A Literature Survey of Common RSA based Cryptosystems

Bharti Choudhary[1], Prof. Apurva Kukade[2]
[1,2]*Alpine Institute of Technology, Ujjain*

***Abstract*- The backbone of the modern world is electronic communication. Data is transferred from one place to another in almost no time using the electronic medium. But it also exposes the confidential data to the intruder. RSA is the most common and efficient cryptography technique that is used for the purpose of encrypting the content and then sending it over the channel, then than at receivers end the content is decrypted and converted in to original form. Although there are many security mechanisms are available. But there is a continuous need to improve the existing methods. Cryptography is a security mechanism which caters the security services of world in perfect manner.**

Index Terms- Cryptography, encryption, decryption, RSA algorithm, modular arithmetic

1. INTRODUCTION

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. While communicating any information via an unsecure channel to its righteous owner, security issue becomes important. To avoid such problem, cryptography and steganography are the main ways of communicating such information in a stealth mode without anyone knowing what it is.

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. There is a need of a system which can control the curious eyes from getting in a harm way. In such a situation, steganography and cryptography emerge as a savior for such important information. [1,2]

With the increase in the content on the web, the increase of viruses and bad eyes in the form of hakers, privacy has become an important issue among many. In such situation, Image Steganography has many important roles and application. Specially, when two parties want to communicate secretly.

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 a days. To overcome such problems have evolved techniques like steganography and cryptography.

If we uncover the pages of history we find that in those times too, secret information was passed from one party to another via various means like invisible ink, tattoos and much more and that has become the brain child for the present techniques like cryptography where the online secret information sharing has become more secure for parties who have a sensitive information that cannot fall in wrong hands.

Cryptography is the craftsmanship and study of accomplishing security by encoding data to make them non-meaningful organization. Cryptography, a word with Greek birthplaces, signifies "mystery composing." However, we utilize the term to allude to the science and craft of changing messages to make them secure and invulnerable to assaults. Figure 2 demonstrates the parts engaged with cryptography [6].

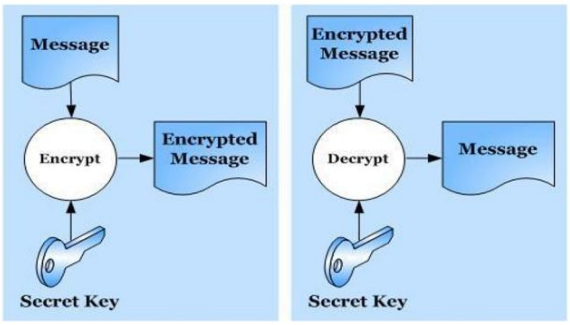

Figure 1 cryptography component

Fundamental terms utilized in cryptography

- Plain content Clear content is an intelligible configuration or unique message comprehend by any individual. For instance, in the event that A needs to make an impression on B + "Hi" at that point here "hi" is a plain instant message.
- Cipher content It is mixed up message or after the encryption the subsequent message is called figure content. For instance, "sd45@#$" is a Cipher Text created for "hi".
- Encryption-The procedure of plain content proselytes figure content called encryption. Cryptography utilizes the encryption method to send private messages through an unreliable channel. An encryption calculation and a key are the fundamental needs of encryption. An encryption calculation implies the strategy that has been utilized in encryption. Encryption happens at the sender side.
- Decryption-The procedure of figure content believers plain content called unscrambling. Cryptography utilizes the decoding procedure at the recipient side to get the first message from figure content. The procedure of decoding requires two things-unscrambling calculation and key. For the most part the encryption and unscrambling calculation are same, with the comprehended invert ideas.

1.1 Types of Cryptographic Systems

Each cryptographic system requires the use of some key to secure the information. Based on the number of keys used, modern cryptosystem can be classified: private key cryptosystem and public key cryptosystem. Both of these cryptosystems are briefly described as follows:

1.1.1 Private Key Cryptosystem

Share a single key in the private key cryptosystem (or symmetric key cryptosystem) (figure 1). This key is used by the sender to scramble the plain content to acquire the content of the figures. To restore the plain content, the beneficiary uses a similar key to unscramble the figure's content.

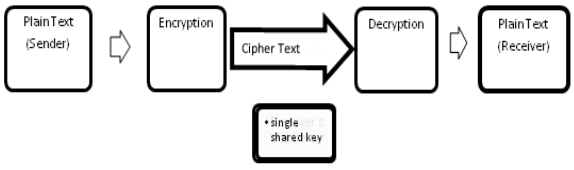

Figure 2: Private Key Cryptosystem

1.1.2 Public Key Cryptosystem

Creator presented the idea of the open key cryptosystem. Diffie just as M. Hellman[3]. Two keys are utilized in the open key cryptosystem (Figure 1.2), one key is known to all freely, while the other key is stayed discreet. Open key is utilized to encode (scramble) the message and to decipher (unscramble) the encoded message utilizing the private key. All open key cryptosystems depend on somebody way (simple to ascertain yet hard to turn around) capacities. Just the planned client can utilize some mystery parameter (Trapdoor one route work) to compute the single direction work.

Legal users have access to the present secret parameter, however the key parameter isn't accessed by amerciable users. 2 giant prime numbers product is assumed to operate a way. conniving the merchandise of 2 giant prime numbers is easy, however it's assumed to be tough to search out the prime numbers from the given giantcomposite whole number. This problem is considered to be the security of RSA[4], Rabin[9] etc.

Other known public key cryptosystems are based on different types of hard problem; e.g. the problem of finding the discrete logarithm used in Diffie-Hellman scheme (key exchange protocol), ElGamal etc. and the problem of computing elliptic curves as used in Elliptic curve cryptography.

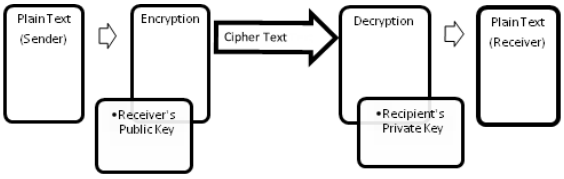

Figure 3: Public Key Cryptosystem

2. LITERATURE SURVEY

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. It widely used in electronic commerce protocols, and is believed that its security depends on the difficulty of decomposition of large numbers. RSA is secure because it is able to Public Key Cryptography is based on the principle of one way functions that can be easily computed while their inverse function is difficult to calculate. It employs two different keys related mathematically such that one is used for encryption and the other for decryption.

Its two main keys are used i.e. in encryption and decryption. RSA is an algorithm based in the theorem of factoring two large prime numbers. [3, 5]

RSA Algorithm has following steps.

1. Select two large prime numbers P and Q.
2. Calculate N=P*Q
3. Select the public key (encryption key) E such that it is not a factor of (P-1) and (Q-1).
4. Select private key (decryption key) D such that the following equation is true:
   (D*E) mod (P-1) * (Q-1) =1
5. For encryption, calculate the cipher text CT from the plain text PT as follows:
   CT=PTE mod N
6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as follows:
   PT=CTD mod N

In 2005, C. Dods, N. P. Savvy and M. Stam [7] talked about different issues related with mark plans dependent on upon hash capacities. Such plans are at present alluring in some constrained applications, however their significance may increment if at any time a down to earth quantum PC was constructed. They additionally examined issues identified with both their execution and their security and give the primary complete treatment of commonsense usage of hash based mark conspires in the writing.

In 2005, Z. Shao [78] proposed another computerized mark conspire dependent on the challenges of at the same time settling the considering and discrete logarithm issues has been proposed by Tzeng et al. in 2004. In the proposed plan, every client utilizes a typical math modulus and just possesses one private key and one open key. Despite the fact that Tzeng and associates guaranteed that their plan can't be overruled by some conceivable confinements, they demonstrated that their plan isn't verify if aggressors can tackle discrete logarithm issues or figuring composite numbers.

In 2006, D. R. Stinson [9] contemplated issues identified with the thought of "secure" hash capacities. A few vital conditions are considered, just as a famous adequate condition (the purported irregular prophet demonstrates). Specifically, he considered the essential inquiry "does impact obstruction suggest preimage opposition?" and gave incomplete responses to this inquiry – both positive and negative! – in view of consistency properties of the hash work under thought.

In 2006, Carlos Cid [10] underscored on cryptographic hash capacities. His paper gives an outline of cryptographic hash capacities and a portion of the ongoing advancements influencing their security, specifically the disclosure of proficient techniques for developing impacts for calculations, for example, MD5 and SHA-1. We additionally talk about the numerous ramifications of these ongoing assaults, and the conceivable bearings for the improvement of the hypothesis of hash capacities.

In 2007, Zanin, Di Pietro, and Mancini [11] in their examination introduced another appropriated mark convention dependent on the RSA cryptographic calculation, which is reasonable for expansive scale impromptu systems. This mark convention is appeared to be disseminated, versatile, and powerful while staying subject to tight security and engineering requirements. The investigation uncovers that the power of this convention plan can be upgraded by including just a small amount of the hubs on the system.

Zanin et al. shown that their convention conspire is right, since it permits a picked number of hubs to create a substantial cryptographic mark; it is secure, in light of the fact that an assailant who bargains less than the given number of hubs can't disturb the administration or produce a sham mark; and it is effective, in view of the low overhead in contrast with the quantity of highlights gave.

The creators in [12] proposed another calculation dependent on RSA. The proposed calculation was having new parameters to build the unpredictability of encryption procedure and decoding process. The proposed technique is secure in contrast with past strategies. Be that as it may, it is computationally over the top expensive. Utilization of numerous parameters in encryption and unscrambling process, makes it very time wasteful.

Work done in [13] introduced another modulus rather than modulus n. in past techniques, n was result of 2 prime numbers. Rather than n , another variable in transmitted to beneficiary. It is increasingly secure yet estimation of new factor is taking a ton of time relatively.

Another refreshed rendition of RSA was proposed by creators in [14], it utilizes the idea of four prime numbers rather than two. Four prime numbers were

duplicated to discover augmentation modulus. They additionally proposed a period effective key age process. Age of open key and private key are reliant on new factor. They were not reliant on augmentation modulus n.

Bunch RSA [15] in 1989; the work was done to achieve numerous unscrambling forms at the expense of roughly one. More than one occupations are consolidated to make a group and unscrambling of the total cluster is performed in a solitary procedure, along these lines lessening the expense of numerous decoding forms.

This variation works for little and distinctive open examples for a similar modulus N. Decoding of the two figure messages in Batch RSA should be possible at the expense of roughly one RSA unscrambling. Pertinence of this variation is confined to figure writings with truth be told, exceptionally little open examples and where decodings must be taken care of in mass, for example in banks.

As this variation does not contribute a lot to the present work just the essential thought is given here. Idea of the calculation can be comprehended by a model.

Key age and Encryption techniques are same as in standard RSA. Two mes-sages (M1 and M2) are encoded with little open examples bringing about two figure writings C1 and C2. Open keys for C1 and C2 are thought to be e1 = 3 and e2 = 5 separately.

MultiPrime RSA[16] was intended to upgrade the unscrambling velocity of RSA cryptosystem by taking multiple primes for the modulus. It comprises of k primes p1, p2 ...pk as opposed to utilizing just two as in standard RSA. This variation is increasingly reasonable for use in asset obliged gadgets as it is progressively proficient regarding computational speed when contrasted with RSA CRT.

From systematic literature review performed in this section, It is clear that the Common Problems in Existing RSA Variants:

- The main disadvantage of RSA decryption is its slower speed
- Large key generation time
- Not secure against wiener's attack
- Problem arise to common modulus attack
- known plaintext attack are possible

3. CONCLUSION

This paper has elaborated the basic concept of cryptography and the key management schemes. A review of modern methods is also done in brief. The most of the modern data security techniques have been reviewed. Each of the method has been analyzed with the advantages and the disadvantages. Then a list of common problems in the current version has been identified. On basis of the research gap identified, the problem was formulated.

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] Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE 2012.

[4] Prof.Dr.Alaa Hussein Al-Hamami,Ibrahem Abdallah Aldariseh ,"Enhanced Method for RSACryptosystem Algorithm" 2012International Conference on Advanced Computer Science Applications and Technologies, IEEE 2012.

[5] V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[6] Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Iss ue 2, June 2011 pp.192-192.

[7] Koji Chida, Shigenori Uchiyama, and Taiichi Saito. A new factoring method of integers N = pr q for large r. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 85(5):1050–1053, 2002.

[8] Alexander May. Secret exponent attacks on RSA-type schemes with moduli N = pr q. In Public Key Cryptography–PKC 2004, pages 218–230. Springer, 2004.

[9] Scott A Vanstone and Robert J Zuccherato. Short RSA keys and their generation. Journal of Cryptology, 8(2):101–114, 1995.

[10] Scott A Vanstone and Robert J Zuccherato. Using four-prime RSA in which some of the bits

are specified. Electronics Letters, 30(25):2118–2119, 1994.

[11] Hung-Min Sun and Mu-En Wu. Design of rebalanced RSA-CRT for fast encryption. In Proceedings of Information Security Conference, pages 16–27, 2005.

[12] R S Dhakar, A K Gupta and P Sharma, "Modified RSA encryption algorithm (MREA)", 2nd ICACCT, IEEE, pp. 426-429, 2012.

[13] R. Minni, K. Sultania and S.Mishra, "An algorithm to enhance security in RSA", 4th ICCCNT, IEEE, pp.1-4, 2013.

[14] 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.

[15] Amos Fiat. Batch RSA. In Advances in Cryptology–CRYPTO'89 Proceedings, pages 175–185. Springer, 1990.

[16] Martin E Hellman and Ralph C Merkle. Public key cryptographic apparatus and method, 1980. US Patent 4,218,582.