An Enhanced Version of RSA to Increase the Security

Jyoti Sahu, Vishal Singh,Vikas Sahu, Ashish Chopra
National Institute of Technology, Kurukshetra, Haryana, India.

Abstract – As everything is becoming digital today, it is very necessary to maintain a high-level of security for online transactions. Rivest, Shamir and Adleman (RSA) algorithm is being used for decades to provide online security. In this paper we are introducing an approach which is more secure than original RSA algorithm by doing some modification in it. Our approach eliminates the need to transfer n, the product of two random prime numbers, in the public key due to which it becomes difficult for the intruder to guess the factors of n and hence the encrypted message remains safe from the attackers. Thus this approach provides a more secure path for transmission and reception of messages through public key cryptography. We have also presented a comparative analysis of the proposed algorithm with the traditional RSA algorithm.

Index Terms – RSA , Security, Encryption, Decryption, Public key, Private key, Cryptography.

1. INTRODUCTION

The asymmetric key cryptosystem involves the use of two distinct but related keys namely, the public key and the private key [1]. Plaintext is converted to cipher text using the public key. This process is known as encryption which is performed by the sender. On the other hand, decoding of the cipher text is performed by making use of the private key by the receiver. This process is known as decryption and is performed by the receiver. Only the receiver posses the knowledge of the private key. In order to maintain the confidentiality of the private key, the public key is disclosed to the public. The public key is used for authentication to ensure that the message is coming from the intended sender. Public key cryptosystem also ensures confidentiality. Only the receiver's private key can decipher the cipher text originating from the sender. Communication of messages can be done in a secure manner since knowledge of the public key is not sufficient to decrypt the cipher text. Because of the above advantage, in our proposed algorithm we are following the asymmetric key cryptography technique.

In RSA scheme, there is a mathematical relation between the two keys. With this fact, it is more likely possible that someone discovers the relation between the keys and successfully derives the private key. Instead, we are applying a mathematical transformation over 'n' to get a replacement for 'n' which make it harder for intruder to find the factors. This improves the security of the RSA algorithm to a greater extent.

2. RELATED WORK

Ritu Patidar and Rupali Bhartiya suggested a new algorithm concept to present the modified form of RSA algorithm in order to speed up the implementation of RSA algorithm during data exchange across the network. They included the architectural design and enhanced form of RSA algorithm through the use of the third prime number in order to make a modulus n which is not easily decomposable by the intruders. A database system was used to store the key parameters of RSA cryptosystem before it starts the algorithm. They compared the original RSA method with their proposed RSA method by some theoretical aspects. Comparative results provided better security with proposed algorithm.[2] Rohit Minni and Kaushal Sultania proposed a secure algorithm in their paper by doing some mathematical modifications in the original RSA algorithm. In RSA , the public key and private key contains a number n which is the product of two prime numbers. So, if the intruder is able to get the factors of the n then there will be problem. So, in their algorithm, they tried to eliminate the distribution of n which is the large number whose factors if found compromises the RSA algorithm. They also presented a comparative analysis of the proposed algorithm with the RSA algorithm. [3]

Alaa Hussein Al-Hamami and Ibrahem Abdallah Aldariseh proposed enhancing the RSA algorithm through the use of additional third prime number in the composition of the public and private key. This will increase the factoring complexity of the variable (n), where the process of its analysis with the development of equipment and tools becomes much easier nowadays. The existence of three prime numbers will give the ability to the enhanced encryption method to increase the difficulty of factoring of the variable (n), as well as speed increasing in the process of encryption and decryption.

They have conducted experiments on a set of numbers randomly, as they proved that the Enhanced Method for RSA Cryptosystem Algorithm is faster than the original algorithm in encryption and decryption process and generating public and private key. Also it shows that the analysis of the variable (n) will take a long time in the Enhanced Method for RSA Cryptosystem Algorithm and this indicates the increasing complexity in the analysis method.

3. RSA ALGORITHM

RSA is an asymmetric key cryptosystem relies on the assumption that it is difficult to find the factors of large integers. It involves distribution of public and private key to sender and receiver to encrypt and decrypt the message respectively.[4] RSA is a three step process that involves Key generation, Message encryption and message decryption. The algorithm is as follows:

A. Key generation –

i. Generate two distinct random prime numbers p and q.

ii. Calculate n = p x q. Its length is the key length which is usually expressed in bits.

iii. Calculate $\varphi(n) = (p - 1) \times (q - 1)$ where φ is the Euler's totient function.

iv. Calculate e based on the following conditions:

- $1 < e < \varphi(n)$
- $GCD(e, \varphi(n)) = 1$ i.e., e and $\varphi(n)$ are coprime.

Now, the Public Key comprises e and n i.e., **(e, n).** The Private Key comprises of d and n i.e., **(d, n).**

B. Message Encryption -

The sender uses the following method to encrypt the message **M**:

• Cipher text **C = Me Mod (n)** where C is the cypher text generated after encryption.

C. Message Decryption -

The receiver uses the following method to decipher the cipher text **C:**

• The original message **M = Cd Mod(n).**

4. LIMITATIONS OF RSA ALGORITHM

There are many limitations of the RSA algorithm. Some of which are as follows:

- As n is transmitted in public key, thus its factors can be found out by hit and trial, due to which the security factor of RSA algorithm gets reduced.
- The attackers can encrypt a plaintext using the public key, and then by hit and trial if any cipher text gets matched to it, then the intruder can come to know about the secret message.

In order to overcome these limitations of RSA algorithm, we have defined a new approach which is explained in the rest of the paper.

5. APPROACH

The modified algorithm introduces 2 more steps to eliminate n from the key so that one cannot trace back to the factors p and q by mathematical factorization of n. So, RSA can be made more secure to some extent [5]. This algorithm also contains three parts: Key generation inside which n is eliminated, Message encryption and Message decryption.

The modification which we have done in RSA is as follows-

A. Key generation

i. Generate two distinct random prime numbers A and B.

ii. Calculate N = A * B.

iii. Calculate $\varphi(N) = (A - 1) * (B - 1)$ where φ is the Euler's totient function.

iv. Calculate e based on the following conditions :

- $\sqrt{N} < e < N$
- GCD (k1,(N)) = 1 i.e., k1 and N are coprime.

v. Compute X (To replace N)

If B < A then consider X such that:

- $(N - A) < X < N$
- GCD (X,N) = 1

If A < B then consider X such that:

- $(N - B) < X < N$
- GCD (X, N) = 1

vi. Find d such that d * e Mod(X)) = 1

Public Key => (e, X) and

Private Key => (d, X).

B. Message Encryption -

The sender encrypt the plain text message P using the method below.

• Encrypt the message P using public key (e, X) by

$$C = P^e \text{ Mod}(X)$$

where C is the cipher text generated after encryption.

C. Message Decryption -

The receiver decrypt the cipher text as follows:

• Decrypt the cipher text C by using the private key (d, X) by $P = \sqrt{(C^d \text{ Mod}(X))}$.

Description

In RSA, both the keys comprise of the large number 'n', which can be factored into prime numbers 'p' and 'q'. The public key is known to all. It is easy to derive the private key if someone can guess the factors of 'n'. In order to get rid of this problem, in our algorithm we are trying to eliminate the distribution of 'n' in both the keys.

Lets understand the above approach by an example –

We have to send a plaintext message whose value is 4

=> P = 4

STEP 1: Take two prime numbers p and q randomly

p = 5 and q = 7

STEP 2: Compute n as

n = p * q

n = 5 * 7

n = 35

STEP 3: Compute φ(n) as

φ(n) = (p-1) * (q-1)

φ(n) = 4 * 6

φ(n) = 24

STEP 4: Compute e:

$\sqrt{n} < e < n$

e must be co-prime to n.

e is the public key exponent.

In our example-

35 < e < 35

5.916 < e < 35

e = 6

STEP 5: Compute f:

If p > q

(n-p) < f < n

f must be co-prime to n

If p < q

(n-q) < f < n

f must be co-prime to n

A general formula to find d :

d* e mod f = 1

where d is the private key exponent

In our example -

q > p

So, 35 – 7 < f < 35

28 < f < 35

Let f = 29

d * e mod 29= 1

d * 6 mod 29 = 1

d = 5

STEP 6: Send the following public and private keys:

Public key: (f, e)

Private Key: (f, d)

Thus, public key = (29,6)

Private key = (29, 5)

STEP 7: Encryption of a message, P=4:

Encrypted message, $C = P^e \bmod (f)$

$C = 4^6 \bmod (29)$

$C = 4096 \bmod (29)$

C = 7

STEP 8: Decryption of the sent message, C:

$P = [\ C^d \bmod (f)\ ]^{1/2}$

$P = [\ 7^5 \bmod (29)\ ]^{1/2}$

$P = [16807 \bmod (29)\ ]^{1/2}$

$P = 16^{1/2}$

P = 4

6. CONCLUSION

Thus, in this paper we presented a better version of RSA algorithm with enhanced security. The security feature here is the elimination of n from the original RSA algorithm and addition of a new number f in place of n. The replacement of n i.e. f is used in both private and public keys. The RSA algorithm is prone to mathematical factorization attacks. Since we have eliminated n with f , it is very hard to factorize it and get the originals numbers i.e. p and q. This makes the algorithm more secure with a slight increase of time complexity.

REFERENCES

[1] Chhabra, Aayush, and Srushti Mathur. "Modified RSA algorithm: a secure approach." *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on*. IEEE, 2011.

[2] Minni, Rohit, et al. "An algorithm to enhance security in RSA." *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*. IEEE, 2013.

[3] Al-Hamami, A. H., & Aldariseh, I. A. (2012, November). Enhanced method for RSA cryptosystem algorithm. In *Advanced Computer Science*
[4] Atul Kahate, "Cryptography and Network Security", ISBN-10:007-064823-9, Tata McGraw-Hill Publishing Company Limited, India, Second Edition, pages 38-62,152-165,205-240.
[5] Patidar, Ritu, and Rupali Bhartiya. "Modified RSA cryptosystem based on offline storage and prime number." *Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on*. IEEE, 2013.
[6] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital for Signatures and Public-Key Cryptosystems", Communications of the ACM, vol. 21 (2), pp. 120-126, 1978.

Applications and Technologies (ACSAT), 2012 International Conference on (pp. 402-408). IEEE.
[7] Somani, U., Lakhani, K., & Mundra, M. (2010, October). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on* (pp. 211-216). IEEE.
[8] Wagner, D. (2004, October). Cryptanalysis of a provably secure CRT-RSA algorithm. In *Proceedings of the 11th ACM conference on Computer and communications security* (pp. 92-97). ACM.