Modified RSA Cryptographic System with Two Public keys and Chinese Remainder Theorem

Aarushi Rai[#1], Shitanshu Jain[*2]
[#]Mtech Research Scholar, Department of Computer Science and Engineering
Gyan Ganga Institute of Technology and Science Jabalpur, India
[*]Assistant Professor, Department of Computer Science and Engineering
Gyan Ganga Institute of Technology and Science Jabalpur, India

Abstract

Network security is 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, the encrypted text is the cipher text which is then decoded on receiver side. 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 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.

Keywords

RSA, Cryptography, Network Security.

I. INTRODUCTION

Network Security and cryptography is the branch 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, to secure the data through various preventative measures whether they are software measures or the hardware.

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

Chinese Remainder Theorem, CRT is one of the important theorems in mathematics. This can also be used in the field of cryptography. Computing was its original area of application, and continues to be important as related to various aspects of algorithmic and modular computations [4]. RSA [5] is an asymmetric key (public key) algorithm which has been being applied extensively in the field 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 directly, 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 RSA works quite slowly when its bit size increases after 1024bits, so 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.

II. 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:

$x \equiv a_1(\bmod(n_1))$
$x \equiv a_2\,(\bmod(n_2))$
.
.
.
$x \equiv a_k\,(\bmod(n_k))$

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
$x = \sum_{i=1}^{k} a_i\, y_i\, z_i$

III. RSA CRYPTOSYSTEM

RSA algorithm was publically described by Ronald Rivest, Adi Shamir and Leonard Adleman [5] at MIT in 1977.For asymmetric key Cryptography, RSA is the well-known algorithm. The first algorithm suitable for signing as well as encryption and decryption, is the RSA algorithm. The RSA algorithm uses modular multiplication and exponentiation [6]. It is one of the best known asymmetric 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 [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.

A) *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.

B) *RSA Encryption*

Sender does the following operations:

Step-1 Obtains the public key.

Step-2 Represent the plaintext message as a positive message as a positive integer.

Step-3 Calculates the cipher text:

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

Step- 4 Send the cipher text to the receiver.

C) *RSA Decryption*

Recipient does the following:

Step-1 Use the private key (n, d) to compute plaintext:

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

Step-2 Extract the plaintext from the message representative M.

D) *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.

IV. PROPOSED SCHEME

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:

A) *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
$ed = 1 \bmod (phi(n))$.

Step-6 Find $dp=d \bmod (p-1)$, $dq=d \bmod (q-1)$,
$dr= d \bmod (r-1)$, $ds=d \bmod(s-1)$.

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

B) *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-
$C1= a^{(j/k)} \bmod n$
$C2= M^{(j/k)}.a \bmod n$

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

C) *Decryption for Proposed Scheme:*

Step-1 Compute the following:-
$C_p=C1 \bmod p$ $C_q=C1 \bmod q$
$C_r=C1 \bmod r$ $C_s=C1 \bmod s$

Then also calculate:
$a_p= C_p^{dp} \bmod p$ $a_q= C_q^{dq} \bmod q$
$a_r= C_r^{dr} \bmod r$ $a_s= C_s^{ds} \bmod s$

Step-2 By using Chinese remainder theorem:
$a=[a_p (qrs)^{p-1} \bmod n + a_q (prs)^{q-1} \bmod n + a_r (pqs)^{r-1} \bmod n$
$+ a_s (pqr)^{s-1} \bmod n]$

Step-3 By using Euclidean theorem, compute the value of unique integer b:
$b*a=1 \bmod n$ and $1<b<n$

Step-4 Compute $M^{(j/k)}$,
$C2*b= (M^{j/k}.a).b = (M^{j/k})a.b= M^{j/k} \bmod n$

Step-5 To compute the value of M (plaintext)
Follow the steps below:
$C'_p= M^{(j/k)} \bmod p$ $C'_q= M^{(j/k)} \bmod q$
$C'_r= M^{(j/k)} \bmod r$ $C'_s= M^{(j/k)} \bmod s$

Then compute:
$M_p= (C'_p)^{dp} \bmod p$ $M_q= (C'_q)^{dq} \bmod q$
$M_r= (C'_r)^{dr} \bmod r$ $M_s= (C'_s)^{ds} \bmod s$

Step-6 Finally recover the plaintext:
$M= [M_p (qrs)^{(p-1)} \bmod n + M_q (prs)^{(q-1)} \bmod n$
$+ M_r (pqs)^{(r-1)} \bmod n+ M_s(pqr)^{s-1} n]$

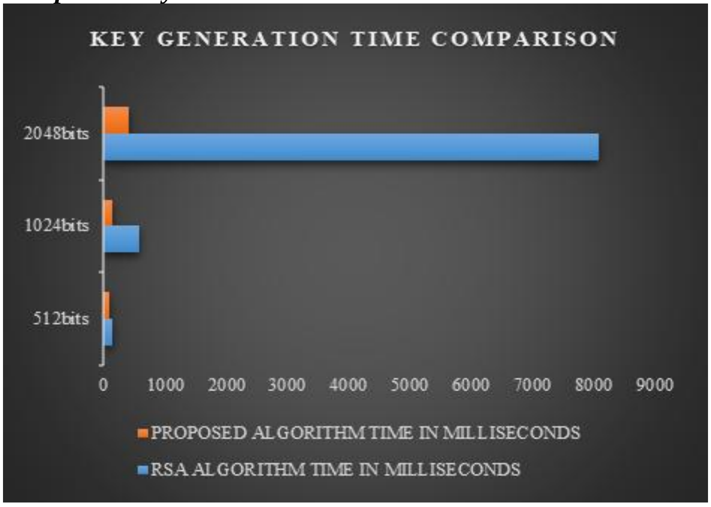
V.EXPERIMENTAL RESULTS

In order to justify the performance different modulus length (256 bits, 512 bits,1024 bits,2048 bits, 4096 bits) and the block sizes (256 bits,512 bits,1024 bits, 2048 bits, 4096 bits). The two following table shows the experimental results of RSA and proposed scheme respectively.

A. *Key Generation Time Comparison*

BIT SIZE IN BITS	RSA ALGORITHM TIME IN MILLISECONDS	PROPOSED ALGORITHM TIME IN MILLISECONDS
512bits	141	96
1024bits	590	142
2048bits	8082	416

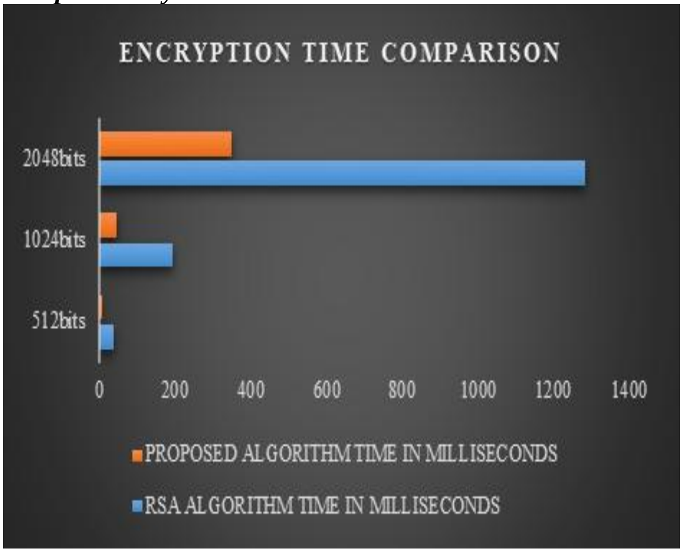
Comparison By Chart



B. *Encryption Time Comparison:*

BIT SIZE IN BITS	RSA ALGORITHM TIME IN MILLISECONDS	PROPOSED ALGORITHM TIME IN MILLISECONDS
512bits	38	7
1024bits	192	45
2048bits	1283	350

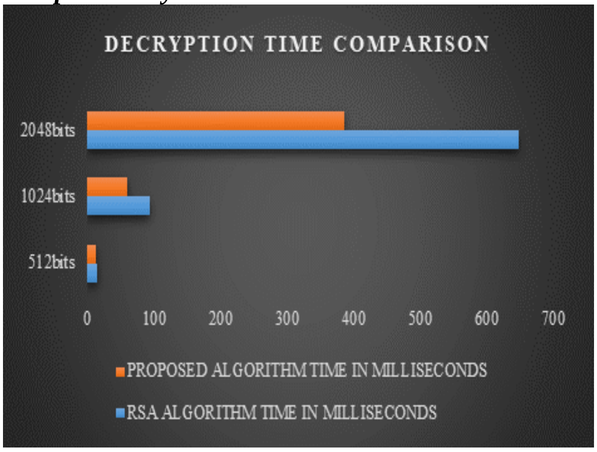
Comparison By Chart:



C. *Decryption Time Comparison:*

BIT SIZE IN BITS	RSA ALGORITHM TIME IN MILLISECONDS	PROPOSED ALGORITHM TIME IN MILLISECONDS
512bits	14	12
1024bits	94	59
2048bits	649	387

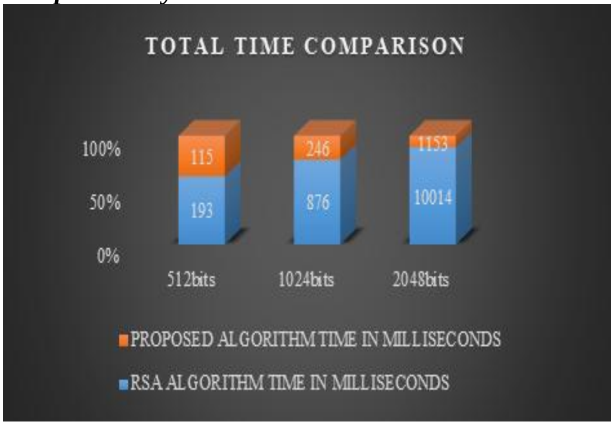
Comparison By Chart:



D. *Total Time Comparison:*

BIT SIZE IN BITS	RSA ALGORITHM TIME IN MILLISECONDS	PROPOSED ALGORITHM TIME IN MILLISECONDS
512bits	193	115
1024bits	876	246
2048bits	10014	1153

Comparison By Chart:



VI. 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 whereas, proposed scheme sends two public keys separately. And since RSA works quite slowly after 2048 bit block size, so to speed up the decryption time, the concept of Chinese remainder theorem is used. This scheme also improves the security of RSA algorithm by using two public key pairs. The future work would be based upon working on the attacks which are possible on RSA and therefore to give more secure RSA cryptosystem.

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] 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/

[14] Mr. Sameer Negi, Mr. Manish Bhardwaj, Mr. Abhinav Ajitsaria, Survey of Wireless Network Security: Attacks &their CountermeasuresSSRG International Journal of Computer Science and Engineering, (SSRG-IJCSE) – volume 3 Issue 8–Aug 2016.