Future Computing and Informatics Journal

Volume 4
Issue 1 *Volume 4 issue 1*

Article 1

2019

Improved RSA security using Chinese Remainder Theorem and Multiple Keys

Hatem Abdulkader
Faculty of Computers and Information, Menoufia University, Egypt, Hatem.abdelkader@ci.menofia.edu.eg

Rasha Samir
rashasamir661@yahoo.com

Reda Hussien
reda_mabrouk@fci.kfs.edu.eg

Special issue

Proceeding of 3rd. International Conference for Computing and Informatics, *Ubiquitous Computing and Engineering* (ICCI, 2018) July 3-4 2018, organized by Future University in Egypt & Helwan University

Improved RSA security using Chinese Remainder Theorem and Multiple Keys

Rasha Samir[a], Hatem Abdulkader[a*], and Reda Hussein[a]*

[a]*Faculty of Computers and Information, Menoufia University, Egypt,*

Hatem.abdelkader@ci.menofia.edu.eg

Abstract

Now a days, have a great dependence on computer and network and the security of computer related to the whole world and everybody. Cryptography is the art and science of achieving security by encoding message to make them non readable, to secure data information transmits over the network, In this paper introduced modified RSA approach based on multi keys and Chinese remainder theorem (CRT), which RSA algorithm is asymmetric key encryption technique. The objective of this Technique is to provide secure transmission of data between any networks. Which is the Network security is an activity which is designed to provide the usage protection and integrity of the Network and data. So that only the user allowed can read and process it, the objective of this paper Enhancement the performance of RSA and increase the security. In proposed model RSA will be implemented using java.

***Keywords*:** Cryptography, Encryption, Decryption, RSA, Multiple key, Chinese Remainder Theorem (CRT).

1.INTRODUCTION

Today the internet provides communication between people and facilitates for payment electronic , military communication and many others. This cause's great anxieties for privacy, security, identify theft, etc. which The main concern related to reliable data transmission is security, the secure data transmission in which like banking online, Credit Card, ATM etc. needs strong security, because most of the transaction is held through the cloud IP. In cloud IP the whole data is accessible and because of these there is chance that the data becomes hacked. For the knowledge secure, used cryptography [1]. The Cryptography is a standard way of the data security. Cryptography is a part of secure the information, [2]Cryptography is a technique to hide the data over channel communication or we can say it is a science of keeping the secrets secret, which the end users ultimate motive is to send or receive the data without any attacked from the thief, especially now day we can send or receive a message from virtually anyone around the world in seconds through using the internet. To provide the protection to the data transmitted from the stealing and attack, we need to hide the message before the send i.e. make the message un reading. In a Computer to communications of Computer, the Sender always does the encryption and the receiver doing the decryption.

There two types of cryptography symmetric key and asymmetric key, the Symmetric Key [2] Cryptography is used the same key at both the ends, but the Asymmetric key Cryptography [3] is used different keys (Public and private key) at both the ends. In this paper we deal the Asymmetric key cryptography [3] since this algorithm overcomes the disadvantages of symmetric key cryptography such as the exchanged of key and also the digital signature can be deployed using this technique .all this is done using the encryption and decryption with two keys at both the ends so that the data can be sent more secure using the advanced RSA Algorithm and the Chinese Remainder Theorem rivest, Shamir, and ad leman discovered method to implement the cryptography public-key In 1978[6].which is known with the RSA cryptosystem. It provides top of security and easy to applyment, so that, it is became quickly the most widely used public-key cryptosystem. Cryptography is referred to “the secret study”, while today is most linked to the encryption definition. The Encryption is process of converting the plain text “unhidden” to a cipher text “hidden” to **s**ecure it against any attack, data thieves. This process needs to make the cipher text “hidden “understood, this is done through decrypting.

1.1. Cryptography goals

Every system of security must provide a package of function of security that can include system confidentiality. These functions referred usually to the goals of the system of security. These goals are the following five categories:

- Authentication: This means that before the data sending and receiving during the system, the sender and receiver must be sure of identity should be verified.
- Confidentiality: this function means how most people identify a system secure. This means that the people authenticated they are the only ones they can see the contents of the message and not someone else.
- Integrity: this means that the content of the data communicated is confirmed to be free from any modification type between the end points.
- Service Availability and Reliability: Since the system secure usually gets attacked from intruders, this may effect on their availability and the service provided to the user. Such that the system should provide method to Guaranteed by the service quality which the users expected it.
- Non-Repudiation: This function means that neither the receiver nor the sender can denies falsely that have sent a message certain [4].

The rest of the paper is organized in sections. Section 2 shows the RSA methodology, Section 3 shows the related work, section 4 shows the proposed model of RSA and RSA using Chinese remainder theorem its algorithm, Section 5shows comparison between standard RSA and RSA-CRT with results, Comparison between standard RSA, RSA-CRT and proposed model, section 6 shows the objective of this paper, section 7 shows the performance and section8 shows the conclusion.

2. Existing techniques

2.1 RSA Methodology

RSA algorithm was publically described by Ron Revister, Adi Shamir and Leonard Ad leman [6] at MIT in 1977.For Public key Cryptography RSA is well-known algorithm.it is the first algorithm suitable for signing as well as encryption and decryption is the RSA. This algorithm uses Multiplication modular and exponentiation [5].

As in asymmetric key cryptography standard or public key cryptography, separate keys are used for encryption and decryption. One is public and other one private key. Then generated the keys by applying some computation mathematic of two large prime numbers [8]. The public key is send to everyone in the system but the private key Retains confidentiality in RSA. The Private key generated by using information of public key. The RSA security of cryptosystem relies on the factorization difficulties of large numbers prime [9]. Which it is including n (the multiplication of prime numbers), an attacker cannot known the factor of prime of n and therefore the private key. Thus the RSA algorithm became secure. Of course the technique of factoring of numbers is improving but still the speed depends on the size of prime numbers. The improvement over the standard RSA is gradually done improving day by day. Working of RSA . In standard RSA algorithm each user of system makes two number public (e, n) called public key and keeps a number secret (d) is also called private exponent. If a user A wants to send to user B message, user A wants to look up user B's public key and have message M (written in the form of integer value) then user A creates the block of message of size < n and then sends the cipher text C=Me mod (n) to user B. then the user B (receiver) decrypt the text by M=Cd mod (n).the algorithm security depends on the choice of public and private keys. They must be significantly large.

RSA Key generation:
Step 1: Generate two large numbers are prime such that p and q almost the same size such that their product n=PQ.
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).

The secret values are d, p, q and phi.

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

RSA Encryption:
Sender does the following operations:

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

RSA Decryption:
Receiver does the following:

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

3. Related Work

- Rivest, Adi Shamir and Adelman has invented RSA algorithm which it is widely most used public key cryptosystem, this algorithm used to encrypt the data to provide security.
- Vivek Choudhary and Mr.N.Praveen has proposed Enhanced RSA cryptosystem based on three prime numbers ,which it becomes difficult for the intruder to guess the factor of n and hence the encrypted message remains safe from the hackers.
- Somesh Kumar have implemented RSA algorithm with free forward artificial neural network.
- Narander Kumar, Chaudhary provide a modify RSA algorithm based on the n-prime numbers. This technique uses n-prime numbers because large prime numbers are not easily factorized.
- Asma Chaouch have evaluated three famous encryption algorithms ECC, RSA and AES in terms of encryption speed, security level, encrypted JPEG image size.
- Abdulameer K.Hussain has proposed a method to eliminate the redundant messages occurred in the RSA method by applying the K-Nearest Neighbor values of either p or q or both.
- All of them have a problem about security, efficiency and performance.
- So that we will be tried to solve this problem through a proposed approach.

4. Modified techniques

4.1 RSA Using CRT

In RSA-CRT the decryption must faster than the decryption of the original RSA [4], The CRT allows to implement the RSA algorithm efficiently. Given input, m, raise it to the e-th (or d-th) power modulo p and modulo q. The results intermediate are then combined through addition and multiplication with some constant predefined to compute the result final,

The execution time is less than 4 times, since the exponentiation modular is performed on half the bit size of n. The complexity of the RSA decryption M = Cd mod n rely directly on the size of d and n. the exponent decryption d determines the multiplications numbers of modular necessary to implement the exponentiation, and the modulus n decide the size of the result intermediate .thus reducing the size of both d and n is considered important advantage in the Chinese Remainder Theorem (CRT). Where the factors of the modulus N (i.e., P and Q) are supposed to be known. By CRT, the computation of M =CD (mod N) can be partitioned into two parts:

$MP = CP^{DP} \pmod P$ (1)

$Mq = Cq^{Dq} \pmod q$ (2)

Where

$CP = C \pmod P$ (3)

$DP = D \pmod{P-1}$ (4)

$Cq = C \pmod q$ (5)

$Dq = D \pmod{q-1}$ (6)

Then using Chinese Remainder Theorem, we find a solution

$M = MP \pmod p = C^d \pmod p$ (7)

$M = Mq \pmod q = C^d \pmod q$. (8)

This reduces the time of computation since DP, DQ <D and CP, CQ < C. In fact, their size is almost half the original size. There are several ways that we can obtain the plaintext original, M using the Chinese Remainder theorem.

4.2 advanced RSA using multiple keys

In RSA algorithm will be altered by generating multiple keys (two public and two private keys) [5]. In RSA modified the time of computation is more because of multiple keys but the security is more compared to the standard algorithm (RSA). We are using two public and private keys in modified RSA algorithm, in which we will be used four prime number and get public key and private key [7], also using two public keys for encrypting and two private keys for decrypting. It is less vulnerable to attack there are 3 phases: Key generation, encryption, and decryption.

Key Generation in advanced RSA Algorithm

In the process of key generation we will generate multiple public key and private keys. In this algorithm the public keys are apparent to both sender and receiver. And private keys became secret. These are steps for process of key generation:

1) Select two set numbers randomly say r, s and p, q.

2). Find the value of (z, n) i.e., z=r*s, n=p*q.

3). Compute the value of ϕ (z) = (r-1)*(s-1), ϕ (n) = (p-1)*(q-1). 4). Select integer random e, g such that 1<e<n, 1<g<z and gcd (e, ϕ (n)) =1, gcd (e, ϕ (z)) =1. 5). Compute the value of T, d such that t*g ≡1 mod (z), d*e ≡1 mod (n) 6). Public Key {e, g, n, z}, Private Key {d, t, n, z}.

Encryption

After generated multiple public and private key in the process of key generation. Now we will encrypt the message with the public keys. Because we are doing the process of encryption two times, the reliability is became more compared to the standard RSA algorithm. We will take the message (M) and the first public key (e) then make the process of encryption and find out C1=M^ e mod (n). By using c1 and the second

Public key (g) we will find the cipher text in process of encryption: C=C1^ g mod (z).

Decryption

In the process of decryption we will decrypt the message original by using private keys d, t. We will decrypt with the first private key (d) which is m1=C ^ t mod (z).then we will get the message decrypted with Second private key (t): M=m1 ^ d mod (n).

Number example on proposed technique:

1. Select four prime numbers
P=3, q=7, r=3 and s=11
Calculate
N=p*q, Z=r*s
N=3*7=21
Z=3*11=33
2. Calculate
ϕ (n) = (p-1)*(q-1), ϕ (z) = (r-1)*(s-1)
ϕ (n) = (3-1)*(7-1) =2*6=12
ϕ (z) = (3-1)*(11-1) =2*10=20

3. Select e such that e is relatively prime to ϕ (n) and less than ϕ (n) i.e. GCD (ϕ (n), e) =1
We choose e=5 and select g such that g is relatively prime to ϕ (z) and less than ϕ (z) i.e. GCD (ϕ (z), g) =1, we choose g=7
4. Determine d and t such that d*e ≡1 mod (n) and t*g ≡1 mod (z)
d, t is generated by calculation using extended Eculid's algorithm and satisfying above condition, here d = 5, t =3
The resulting keys are
First public key is (e, n) = (5, 21)
Second public key is (g, z) = (7, 33)
First private key is (t, z) = (3, 33)
Second private key is (d, n) = (5, 21)
Consider the plain text M=2

Figure 1, 2: Generated Key Generation

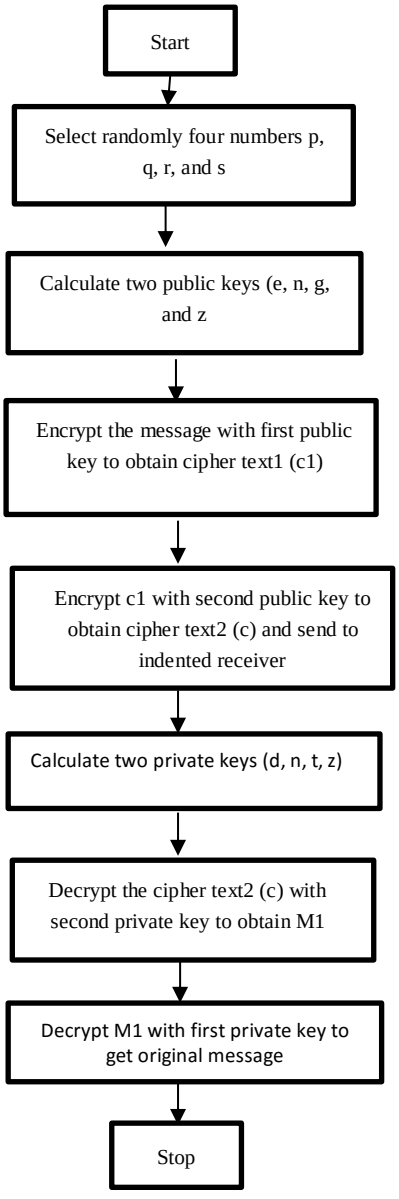
Plain text is M<n
Cipher text C1=M^ e mod n
C1=2^5 mod 21
C1=32 mod 21
C1=11
C=C1^ g mod (z)
C=11^7 mod33
C=19,487, 171 mod 33
C=11

Figure 3: Encryption

Cipher text is C
Plain text
M1=C ^ t mod z
M1=11^3 mod33
M1=1331 mod 33
M1=11
M=M1 ^ d mod (n)
M=11^5 mod 21
M=161051 mod 21
M=2

Figure 4: Illustrates the Sequences of Events for Key Generation, Encryption and Decryption in Advanced RSA Using Multiple Keys

Figure 4: Decryption



5. Comparison of algorithms used

5.1 compared between standard RSA and RSA using Chinese Remainder theorem.

In this section we show compared between standard RSA and RSA-CRT with result. RSA_CRT algorithm faster as compared to standard RSA algorithm. The RSA algorithm with CRT requires less number of iterations as compared to standard RSA algorithm. It reduces

Iterations as compared to standard RSA algorithm. It reduces computational cost. The performance of RSA is enhanced using CRT.

The improvement has occurred in the decryption of RSA-CRT because the Chinese Remainder Theorem is applied during decryption.

Table 1, Table 2: The Results of First Comparison

Size in bits	RSA		All time	RSA-CRT		All time
	Encryption time in MS	Decryption time in MS		Encryption time in MS	Decryption time in MS	
640	14	28	42	14	8	26
1040	15	33	48	15	10	29
1136	16	47	63	16	13	32

Size in bits	All time of encryption and decryption of RSA	All time of encryption and decryption of RSA-CRT
640	42	22
1040	48	25
1136	63	29

5.2 Comparison between standard RSA, RSA-CRT and advanced RSA.

In this section we show compared between standard RSA, RSA-CRT and advanced RSA with result. In advanced RSA we used four prime numbers to generate multiple public keys and private keys which this technique provides more security compared with RSA algorithm [6] and RSA_CRT [9]. In advanced RSA we are using two public and private keys, this makes him safer since he is not attacked or robbed by unauthorized people and improving security and efficiency in data sharing over the network, but less speed compare to RSA algorithm and RSA_CRT. Since the standard RSA used two prime numbers to generate one public key and one private key to make encryption and decryption this make it less secure which it is easily decompose and take time to encrypt and decrypt more than RSA_CRT, By using CRT in RSA algorithm it requires less processing time compared and smaller amount of memory for final decoded result, and declared this comparison through

The tables 1,2,3,4 and figures 5 and 6 [10] shows the relation between the all-time of the RSA algorithm & the all-time of RSA using Chinese remainder theorem, and between RSA&RSA using Chinese and advanced model.

Table 3. Comparison between RSA, RSA_CRT and Advanced RSA

RSA	RSA using CRT	advanced RSA
Use only one public key Use only one private key	Use only one public key Use only one private key	Use 2 public key Use 2 private key
Process very slow	Process speed is fast	Process speed is very low
It has less security	It has less security	It is provide more security
More permeable to brute force attack	Less permeable to brute force attack	Little permeable to brute force attack
Using encryption and decryption required time is more	Using encryption and decryption required time is less	Using encryption and decryption required time is very more

Table 4. The Results of RSA, RSA_CRT and Advanced RSA

Size in bits	All time of encryption and decryption in RSA in MS	All time of encryption and decryption in RSA_CRT in MS	All time of encryption and decryption in advanced model in MS
640	42	22	84
1040	48	25	93
1136	63	29	113

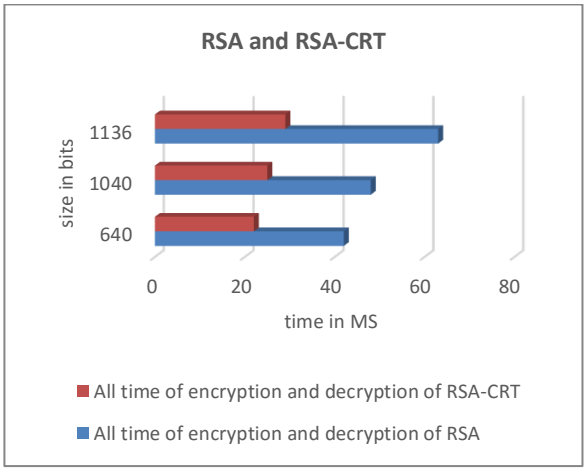


Figure 5: RSA and RSA with Chinese remainder theorem (Part 1)

6. The Objective of this paper

Enhancement the performance of RSA and increase the security and evaluated the security according to Randomness testing (using NIST statistical tests) has developed a package of 15 statistical tests to assure the randomness of a cryptography algorithm, The NIST Test Suite is developed to test the randomness of binary sequences produced by either hardware or software based cryptographic random number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence, the 15 tests are:

1- The Frequency (Mon obit) test
2- Frequency test within a block
3- The Run test
4- Tests for the longest-Run-of-ones in a block
5- The Binary matrix rank test
6- The Discrete Fourier transform test
7- The Non-overlapping template matching test
8- The Overlapping template matching test
9- Maurer's "Universal statistical" test
10- The Linear complexity test
11- The Serial test
12- The Approximate entropy test
13- The cumulative sums test
14- The Random excursions test
15- The Random excursions variant test

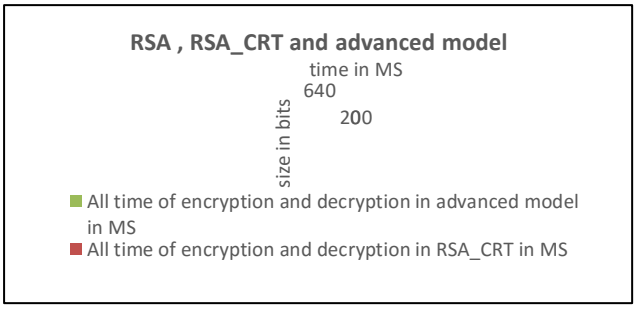


Figure 6: RSA and RSA with Chinese remainder theorem (Part 2)

After NIST tests have been run there are some of tests with P- value as follow since the P-value is ≥ 0.01, accept the sequence as random.

Table5. The Results of NIST Tests on Advanced Model

Test name	p-value	conclusion
Overlapping template matching test	0.980204	Random
Runs test	0.550989	Random
Frequency test	0.101978	Random

Explain to P-value:

Each test is based on a calculated test statistic value, which is a function of the data. If the test statistic value is S and the critical value is t, then the Type I error probability is P(S > t || Ho is true) = P(reject Ho | H0 is true), and the Type II error probability is P(S ≤ t || H0 is false) = P(accept H0 | H0 is false). The test statistic is used to calculate a P-value that summarizes the strength of the evidence against the null hypothesis. For these tests, each P-value is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by the test. If a P-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A P-value of zero indicates that the sequence appears to be completely non-random. A significance level (α) can be chosen for the tests. If P-value ≥α, then the null hypothesis is accepted; i.e., the sequence appears to be random. If P-value < α, then the null hypothesis is rejected; i.e., the sequence appears to be non-random. The parameter α denotes the probability of the Type I error. Typically, α is chosen in the range [0.001, 0.01].

- An α of 0.001 indicates that one would expect one sequence in 1000 sequences to be rejected by the test if the sequence was random. For a P-value ⩾ 0.001, a sequence would be considered to be random with a confidence of 99.9%. For a P-value < 0.001, a sequence would be considered to be nonrandom with a confidence of 99.9%.
- An α of 0.01 indicates that one would expect 1 sequence in 100 sequences to be rejected. A P-value ⩾ 0.01 would mean that the sequence would be considered to be random with a confidence of 99%. A P-value < 0.01 would mean that the conclusion was that the sequence is non-random with a confidence of 99%.

7. Performance

The advanced RSA model is more secure as compared to original RSA algorithm. The RSA with CRT requires less number of iterations as compared to original RSA algorithm. It reduces the cost of computation. The performance of RSA is enhanced with Chinese Remainder Theorem and became more secure using the advanced RSA model (two public and private keys) although it takes long time to

Perform it as compared to original RSA.

8. Conclusion and future work

The results observed from our work mention clearly that when using a single (public and private key)the time required of computation is less but problem is less secure, and when used RSA with CRT the time of evaluation is reduced. In order to provide safety transmission of information and more security we can use advanced RSA model.so that to have both secure transmission and time bound application we will use Hybrid model from mix between the advanced RSA model of RSA and Chinese remainder theorem ,When the encryption time increases The CRT can be applied in decryption process.

REFERENCES

[1] S. Saraireh "A Secure Data Communication System Using Cryptography and Steganography", International journal of Computer Networks & Communications, 5(3):125-137, May 2013.

[2] L. Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, 15(1):1-6, 2014.

[3] T Ritu, and A. Sanjay, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Innovative Research in Science, Engineering and Technology, 4(3):1028-1031, 2014.

[4] M. Bhumi, J. Patel and N. J. Janwe, "To Design and Implement a Novel Method of Encryption Using Modified RSA Algorithm and Chinese Remainder Theorem", International Conference on Industrial Automation and Computing, 12-13, April 2014.

[5] K. Sony, D. Shaik, B.D. Sri and G. anitha, "Improvised Asymmetric Key Encryption Algorithm Using MATLAB" , Journal of Electronics and Communication Engineering 10(2):31-36, 2015.

[6] L. Ronald, A. Shamir, and L. Adelman, "On Digital Signatures and Public Key Cryptosystems, ", a research in Massachusetts Institution of Technology Cambridge Lab For Computer Science, 82-83, April 1977.

[7] V. Kapoor, "Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and prime Number" International Journal of Scientific Research in network security and communication, 1(2):35-38 2013.

[8] G. N. Shinde and H. S. Fadewar " Faster RSA Algorithm for Decryption Using Chinese Remainder Theorem", In International Conference on Computational and Experimental Engineering and Sciences, 5(4):255-262, 2008.

[9] N. Suganya, M. E. Boopal, M Naveena, " Implementing Multiprime RSA Algorithm to Enhance the Data Security in Cloud Computing", International Journal of Innovative Research in Science, Engineering and Technology, 4(1): 2347-6710, January 2015.

[10] A. Rai, and S. Jain, " Modified RSA Cryptographic System with Two Public keys and Chinese Remainder Theorem", International Journal of Computer Science and Engineering, 26(6):726-729, July 2017