AN EFFICEIENT ENCRPYTION ALGORITHM BASED ON PUBLIC KEY CRYPTOGRAPHY

Dhananjay Pugila[1], Harsh Chitrala[2], Salpesh Lunawat[3], P.M.Durai Raj Vincent[4]
[1,2,3]IIIrd B.Tech(IT),SITE, VIT University
[4] Assistant Professor(Senior), SITE, VIT University.

***Abstract*— In asymmetric key cryptography, also known as Public Key cryptography. There are two different keys which are used that form a key pair. One key is used for encryption and the other is used for decryption, therefore, no other key can decrypt the message. The advantage of this scheme is that every communicating party needs just a key pair for communicating with anyone else.**

RSA is a well-known public-key cryptography algorithm and it is suitable for signing as well as encryption. Thereby, it was considered one of the first great advances in public key cryptography. In RSA, n is transmitted in public key, and if n's factors can be found by brute force attack it will reduce the security of the algorithm. In this paper, we describe a new algorithm which is similar to RSA algorithm with some modification. This helps in increasing the security of RSA algorithm. There are two n values: n_1 and n_2. We have used four variables to determine the value of n_1. This make it difficult to factorize n_1 value. n_1 is used during encryption and n_2 is used during decryption.

Keywords- Cryptography, Co-prime, Encryption and Decryption, Key, Symmetric Key and Asymmetric Key Cryptography.

I. INTRODUCTION

We have seen over the past years an increase in demand for data communication and internet services like electronic commerce, along with increasing security problems over the network. Therefore, secure techniques for communication in the presence of third party (hacker), such as Cryptography, is used. Symmetric-key cryptography is an encryption technique in which sender and receiver share a common key that is used to encrypt and decrypt a message. The main drawback is sender and receiver must exchange a key in a secure way. To overcome this problem public key cryptography is used. Each user's public key is published while the private key is kept secret and thereby this eliminates the need to exchange a key in a secure way.

Two keys are mathematically related, even though knowing of one key does not allow someone to easily determine the other key. Among the two keys, one key is used to encrypt the plaintext and the other is used to decrypt the cipher text. As a pair of keys are required - one for encryption and another for decryption - this approach is also known as asymmetric cryptography. [1, 2] RSA algorithm is most commonly used algorithm among other asymmetric key algorithms. It consists of three major steps: first step is the Key generation, then the encryption of the plaintext and finally the decryption of the encrypted text. Moreover, there are two keys which are used in RSA algorithm: the public key, which is used for encrypting a message and it is known to everyone, and the private key, which is used to decrypt the message and it is known only to the intended receiver.

In this paper we describe an algorithm that is a modification to the existing RSA algorithm. It is also a public key cryptography algorithm. In this algorithm we have used four variables among them two are prime and other two are random numbers. There are two n values $\mathbf{n_1}$ and n_2. n_1 is extremely large number which is product of two prime and two random numbers which makes it difficult for hacker to factorize value and n_2 is the product of prime numbers. n_1 is used during encryption and n_2 during decryption. Even if the hacker manages to factorize n_1, it will be hard to determine the prime numbers from factors, so that he/she can calculate n_2 and decrypt the message. This modification increases the security of the cryptosystem.

A. Encryption and Decryption:

Encryption is defined as the process by which given information is transformed into some other form in order to prevent it from the strangers or hackers, so that only receiver with a key can read the message. Moreover, the message which we get after encryption is called encrypted message. Whereas, decryption is defined as the process of retrieving the original message from the encrypted message with the help of the secret key (private key). [8]

B. Co-prime numbers:

Two numbers are said to be co-prime [9] if they only have common divisor as 1 or if their greatest common divisor is 1. Examples are 7 and 9 or 11 and 13. The multiplicative inverse property of co-prime numbers is used

in RSA algorithm. According to the property, consider two co-prime numbers a and b, such that a has a multiplicative inverse modulo b, then there exists an integer c such that [8]

$$b * c = 1 * \mod (a)$$

II. RSA CRYTOSYSTEM

RSA algorithm [5, 9] is named after Rivest, Shamir and Adleman. This algorithm is one of the example of public key cryptography algorithms which uses multiple keys for encryption and decryption leading to secure transmission of messages. RSA works better if the value of the key is long, as it becomes difficult to figure out the factors of n. RSA algorithm involves three steps:

(a) Key Generation:

RSA involves public key and private key. Public key is used for encryption and private key is used for decryption of message. The key generation takes place in the following way:

STEP 1:

Take any two large value prime numbers x and y.

STEP 2:

Compute z by using the given formula

$$z = x * y$$

STEP 3:

Compute Phi (z):

$$\text{Phi}(z) = (x-1) * (y-1)$$

Here, Phi (z) is Euler's totient.

STEP 4:

Choose the public key exponent e such that

$1 < e < \text{Phi}(z)$ and, e and Phi (z) are co-prime

Which means that GCD (e, Phi (z)) = 1

STEP 5:

Determine private key exponent d through the

given formula:

$$d * e = 1 * \mod (\text{Phi}(z))$$

this means that d is the multiplicative inverse of

e *mod (Phi (z)).

Thus the public key consists of public key exponent e and n. And private key consists of n and private key exponent d.

Public Key : (z, e)

Private Key: (z, d)

(b). Encryption:

For encrypting a message, first the algorithm convert the given message into an integer number by using a suitable padding scheme. Then following formula is used to generate encrypted message **C**:

$$C = M \wedge e \mod (z)$$

(c). Decryption:

Following formula is used to decrypt the encrypted message:

$$M = c \wedge d \mod (z)$$

III. APPROACH

Our approach is quite similar to RSA algorithm with some modifications in it.

(a) Key Generation:

STEP 1:

Take two prime numbers p and q and two random numbers x and y.

Note: the values of x, y, a and b must be greater than 1.

STEP 2:

Compute z_1, z_2 by using following formula:

$z_1 = x*y*a*b$

$z_2 = x*y$

STEP 3:

Compute Phi (z) as

Phi (z) = (x-1)*(y-1)*(a-1)*(b-1)

STEP 4:

Choose the public key exponent e such that 1< e < Phi (z) and GCD (e, Phi (z)) =1

Note: e and Phi (z) must be co-prime

STEP 5:

Determine private key exponent d through the

Following formula:

d *e= 1*mod (Phi (z))

Thus the public key consists of public key exponent e and z_1. And private key consists of z_2 and private key exponent d.

Public Key: (e, z_1)

Private Key: (d, z_2)

(b)Encryption:

Similar to RSA, the given message to be encrypted is to be converted to an integer number by using a suitable padding scheme. Encryption of message M is done using following formula:

C=M ^ e mod (z_1)

(c)Decryption:

Decryption of Message is done using following formula:

M=C ^ d mod (z_2)

IV. EXAMPLE

LET US CONSIDER THAT, WE HAVE TO SEND A MESSAGE WHOSE VALUE IS 10 I.E. M=10

STEP 1:

Take two prime numbers x and y.

x=5 and y=3

Take two random numbers a and b.

a=4 and b=6

STEP 2:

$z_1 = (5*3*4*6)$

$=> z_1 = 360$

$z_2 = (5*3)$

$=> z_2 = 15$

STEP 3:

Phi (z) = (5-1)*(3-1)*(4-1)*(6-1) =4*2*3*5

=>Phi (z) = 120

STEP 4:

GCD (e, 120) = 1

Thus, e= 7 as its co-prime to 120

STEP 5:

7 * d = 1 mod (120)

=> d = 103

Public Key = (7,360)

Private Key = (103, 15)

Encryption:

Let us consider Encryption of Message M=10

Thus,

C = 10 ^ 7 mod (360)

=> C = 280

Decryption:

M=280^103 mod (15)

=> M = 10

V. Analysis of the Algorithm

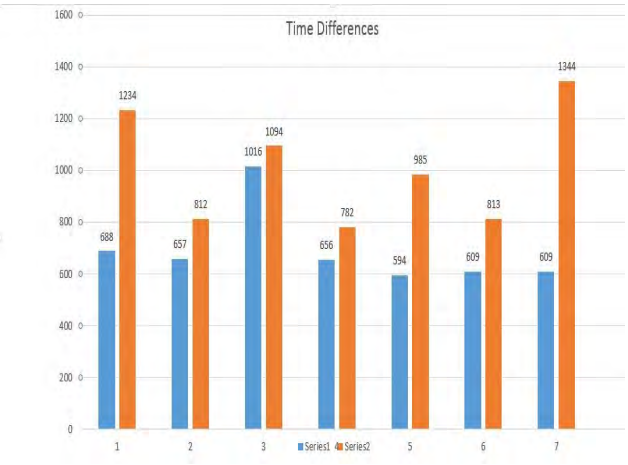
Both the algorithm are compared on the bases of the

i. Time

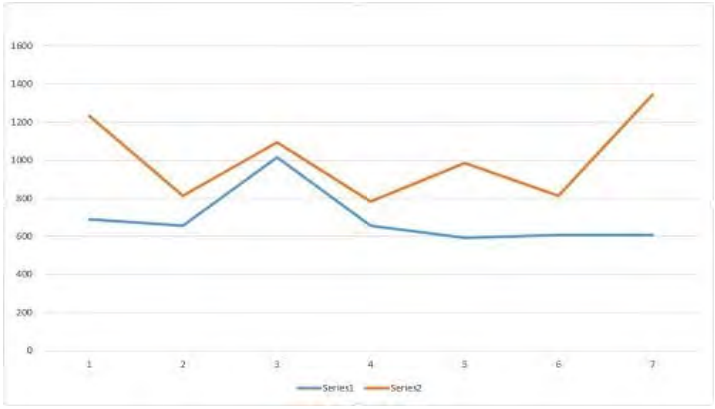
ii. Brute-force Attack

Time:

The following graphs show a comparison of the Encryption and decryption time taken by the algorithms



Series 1-RSA Series 2-Modified RSA



Series 1-RSA Series 2-Modified RSA

Brute-force Attack:

As mentioned before, n_1 is product of two prime and two random numbers and n_2 is product of two prime numbers. It becomes hard to factorize n_1 and time taken for brute force attack is more compared to RSA algorithm. This increases the security of cryptosystem

VI. Conclusions

This approach is more secure than RSA algorithm. The advantage with this algorithm is that, the time taken for brute-force attack is more compared to RSA algorithm. Even if the hacker manages to factorize n_1, it will be hard to determine prime numbers from factors, so that he/she can calculate n_2 and decrypt the message.

References

[1] Atul Kahate, Cryptography and Network Security, ISBN-10:0-07-064823-9, Tata McGraw Hill Publishing Company Limited, India, Second Edition, pages 38-62,152-165,205-240.

[2] Ralph C. Merkle, Martin E. Hellman. Hiding Information and Signatures in Trapdoor Knapsacks, IEEE Transactions on Information Theory, vol. IT-24, 1978, pp. 525-530.

[3] R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of The ACM, February 1978, pages 120-126.

[4] RSA Laboratory (2009), RSA algorithm time Complexity, Retrieved from http://www.rsa.com/rsalabs/node.asp?id=2215 (22 ct. 2009).

[5] Allam Mousa, Sensitivity of Changing the RSA Parameters on the Complexity and Performance Of the Algorithm, ISSN 1607 8926, Journal of Applied Science, Asian Network for Scientific Information, pages 60-63, 2005

[6] Amit Kumar Gupta, Ravi Shankar Dhakar, Prashant Sharma, Modified RSA Encryption Algorithm (MREA), ACCT'12 proceeding of 2012 Second international conference on Advance computing and communication technologies page 426-429

[7] Aayush Chhabra, Srushit Mathur Modified RSA Algorithm, CICN 2011 proceeding Of the 2011 International Conference on Computer Intelligence and Communication Networks Page 545-548

[8] Graham, R. L.; Knuth, D. E.; Patashnik, O. (1989), Concrete Mathematics, Addison-Wesley

[9] William Stallings, Cryptography and Network Security, ISBN 81-7758-011-6, Pearson Education, Third Edition, pages 42-62,121-144,253-297