ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A SYSTEMATIC STUDY OF RSA AND ITS VARIOUS VERSIONS

Rahul Mishra[1*], Tryambak Hiwarkar[2]
[1,2] Department of Electronics & Communication, Sri Satya Sai University of Technology & Medical Sciences, Sehore (M.P.), India
*Corresponding author Email: rmishra_sati@yahoo.com

ABSTRACT

The term cryptography is derived from the Greek word crypto's. Cryptography is playing a vital role in keeping information secure. Public key cryptography or asymmetric key cryptography makes use of two keys, one is public key and another is private key for performing encryption and decryption respectively. Public key cryptography achieves confidentiality, integrity and availability. Researchers have proposed many public key cryptography systems. One of most popular and widely used public key cryptosystem is RSA. RSA allows key generation, encryption, and decryption. RSA is a block cipher. It divides input data into the fixed size blocks. This paper presents an in depth literature survey of various public key cryptosystems along with latest versions of RSA.

Keywords: Cryptography, Cryptosystems, Public key cryptography, key generation, encryption, decryption, RSA.

I. INTRODUCTION

Cryptography is a Greek word for providing disguised information. It includes transformation of information (Plaintext) into some other form (Ciphertext). The main feature of cryptography is to solve the problems, which are associated with verification, integrity and privacy. A protocol is the sequence of actions, which is designed with two or more sides, through which a goal can be fulfilled. Cryptography also, is associated with the meaning of protocol. Thus, a cryptographic protocol is a protocol that deals with the use of cryptography. This protocol uses cryptographic algorithm and intends to halt attempts of thefts and invasions [1].

The network security becomes more important with the development of various techniques of network development. With the growth in the use of world wide web, this has become even more important as the users can access tools and edit the information. The global society has faced many changes because of the digital revolution. Along with all, this has also increased the number of hackers and viruses.
With the increase in the content on the web, the increase of viruses and bad eyes in the form of hackers, privacy has become an important issue among many.
In today's world, security is a major problem especially when it comes to hiding secret information from total strangers. So, converting a message into a form that cannot be easily cracked is an ultimate option for all. Due to the new and improved techniques used by hackers, sharing information on the internet is less secure now days. To overcome such problems have evolved techniques like steganography and cryptography. Encrypting and decrypting keys are different. [2]

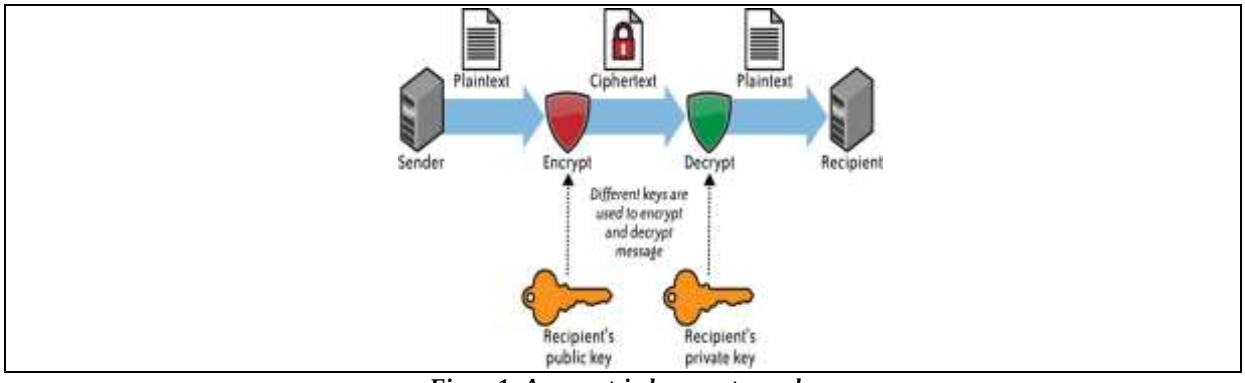

Figure1: Asymmetric-key cryptography

Figure 1 presents asymmetric key cryptography. The data is encrypted and decrypted using a pair of keys. The secret key and shared key is available at sender side as well as receiver's side.

In figure 2, model of cryptography is shown. The message is transformed in to cipher text. The cipher text is transmitted from sender side to receiver side by using the internet. At receivers end, the cipher text is received. Then the cipher text is transformed into the original plain text by using the decryption algorithm and the key. The decryption process is exactly a reverse of encryption process.
The security services include [3]:

- Data Confidentiality
- Data Integrity
- Authentication
- Non repudiation
- Access Control

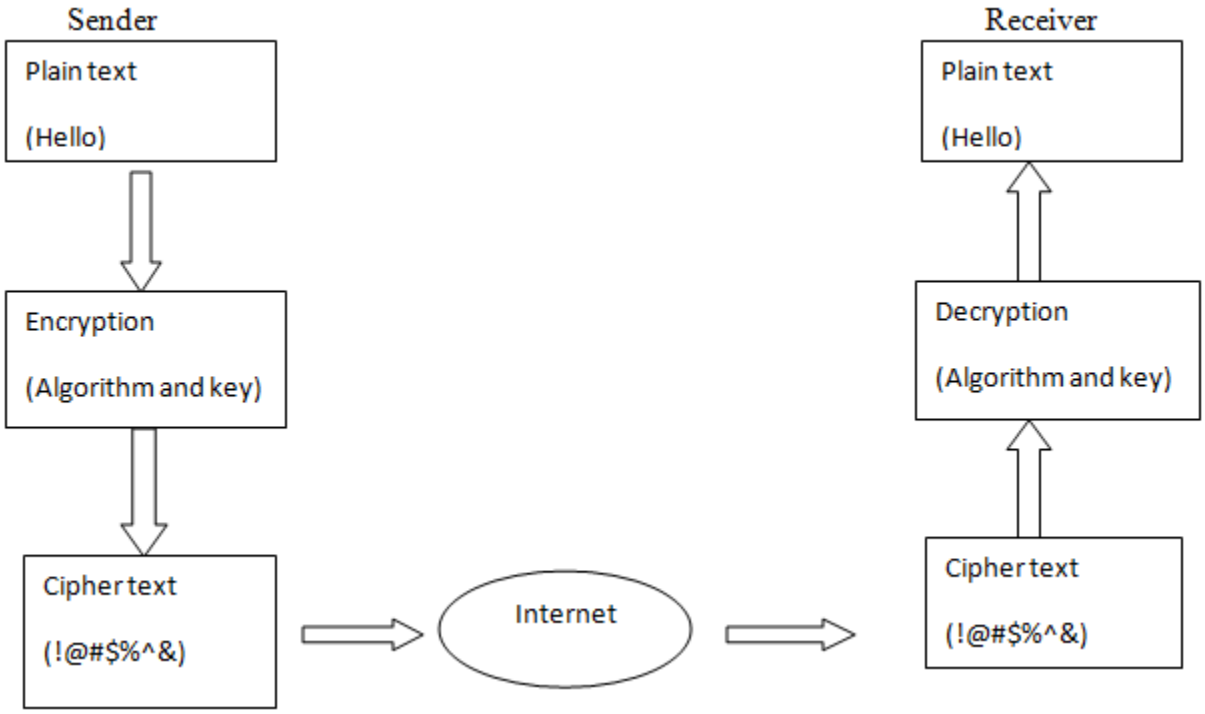

Figure 2: Basic Model of Cryptography

II. LITERATURE SURVEY

The most important part of RSA performance covers the decryption performance. Because of the security constraints, decryption exponent is usually considered to be very large of the order of the modulus size. Large size of the decryption exponent (d) lowers down the speed of decryption side. In this section, RSA variants which are based on the improvement in decryption speed are discussed. This is required in almost every case where RSA cryptosystem is used. Practical relevance of these variants lies in the signature generation (or decryption method) in heavily loaded web servers or small handheld devices, e.g. the bank customer is required to generate the signature (using his/her private key) on small device (like smart phones). The decryption method needs to be optimized in this case by reducing the computational complexity of the

decryption method. This can be achieved by reducing the bit size of the decryption exponent in the computations involved in decryption method.

One of most popular and widely used public key cryptosystem is RSA. RSA allows key generation, encryption, and decryption. RSA is a block cipher. It divides input data into the fixed size blocks [4].The steps involved in the RSA algorithm is given below:

Step1: Choose two random prime numbers p and q such that p is not equal to q.
Step2: Compute n=pq.
Step3: Compute f(n)=(p-1)(q-1) where f is Euler's totient function. This value is used as private.
Step4: Select an integer e for encryption such that gcd((f (n),e)=1 and 1<e< f(n).
Step5: Compute $d = e^{-1} \pmod{f(n)}$. d is the modular multiplicative inverse of e. This is a private key.
Step6: Compute Ciphertext $C = M^e \bmod n$ where M is the plaintext or the actual message.
Step7: Send the cipher text to receiver
Step8: Obtain plaintext $M = C^d \bmod n$.

In any communication system including internet, satellite and mobile, it is impossible to prevent the important or sensitive information from eavesdropping or losses when the information is broadcasted through the channel (wire or wireless). So security of information has become increasingly important for any application [6].

The protection of information for long period time is very critical in many environments. One way of implementation this protection with high activity is RSA cryptosystem. In this paper the old algorithm of RSA system is showed. And for more complexity and to increase time of attack coding. A new coefficient is z has been added to generator function Φ(n) in additional to selected p and q which are depended in old algorithm[5].

To ensure the proper complexity of RSA algorithm, a new coefficient is Z has been added to generator function j(n) as follow:

$$\Phi(n)=(p-1)x(q-1)x(Z\ 1)$$

And then complete all steps of last section take Z in our consideration. It is clear that the degree of eq. becomes grater by 1 about that similar in previous section, consequentially that effects on all equations of RSA algorithm and their attacks [7].

The authors in [8] proposed a new algorithm based on RSA. The proposed algorithm was having new parameters to increase the complexity of encryption process and decryption process. The proposed method is secure in comparison to previous methods. But it is computationally very expensive. Use of many parameters in encryption and decryption process, makes it very time inefficient.

Work done in [9] presented a new modulus instead of modulus n. in previous methods, n was product of 2 prime numbers. Instead of n , a new variable in transmitted to receiver. It is more secure but calculation of new variable is taking a lot of time comparatively.

Another updated version of RSA was proposed by authors in [10], it uses the concept of four prime numbers instead of two. Four prime numbers were multiplied to find multiplication modulus. They also proposed a time efficient key generation process. Generation of public key and private key are dependent on new variable. They were not dependent on multiplication modulus n.

Batch RSA [11] in 1989; the work was done to accomplish many decryption processes at the cost of approximately one. More than one jobs are combined to make a batch and decryption of the complete batch is performed in a single process, thus reducing the cost of multiple decryption processes.

ISSN 2348 – 8034
Impact Factor- 5.070

This variant works for small and different public exponents for the same modulus N. Decryption of the two cipher texts in Batch RSA can be done at the cost of approximately one RSA decryption. Relevance of this variant is restricted to cipher texts with only very small public exponents and where decryptions have to be handled in bulk, e.g. in banks.

As this variant does not contribute much to the present work only the basic idea is given here. Concept of the computation can be understood by an example.

Key generation and Encryption methods are same as in standard RSA. Two mes- sages (M_1 and M_2) are encrypted with small public exponents resulting in two cipher texts C_1 and C_2. Public keys for C_1 and C_2 are assumed to be $e_1 = 3$ and $e_2 = 5$ respectively.

MultiPrime RSA[12] was designed to enhance the decryption speed of RSA cryptosystem by taking more than two primes for the modulus. It consists of k primes $p_1, p_2 ... p_k$ instead of using only two as in standard RSA. This variant is more suitable for use in resource constrained devices as it is more efficient in terms of computational speed as compared to RSA CRT.

In this variant [13] also, the purpose was to improve the decryption time of RSA algorithm. Instead of using multi- ple primes for the modulus, only two primes are used but with smaller sizes as compared to standard RSA. In the algorithm $N = p^{b-1}q$, where p and q are n/b bits. Due to the use of only two primes MultiPower RSA is more efficient than MultiPrime RSA [12].

In [14], the public and private exponents (e, d) are generated and shared by two instances with different modulus. Sharing of the parameters by two RSA instances reduces the memory requirement by the cryptosystem.

Three schemes are proposed for Dual RSA; Dual RSA Small-e, Dual RSA Small-d and Dual Generalized Rebalanced RSA (DGRR). These three schemes are based on small public exponent, small private exponent and balanced public/private exponents respectively. The schemes are suitable for applications like blind signatures and authentication/secrecy.

III. CONCLUSION

RSA is most widely used technique for keeping data secret. This paper presented the systematic literature review of basic RSA method along with all the crucial versions of RSA. Although many versions of RSA have been proposed by different authors around the world. RSA uses large prime numbers for data handling. So there is always a scope of improvement in terms of computation time and memory space used.

References:

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
[2] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.
[3] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM vol. 21 (2) , pp.120–126, 1978.
[4] A.H. Al-Hamami and Aldariseh IA, "Enhanced method for RSA cryptosystem algorithm", international conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, IEEE, pp. 402-408, 2012.
[5] P. Anuradha Kameswari*, R. Chaya Kumari and L. Praveen Kumar 2011. SCHEME OF ENCRYPTION FOR BLOCK CIPHERS AND MULTI CODE GENERATION BASED ON SECRET KEY, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011
[6] Shamir, A. 1984. A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem;

Information Theory, IEEE Transactions on , Volume: 30 Issue: 5 , Sep 1984
Page(s): 699704
[7] Forouzan (2007), Cryptography And Network Security, Special Indian Edition
[8]. R S Dhakar, A K Gupta and P Sharma, "Modified RSA encryption algorithm (MREA)", 2nd ICACCT, IEEE, pp. 426-429, 2012.
[9]. R. Minni, K. Sultania and S.Mishra, "An algorithm to enhance security in RSA" , 4th ICCCNT, IEEE , pp.1-4, 2013.
[10]. M.Thangavel, P. Varalakshmi, M. Murrali and K.Nithya, "An enhanced and secured RSA key generation scheme" Journal of Information Security and applications, Elsevier, vol 20, pp.3-10, 2015.
[11] Amos Fiat. Batch RSA. In Advances in Cryptology–CRYPTO'89 Proceed- ings, pages 175–185. Springer, 1990.
[12] Martin E Hellman and Ralph C Merkle. Public key cryptographic apparatus and method, 1980. US Patent 4,218,582.
[13] Tsuyoshi Takagi. Fast RSA-type cryptosystem modulo pk q. In Advances in Cryptology–CRYPTO'98, pages 318–326. Springer, 1998.
[14] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M Jason Hinek. Dual RSA and its security analysis. Information Theory, IEEE Transactions on, 53(8): 2922–2933, 2007.