Encryption and Decryption through RSA Cryptosystem using Two Public Keys and Chinese Remainder Theorem

Aarushi Rai
M. Tech Research Scholar
Gyan Ganga Institute of Technology and Science
Jabalpur, M.P., INDIA

Shitanshu Jain
Assistant Professor
Gyan Ganga Institute of Technology and Science
Jabalpur, M.P., INDIA

ABSTRACT
Network security refers to an activity which is designed to protect the usability and integrity of the network and data. In network security, cryptography is the branch in which one can store and transmit data in a particular format so that only the intended user can read and process it, RSA algorithm is an asymmetric cryptography technique, which works on two keys i.e. public key and private key. The proposed method takes four prime numbers in RSA algorithm. Instead of sending public key directly, two positive integers are used, on which some mathematical calculation is done. And by using those integers two public keys would be sent to the user. The scheme has speed enhancement on RSA decryption side by using Chinese remainder theorem. So that the algorithm overcomes several attacks which are possible on RSA.

General Terms
RSA(Rivest, Shamir, Adlemen) Algorithm, Network Security, Chinese Remainder Theorem, Number theory.

Keywords
RSA, Cryptography, Network Security.

1. INTRODUCTION
Network Security and cryptography is a subject which covers wide range about how to protect information in digital form and to provide security services [1]. A large amount of data, which is shared through computer networks every day, network security has become one of the most essential aspects of networking. And thus the security is indeed.

Number theory may be one of the purest branches of mathematics which is also the most useful when it comes to computer security [3].

Chinese Remainder Theorem, CRT is one of the main theorems of mathematics. This can be used in the field of cryptography. Computing was its original field of application, and continues to be important as regards various aspects of algorithmic and modular computations [4]. RSA [5] is a public key algorithm which has been being applied extensively in the area of information security because of its concise preliminary, believable security.

The proposed scheme for RSA cryptosystem contains four prime numbers and by using two key pairs instead of sending the public key alone and use some mathematical calculations so that if an attacker has an opportunity of getting the public key component they cannot find the private key value by brute force search. On the other hand it has a speed improvement on RSA decryption side by using the Chinese remainder theorem (CRT) [12] by which the scheme is semantically secure also.

2. CHINESE REMAINDER THEOREM
Given pairwise coprime positive integers $n_1,n_2...n_k$

And integers $a_1,a_2,...a_k$,

the system of simultaneous congruences are as follows:

$$x \equiv a_1 (\text{mod}(n_1))$$
$$x \equiv a_2 (\text{mod}(n_2))$$
.
.
.
$$x \equiv a_k (\text{mod}(n_k))$$

These congruences have a solution, and the solution is unique modulo:

$$N = n_1 n_2 \ldots n_k$$

The following is a general method to find a solution to the system of congruences using the Chinese remainder theorem:

1. Compute $N=n_1 \times n_2 \times \ldots n_k$.
2. For each i=1,2,…k, compute
   $y_i = \frac{N}{n_i} = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k$
3. For each i=1,2,3…k , Compute
   $Z_i = y_i^{(-1)} \bmod n_i$
4. By using Euclid's extended algorithm
   (z_i exists since $n_1 n_2 \ldots n_k$ are pairwise coprime).
5. The integer
   $$x=\sum_{i=1}^{k} a_i y_i z_i$$
   will be a solution to the system of congruences, and x mod N is the unique solution modulo N.[13]

3. RSA CRYPTOSYSTEM
RSA algorithm was publically described by Ron Rivest, Adi Shamir and Leonard Adleman [5] at MIT in 1977.For Public key Cryptography, RSA is the well-known algorithm. The first algorithm suitable for signing as well as encryption is the RSA algorithm. The RSA algorithm uses modular multiplication and exponentiation [6]. It is one of the best known public key cryptosystem for key exchange or digital signatures or encryption of blocks of data, which uses prime numbers.

Finding a way to write certain 1000 digit number as a product of primes seems out of reach of present technology, an observation that is used by millions of people every day when they buy things online [2].

In public key cryptography or asymmetric cryptography different keys are used for encryption and decryption. One key would be public and one would be private. The keys are

generated by applying some mathematical computation of two large prime numbers. The public key is sent to everyone in the system, but the private key is kept secret in RSA. The security of RSA cryptosystem depends upon the difficulties of factorization of large prime numbers. Private Key can be generated by using public key information, which includes n (multiplication of prime numbers), an attacker cannot determine the prime factor of n and therefore the private key. And this makes the RSA algorithm secure.

3.1 RSA Key Generation

Step 1: Generate two large prime numbers p and q of approximately same size such that their product n=pq is of required bit length for example 1024.

Step 2: Compute n=pq and phi(n) = (p-1)(q-1).

Step 3: Choose a random encryption integer such that GCD[e,phi(n)] = 1 and 1<e<phi(n).

Step 4: Compute the secret exponent d in the range 1<d<phi such that: ed= 1 mod phi(n).

Step 5: The public key is (n,e) and the private key is (n,d). d, p, q and phi are the secret values.

- n is known as the modulus or multiplication of the prime numbers.
- e is known as the public exponent or encryption exponent or just the exponent.
- d is known as the private exponent or decryption exponent.
-

3.2 RSA Encryption:

Sender does the following operations:

(1) Obtains the public key.
(2) Represent the plaintext message as a positive message as a positive integer.
(3) Calculates the cipher text:
$C=M^e \bmod (n)$
(4) Send the cipher text to the receiver.

3.3 RSA Decryption:

Recipient does the following:

(1) Use the private key (n, d) to compute calculate plaintext:
$M=C^d \bmod (n)$
(2) Extract the plaintext from the message representative M.

3.4 RSA Number Theory:

There are different factors behind prime numbers, key generation process in RSA:

(1) It is easy to find a random prime numbers of a given size.
(2) A prime numbers cannot be factorized easily; to find a factor of a large prime number still takes a long time.
(3) Modular root extraction is hard i.e. given only n (product of prime number), e (public key), C (cipher text) but not the prime factors, it appears to be quite hard to recovers the value of M.

4. PROPOSED SCHEME OF IMPROVED RSA

The proposed scheme is trying to provide an enhancement to the RSA cryptosystem by giving a method that has a speed improvement on the RSA decryption side by using Chinese remainder theorem [12] and also provide the security by using two key pairs in place of single public key [10].

This scheme avoids various attacks possible on RSA. Using the random integer 'a' if same message is encrypted more than one time it will look different every time.

The general idea towards this scheme is to make the algorithm more secure and decrease the decryption time both at the same time.

By the existence of four prime numbers, and two cipher texts for each message, the difficulty of analysis of algorithm must increase. RSA is a block cipher in which the plaintext and cipher text are integer between 0 and n-1. For some n and decryption can be done by the following steps:

4.1 Key Generation for the Proposed Scheme:

Step 1: Generate four large prime numbers p, q, r and s.

Step 2: Calculate n=p*q*r*s and phi(n) = (p-1)(q-1)(r-1)(s-1).

Step 3: Select e such that (e, phi(n)) are relatively co-prime.

Step 4: Choose two integers j and k such that j/k=e.

Step 5: Extract the value of d by using the formula
ed = 1 mod (phi(n)).

Step 6: Find dp=d mod (p-1), dq=d mod (q-1),
dr= d mod (r-1), ds=d mod(s-1).

Step 7: Public key KU=<e,n> and private key
KV=<d, p, q, r, s, dp, dq, dr, ds>.

4.2 Encryption for Proposed Scheme:

To encrypt the message M steps are as follows:

Step 1: Represent the message M as integer form in the range [0 to n-1].

Step 2: Select the random integer 'a' such as:
GCD (a, n) = 1 and 1<a<n-1

Step 3: Calculate Cipher texts-
C1= a(j/k) mod n
C2= M(j/k).a mod n

Step 4: Send the cipher text value to the sender.

4.3 Decryption for Proposed Scheme:

Step 1: Compute the following:-

Cp=C1 mod p	Cq=C1 mod q
Cr=C1 mod r	Cs=C1 mod s

Then also calculate:

ap= Cpdp mod p	aq= Cqdq mod q
ar= Crdr mod r	as= Csds mod s

Step 2: By using Chinese remainder theorem:

a=[ap (qrs)p-1 mod n + aq (prs)q-1 mod n + ar (pqs)r-1 mod n

+ as (pqr)s-1mod n]

Step 3: By using Euclidean theorem, compute the value of unique integer b:

b*a=1 mod n and 1<b<n

Step 4: Compute M(j/k),

C2*b= (Me.a).b = (Me)a.b= Me mod n

Step 5: To compute the value of M (plaintext)

Follow the steps below:

C'p= M(j/k) mod p C'q= M(j/k) mod q

C'r= M(j/k) mod r C's= M(j/k) mod s

Then compute:

Mp= (C'p) dp mod p Mq= (C'q) dq mod q

Mr= (C'r) dr mod r Ms= (C's)ds mod s

Step 6: Finally recover the plaintext:

M= [Mp (qrs)(p-1) mod n + Mq (prs)(q-1) mod n + Mr (pqs)(r-1) mod n+ Ms(pqr)s-1 n]

5. ATTACKS ON RSA AND THEIR EFFECTS ON PROPOSED SCHEME

5.1 Brute Force Attack:

In the proposed scheme two public key pairs are sent to the receiver rather than sending one public key directly, so if an attacker has an opportunity of getting the public key component then the private key cannot be obtained easily by brute force search. By using four prime numbers, the factorisation of n is more difficult as well.

5.2 Timing attack:

Timing attack is one that occurs at RSA implementation Kocher [21] shows that an attack can determine the value of private key by maintaining the track of how much time a computer takes to decrypt the encrypted message. Timing attack is applicable in the original RSA algorithm because, by previously measuring the time for encryption and decryption, and time for key generation one can determine the value of the secret key exponent d. But in proposed scheme; key pairs are used for single key (e) and one random integer a is used for encryption and decryption process that makes it difficult to distinguish and measure between the time for public key e or private key d and time for unique integer 'a'.

5.3 Known Plaintext attack:

The known plaintext attack is the one in which the attacker knows some quantity of plaintext and corresponding cipher text such as a sorted set [9]:

W= { KP, CP}

Where KP the known plaintext set and CP cipher text, in W.

Known plaintext attack deals with some known plaintext corresponding to the cipher text. It is applicable in the original RSA algorithm.

But it cannot be applied to the proposed scheme because it has two cipher texts for one plaintext. So if one applies the attack to the proposed scheme then it will be very difficult to get the value of particular plaintext by apply these attack.

6. A WORKING EXAMPLE

Here small prime numbers are used for convenience; Let the plaintext: 2530

6.1 Key Generation:

(1) Generate three large prime numbers:
p = 131, q = 193, r =233, s = 227

(2) Calculation of parameters: n = 1337243153
phi(n)= 1308702720

(3) Gcd(e,phi(n))=1 public key e= 137

(4) Choose two integers j and k such that {j/k=e}.
The public key pairs are: {j, n}:{8220,1337243153}
{k, n}:{60,1337243153}

(5) private key d= 47762873

(6) Parameters: dp=93, dq=185,
dr=105, ds=33.

6.2 Encryption:

(1) Selecting the random integer 'a' such as:
GCD(a, 1337243153) = 1 a=202

(2) Cipher texts: [C1= 106310778] [C2= 707324781]

6.3 Decryption for Proposed Scheme:

(1) Calculation of Cp=86, Cq= 9, Cr=101, Cs= 95

(2) Calculation of parameters: a_p=71, a_q=9, a_r=202, a_s=202

(3) The unique integer b=1184982794

(5) Compute $M^{(j/k)}$= 1320884714

(6) Calculation of parameters: C'_p=55, C'_q=48 ,C'_r=25, C'_r=89 (7) Calculation of parameters: M_p=41, M_q=21, M_r=200, M_s=33

(8) Plaintext: M= 2530

7. CONCLUSION AND FUTURE WORK

This paper shows the study of number theory and Chinese remainder theorem and public key cryptosystem. RSA cryptographic system produces one public key for encryption. Proposed scheme sends two public keys separately. And to speed up the decryption time, the concept of Chinese remainder theorem is used. This scheme also improves the security of RSA algorithm by avoiding some attacks which are possible in RSA like: Brute force attack, timing attack, known plaintext attack.The future work would be based upon working on the attacks in detail and considering those attacks which are not discussed in this paper and to reduce the encryption time and therefore to give more secure RSA cryptosystem.

8. REFERENCES

[1] T.R. Devi, "Importance of cryptography in network security" IEEE International Conference, Communication System and network Technologies (CSNT), 2013

[2] William Stein, elementary Number Theory, Primes Congruences and Secrets. January 23, 2017

[3] Number theory concepts and Chinese remainder theorem: "https://crypto.stanford.edu/pbc/notes/numbertheory/crt.html."

[4] Saurbh Singh and Gaurav Agarwal, "Use of Chinese Remainder theorem to generate radom numbers for cryptography" Research article in international journal of

applied engineering research, DINDIGUL. ISSN- 0976-4259

[5] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public-key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[6] G. R. Blakey, "A Computer Algorithm for Calculating the Product AB Modulo M," IEEE Transaction on Computers, vol. 32, no. 5, pp. 497-500, 1983.

[7] Network security Concepts, "http://williamstallings.com/Extras/Security-Notes/lectures/publickey.html

[8] P.C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other Systems" Advances in cryptography- CRYPTO '96, pp. 104-113, 1996.

[9] Celine Blondeau and Kaisa Nyberg, "On Distinct Known Plaintext Attacks", Aalto University Finland, WCC_2015

[10] Israt Jahan, Mohammad Asif, Liton Jude Rozario " Improved RSA cryptosystem based on the study of the number theory and public key cryptosystems" volume-4 Issue-1, pp-143-149.

[11] RSA Algorithm in Cryptography http://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[12] Nikita Somani, Dharmendra Mangal, " An improved RSA cryptographic System". International Journal of Computer Applications (0975-8887) volume 105-No. 16 November 2014.

[13] Chinese remainder theorem and proof https://brilliant.org/wiki/chinese-remainder-theorem/