International Engineering Journal For Research & Development

Vol.5
Issue 4

E-ISSN NO:-2349-0721

Impact factor : 6.549

A HYBRID MULTILEVEL KEY GENERATION ALGORITHM FOR FAST TRANSACTION BASED ON STANDARD RSA ALGORITHM

[1]Mr. MayurPatil , [2]Prof.Nitin Mandaogade
Student (M.tech EXTC)[1] , HOD(EXTC)[2], G.H.Raisoni University Amravati,India
mayur.map.patel@gmailcom, nitin.mandaogade@raisoni.net

ABSTRACT-

As most of the data transactions now-a-days are being made through secured smart cards owing to their low cost and ease of usage, it has become necessary to speed up the Key generation in the RSA algorithm [4]. Moreover, public key cryptography is a popular method that provides security, identification and authorization in secure transactions [5].The cryptography is classified into two types: Symmetric Key Systems and Asymmetric Key Systems. In Symmetric Key Systems same keys are used by the transmitter and receiver whereas in Asymmetric Key Systems different keys are used for encryption by the sender and decryption by the receiver. Hence these two aspects, namely speed of key generation at the same time maintaining the security are of prime importance and the major sources of motivation in carrying out the present work.

During the study of the RSA algorithm, the following problems have been identified: a) the mathematical solutions of cryptographic algorithms require a large amount of calculation, which implies a higher consumption of computing resources and greater bandwidth for transaction; b) in order to store information in a database, for example four bytes, encrypted fields of approximately 600 bytes are required thus enhancing the space required; c) increasing threats and vulnerabilities, due to the development of technologies [19, 20], result in the improvement of information security, which means higher cost and consumption of computational resources. This work proposes a generic model that optimizes the RSA method for information encryption, combining two different methodologies of key generation. This generic RSA model is expected to meet all the requirements and processes based on standard models accepted like cryptographic protocols and to make it suitable for transaction through smart devices like POS and other such transaction terminals.

INTRODUCTION

Cryptography is the technique of hiding the data from unauthorized users for secured transaction. It is a method [1, 2] that stores and transmits data in a particular form so that only intended user can interpret and processes in order to maintain the confidentiality and integrity of data [3]. Cryptography technique provides Confidentiality, Integrity, Authentication and Non-Repudiation services to the data being transmitted by the sender to the receiver. Cryptography is utilized wherever a secure transaction is needed like in email, financial transaction, corporate information etc. Cryptography is suitable for wired as well as wireless transmission media. In order to perform encryption and decryption various cryptographic techniques are used such as AES, DES, 3DES, Blowfish and RSA. These techniques have different key size, block size and number of round and each method has different execution time and throughput. The cryptography is classified into two types: Symmetric Key Systems and Asymmetric Key Systems. In Symmetric Key Systems same keys are used by the

transmitter and receiver whereas in Asymmetric Key Systems different keys are used for encryption by the sender and decryption by the receiver.

RSA algorithm was publically described by Ron Revister, Adi Shamir and Leonard Adleman [6] at MIT in 1977. For Public key Cryptography RSA is a well known algorithm. The RSA algorithm uses modular multiplication and exponentiation [7, 8]. As in Public key cryptography or asymmetric key cryptography standard, separate keys are used for encryption and decryption. One is public and other one private key. The keys are generated by applying some computational effect on the product of two large prime numbers [9]. The public key is then sent to everyone in the system but the Private Key is kept secret in RSA. The security of the RSA cryptosystem depends upon the difficulty of factoring large prime numbers [10]. Of course the technique of factoring of numbers is improving but still the speed depends on the size of prime numbers. The improvement over the standard RSA is gradually done improving day by day. In 1982, J.J. Quisquater and C. Couveur [11] described and proposed a technique to increase the speed of RSA decryption algorithm. Quisquater used the concept of Chinese remainder theorem (CRT), which was called QCRSA that improved the basic RSA decryption performance. Furthermore the concept of Batch RSA [12] was introduced in 1989, the concept of Batch RSA is that, if small public exponent *e* are used for some modulus *n*, the decryption of the two cipher text can be done at the cost of one but that technique is only valuable when the public key exponents *e1* and *e2* have small values. In 1989 the concept of MultiPrime RSA [13, 14] was introduced, the RSA system modulus was enhanced so that it consist of k prime numbers p1, p2,……pk. instead of only two using in RSA. After that the concept of MultiPower RSA [15] was invented in 1998, in this method, n = p(k-1).q here p and q are n/k bits long. Furthermore the concept of Rebalanced RSA [13] was proposed in 1990. In 2009 D. Garg and S. Verma [17] gave the comparisons of RSA variants namely Batch RSA [12], Multiprime RSA [13, 14], Multipower RSA [15], Rebalanced RSA [13], Rprime RSA [16]. In 2012, A.H. Al-Hamami and I.A. Aldariseh [18] proposed a new concept in RSA cryptosystem by enhancing the RSA algorithm by the use of additional third prime number in the composition of the public and private key with reduced size, instead of two large prime numbers. In this method they generate the variable *n* Large and the process of analysis of the factors is more complex than the original algorithm.

LITERATURE REVIEW

RSA algorithm was publically described by Ron Revister, Adi Shamir and Leonard Adleman [6] at MIT in 1977. For Public key Cryptography RSA is a well known algorithm. The RSA algorithm uses modular multiplication and exponentiation [7, 8]. As in Public key cryptography or asymmetric key cryptography standard, separate keys are used for encryption and decryption. One is public and other one private key. The keys are generated by applying some computational effect on the product of two large prime numbers [9]. The public key is then sent to everyone in the system but the Private Key is kept secret in RSA. The security of the RSA cryptosystem depends upon the difficulty of factoring large prime numbers [10]. Of course the technique of factoring of numbers is improving but still the speed depends on the size of prime numbers. The improvement over the standard RSA is gradually done improving day by day. In 1982, J.J. Quisquater and C. Couveur [11] described and proposed a technique to increase the speed of RSA decryption algorithm. Quisquater used the concept of Chinese remainder theorem (CRT), which was called QCRSA that improved the basic RSA decryption performance. Furthermore the concept of Batch RSA [12] was introduced in 1989, the concept of

Batch RSA is that, if small public exponent *e* are used for some modulus *n*, the decryption of the two cipher text can be done at the cost of one but that technique is only valuable when the public key exponents *e1* and *e2* have small values. In 1989 the concept of MultiPrime RSA [13, 14] was introduced, the RSA system modulus was enhanced so that it consist of k prime numbers p1, p2,……pk. instead of only two using in RSA. After that the concept of MultiPower RSA [15] was invented in 1998, in this method, n = p(k-1).q here p and q are n/k bits long. Furthermore the concept of Rebalanced RSA [13] was proposed in 1990. In 2009 D. Garg and S. Verma [17] gave the comparisons of RSA variants namely Batch RSA [12], Multiprime RSA [13, 14], Multipower RSA [15], Rebalanced RSA [13], Rprime RSA [16]. In 2012, A.H. Al-Hamami and I.A. Aldariseh [18] proposed a new concept in RSA cryptosystem by enhancing the RSA algorithm by the use of additional third prime number in the composition of the public and private key with reduced size, instead of two large prime numbers. In this method they generate the variable *n* Large and the process of analysis of the factors is more complex than the original algorithm.

III. METHODOLOGY OF PROPOSED WORK

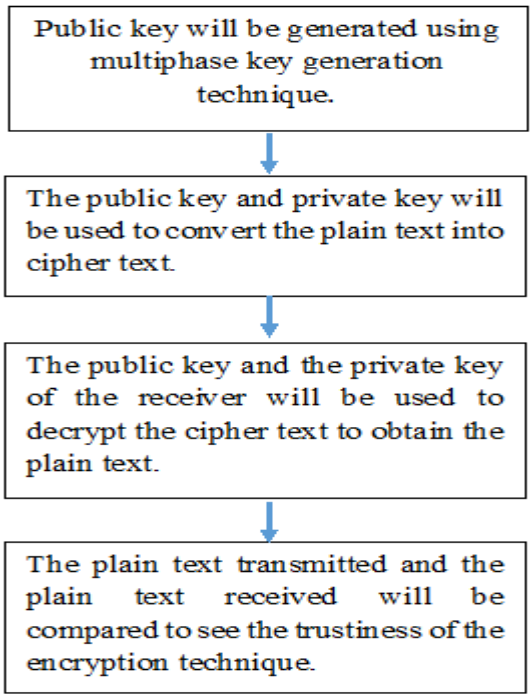
This work will focus on improving the standard RSA encryption algorithm. To achieve this, a generic solution capable of encrypt and decrypt information is to be designed and implemented in order to increase efficiency and security of messages transmitted over the network. This solution will include the review of the model, optimization of the mathematical expression model, which has improved the encryption method, and implementation of algorithms for secure transmission of messages on the network. It has been planned to use MATLAB and/or JAVA as the platform for the implementation of the project. The proposed work will be divided into the following phases:

Generation of the Key

- Encryption of the message
- Decryption of the message
- Effects of various attacks on the encrypted text
- Performance analysis of the proposed technique
- Comparison of the proposed technique and the existing technique

Methods of generating cryptographic keys

Generating keys for cryptography is known as key Generation. The key is used to encrypt and decrypt data whatever the data is being encrypted or decrypted. Modern cryptographic systems are of two type symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA). To secure the communication, key size is the most important parameter in symmetric and asymmetric cryptography. The key size of symmetric cryptography is less than the asymmetric cryptography which makes symmetric cryptography less secure for more sensitive data.



Proposed Flow Diagram

IV. IMPLICATIONS

The proposed work aims at the following expected implications

1) A detailed survey and comparison of various algorithms of key generation techniques
2) Development of a hybrid key generation method
3) Implementation of the key generation method
4) Improvement in security, time and space complexity of data transaction.

V. REFERENCES

1. A William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
2. AtulKahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.
3. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, "Handbook of applied cryptography," CRC press, 1996.
4. Milad Bahadori1, Mohammad Reza Mali, OmidSarbishei, MojtabaAtarodi, Mohammad Sharifkhani,"Novel Approach witch is the Secure and Fast Generation of RSA Public and Private Keys on Smart-Card", 978-1-4244-6805-8/10/$26.00 ©2010 IEEE.
5. H. Handchuh, and P. Paillier, "Smart Card cryptocoprocessors for Public-key cryptography," RSA Laboratories,4 (summer 1999), 6-10.

6. 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.
7. 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.
8. 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.
9. 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.
10. D. Boneh, "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, vol. 46, no. 2, pp. 203-213, 1999.
11. J. J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," Electronic Letters, vol. 18, no. 21, pp. 905-907, 1982.
12. A. Fait, "Batch RSA," Advance in Cryptology CRYPTO '89, vol. 435, pp. 175-185, 1989.
13. D. Boneh and H. Shacham, "Fast Variants of RSA," CryptoBytes, vol. 5, no. 1, pp. 1-10, 2002.
14. T. Collins, D. Hopkins, S. Langford and M. Sabin, "Public Key Cryptographic Apparatus and Method". US Patent #5848, 1997.