ISSN No. 0976-5697

Volume 2, No. 3, May-June 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Variants of Public Key Cryptosystem RSA

Mr. Amit Manakshe*
Dept of CE
Sipna's College of Engineering and Technology,
Amravati, India
manakshe.amit@gmail.com

Prof. Vijay Gulhane
Associate Prof, Dept of CSE and IT
Sipna's College of Engineering and Technology,
Amravati, India
v_gulhane@rediffmail.com

Abstract: This paper gives overview of various variants of public key cryptosystem RSA. It also presents performance analysis by comparing these methods.

Keywords: encryption, decryption, plaintext, cipher text, key generation

I. INTRODUCTION

In this article we have developed a new Public Key Cryptosystems which was extension of the work of Cesar Alison Monteiro Paixao. Some variants analyzed here uses the properties of Jordan Totient function. We briefly discuss the possibility and validity of combining such variants to obtain a new efficient and general Cryptosystems.

II. JORDAN – TOTIENT FUNCTION

A. *Definition*

A generalization of the famous Euler's Totient function is the Jordan's Totient Function defined by

$$J_k(n)= n^k \prod_{p/n}(1 - p^{-k}), \text{ where } k, n \in Z^+ \qquad (1)$$

We define the conjugate of this function as

$$\bar{J}_k(n) = n^k \prod_{p/n}(1 + p^{-k}) \qquad (2)$$

B. *Properties*

a. $J_k(1)=1$, $J_k(2) = 2^k-1 = 1 \pmod 2$

b. $J_k(n)$ is even if and only if $n \geq 3$

c. If p is a prime number, then

a. $J_k(p) = p^k (1-p^{-k}) = (p^k-1)$

b. $J_k(p^{\square}) = p^k (1-p^{-k}) = (p^k-1)$

d. If $n= p_1^{\square 1}, p_2^{\square 2}, \ldots\ldots\ldots p_r^{\square r}$, Then

a. $J_k(n) = p_1^{(\square 1-l)}. p_2^{(\square 2-l)k} \ldots\ldots p_r^{(\square r-l)k}. (p_1^k-l). (p_2^k-l) \ldots\ldots\ldots\ldots (p_r^k-l)$

e. $J_1(n) = \square\ (n)$

C. *Definition : (Multiplicative Function):*

A function f defined over the set of positive integers is said to be multiplicative if for each pair (m,n) with gcd (m,n)=1 then f(mn)= f(m) f(n).

D. *Theorem:*

Jordan Totient function is multiplicative.

E. *Theorem:*

Let p,q be two positive distinct prime numbers and n=pq.

If a be any positive integer such that gcd(a,n)=l then $a^{Jk(n)} \square 1 \pmod n$

Proof : Given that p, q be two positive distinct prime numbers and n=pq.

According to the definition of Jordan-toient function, we have

$$J_k(n) = n^k \prod_{p/n}(1 - p^{-k})$$

for n=pq we have $J_k(n) = (pq)^k (1-p^{-k}) (1-q^{-k})$

$$J_k(n) = (p^k-1) (q^k-1) \qquad (1)$$

Let a be any positive integer such that gcd (a,n)=1

□ gcd(a,pq)=l

□ gcd(a,p)=l and gcd(a,q)=l

According to Fermat's Theorem

$$a^{p-1} \square 1 \pmod p \qquad (2)$$

We know that for k □ 2

$$p^k-1=(p-1) (p^{k-1}+ p^{k-2}+\ldots\ldots\ldots\ldots\ldots+1) \qquad (3)$$

From (2) & (3) we have

$a^{p-1} \square \pmod p$

$$(a^{p-1})^{(p^{k-1}+p^{k-2}+\ldots+1)} \square\ 1^{(p^{k-1}+p^{k-2}+\ldots+1)} \pmod p$$

$$a^{p^k-1} \square\ 1 \pmod p$$

$$\left(a^{p^k-1}\right)^{q^k-1} \square\ (1)^{q^k-1} \pmod p$$

$$a^{Jk(n)} \square\ 1 \pmod p \qquad (4)$$

F. *Corollary*

Suppose $p_1, p_2, \ldots\ldots\ldots\ldots p_r$ are any r distinct positive prime numbers and $n= p_1.p_2. \ldots\ldots\ldots\ldots p_r.$ If a be any positive integer such that gcd(a,n)=1 then $a^{Jk(n)} \square\ 1$ (mod n).

III. NEW VARIANT J_K – RSA CRYPTOSYSTEMS

A. *RSA Cryptosystem:*

The RSA algorithm (named after its founders, Ron Rivest, Adi Shamir, and Leonard Adleman) [11] has become almost synonymous with public key cryptography. There are two interrelated components of RSA:

a. The choice of the public key and the private key

b. The encryption and decryption algorithm

In order to choose the public and private keys, we must perform the following steps.

c. Choose two large prime numbers, p and q? The larger the values, the more difficult it is to break RSA, but the longer it takes to perform the encoding and decoding. An RSA laboratory recommends that the product of p and q be on the order of 1024 bits for corporate use and 768 bits for use with "less valuable information".

d. Compute n = p*q and z = (p - 1)*(q - 1)

e. Choose a number e, less than n, which has no common factors (other than 1) with z. (In this case e and z are said to be relatively prime.) The letter e is used since this value will be used in encryption.

f. Find a number, d, such that (e *d – 1) is exactly divisible (that is, with no remainder) by z. The letter d is used because this value will be used in decryption. Put another way, given e, we choose d such that the integer remainder when e*d is divided by z is 1 (The integer remainder when an integer x is divided by the integer n. is denoted x mod n).

g. The public key that receiver makes available to the world is the pair of numbers (n, e); his private key, is the pair of numbers (n, d).
The encryption by Sender and the decryption by receiver are done as follows.

h. Suppose sender wants to send receiver a bit pattern or number, m, such that m < n. To encode, sender performs the exponentiation, m^e, and then computes the integer remainder when m^e is divided by n. Thus, the encrypted value, c, of the plaintext message, m, that Sender sends is

$$c= m^e \bmod n$$

i. To decrypt the received ciphertext message c, receiver computes m = c^d mod n which requires the use of his private key (n, d).

B. J_k – RSA Cryptosystem:

The main role of RSA cryptosystem is the usage of Euler's Totient function □(n) and Euler's theorem [1]. Now we replace □(n) by Jordan-Totient function $J_k(n)$ [1]with the same property.

a. Key Generation

[i] Choose two large prime numbers, p and q. How large should p and q be? The larger the values, the more difficult it is to break RSA, but the longer it takes to perform the encoding and decoding.

[ii] Compute n = p*q and $J_k(n) = (p^k - 1)*(q^k - 1)$

[iii] Choose a number e, less than n, which has no common factors (other than 1) with $J_k(n)$ (In this case, e and $J_k(n)$ are said to be relatively prime.)

[iv] Find a number, d, such that (e *d – 1) is exactly divisible (that is, with no remainder) by $J_k(n)$.

[v] Public Key = (k, e, n)
Private Key = (k, d, n)

b. Encryption

Given a plaintext M and the public key = (k, e, n) compute the ciphertext C by using the formula.

C□M^e (mod n)

c. Decryption :

Given a ciphertext C and the Private Key =(k, d, n), compute the plaintext M by using the formula

M□ C^d (mod n)

C. M-Prime RSA Cryptosystem

Multi Prime RSA Cryptosystem [2] was introduced by Collins who modified the RSA modules so that it consists of r primes $p_1, p_2, \ldots\ldots p_r$ instead of the traditional two primes p and q.

a. Key Generation:

The key generation algorithm receives as parameter the integer r, indicating the number of primes to be used. The key pairs are generated as in the following steps.

[i] Choose r distinct primes $p_1, p_2, \ldots\ldots p_r$ each one $\left\lfloor \frac{Logn}{r} \right\rfloor$ bits in length and
n = $\prod_{i=1}^{r} p_i = p_1 \cdot p_2 \ldots\ldots\ldots p_r$

[ii] Compute E and D such that d=e^{-1} (mod □ (n))
where gcd (e, □(n))=1, where
. □(n) = $\prod_{i=1}^{r} (p_i - 1)$
= $(p_1-1)\ (p_2-1) \ldots\ldots(p_r-1)$ (1)

[iii] For 1 □ i □ r compute d_i □ d (mod p_i-1)
Public Key = (n,e)
Private Key = $(n, d_1, d_2, \ldots\ldots d_r)$

b. Encryption:

Given a public Key (n,e) and a message M□ Z_n encrypt M exactly as in the original RSA, thus

C □ M^e (mod n)

c. Decryption :

The decryption is an extension of the quisquater-couvreur method. To decrypt a ciphertext C, first calculate

M_i □ C^{di} (mod p_i)

for each i = 1, 2, ………. r

Next apply the Chinese reminder theorem to the M_i's to get

M □ C^d(mod n)

D. M – Prime J_k – RSA Cryptosystem:

By replacing □ (n) by $J_k(n)$ with the same property we can generate a new variant cryptosystem. Modified key generation, encryption and decryption are given below

a. Key Generation

[i] Choose r distinct primes p1, p2, …….. pr each one $\left\lfloor \frac{Logn}{r} \right\rfloor$ bits in length and
n = $\prod_{i=1}^{r} p_i = p_1 \cdot p_2 \ldots\ldots\ldots p_r$

[ii] Compute E and D such that D=e-1 (mod Jk(n))
i.e.ED=1(mod Jk(n)) where gcd (e, Jk(n))=1 and
Jk(n) = $n^k \prod_{p|k} (1 - p^{-k})$
= $(p_1^k - 1)(p_2^k - 1) \ldots\ldots\ldots (p_r^k - 1)$
= $\prod_{i=1}^{r} (p_1^k - 1)$

[iii] For 1 □ i □ r compute d_i □ d (mod $(p_i^k - 1)$)
Public Key = (k, E, n)
Private Key = (k, D, n)

b. Encryption

Given a Public Key (k, e, n) and a message M □ Z_n, encrypt M exactly as in the original RSA, thus

C □ M^E (mod n)

c. Decryption

The decryption is an extension of the Quisquater Couvreur method. To decrypt a ciphertext C, first calculate $M_i=C^{di}$ (mod p_i) for each 1 □ i □ r, next apply Chinese Remainder Theorem to the M_i's to get

M □ C^D(mod n)

IV. PERFORMANCE ANALYSIS

RSA encryption system, mainly based on integer factorization as a hash function. For two primes p and q, compute h = F(p,q) is easy, this can be treated as polynomial time solution problem. But comuting F^{-1}(n) polynomial time solution problem. But computing F^{-1}(n) is difficult, this can be treated as non polynomial time solution problem. This problem can be solved by providing some trapdoor information (i.e., secret information), security lies with the multiplicative exponent. For example let us take p=11, q=3, the performance between RSA and J_2=RSA are given below.

Table: 1

Sr. No.	RSA Cryptosystem	Sr. No.	J2-RSA Cryptosystem
1	Select two primes p=11, q=3	1	Select two primes p=11, q=3
2	Compute n=pq=33 z=(p-1)(q-1)=20	2	Compute n=pq=33 $J_2(n)=(p^2-1)(q^2-1)=960$
3	Choose e=7 Since 7 has no common factors with 20 other than 1.	3	Choose e=7. Check gcd(e,p^2-1)= gcd(7,120) Check gcd(e,q^2-1)= gcd(7,8)=1 Check gcd (e, ($^{p2-}$1)(q^2-1)) =gcd(7,960)=1
4	Find a number, d, such that (e *d – 1) is exactly divisible (that is, with no remainder) by z i.e., find a unique value d such that 7*d -1 exactly divides 20 simple testing with d=1,2,3,……. gives d=3	4	Compute D such that ed□1(mod J_2(n)) i.e., compute D□e^{-1} (mod J_2(n) D□7^{-1} (mod 960) i.e., find a unique value d such that 960 divides 7d-1 Simple testing with d=1,2,3,……J_2(n) □This gives D=823 range increases
5	Public key = (n,e)= .(33,7) Private key = (n,d)=(33,3)	5	Public key = (n,E) =(33,7) Secret key =(n,D)= (33,823)
6	Now if we want to encrypt the message M=8 we have C□M^e(mod n) □ 8^7 (mod 33) C□2 (mod 33) □Ciphertext C=2	6	Now if we want to encrypt the message M=8 we have C□M^E (mod n) □ 8^7 (mod 33) C□2 (mod 33) □Cipher text C=2
7	To decrypt the cipher text we have M□C^d (mod n) □ 2^3 (mod 33) M□8 (mod 33) □Plain text M=8	7	To decrypt the cipher text we have M□C^D (mod n) □ 2^{823} (mod 33)(Hard) M□8 (mod 33) □ Plain text M=8

V. CONCLUSION

In this paper we analyzed three variants of RSA namely (1) J_k – RSA cryptosystem (2) M- Prime RSA cryptosystem (3) M- Prime J_k -RSA cryptosystem which are developed on the properties of Jordan – Totient function with standard RSA – cryptosystem. In some of our schemes, we implemented the computation on exponential values based on Jordan – Totient function. This results in increase in the block size for plaintext and enhances the range of public/private key. The increase in the size of private key avoids the attacks on private key.

V. REFERENCES

[1] Apostal T. M. "Introduction to the Analytic Number Theory" Springer International Students Edition (1980).

[2] Beak J. Lee B. and Kim K. " Provable Secure Length- Saving Public key Encryption scheme under the computational Diffie- Hallman Assumption Electronics and Telecommunications Research institute (E TRI) Journal, 22 (4) (2000) 25 – 31.

[3] Bellare M. "Practice Oriented Provable Security. Lectures on Data Security (Modern Cryptology in Theory and Practice), LNCS 1561 Springer Verlag, (1999) 1- 15

[4] Bellare M. Desai A. Pointcheval D. and Rogaway P. "Relations Among Notations of Security for Public Key Eneryption scherre, Advaneon in cryptogy prees like of CYPTO 98, LNCS 1462, Springer Verlag (1998) 26 – 45.

[5] Bellare M. and Rogaway P. "Random Oracles are Practical A Paradigm for Designing Efficient Protocols. ACM Conference on Computer and Communications Security.

[6] Bellary M. and Rogaway P. "Exact Security of Digital Signatures – How to Sign with RSA and Rabin Schemes "Advances in Cryptology Proceedings of EUPOCRYPT' 96. LNCS 1070.

[7] Boneh D. and Shacham H. " Fast Variants of RSA" RSA Laboratories (2002).

[8] Collins T. Hopkins D. Langford S. and Sabin M., "Public-key Cryptographic Apparatus and method "U.S. Ptent # 5.848, 159.(January 1997).

[9] Cramer R. and Shoup V. "A Practical Public Key Cryptosystem Provably Secure Against Adoptive Chosen Ciphertext Attack, Advances in Cryptology – Proceedings of CRYPTO 98 LNCS 1462, Springer Verlag, (1998) 13- 25.

[10] Diffie W. and Hellman M. "New Directions in Cryptography, IEEE Transactions on Information Theory, IEEE 10 (1977) 74- 84.

[11].Mao M. "Modern Cryptology: Theory and Practice", Prentice Hall, (2004)

[12].Computer networking: A Top-Down Approach Featuring the Internet, 2/e by Kurose and Ross

[13].Proceedings of ACM CCS's 93 ACM, (1993) 62 – 93.

[14].Quisquater J.J. and Couvreur C., Fast Decipherment Algorithm for RSA Public-key Cryptosystem" Electronic Lectures,18 (1982) 905 -907.

[15].Rivest R. Shamir A. and Adleman L., "A Method for obtaining Digital Signatures and Public-key Cryptosystems Communications of the ACM" 21 (2) (1978) 120 – 126.