International Journal of IT & Knowledge Management (ISSN: 0973-4414)
July-Dec 2008, Vol 1, Number-2, pp 571-577

J_k^* - RSA CRYPTOSYSTEMS AND J_k^* - RSA SIGNATURE SCHEMES

Dr.S.Thajoddin[1] , S. Makbul Hussian[2], Dr.SAM Gazni[3]

[1,2]Lecturer in Mathematics , [3]Lecturer in Physics, Osmania College , Kurnool AP, India

Abstract: By using $J_k(n)$ and by considering $\left(Z_{J_k(n)}, +_{J_k(n)}, X_{J_k(n)}\right)$, a commutative ring with unity as a message space we develop new variants of RSA cryptosystem and RSA signature schemes. We name them as J_k^* RSA cryptosystem and J_k^* RSA signature schemes. These schemes are explained and also analyze the signifance and complexity of the above schemes.

Keywords : $J_k(n)$, RSA cryptosystem, signature schemes, analyze, signifance.

INTRODUCTION

The RSA Cryptosystem was the first public key cryptosystem and it is still most widely used cryptography algorithm in the world. This cryptosystem would come a year later as an application of famous problem, integer factorization. We develop new variants of RSA cryptosystem and RSA signature schemes. We name them as J_k^* RSA cryptosystem and J_k^* RSA signature schemes. These schemes are explained and also analyze the signifance and complexity of the above schemes.

J_k^* - RSA Cryptosystem:

The algorithm for key generation, encryption and decryption of J_k^*-RSA Cryptosystem is described as follows.

Key Generation:

Choose two large primes p and q such that n = pq.

Let K be an integer such that 1 ≤ K ≤ n.

Compute $J_K(n) = n^k \underset{p/n}{\pi}\left(1-1/p^k\right)$ and consider

$\left(Z_{J_K}(n),^{+} J_K(n),^{X} J_k(n)\right)$a Commutative ring with unity of order $J_K(n)$ as a message space. Assign the numerical equivalents to the alphabets taken from $Z_{J_K}(n)$

M is the message belongs to. $Z_{J_K}(n)$

Select a random integer e such that gcd (e, $J_K(n)$=1, where 1<e< $J_K(n)$

e M mod $J_K(n)$ ∈ message space $Z_{J_K}(n)$

Select integer such that ed ≡ 1 (mod $J_K(n)$)

i.e., d=e[-1] mod $J_K(n)$), 1<e < $J_K(n)$

Public – Key PK = J_k (n), e)
Private Key SK = (J_k (n), d)

Encryption:

Given a public-key ($J_K(n)$, e) and a message M∈ $Z_{J_K(n)}$, compute the ciphertext

C = M^e mod J_k (n)
= eM mod J_k (n)

Decryption:

Given a public-key ($J_K(n)$, d) and cipher text C, compute the message

M = C^d mod J_k (n)
= d.C mod J_k (n)

The correctness of J_k – RSA decryption is verified as follows

C^d mod J_k (n) = $(M^e)^d$ mod J_k (n)
= M^{ed} mod J_k (n)
= (ed). M mod J_k (n)
= I.M. mod J_k (n)
= M

Simple example of J_k^* - RSA Cryptosystem:

Choose p =3, q=5
∴ n = pq = 15

Let k = 2

$$J_k(n) = J_2(15) = J_2(3\times5) = (3^2-1)(5^2-1)$$
$$= 8\times24 = 192$$

$\therefore (Z_{192}, +_{192}, X_{192})$ is a commutative ring with unity of order 192. Consider this as a message space.

Assign the numerical equivalents to the alphabets taken from Z_{192}. We can assign the numerical values randomly to the alphabets taken from Z_{192} to use this system to keep secret.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Key Generation:

Since gcd (5,192) = 1 and 1<5<192,

∴ We take e = 5

Selected d such that ed ≡1 mod J_k (n)
i.e. 5d ≡1 mod 192
5 x 77≡1 mod 192
∴ d = 77

Public – Key PK = (J_k (n), e) = 192.5)
Private Key SK = (J_k (n), d) = (192, 77)

Plaint text	H	E	L	L	O	W	O	R	L	D
Numerical equivalents	8	5	12	12	15	22	15	18	12	4
Message	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}

ENCRYPTION	**DECRYPTION**
$C_1 = M_1^e \bmod J_K(n)$ $= eM_1 \bmod J_K(n)$ $= 5 \times 8 \bmod 192 = 40$	$M_1 = C_1^d \bmod J_K(n)$ $= dC_1 \bmod J_K(n)$ $= 77 \times 40 \bmod 192$ $= 3080 \bmod 192 = 8$
$C_2 = eM_2 \bmod J_K(n)$ $= 5 \times 5 \bmod 192$ $= 25 \bmod 192 = 25$	$M_2 = dc_2 \bmod J_K(n)$ $= 77 \times 25 \bmod 192$ $= 1925 \bmod 192 = 5$
$C_3 = eM_3 \bmod J_K(n)$ $= 5 \times 12 \bmod 192$ $= 60 \bmod 192 = 60$	$M_3 = dc_3 \bmod J_K(n)$ $= 77 \times 60 \bmod 192$ $= 4620 \bmod 192 = 12$
$C_4 = eM_4 \bmod J_K(n)$ $= 5 \times 12 \bmod 192$ $= 60$	$M_4 = dc_4 \bmod J_K(n)$ $= 77 \times 60 \bmod 192$ $= 4620 \bmod 192 = 12$
$C_5 = eM_5 \bmod J_K(n)$ $= 5 \times 15 \bmod 192$ $= 75$	$M_5 = dc_5 \bmod J_K(n)$ $= 77 \times 75 \bmod 192$ $= 5775 \bmod 192 = 15$
$C_6 = eM_6 \bmod J_K(n)$ $= 5 \times 22 \bmod 192$ $= 110$	$M_6 = dc_6 \bmod J_K(n)$ $= 77 \times 110 \bmod 192$ $= 8470 \bmod 192 = 22$
$C_7 = eM_7 \bmod J_K(n)$ $= 5 \times 15 \bmod 192$ $= 75$	$M_7 = dc_7 \bmod J_K(n)$ $= 77 \times 75 \bmod 192$ $= 5775 \bmod 192 = 15$
$C_8 = eM_8 \bmod J_K(n)$ $= 5 \times 18 \bmod 192$ $= 90$	$M_8 = dc_8 \bmod J_K(n)$ $= 77 \times 90 \bmod 192$ $= 6390 \bmod 192 = 18$
$C_9 = eM_9 \bmod J_K(n)$ $= 5 \times 12 \bmod 192$ $= 60$	$M_9 = dc_9 \bmod J_K(n)$ $= 77 \times 60 \bmod 192$ $= 4620 \bmod 192 = 12$
$C_{10} = eM_9 \bmod J_K(n)$ $= 5 \times 4 \bmod 192$ $= 20 \bmod 192$ $= 20$	$M_{10} = dc_{10} \bmod J_K(n)$ $= 77 \times 20 \bmod 192$ $= 1540 \bmod 192$ $= 4$

J_k^* - RSA SIGNATURE SCHEME :

The algorithm for key generation, signature generation and verification of J_k-RSA Signature Scheme is described as follows.

Key Generation:

Choose two large primes p and q such that n =pq.

Let k be an integer such that 1 < k < n.

Compute $J_k(n) = n^k \underset{p|n}{\pi} \left(1 - 1/p^k\right)$ and

Consider $\left(Z_{J_k(n)}, +_{J_k(n)}, X_{J_k(n)}\right)$ a commutative ring with unity of order $J_k(n)$ as a message space. Assign the numerical equivalents to the alphabets taken from $Z_{J_K(n)}$

M is the message belongs to $Z_{J_K(n)}$

Select a random integer e such that

gcd (e, J_k (n)) =1, where 1 < e < J_k (n) and

eM mod J_k (n) ∈ message space $Z_{J_K(n)}$

Select integer d such that ed ≡ 1 (mod J_k (n))

i.e., d = e^{-1} mod J_k (n) where 1 ≤ d ≤ J_k (n)

Public-Key PK = (J_k (n), e)
Private Key SK = (J_k (n), d)

Signature Generation: Given a private key (J_k (n), d) and a message $Z_{J_k(n)}$,

Compute the signature C = M^d mod J_k (n)

= dM mod J_k (n)

Signature Verification: Given a public-key (J_k (n), e) and a signature C, compute the message

M = C^e mod J_k (n)

= e.C mod J_k (n)

The correctness of signature verification algorithm of J_k^* RSA Signature scheme is verified as follows.

C^e mod J_k (n) = $(M^d)^e$ mod J_k (n)

= M^{ed} mod J_k (n)

= (ed) M mod J_k (n)

= l.Mmod J_k(n) = M

Simple example of J_k-RSA Signature Scheme.

Choose p = 3; q = 5

∴ n = pq = 15 Let k = 2

$J_k(n) = J_2(15) = J_2(3 \times 5)$ = $(3^2 - 1)(5^2 - 1)$

= 8 x 24

= 192.

(Z_{192}, $+_{192}$, X_{192}) is a commutative ring with unity of order 192. Consider this as a message space.

Assign the numerical equivalents to the alphabets taken from Z_{192}. We can assign the numerical values randomly to the alphabets taken from Z_{192} to use this system to keep secret.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Key Generation:

Since gcd (5, 192) = 1 and 1 < 5 < 192
∴ we take e = 5
Select d such that ed = 1 mod J_k (n)
i.e. 5d ≡ l mod_{l92}
5 x 77 ≡ 1 mod 192
∴ d = 77

Public-Key PK = (J_k (n), e) = (192, 5)
Private Key SK = (J_k (n), d) = (192, 77)

Plaint text	H	E	L	L	O	W	O	R	L	D
Numerical equivalents	8	5	12	12	15	22	15	18	12	4
Message	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}

SINGATURE GENERATION	SIGNATURE VERIFICATION
C_1 = M_1^d mod J_K (n) = dM_1 mod J_K (n) = 77 x 8 mod 192 = 616 mod 192 = 40	M_1 = C_1^e mod J_K (n) = ec_1 mod J_K (n) = 5 x 40 mod 192 = 200 mod 192 = 8
C_2 = dM_2 mod J_K (n) = 77 x 5 mod 192 = 385 mod 192 = 1	M_2 = eC_2 mod J_K (n) = 5 x 1 mod 192 = 5
C_3 = dM_3 mod J_K (n) = 77x 12 mod 192 = 924 mod 192 = 156	M_3 = ec_3 mod J_K (n) = 5 x 156 mod 192 = 780 mod 192 = 12
C_4 = dM_4 mod J_K (n) = 77 x 12 mod 192 = 924 mod 192 = 156	M_4 = ec_4 mod J_K (n) = 5 x 156 mod 192 = 12
C_5 = dM_5 mod J_K (n) = 77 x 15 mod 192 = 1155 mod 192 = 3	M_5 = ec_5 mod J_K (n) = 5 x 3 mod 192 = 15

$C_6 = dM_6 \bmod J_K(n)$ $= 77 \times 22 \bmod 192$ $= 1694 \bmod 192 = 158$	$M_6 = ec_6 \bmod J_K(n)$ $= 5 \times 158 \bmod 192$ $= 790 \bmod 192 = 22$
$C_7 = dM_7 \bmod J_K(n)$ $= 77 \times 15 \bmod 192$ $= 1155 \bmod 192 = 3$	$M_7 = ec_7 \bmod J_K(n)$ $= 5 \times 3 \bmod 192$ $= 15$
$C_8 = dM_8 \bmod J_K(n)$ $= 77 \times 18 \bmod 192$ $= 1386 \bmod 192=42$	$M_8 = ec_8 \bmod J_K(n)$ $= 5 \times 42 \bmod 192$ $= 210 \bmod 192 = 18$
$C_9 = dM_9 \bmod J_K(n)$ $= 77 \times 12 \bmod 192$ $= 156$	$M_9 = ec_9 \bmod J_K(n)$ $= 5 \times 156 \bmod 192$ $= 12$
$C_{10} = dM_{10} \bmod J_K(n)$ $= 77 \times 4 \bmod 192$ $= 308 \bmod 192$ $= 116$	$M_{10} = ec_{10} \bmod J_K(n)$ $= 5 \times 116 \bmod 192$ $= 580 \bmod 192$ $= 4$

SIGNIFICANCE AND COMPLEXITY OF THE J_K^*-RSA AND J_K^*-RSA SIGNATURE SCHEMES:

J_K^*-RSA and J_K^*-RSA Signature Schemes have the following significant features.

1) Both J_K^*-RSA and J_K^*-RSA Signature Schemes are based on famous integer factorization problem.

2) The encryption algorithms of J_K^*-RSA and J_K^*-RSA Signature Schemes are one way functions unless, some trap door function is given, we cannot decrypt the plaintext from the cipher text.

3) Since, we have taken $\left({}^{z}J_{K(n)}, {}^{+}J_{K(n)}, {}^{X}J_{K(n)}\right)$ a commutative ring with unity as a message space we can use both the operations ${}^{+}J_{K(n)}$, and ${}^{X}J_{K(n)}$ in these cryptosystems.

4) Since, k is a positive integer such that $1 \leq k \leq n$, therefore k is our' choice. By choosing appropriate k, we can make the message space as large as possible. If we assign numerical equivalents to the alphabets; randomly from this message space, certainly it is very difficult to recover the plain text from ciphertext. So these cryptosystems are very much secure and complex.

REFERENCES:

1) Solomon, D.Data Privacy and security, Berlin : Springer 2003.

2) Trappe W and Washington L Introduction to cryptography and coding theory. Upper Saddle River, NJ : Prectice Hall, 2006.

3) Preprzyk, J.Hardjono I, and Seberry J.Fundmentals of Computer security Berlin : Springer, 2003.

4) Mao.W.Modrn Cryptography, Upper Saddle River, NJ: Practice Hall 2004.

5) Kanfman, C.Perlman, R. and Specimer, M.Network Security, Upper Saddla River, NJ : Practice Hall, 2004.

6) Menezes.A. Oorschot.P, and Vanstone, S.Handbook of applied cryptography. Newyork CRC press, 1997.

7) R.Rivest : A. Shamir and L.Adleman : A Method for obtaining Digital signatures and public –key cryptosystems communications of the ACM 21 (2), pages 120-126, 1978.

8) J.J.Quisquater and C.Couvreur. Fast Deciphernent Algorithm for RSA public – key cryptosystem. Electronic Lectures, Vol-18, 905-907, 1982.

9) T.Collins, D,Hopkins, S.Langform and M.Sabin public key cryptographic Apparatus and Method U.S.Parent #5,848, 159, January – 1997

10) D.Bone and H.Shacham. Fast variantsof RSA. RSA laboratus 2002.

11) Alison Monteiro Paixao : An efficient of vaciant of the RSA cryptosystem.

12) T.M.Apostal, introduction to analytic number theory, springer International Students Edition 1980.