ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Design & Implementation of Multi Power RSA – CRT Cryptosystem with $N=P^mQ$

E.Sreedevi[1], Prof.M.Padmavathamma[2]

Research Scholar, Dept. of Computer Science, S.V. University, Tirupati, A.P. India[1]

Professor, Dept. of Computer Science, S.V. University, Tirupati, A.P. India[2]

ABSTRACT: In the current situation, security plays an important issue to deal with in various ways of communication between multiple users and is the largest tool used in the field of medical diagnosis, cloud computing, resource sharing etc., one of the necessary aspects for the secured communication is the field of cryptography. Cryptography, defined as the science and study of secret writing. RSA cryptosystem is an emerging area of public key cryptography. Some variants of RSA, such as RSA-CRT, multifactor RSA, and rebalanced RSA, are designed to speed up RSA decryption or encryption. In this paper we propose design and implementation of faster security algorithm i.e., Multi Power RSA – CRT cryptosystem with $N= P^m$ x Q. Here we have analyzed the performance of different variants of RSA along with the Multi power RSA –CRT with $N=P^3$ Q and given the results.

KEYWORDS: RSA Algorithm, Chinese Remainder Theorem, Multi Power RSA Algorithm, Encryption, Decryption.

I. INTRODUCTION

The RSA cryptosystem is still an emerging area in all aspects of public key cryptography. Public key algorithms are 100 times slower than Symmetric key algorithms. Many researchers are trying to improve the computational efficiency of Public key cryptography. The encryption and decryption in RSA takes heavy exponential multiplications modulus of a large integer N which is the product of two large prime numbers p and q . Commonly, the RSA algorithm takes more encryption and decryption time. To reduce the encryption, we may make use of small public exponent e. But for decryption, there is no chance. It takes more time. So, Quisquater and Couvreur proposed Chinese Remainder Theorem (CRT) to reduce decryption time. This CRT is used in some variants of RSA such as RSA CRT, Rebalanced RSA. In 1990, Wiener recommended another variant, called Rebalanced RSA-CRT, which further speeds up RSA decryption by shifting decryption costs to encryption costs.

Security plays an important role in medical diagnosis system. Cryptography has several important aspects in supporting the security of the data, which guarantees confidentiality, integrity and the guarantee of validity (authenticity) data. One of the public-key cryptography is the RSA cryptography. In this paper we propose and implement Multi Power RSA – CRT cryptosystem with $N= P^m$ x Q for providing security and analysis has been made with different variants of RSA.
This paper is organized as follows: Section 2 deals with review of literature, Section 3 gives brief description about the RSA and its variants, Section 4 discussed about Multi power RSA-CRT with N= Pm x Q, Section 5 discussed about results and analysis of different RSA and its variants and proposed multi power RSA-CRT with N= P3 x Q, and finally conclusion reached to last section.

II. REVIEW OF LITERATURE

Klaus Hansen et.al,[2] explored the efficiency on modern mobile phones of variants of the RSA cryptosystem, covering CRT, Multi-Prime RSA, Multi-Power RSA, Rebalanced RSA and R-Prime RSA by comparing the encryption and decryption time using a simple Java implementation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Hung-Min Sun et.al., [6] discussed two variants of Rebalanced RSA-CRT in which the public exponent e is much smaller than the modulus, thus reducing the encryption costs, while maintaining low decryption costs.
J.B. Awotunde et.al., [3], proposed Medical Diagnosis System that will predicts possible disease related to symptoms entered by the user by using probabilistic analysis and proposed systematic technique for mounting poisoning attacks against machine learning algorithms used for medical datasets, and implemented countermeasures against them.
S.Venkateswarlu et.al., [10] proposed threshold φ(n)2 – φ(N)-RSA Algorithm to provide hierarchy implementation of encryption and decryption phases and given that it has better performance than RSA and its variants like Batch-RSA, Multi- Prime RSA, Rebalanced – RSA.
Dr. D.W.Chadwick et.al., [11] proposed a secure access to patient information systems over the internet using the Application architecture , but for distributed access to patient information systems. They used Public Key Infrastructure, digital signatures for providing security for application.
Wong Kok Seng et.al., [12] proposed a model for secure data sharing, where hospitals within the Telemedicine system do not need to construct a central repository to share their local databases. They only need to answer to the queries made by the data miner and contribute requested dataset into the union dataset.
Liang Xiao et. al., [13] presented a link-anonymised data scheme and in addition to that, a security model that together enforce privacy data security and secure resource access for distributed clinical centres. Their approach involves a prototype medical decision support system, HealthAgents, for brain tumour diagnosis.
Seema Verma et.al., [14] proposed scheme that gives the same advantage in encryption side as in rebalanced CRT variants, besides it is 2 times faster at decryption side than rebalanced CRT variants. They described that It has been decreased approximately by a factor of 2.39 from rebalanced RSA CRT variant. Comparison of the RSA variants with the new scheme are also given for better analysis

III. EXISTING RSA ALGORITHM AND SOME OF ITS VARIANTS

In the following subsections, we review the original RSA and the variants of RSA-CRT, multi-prime RSA, multi-power RSA-CRT

A. Basic RSA Algorithm:

There are three main operations which are to be performed in the algorithm. The three operations are: key generation, encryption and decryption.

i) Key Generation

RSA consists of two keys – public key and private key. The public key can be known to the public and this key is used for encrypting the messages. Messages encrypted with the public key can only be decrypted by using the private key. The public key exponent is e and d is kept back as the private key exponent. The steps for key generation are explained below:

1. Generate two distinct n-bit primes, p and q, and
2. Calculate N = p q
3. Calculate φ (n)=(p-1)(q-1)
4. Choose an integer e such that gcd (φ (n), e) = 1 and 1 < e < φ (n)
5. Compute d =e^{-1} mod (p − 1) (q − 1).
6. The public key is (e, N
7. The private key is (d, N).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

ii) Encryption:

The steps for encryption of message in order to get the cipher-text are explained below:

1. Obtain a plain text M.
2. Compute the cipher text as C = Me mod N

iii) Decryption:

The steps for decryption of cipher-text in order to get the original message are explained below:

1. Get the cipher text C.
2. Calculate the plain text as $M = C^d \bmod N$

B. Multi prime RSA:

The multi-prime RSA fundamentally employs RSA algorithm with more than two prime numbers. The algorithm is described below:

i) Key Generation

1. Generate three distinct n-bit primes, p , q , r and
2. Calculate N = p q r and φ (n)=(p-1)(q-1)(r-1)
3. Choose an integer e such that gcd (φ (n), e) = 1 and 1 < e < φ (n)
4. Compute $d = e^{-1} \bmod (p - 1)(q - 1)(r - 1)$.
5. The public key is (e, N)
6. The private key is (d, N).

ii) Encryption Operation

For a given plain text m and the encryption algorithm is the same as that of the original RSA:

$$c = M^e \bmod N$$

iii) Decryption Operation

For a given Cipher text c and the decryption algorithm is the same as that of the original RSA

$$M = Cd \bmod N$$

C. RSA-CRT:

The key generation and encryption algorithm is identical to that of the original RSA, except that the private key is the tuple (p, q, dp, dq) where

1. Compute $d_p = d \bmod p - 1$ and $d_q = d \bmod q - 1$
2. Get a cipher-text C. The decipher can first compute $Mp = C^{d1} \bmod p$ and $Mq = C^{d2} \bmod q$
3. Next, using the Chinese Remainder Theorem (CRT) in order to obtain plaintext
4. $M = (Mp\ q\ (q^{-1} \bmod p) + Mq\ p\ (p^{-1} \bmod q)) \bmod (p \times q)$

IV. PROPOSED MULTI POWER RSA – CRT ALGORITHM WITH $N=P^MQ$

One can further speed up RSA decryption using moduli of the form N = p m q where q and q are prime numbers. Here we use Chinese Remainder Theorem to speed up the calculation at decryption side and we are calculating N = p m q so that the data can be transmitted in a more secured way.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

In Multi power RSA-CRT, it is a common practice to employ the Chinese Remainder Theorem during decryption. In decryption, it gives results much faster than modular exponentiation. Multi power RSA-CRT is different from the standard RSA in key generation and decryption.

i) Key generation:

It generates an RSA public/private key pair as follows:

1. Generate two distinct n-bit primes, p and q, and
2. Calculate $N = p^m \times q$.
3. Choose an integer e such that gcd (φ (n), e) = 1 and 1 < e < φ (n)
4. Compute $d = e^{-1} \bmod (p-1)(q-1)$.
5. Compute $d_p = d \bmod p-1$ and $d_q = d \bmod q-1$.
6. The public key is (e, N) and the private key is (p,q,dp,dq).

ii) Encryption:

Same as in standard RSA.

1. Obtain a plain text M.
2. Compute the cipher text as $C = M^e \bmod N$

iii) Decryption:

To decrypt a ciphertext C using the private (p, q , d1, d2) one does:

1. Compute $Mp = C^{dp} \bmod p$ and $Mq = C^{dq} \bmod q$
2. **Next use Chinese Remainder Theorem Procedure to get plaintext:**

$M = (Mp\ q\ (q^{-1} \bmod p) + Mq\ p\ (p^{-1} \bmod q)) \bmod (p \times q)$

V. RESULTS AND ANALYSIS

RSA , Multi prime RSA , RSA-CRT and Multi power RSA are implemented in java. These algorithms are tested and calculate the Key generation, encryption and decryption times. Each algorithm is executed for 10 times and Mean average time of Key generation, Encryption and Decryption are tabulated as follows

Key Generation	
Algorithm	**Average Time (millisec)**
RSA	**2071.5**
MPrimeRSA	**3753**
RSA CRT	**1992.7**
MPowerRSA2	**1984.6**
MPowerRSA3	**1277.9**

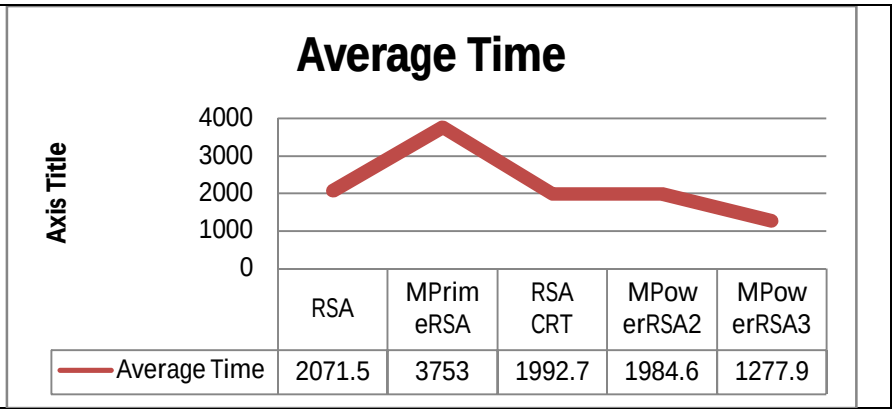

Fig1: Average mean time taken for Key generation Process

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

The above fig1 shows average time taken in Key generation process for RSA , Multi prime RSA , RSA-CRT and Multi power RSA with N=P2Q and Multi power RSA with N=P3Q .From the above fig 1, Multi power RSA with N=P3Q is taking less key generation average mean time when compared to other RSA variants.

Encryption	
Algorithm	Average Time (millisec)
RSA	37.5
MPrimeRSA	125
RSA CRT	40.6
MPowerRSA2	82.6
MPowerRSA3	120.3

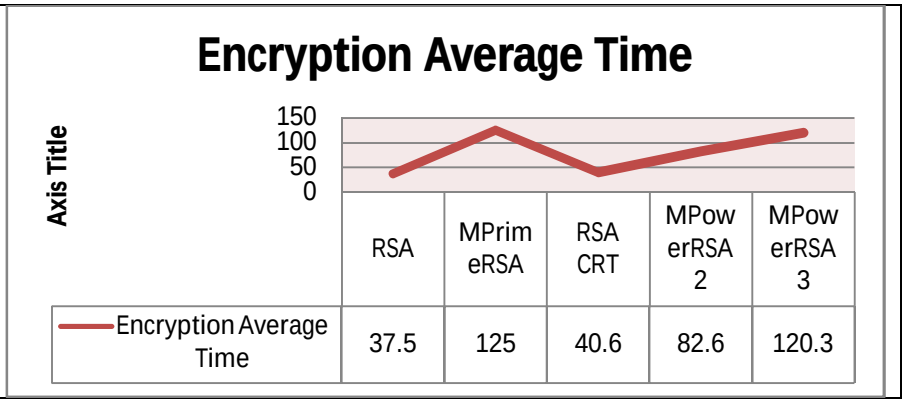

Fig2: Average mean time taken for Encryption Process

The above fig2 illustrates average time taken in Encryption process for RSA , Multi prime RSA , RSA-CRT and Multi power RSA with N=P2Q and Multi power RSA with N=P3Q . From the above fig 2, RSA is taking less encryption average mean time when compared to other RSA variants. But it is not more secure when compared to Multi power RSA with N=P3Q.

Decryption	
Algorithm	Average Time (millisec)
RSA	100.4
MPrimeRSA	646.1
RSA CRT	54.8
MPowerRSA2	50.2
MPowerRSA3	56.2

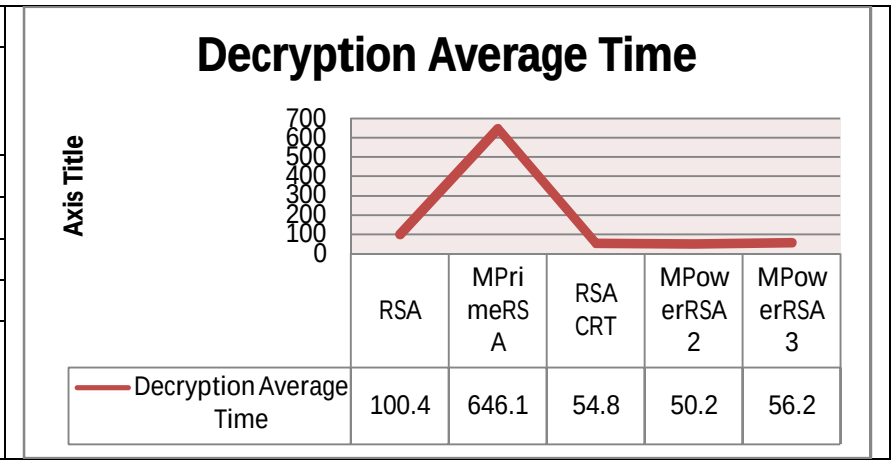

Fig3: Average mean time taken for Encryption Process

The above fig3 illustrates average time taken in Decryption process for RSA , Multi prime RSA , RSA-CRT and Multi power RSA with N=P2Q and Multi power RSA with N=P3Q . . From the above fig 3, Multi power RSA with N=P2Q is taking less encryption average mean time when compared to other RSA variants. But it is not more secure when compared to Multi power RSA with N=P3Q.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Finally we are calculating the total time taken for executing the RSA , Multi prime RSA , RSA-CRT and Multi power RSA with N=P2Q and Multi power RSA with N=P3Q. Analysis has been made and shown in below figure 4.

Algorithm	Average Keygeneration Time	Encryption Time	Decryption Time	Total Time
RSA	2071.5	37.5	100.4	2209.4
MPrimeRSA	3753	125	646.1	4524.1
RSA CRT	1992.7	40.6	54.8	2088.1
MPowerRSA2	1984.6	82.6	50.2	2117.4
MPowerRSA3	1277.9	120.3	56.2	1454.4

Table 1: Total time taken to execute different algorithms of RSA

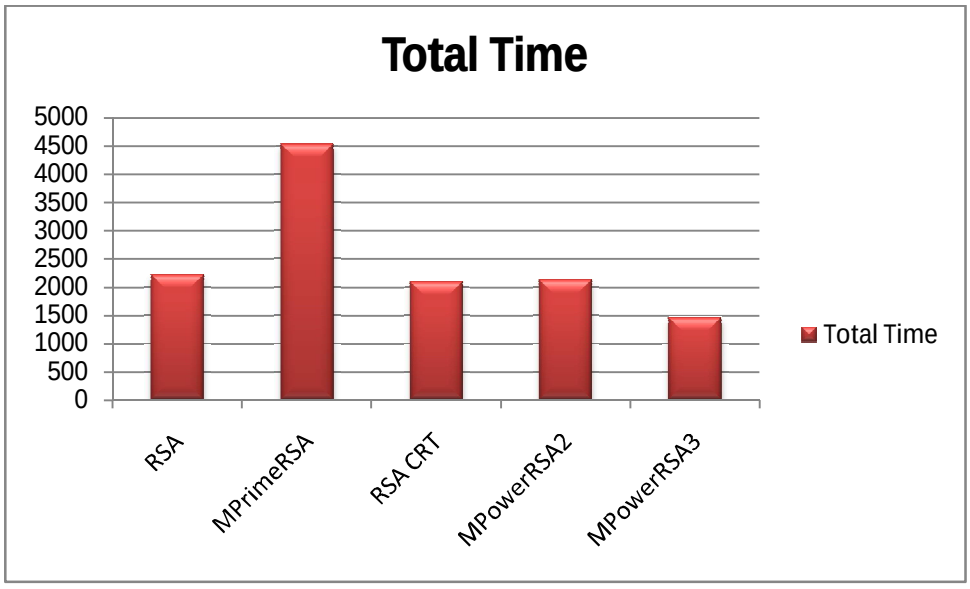

Fig 4: Column chart showing Total time taken for existing and proposed algorithms

The above table shows the average time cost in milliseconds of different variants of RSA. Here we have analyzed RSA, Multi prime RSA, RSA CRT , Multi power RSA-CRT with N=P2Q and Multi power RSA-CRT with N=P3Q. We have calculated the cost time of Key generation, Encryption and decryption process. When compared to RSA and Multi prime RSA , RSA CRT and Multi power RSA is giving more performance. When comparing with other variants of RSA , Multi power RSA-CRT with N=P3Q is taking less execution time, giving more performance and more security when compared to other methods. It is decreasing decryption time and giving more security for the data.

VI.CONCLUSION

Providing security for Medical diagnosis system has become an emerging trend in the area of research. This paper proposes faster Multi power RSA –CRT with $N=P^m Q$ using Chinese Remainder Theorem for faster decryption process in a more secured way. Proposed Multi power RSA-CRT with $N=P^mQ$ is taking less execution time, giving more performance and more security when compared to other methods. The proposed approach in the paper gives better

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

performance at the cost of a small decrease in decryption side. Besides it provides the semantic security to the system which is not provided by Multi prime RSA & RSA CRT. Here we have analyzed the performance of different variants of RSA along with the Multi power RSA –CRT with N=P3 Q by means of Key generation, Encryption and Decryption time and given the results by implementing in java.

REFERENCES

1. N.G.Bhuvaneswari Amma , K.Malathi , P.Balasubramanian,"Secured Neuro Genetic Approach for Predicting the Risk of Heart Disease", International Journal of Innovative Research in Computer and Communication Engineering , Vol. 2, Issue 11, November 2014
2. Klaus Hansen, Troels Larsen and Kim Olsen,"On the Efficiency of Fast RSA Variants in Modern Mobile Phones ",(IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009
3. J.B. Awotunde , O.E. Matiluko , O.W Fatai, "Medical Diagnosis System Using Fuzzy Logic ",African Journal of Computing & ICT, IEEE, Vol 7. No. 2 - June, 2014.
4. Huayin Ou, Baodian Wei, "Multi-Factor Rebalanced RSA-CRT Encryption Schemes", 2009 2nd International Conference on Biomedical Engineering and Informatics, IEEE Explore, 17-19 Oct. 2009
5. Dr. Abdullah Al-Malaise Al-Ghamdi, Majda A.Wazzan, Fatimah M. Mujallid, Najwa K.Bakhsh, "An Expert System of Determining Diabetes Treatment Based on Cloud Computing Platforms ",(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, pp. 1982-1987
6. Hung-Min Sun , M. Jason Hinek , Mu-En Wu,"On the Design of Rebalanced RSA-CRT ",Nov.2007
7. Seema Verma , Dr Deepak Garg ,"Improvement in RSA Cryptosystem , "JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY, VOL. 2, NO. 3, AUGUST 2011
8. Prasad Vanjari , Rahul Patil , Nehali Patil, "Medical Diagnosis System and Security ",International Journal of Recent Trends in Engineering & Research (IJRTER), Volume 03, Issue 01; January - 2017 [ISSN: 2455-1457].
9. Hung-Min Sun and Mu-En Wu, "An Approach Towards Rebalanced RSA-CRT with Short Public Exponent ",o Eurocrypt'05
10. S.Venkateswarlu , Dr.R.Seshadri , "THRESHOLD Φ (n)2 – Φ(N)-RSA ALGORITHM " , INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, Sep-2015, ISSN: 2277-9655
11. Dr. D.W.Chadwick, Dr. J.P.New, Dr. D.M.McDowall , D.P.Mundy, "Providing Secure Access to Confidential Patient Information Detailing Diabetic Condition",
12. Wong Kok Seng,Myung Ho Kim, Rosli Besar, Fazly Salleh, "A Secure Model for Medical Data Sharing", International Journal of Database Theory and Application, pp.45-52
13. Liang Xiao et. al., "A Security Model and its Application to a Distributed Decision Support System for Healthcare", The Third International Conference on Availability, Reliability and Security, IEEE Explore, 0-7695-3102-4/08, 2008
14. Seema Verma and Deepak Garg, "Improvement in Rebalanced CRT RSA", The International Arab Journal of Information Technology, Vol. 12, No. 6, November 2015
15. Hung-Min Sun and Mu-En Wu, "Design of Rebalanced RSA-CRT for Fast Encryption", National Science Council, Taiwan, under contract NSC-93-2213-E-007-102.