A Literature Review of Some Modern RSA Variants

Akansha Tuteja[1] Amit Shrivastava[2]
[1,2]Department of Computer Science & Engineering
[1,2]RGPV University, SVCE Indore, India

Abstract— RSA cryptosystem is the most commonly used public key cryptosystem. It is the first public key cryptosystem. The strength of this cryptosystem is based on the larger key size. There are many algorithms and variants of RSA. But, it is steal a burning topic of research. Because the thrust to store data secret is never going to end. In this paper, we have proposed a literature review of some modern variants of the RSA algorithm. All the algorithms have been analyzed. Their merits and demerits are also discussed.

Keywords*:* Public Key Cryptography, RSA Variant, Data Secrecy

I. INTRODUCTION

In this age of universal electronic connectivity, the electronic fraud is a matter of concern. There is indeed need to store the information securely. This has led to a heightened awareness to protect data and resources from disclosure, to ensure the authenticity of data and messages, and also to protect systems from network based attacks. Cryptography is the science of encryption. Cryptography plays a central role in mobile phone communications, electronic commerce, sending or receiving private emails, transaction processing, providing security to ATM cards, securing computer from unauthorized access, digital signature and also touches on many aspects of our daily lives. Cryptography consists of all the principles and methods of transforming an intelligible message called plaintext into one that is unintelligible called cipher text and then retransforming that message back to its original Form. In modern era, the cryptography is considered to be a branch of both mathematics and computer science. It is also affiliated closely with information & communication theory. Although in the past, the role of cryptography referred only to the encryption and decryption of message using secret keys. But nowadays, the cryptography is used in many areas; it is because of the digitization.

It is generally classified into two categories, the symmetric and asymmetric. The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted or scrambled by any encryption algorithm using the key. The user having the access to the same key can decrypt the encrypted data. Such a cryptosystem is known as private key or symmetric key cryptography. There are many standard symmetric key algorithms available. Some popular ones are as:. AES advanced encryption standard, 3DES triple data encryption standard etc. All these standard symmetric algorithms defined are proven to be highly secured and time tested. The main problem related to these algorithms is the key exchange. All the communicating parties require a shared secret key. This key is required to exchange between them to establish a secured communication. Therefore the security of the symmetric key algorithm depends on the security of the secret key. The Key size is typically hundreds of bits in length. The key size also depends on the algorithm used. The key cannot be shared online. Also when a large number of communicating parties are there, then in that case the key exchange is infeasible & very difficult too. All such problems are countered by the public key cryptography. In public key algorithm a shared secret can be established online between communicating parties without any need for exchanging any secret data

II. LITERATURE SURVEY

Fault-based attacks are the attacks which are capable of recovering secret keys by. The fault based attacks introducing one or more faults in and then analyzes the output. It is a very powerful method to crack the key. The work done by Kun Ma et al in [1] contains a novel Concurrent Error Detection scheme to overcome the problem due to fault-based attack against RSA. This proposed method is based on the concept of the multiplicative homomorphism property. The time overhead of this technique is more. Alexandra Boldyreva, Hideki Imai proposed another variant of RSA[2]. It is known as RSA-OAEP. It is based on OAEP. OAEP is one of the most popular and well formatted public-key encryption scheme. It was originally designed by Bellare and Rogaway.The OAEP is based on a trapdoor permutation. But the guaranteed level of security is not very high for a practical parameter choice. The authors [2] proposed a very simple modification of the OAEP encryption in which the trapdoor permutation instance is only applied to a part of the OAEP transform. The security is tight in this updated version. OAEP can also be used to encrypt long messages without using hybrid encryption.

The work done in [3] focuses on the problem of how to prevent the fast RSA signature and decryption computation with residue number system speedup from a hardware fault cryptanalysis in a highly reliable and efficient approach. It is a well known fact that the CRT-based speedup for RSA signature has been widely used. But it is a possibility that a hardware fault cryptanalysis can totally break the RSA system by factoring the public modulus. Many solution exist to counter this problem. But we have observed that very few of these existing solutions are both sound and efficient. Experimental results have shown that the expanded modulus approach proposed by Shamir is superior to the approach of using a simple verification function when other physical cryptanalysis. The proposed work is based on the concepts of fault infective CRT computation and fault infective CRT recombination.RSA is the asymmetric or public key cryptography system. The security of RSA public key

cryptosystem is based on the larger value of modulus. One of the main problems associated to RSA cryptosystem is factorization. The authors [4] proposed a new special purpose algorithm to perform factorization. This algorithm is compared with trial division algorithm TDM. The experimental results prove that the" and "References". Proposed algorithms runtime depends on the difference of factors and is independent of size of the modulus. So it is more effective whenever factors are close to each other & in that particular case it outperforms the TDM.Giraud [7] proposed a new countermeasure scheme based on the concept of Montgomery Ladder Exponentiation. The proposed algorithm performs two modular multiplications for each bit of exponent. Whereas the square and multiply algorithm which performs on average 1.5 modular multiplications per bit of the exponent. Therefore the proposed method is faster.

The authors of [5] proposed an enhance algorithm for the RSA cryptosystem. This new proposed cryptosystem uses a third prime number in calculating the value of n. This additional third prime number increases the factor complexity of n. It will provide more security to the RSA.

The public key cryptosystem RSA is the first and most popular cryptosystem for performing encryption and decryption of data, to keep data secret, to transfer data from one location to another. Also it is known that the security of RSA depends on large factorization. If the factorization is possible then the whole algorithm can become breakable. Authors [6] proposed a new methodology to change the original modulus with the fake modulus. Therefore if the hacker factorizes this new modulus value then he will not be able to locate the original decryption key.

III. Common Problems In Existing Rsa Variants

The main disadvantage of RSA encryption its slower speed.

(1) Not secure against Weiner's attack
(2) Not secure against common modulus attack
(3) Not secure against known plaintext attack
(4) Not secure against low decryption exponent attack

IV. Conclusion

In this paper, the introduction & the application of cryptography is given. The problems related to private keys are discussed. The public key cryptography & its utility in so many areas of the life are discussed. The modern variants of the RSA cryptosystem are discussed with their merits and demerits. RSA is the most popular method for encryption & decryption. It provides a large level of security. It provides strong security because of the large key size. In this paper, we have proposed a comprehensive survey over the various variant of the RSA algorithm. Each RSA variant is discussed with its advantages & disadvantages. This review will help the researchers in making a much strong & secure RSA cryptosystem.

References

[1] Kun Ma, Han Liang, and Kaijie Wu, Member, IEEE, "Homomorphism Property-Based Concurrent Error Detection of RSA: A Countermeasure to Fault Attack", IEEE TRANSACTIONS ON COMPUTERS, VOL. 61, NO. 7, JULY 2012
[2] Alexandra Boldyreva, Hideki Imai, Life Fellow, IEEE, and Kazukuni Kobara, "How to Strengthen the Security of RSA-OAEP", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 11, NOVEMBER 2010
[3] Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sang-Jae Moon," RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis"IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 4, APRIL 2003
[4] Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE 2012.
[5] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. Of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[6] Wireless LAN Medium Access Control(MAC)and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.
[7] m. Wegmuller, j. P. Von der weid, p. Oberson, and n. Gisin, "high resolution fibber distributed measurements with coherent ofdr," in proc. Ecoc'00, 2000, paper 11.3.4, p. 109.
[8] r. E. Sorace, v. S. Reinhardt, and s. A. Vaughn, "high-speed digital-to-rf converter," u.s. patent 5 668 842, sept. 16, 1997.
[9] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/
[10] M. Shell. (2002) ieeetran homepage on CTAN. [Online]. Available:http://www.ctan.org/tex archive/macros/latex/contrib/supported/ieeetran/
[11] FLEXChip Signal Processor (MC68175/D), Motorola, 1996
[12] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[13] Karnik, "performance of tcp congestion control with rate feedback: tcp/abr and rate adaptive tcp/ip," m. Eng. Thesis, indian institute of science, bangalore, india, jan. 1999.
[14] j. Padhye, v. Firoiu, and d. Towsley, "a stochastic model of tcp reno congestion avoidance and control," univ. Of Massachusetts, Amherst, ma, cmpsci tech. Rep. 99-02, 1999.
[15] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

