A SURVEY PAPER ON RSA CRYPTOSYSTEMS AND SUGGESTIVE ENHANCEMENTS

Suhrid Barthakur, Partha Pritam Paul, Anirban Chatterjee, Jasbir Singh Birdi

National Institute of Technology Silchar
Cachar,Assam,India

suhrid53@gmail.com , Parthap177@gmail.com , reachanirban95@gmail.com , jappy95jasbir@gmail.com

***Abstract*— Nowadays, security is used over the network to protect the transmission of information. It is also used in a variety of applications in which cryptographic algorithms play an important role against malicious attacks. Rivest–Shamir–Adleman algorithm is widely used in the popular implementation of public-key infrastructures. In this research work, we present a comparative survey on cryptographic algorithms including their benefits and drawbacks. Finally, we present a modified version of RSA model which enhances the network security.**

***Keywords*— Encryption, Decryption , RSA , Cryptography, Computer Security.**

I. INTRODUCTION

Cryptography is a science used for secure communication. Data is encrypted and sent over the network in such a way that only the receiver can transform it to the original text. In traditional cryptography, such as prior to the 1970s, the encryption and decryption operations are performed with the same key. This means that the party encrypting the data and the party decrypting it need to share the same decryption key.Its main goal is to keep data safe from adversaries or third parties. The main challenge is to ensure that the sender and the recipient agree on the secret key without anyone knowing.

A. Types of Cryptography[12]

1. *Secret-key cryptography:* It is a cryptography where same key is used for encryption and decryption.
   Eg: DES, AES.
2. *Public-key cryptography:* It is a cryptography where different keys are used for encryption and decryption. It is also known asymmetric cryptography.
   Eg: RSA.

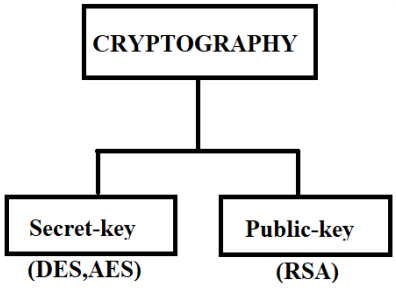

Fig 1: classification of cryptography

B. Fundamental Concepts

1. Plain Text: The message sent by the Sender(non-encoded).
2. Ciphertext: The plaintext is encrypted known as cipher text.
3. Key: The key used for Encryption and decryption.
4. Encryption: It is a method used for encrypting plain text (data) to cipher text.
5. Decryption: It is a method used for decrypting plain text (data) from the ciphertext.

RSA (Rivest–Shamir–Adleman)

RSA is a cryptosystem for public-key encryption also known as asymmetric cryptography. It is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. It is based on the fact that it is difficult to factorize a large integer.

It involves four steps:

1. Key generation.
2. Key distribution.
3. Encryption.
4. Decryption.

RSA uses two pairs of related keys (**Public key**) uk{ e, n} for encryption and (**Private key**) vk{d,p,q} for decryption. So, let's see how these four steps are implemented:-

1. Key Generation

a. Receiver chooses two very large prime numbers p & q.

b. Calculating the modulus as: $n = p * q$.

c. Calculate Euler's value as

$$(p. q) = (p - 1)*(q - 1).$$

d. Now, Choose an integer 'e' such that

$$1 < e < (p. q) \quad \text{and} \quad \gcd[e, (p. q)] = 1$$

e. Calculate 'd' from the equation: $d * e \equiv 1 \bmod()$.

which implies:-

$$(d * e) \bmod() = 1.$$

$$d * e = k * + 1$$

,where k is quotient

f. After the key generation Receiver announces uk{ e, n} as public Key and vk{d, p,q} is kept secret as private key.

2. Key Distribution

Now if Sender wants to send a secret message to Receiver using RSA then the sender must know the public key to encrypt the message and the receiver uses its private key to decrypt the message.

3.Encryption

The message or the plaintext(P) that the sender wants to send is encrypted to Ciphertext(C) as:

$$C = P^e \bmod(n)$$

4.Decryption

After receiving the ciphertext the receiver uses its private key(d,p,q) to decrypt the message as:

$$P = C^d \bmod(n)$$

Weaknesses of RSA

- If the primes(p & q) used are small enough then a computer will make easy work of factoring 'n'.
- If private keys of users are not available, it is vulnerable to impersonation.
- The maximum size of the message(P) transferrable at once is such that size of P is less than size of the key(n). Currently the maximum recommended key size is 2048 bits.
- It is very slow for long messages.

II. LITERATURE SURVEY

This section discusses about the survey on some following papers in RSA cryptography:

Jia-Lin Sheu *et al.*[1], worked on efficient VLSI implementation of the modular exponentiation, commonly used in RSA cryptography, based on the asynchronous behaviour of the modular multiplication, which increases the throughput rate of modular exponentiation in RSA cryptosystem. The limitation of this approach is that to increase the efficiency, hardware requirements need to be high.

Yong-Kyu Kang et al.[2] proposed two implementation methods to optimize a 1024- bit RSA processor are presented. They used modified Montgomery algorithm which made the modular exponentiation simple using one additional multiplication in L-R method or parallel processing in R- L method. As a result, the former minimized the hardware requirement and the latter efficiently reduced the operating time.

Hung-Min Sun et al. [3] proposed dual RSA algorithm and also analyzed the security of the algorithm. They presented new variants of RSA whose key generation algorithms output two distinct RSA key pairs having the same public and private exponent's two applications for Dual RSA were blind signatures and authentication. The security of Dual RSA was raised in comparison to RSA when there were values of e and d is small. The main disadvantage of using dual RSA was that the computational complexity of the generation of key algorithms is increased

K.Gomathi et al.[4] proposed Weight based Clustered Key Management scheme using RSA for Wireless Mobile Ad hoc Networks . This approach is based on combined weight metric that takes into account of several system parameters like the degree difference of the node, transmission range, battery power and mobility of the sensor node. The major limitation of these schemes is that most of them rely on a Trusted Third Party (TTP), thus not fulfilling the self-organization requirement of an ad hoc network.

H. C. Williams [5] modified RSA public-key encryption algorithm. His opinion is, if the encrypting message procedure was broken into a certain operations than remainder used as modulus could be factored after few more operations. This technique was in similar appearance to RSA. The main limitation of this scheme was that very large prime numbers were used and generated mathematical errors were observed.

Ravi Shankar Dhakar *et al.*[6] presented modified RSA encryption algorithm. They improved the security by presenting a new cryptography algorithm based on additive homomorphic properties called Modified RSA Encryption Algorithm (MREA).The main disadvantage is that involvement of many parameters makes the system overloaded.

Gaurav R. Patel *et al.*[7] designed a new algorithm which is combination of RSA and Diffie-Hellman. The main applications of RSA algorithm are cryptography and digital signature. The security of RSA depends on the confidentiality of the keys. The corresponding keys should be provided to the communicating parties prior to communication and for this purpose, Diffie- Hellman is applied.

Aarushi Rai *et al.*[8] proposed a method that takes four prime numbers in RSA algorithm. Instead of sending public key directly, two key pairs of public keys are sent to the receiver. And two public keys would be sent to the user. The scheme has speed enhancement on RSA decryption side by using Chinese remainder theorem. The limitation of this scheme is by including more keys, difficulty of analysis of algorithm is increased.

Prabhat K. Panda *et. al.*[9] presented a new Hybrid security algorithm for RSA cryptosystems named as Hybrid RSA (HRSA).This scheme used four prime numbers which increases the key generation time and consequently increases the system breaking time. The main disadvantage with this is, it has been achieved at expense of increased time-complexity.

R. Minni et al. [10] introduced a security feature where n was replaced by a new variable and used for encryption and decryption process. So it becomes difficult to trace back the factor of n and as a result the security level increases as compared to RSA, where n is the product of two prime numbers. This has been achieved at the expense of slightly increase in time complexity.

III. PROPOSED RSA MODEL

Motivated by the above research trends and challenges, we proposed a modified RSA model which is based on mainly:

a. Protecting the private key in case the attacker successfully factorizes the modulus n .
b. Increase the ability to send larger messages through RSA.
c. Faster key generation.

The modifications suggested are listed below :

a. In our model unlike the base model which uses two large random primes p,q we use a random number of large primes to generate N. This adds an extra level of security as factoring N becomes harder by multiple folds.
b. To further enhance the security further we introduce a pseudo Modulus say F(N).
c. In order to permit large message to be transferred we split the message into blocks of sizes 1024 bits We then encrypt each of the message blocks and send it through the channel.

Flow Chart of The Modified RSA is given below[11].

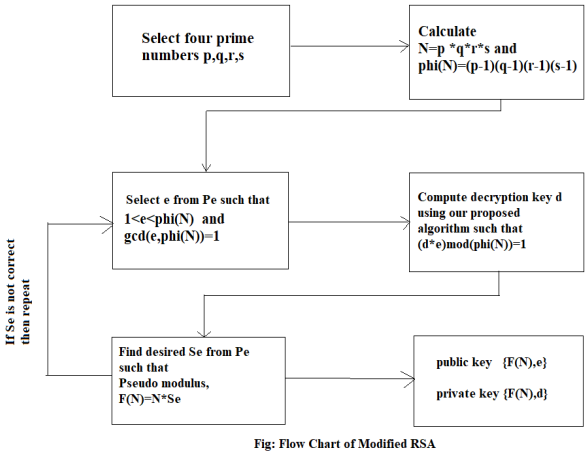

Fig: Flow Chart of Modified RSA

The modified algorithm is depicted below :

1. Select a random number (say 4) of large prime numbers p,q , r , s.
2. Compute φ(N)=(p-1)*(q-1)*(r-1)*(s-1).
3. Now we compute a variable Pe (consists all possible values of e) such that gcd[e ,φ(N)]=1.
4. In next step select a value of e from Pe and calculate "d" such that [e*d mod φ(N)] = 1
5. In this step, finds the desired "S_e" where "S_e" are special value over the range of values "P_e" ,which are multiplied by 'n' to produce pseudo modulus F(N)=n*S_e. The new modulus "F(N)" is used in place of actual modulus "n" as shown in figure 2 and do the process of encryption and decryption. If the results of decryption and plaintext are matched, then the selected value that was considered "S_e" will be the desired value. Otherwise if the plaintext and decryption results are not matched then the selected number must be again set for S_e.
6. If "S_e" has not found go back to step 4 change the value of "e" and compute "d" then repeat step 5.

Finally after S_e has been found we get our fake modulus F(N)=n*S_e .This gives us the public key (F(N) , e) and private key:(F(N),d).The encryption is done as $C=P^e \bmod F(N)$,And the decryption as $P=C^d \bmod F(N)$ .The encryption can be made faster by using Chinese Remainder Theorem.

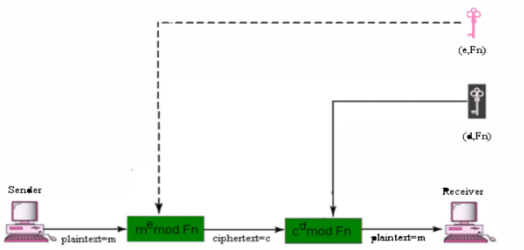

Figure 2: encryption & decryption using"*Fn*"

IV. Performance Evaluation

Based on the original model and proposed model different comparisons have been made.

RSA vs PSC(proposed scheme)

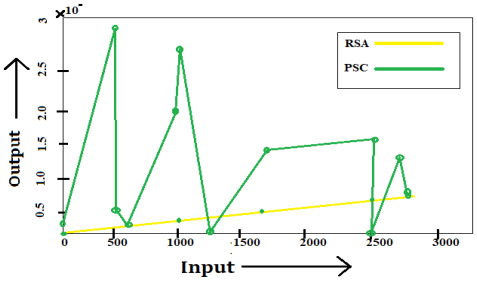

Fig: 3 RSA vs PSC

This figure depicts the comparison between the RSA and Modified RSA scheme to find the inverse using public key. In RSA the input primes and result of inverse on output are the same, while not so in case of the modified scheme.

Comparison of Time-complexity between RSA and PSC.

Time Complexity	RSA	Modified RSA
Encryption	$O(\log(N)^3)$	$O(\log(N)^3 k)$
Decryption	$O(\log(N)^2)$	$O(\log(F(N))^2)$

k=no.of iterations after which correct S_e is found. k<=sizeOf(P_e).

Overall Comparison between RSA and PSC

RSA	Modified RSA
Uses two prime numbers	Uses four Prime numbers
Less Secure	More Secure
Key generation slower	Key generation Faster
More Vulnerable to attacks	Less Vulnerable to attacks

V. Conclusion

In this paper we proposed a modified model of RSA that has the advantage over base model that if anyone is able to factorize the modulus "n" in RSA, can easily decrypt the message. However, in our case the result produced by "S_e" will

produce pseudo modulus "F(n)" and this is publically announced. If anyone tries to factorize the "F(n)", he can't find out the original value of decryption key, because the input primes are not the actual result of factorization, and also using random number of initial input primes increases the overhead of finding them ,hence result produced by just initial factorization of F(n) will not give the decryption key. This thereby adds extra security to the algorithm.

REFERENCES

[1] Ming-Der Shieh, Chien-Hsing Wu , Ming-Hwa Sheu, Jia-Lin Sheu and Che-Han Wu,*" Asynchronous implementation of modular exponentiation for rsa cryptography"* , 30-30 Aug. 2000, Cheju, South Korea.

[2] Taek- Won Kwon, Chang-Seok You, Won-Seok Heo, Yong-KyuK ang, and Jzin-Rim Choi," *Two implementation methods of a 1024-bit rsa cryptoprocessor based on modified montgomery algorithm*", pp: 650 - 653 vol. 4,2001

[3] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek." Dual RSA and Its Security Analysis",pp. 2922 – 2933.vol:53,2007.

[4] K.Gomathi and Dr.Meera Gandhi,"Weight based Clustered Key Management scheme using RSA for Wireless Mobile Ad hoc Networks",pp. 359 – 364, 14-16 Dec. 2011, Chennai, India

[5] H. C. Williams, "A Modification of the RSA Public-Key Encryption Procedure", IEEE Transactions on Information Theory, Vol. 26, No. 6, pp. 726-729, 1980.

[6] Ravi Shankar Dhakar,Amit Kumar Gupta, Prashant Sharma," Modified RSA Encryption Algorithm (MREA)",pp. 426 – 429, 7-8 Jan. 2012, Rohtak, Haryana, India.

[7] Gaurav R. Patel, Prof. Krunal Panchal and Sarthak R. Patel " A Comprehensive Study on Various Modifications in RSA Algorithm".

[8] Aarushi Rai, Shitanshu Jain, " Modified RSA Cryptographic System with Two Public keys and Chinese Remainder Theorem", volume 4 Issue 7 – July 2017, Jabalpur, India.

[9] Prabhat K. Panda and Sudipta Chattopadhyay, " A Hybrid Security Algorithm for RSA Cryptosystem", Jan. 06 – 07, 2017, Coimbatore, India.

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

[11] Manoj Agrawal , B. L. Pal , Rohit Maheshwari," Improvement Over Public Key Cryptosystem RSA by Implementing New Decryption Key Generation Algorithm" ,pp 300-304,Volume-5, Issue-6, December-2015

[12] A. Joseph Amalraj, Dr. J. John Raybin Jose," a survey paper on cryptographic techniques", pp. 55 – 59 Vol. 5, Issue. 8, August 2016.