheme proposed by Malhotra [11] uses three large prime numbers. The method is an integration of the Enhanced RSA and Elgamal cryptosystem.

IV. COMPARISON OF RSA VARIANTS

RSA uses arithmetic on integers at least 1024 bits long. Its implementation is fast enough if used for key exchange. Here, we use BigInteger class of java [12, 13]. Figure 3 below shows the comparison of the total execution time taken among all the variants described above i.e. traditional RSA, Enhanced RSA, Elgamal and RSA-Elgamal encryption algorithms.

V. CONCLUSION AND FUTURE SCOPE

RSA is globally accepted encryption algorithm due to its hardness against various possible attacks. This paper deals with different variants of RSA. The decryption exponent d along with two primes p and q are required for CRT version of decryption. Due to this, there is an added source of insecurity. Nevertheless, if the decryption component d is given then it is effortless to factor the modulus n. Therefore, no security is lost in using this method. There are definitely some more ways in order to speed up any algorithm. In future, we will try to minimize the time taken by the extended Euclid algorithm to compute the inverse of a number. This work will definitely help some other researchers who are working in this field.

ACKNOWLEDGMENT

The authors would like to thank Sagar Institute of Science, Technology & Engineering (SISTec-E), Bhopal, India for providing their academic support.

REFERENCES

[1] Sarika Khatarkar and Rachana Kamble, "*Encrypted RSA Public Key Sharing By Using Image Pixel Color Value*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.5, pp.231-235, 2015.

[2] A. Menezes, P. van Oorschot and S. Vanstone, "*Handbook of applied cryptography*", CRC Press, 1996.

[3] Cetin Kaya Koc, "*High speed RSA implementation*", Technical Report, RSA Laboratories, California, 1994.

[4] T. Takagi., "*Fast RSA-type cryptosystem modulo pkq*", In the Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 1998), Santa Barbara, California, USA, pp.318-326, 1998.

[5] Yonghong Yang, Z. Abid and Wei Wang, "*CRT-based three-prime RSA with immunity against hardware fault attack*", In the Proceedings of the 4th IEEE International Workshop on System-on-Chip for Real-Time Applications (IWSOC 2004), Banff, Alta., Canada, pp.73-76, 2004.

[6] Anand Krishnamurthy, Yiyan Tang, Cathy Xu and Yuke Wang, "*An efficient implementation of multi-prime RSA on DSP processor*", In Proceedings of the 2003 IEEE lnternational Conference on Acoustics, Speech and Signal Processing (ICASSP 2003), Hong Kong, China, pp.413-416, 2003.

[7] Al-Hamami, A. H., Aldariesh, I. A., "*Enhanced method for RSA cryptosystem algorithm*", In the Proceedings of IEEE Advanced Computer Science *Applications* and Technologies (ACSAT), Kuala Lumpur, Malaysia, pp.402-408, 2012.

[8] S. Mewada, P. Sharma and S. S. Gautam, *"Exploration of efficient symmetric algorithms,"* 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), *India, pp. 663-666, 2016.*

[9] Rashmi Singh and Shiv Kumar, "*Elgamal's algorithm in cryptography*", International Journal of Scientific and Engineering Research, Vol.3(12), pp.1-4, 2012.

[10] Ahmed, J. M. and Ali, Z. M, "*The enhancement of computation technique by combining RSA and Elgamal cryptosystems*", In the Proceedings of IEEE Electrical Engineering and Informatics (ICEEI 2011), Bandung, Indonesia, pp.1-5, 2011.

[11] Mini Malhotra, "*A new encryption scheme based on enhanced RSA and Elgamal*", International Journal of Emerging Technologies in Computational and Applied Sciences, Vol.14(336), pp.138-142, 2014.

[12] Cay S. Hostmann and Gary Cornell, "*Core Java*," Volume 1-Fundamentals, Nineth Edition, Prentice Hall, USA, 2013.

[13] Cay S. Hostmann and Gary Cornell, "*Core Java*," Volume 2-Advanced Features, Nineth Edition, Prentice Hall, USA, 2013.

Authors Profile

Mr. R Kumar has completed B.E. (Bachelor in engineering) in computer science and engineering branch from people's college of research & technology under RGPV Bhopal. He is pursuing M.Tech from SISTec-E under RGPV Bhopal. His interested subjects are software engineering, web engineering and computer network.

*Prof. A K Jain (*M.Tech CSE) is a proficient and enthusiastic professional in the area of Computer science and has experience of more than 8 years in academics. He has obtained M.Tech from SIRT under RGPV Bhopal. His expertise lies in the field of NLP, Cloud Computing, Computer programming & Algorithms, and Image processing.

