Survey of Current RSA Variants

Chandan Kumar[1], Afreen Ali[2]

[1]*MTech Scholar*, [2]*Assistant Professor*
Department of Computer Science and Engineering
Bhabha College of Engineering, RKDF University, *Bhopal, India*

ABSTRACT

Protecting the privacy and the confidentiality of sensitive data of users has become an urgent problem to be solved in the cloud storage environment. This is also the biggest obstacle facing the popularity of the cloud storage services. RSA is one of the well-known public key cryptosystem being used to secure any system like smart cards and e-commerce applications. The purpose of this paper is to analyse the current RSA variants found in the literature.

Keywords: RSA, Security, Cryptography, Encryption, Decryption

I. INTRODUCTION

The object of cryptography is security, to provide it to the message for it safe bestowal. In public key cryptography, the security is obtained in terms of a hard mathematical problem. The security of most popular public key cryptosystem known as RSA is formulated as of factorization. Since then, the problem of factorization is characterized using various mathematical tools.

In recent years, the rapid development of technologies such as the Internet of Things, Cloud Computing, the Internet and Big Data, etc., have resulted in a large number of mobile devices, RFID readers, wireless sensor devices, etc. generating massive amounts of data almost instantaneously. This posse a challenge to the existing technology for real-time data processing and storage. Cloud computing has become one in all the foremost necessary evolutions computing has seen recently. The success for Clouds is attributed to the power to supply apparently unlimited computing resources nearly outright and conjointly to the pay-per-use evaluation schemes.

Protecting the privacy and the confidentiality of sensitive data of users has become an urgent problem to be solved in the cloud storage environment. This is also the biggest obstacle facing the popularity of the cloud storage services. RSA is one of the well-known public key cryptosystem being used to secure any system like smart cards and e-commerce applications. The objective of this paper is to analyze existing variants of RSA cryptosystem found in the literature i.e. Original RSA, Takagi RSA, Krishnamurthy et al. RSA and Abdeldaym et al. RSA.

II. RELATED WORK

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) [1-2]. 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 [3]. A different approach is provided by [4-5]. In these articles, they are using three-prime RSA or multi -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 [6]. Taher has proposed an asymmetric key algorithm using Diffie-Hellman key exchange algorithm and it is named as "Elgamal" [7]. Its working is over finite fields [8]. 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 Elgamal cryptosystems [9]. In order to generate the public and private keys, a new encryption scheme proposed by Malhotra [10] uses three large prime numbers. The method is an integration of the Enhanced RSA and Elgamal cryptosystem.

Strong encryption technology is required to encrypt user data to ensure storage and backup security in the cloud. Currently, research work is being carried out in the following areas: confidentiality of data for storage, the security audit, and the ciphertext accesses control [11]. Common data encryption algorithms, based on the different key types, can be divided into symmetric encryption algorithms and asymmetric encryption algorithms (public-key encryption algorithms). The Data Encryption Standard (DES) is a classic symmetric encryption algorithm, which is characterized by its high encryption and decryption efficiency, but its key length is too short [12]. To overcome this shortcoming of the DES, a triple DES (3DES) encryption method is proposed ill [13]. This method extends the key length from the original 56 bits to 112 bits; however the software implementation of the algorithm is inefficient. With the rapid development of encryption technology, DES has gradually been replaced by the Advanced Encryption Standard (AES), which is highly efficient, safe and reliable.
The RSA algorithm [14] is a typical asymmetric encryption algorithm, which is widely used not only for user data encryption, but also as a digital signature. However, considering that the encryption and decryption efficiency of the algorithm is low, it is not suitable for encryption of large amounts of data. To enhance the level of security, Jaju and Chowhan [15] proposed modified RSA algorithm. Its efficiency relies on key generation speed and security level.

In network security, the branch of cryptography is which one can save and transmit data in format particular so that only the user intended can read and process it, the text encrypted is the cipher text which is then decoded on the receiver side. The

algorithm of RSA is an asymmetric cryptography technique, this is working on two keys i.e. public key and private key. The proposed model [16] takes four prime numbers in RSA. Instead of sending one public key directly, send two public keys to the receiver. But there is problem of the speed, so that in RSA decryption used Chinese remainder theorem to enhancement the speed of RSA decryption.

III. RESULT ANALYSIS

This section brings detailed result analysis of our work. Experiments are carried out using the following hardware and software specifications: Windows7 64-bit operating system, Core i3 CPU with 2.1 GHz, 4 GB RAM, and 500 GB hard disk. Plaintext files of 640 bits, 1040 bits and 1136 bits are used as experimental data. The Original RSA [1], Takagi RSA [3], Krishnamurthy et al. RSA [5] and Abdeldaym et al. RSA [16] algorithm are used to encrypt and decrypt the plain text files of different sizes a 100 times and the average time is noted.

The key length of the modulus of the RSA algorithm is 2048-bit. Here, we use BigInteger class of java [17]. Figure 1 shows comparison of the total time taken with different message sizes 640 bits, 1040 bits and 1136 bits.

Table 1: Comparison of the Total Time Taken (in ms) with Different Message Sizes

Message Size	Original RSA [1]	Takagi RSA [3]	Krishnamurthy et al. RSA [5]	Abdeldaym et al. RSA [16]
640 bits	265	62	78	52
1040 bits	266	63	93	53
1136 bits	270	62	94	56

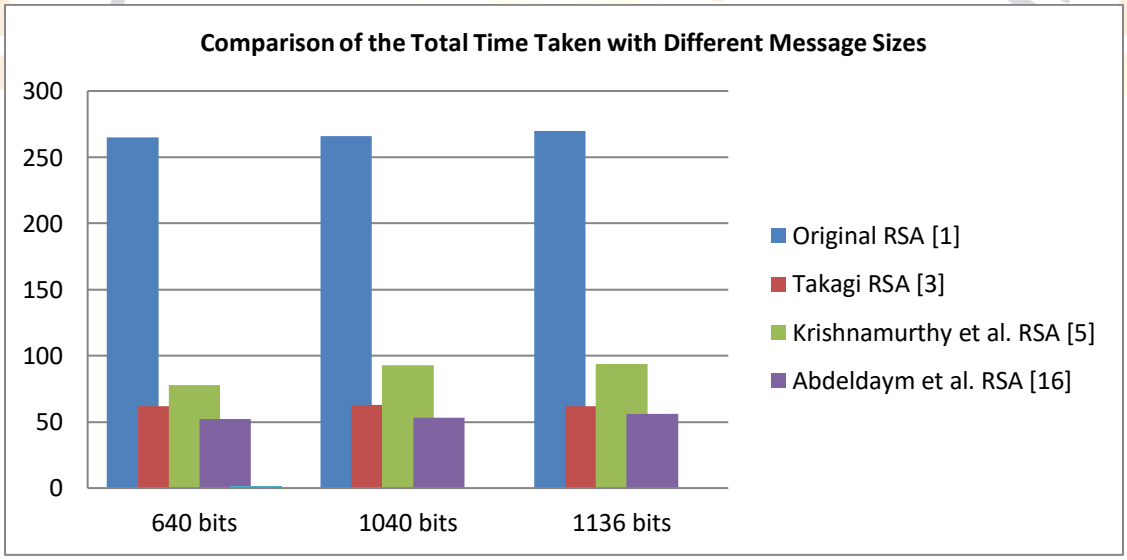

Figure 1: Comparison of the Total Time Taken with Different Message Sizes

IV. CONCLUSION

The purpose of this work is to compare various RSA variants found in the literature. Through this work, we can conclude following points:-

- This work shows the comparison of speed up factor between various variants of RSA cryptosystem i.e. Original RSA [1], Takagi RSA [3], Krishnamurthy et al. RSA [5] and Abdeldaym et al. RSA [16] algorithms.
- Compared to conventional algorithms, Abdeldaym et al. RSA provides higher operational speed for message sizes 640 bits, 1040 bits and 1136 bits.

REFERENCES

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

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Al. Hasib, A. Haque, A. A. M. M, "A comparative study of the performance and security issues of AES and RSA cryptography", In the Proceedings of IEEE Convergence and Hybrid Information Technology (ICCIT 2008), Busan, South Korea, pp.505-510, 2008.

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

[9] 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.

[10] 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.

[11] Takabi H, Joshi J B D, A hn G, "Security and privacy challenges in cloud computing Environment," JEEE Security & Privacy, 2010, 8(6):24-31.

[12] Qiu Weixing, Xiao Kezhi, Li Fang, etc, "A kind of method of extension of the DES key," Computer Engineering, 2011, 37 (5): 167-168, 171.

[13] Jiang Bo, "DES integrated with RSA encryption methods," Microcomputer Information, 2007 (6): 52-54.

[14] RlVEST R L, SHAMlR A, and ADLEMANL, "A method for obtaining digital signatures and public key cryptosystems," Communications of the Association for Computer Machinery, 1978.

[15] Sangita A. Jaju, Santosh S. Chowhan, "A Modified RSA algorithm to enhance security for digital signature," International Conference and Workshop on Computing and Communication (IEMCON), Canada, 2015.

[16] Rasha Samir Abdeldaym, Hatem Mohamed Abd Elkader, Reda Hussein, "Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem," International Journal of Electronics and Information Engineering, vol. 10, no. 1, 2019, pp. 51-64.

[17] Cay S. Hostmann and Gary Cornell, "Core Java ™2 Volume 1- Fundamentals", Seventh Edition, Sun Microsystems, Inc. 2005.