A Novel Key Generation Based RSA for Performing Encryption and Decryption of Data

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. This paper will propose a novel key generation technique for both sender and receiver. This proposed technique results will be compared with existing techniques.**

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

1. INTRODUCTION

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 1 demonstrates the parts engaged with cryptography [6].

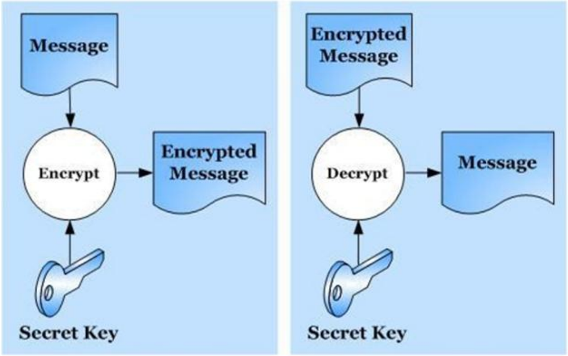

Figure 1 cryptography component

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.

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:
   $CT=PT^{E}$ 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:
   $PT=CT^{D}$ 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 demonstrate). 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.

In [15], a new version of RSA was proposed. This version makes use of four prime numbers. It has also given a new encryption key generation method. Although this key generation method is complex and taking a lot of time. In place of n they have used a single prime number w in encryption and decryption. This makes multiplication modulus weaker. Decryption time is also more.

3 PROPOSED METHODOLOGY

The steps of proposed methodology are as follows:

Modified RSA Key Generation:

Algorithm is as follows:

1. Start
2. Read four prime numbers p, q, r and s
3. Calculate t = p * q * r * s
4. Calculate phi(w) as follows
   - Phi(w) = (p-1) * (q-1) * (r-1) * (t-1)
5. Generate two unique random number P1 and P2, which are not co prime to phi(w) using random number generator
6. Calculate v = (P1 *P2) mod t
7. Calculate public key e such that it is not co prime of (phi(w) * v)
8. Calculate private key d such that (d * e) mod (phi (w) * v) =1
9. Calculate n such that
   - x= nextprime(p * q)
   - y = nextprime (r * s)
   - n= x * y
10. stop

Modified RSA encryption algorithm:

1. start
2. calculate $C = M^e$ mod n, where C is cipher text, M is plain text and e is encryption key
3. stop

Modified RSA decryption algorithm:

1. start
2. $M = C^d$ Mod n
3. stop

4. RESULT ANALYSIS

In this section, the key generation time and encryption time of modified RSA algorithm are compared with HRSA. Both algorithms are implemented in java on 2.8 Ghz dual core processor with 2 GB RAM. Random numbers are generated using inbuilt java methods.

The input plain text is:
123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210123456789098765432101234567890987654321012345678909876543210

The key generation time and Decryption time of both the algorithms is shown below in table:

Algorithm Name	Decryption Time in ms	AliceKey Generation Time in ms	Bob Key Generation Time in ms
HRSA	114	3810	4258
Modified RSA	64	2454	2253

Table1: Result Comparison

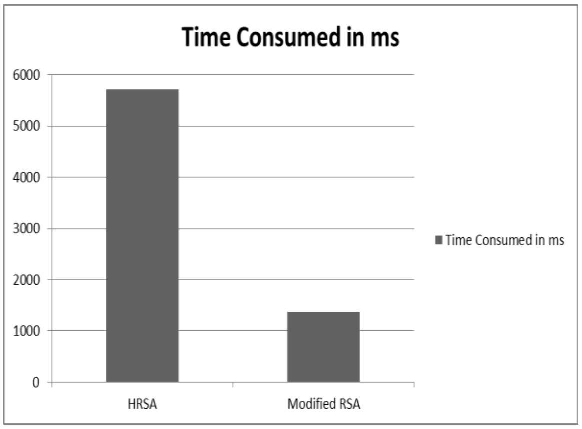

Figure 2: Comparison of Alice Key Generation Time

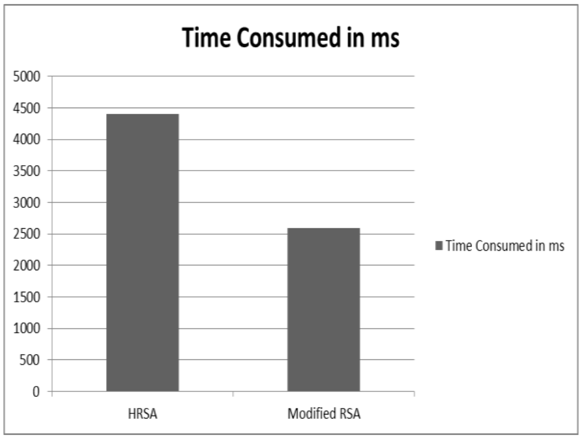

Figure 3: Comparison of BoB Key Generation Time

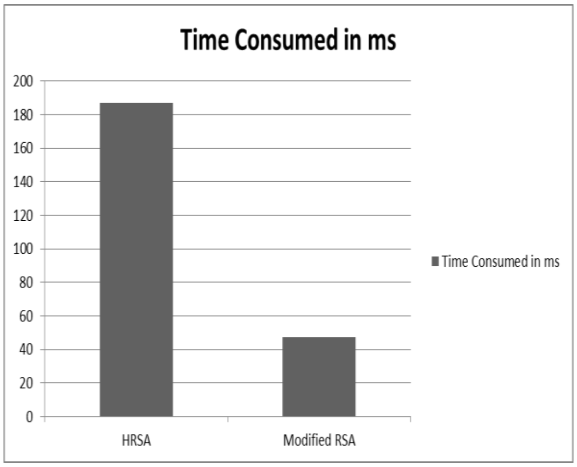

Figure 4: Comparison of Decryption Time

5. 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. This paper has proposed a new method for sender and receiver key generation. The proposed key generation technique is taking less time in comparison to existing technique.

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 onAdvanced 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] 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] Prabhat K. Panda, Sudipta Chattopadhyay,” A Hybrid Security Algorithm for RSA Cryptosystem”, 2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017), Jan. 06 – 07, 2017, Coimbatore, INDIA