Rebalanced Elatrash RSA Public-Key Cryptosystem

[1]P.Vasudeva Reddy [2]B.Umaprasada Rao [3]B.Muniswamy [4]K.Venkata Rao [5]T.Gowri

Abstract

RSA Cryptosystem is one of the most practical Public-Key Cryptosystem. In which the plaintext and ciphertext messages are taken from the multiplicative group Z_n, where n is a product of two large primes. Recently, Fayik Ramadan EL – Naowk proposed an extension of RSA, called Elatrash scheme, in which the plaintext and ciphertext messages are taken from the general linear group of k'k non singular matrices over Z_n In this scheme the encryption is much faster than decryption process. But in some applications one would like to have the reverse behavior i.e. fast decryption. In this paper, we present a variant of Elatrash scheme called Rebalanced Elatrash RSA Cryptosystem. In the proposed scheme we can encrypt/decrypt k^2 blocks at a time and the decryption process is approximately four times faster than Elatrash RSA scheme.

Keywords : RSA cryptosystem, Elatrash RSA scheme, general linear group, Chinese Remainder Theorem.

[1&2]Department of Engineering and Mathematics, College of Engineering, Andhra University, Visakhapatnam, A.P, India. Email : vasucrypto@yahoo.com, munistats@gmail.com

[3]Department of Statistics, Andhra University, Visakhapatnam, A.P, India. Email : buprasad@yahoo.co.in

[4]Department of Computer Science & Systems Engineering, Andhra University, Visakhapatnam, A.P, India. Email : prof_venkat@yahoo.com

[5]Department of Electronics and communication Engineering, ASCET, Gudur, A.P, India. Email :gowri3478@yahoo.com

1. Introduction

Information is recognized by many organizations as an important asset. Few businesses could function effectively without the ability to rely, to some extent, on information as a resource: banks need to know the details of each account, and hospitals need to access patient medical records. Information security is concern with providing assurances about data.

Broadly speaking, information security is frequently classified as the provision of the following services: confidentiality, integrity and availability.Communication over open networks is very cheap, but represents easy picking for an adversary who wants to intercept, modify, or inject data; data stored on networked computers faces similar threats. If society is to benefit from the advantages offered by electronic data storage and open networks, information security must therefore provide techniques capable of supplying confidentiality, integrity, and availability in this new environment.

In order to establish a confident channel between two users of such a network, classified single key cryptography requires them to exchange a common secret key over a secure channel. This may work if the network is small and local, but it is not feasible in non-local or large networks. To simplify the key exchange problems, modern Public-Key Cryptosystem provides a mechanism in which the keys to be exchanged do not need to be secrete. In such a frame work, every user possesses a key pair consisting of a public-key and a private key. Achieving authenticity of public keys can be done in several ways. Public-Key Cryptosystem is essential for e-commerce or

e-banking transactions; they assure privacy as well as integrity of the transactions between the two parties.

The pioneering research in this study by Diffie Hellman [2] introduced a new approach to cryptography and challenged cryptologists to come up with cryptographic algorithms that met their requirements for public-key systems. One of the first responses to the challenge was developed in 1977 by Ron Rivest et.al, at MIT. The Rivest-Shamir- Adleman (RSA) scheme [11] is a block cipher in which the plaintext and ciphertext are integers in the interval [0, n-1], where n is a composite modulus. The intractability of the RSA problem forms the basis for the security of the RSA public-key cryptosystem. The RSA problem is the difficulty of solving the integer modulus n as a product of two distinct odd large primes p and q [6].

2. Related Work

The first revaluation event in the era of the Public-Key Cryptography is coming on 1976 when Diffie Hellman [2] published their well known paper "New Directions in Cryptography". In 1978, Rivest, Shamir and Adleman (RSA) [11] introduced the first applied scheme which is the most popular public-key scheme. The security of RSA Public-Key Cryptosystem is based on Integer Factorization Problem. In 1979, Rabin [10] suggested a scheme which is also relied on the Integer Factorization Problem, but it is product of factoring of large Blum integers and the result of description scheme is four messages; just one from the results represent the original message. In 1992, Shimada [12] enhanced Rabin scheme using the extension Rabin Public Key Encryption scheme employing certain assumptions in a private key utilizing Jacob symbol. But in 1998, Okamoto [7] proposed a new Public Key Cryptosystem (PKC) as secure as factorizing relied on RSA and Rabin schemes. In 1999, Pointcheval [8] introduced a new public key encryption scheme based on the dependent RSA and Rabin schemes. Many variants of RSA public-key cryptosystem have been proposed [1, 3, 9, 13, 14].

In 2007, Fayik Ramadan EL-Naowk [4] proposed a public-key cryptosystem called Elatrash scheme, analogous to RSA, in which the plaintext and cipher texts are taken from the general linear group of k×k matrices over Z_n. This scheme also supports digital signatures. In the Elatrash RSA scheme, the encryption and signature verification are much faster than decryption. But in some applications, one would like to have the reverse behavior. For Example, when cell phone needs to generate an RSA signature that will be later verified on a fast server one would like signing to be easier than verifying. Similarly, SSL web browsers (doing RSA encryption) typically have idle cycles to burn where as SSL web servers (doing RSA decryption) are over loaded.

In this paper we present a variant of the Elatrash RSA scheme which employs the general linear group of matrices of order k with values selected randomly from Z_n, where n is a product of two large distinct primes. The decryption process of the proposed scheme uses Chinese Remainder Theorem (CRT) [9] for fast description. The rest of the paper is as follows. Section 3 describes the classical RSA scheme with an example. In Section 4, we present some main results which are building blocks of the proposed scheme. In Section 5 we present the extended, fast RSA Elatrash scheme with an example. Section 6 concludes this paper.

3. RSA Scheme

In this section we review classical RSA cryptosystem [11]. In which the plaintext is encrypted in blocks. The RSA PKC consists of the following three algorithms.

Key Generation:

- Select two large and distinct primes p and q, both are roughly the same size.
- Compute n = pq and $\varphi(n) = (p-1)(q-1)$.
- Select a random integer e, $1 < e < n$, such that gcd (e, n) = 1.
- Use Extended Euclidean Algorithm to compute the unique integer d, $1<d<n$, such that $ed \equiv 1 \pmod{\phi(n)}$.
- A's public key is (n, e); A's private key is (n, d).

Encryption: To encrypt a message $m \in Z_n$ for B, A should do the following.

- Obtain B's public-key (n, e) and represent the message $m \in [0, n-1]$.
- Compute the ciphertext $c = m^e \pmod n$ and send the ciphertext c to B.

Decryption: To recover the plaintext m from the ciphertext c, A should do the following.

$m = c^d \pmod n$.

Example [15]:

- Select p = 17 and q = 11.
- Compute n = pq = 187 and $\phi(n) = (p-1)(q-1) = 160$.
- Select e = 7 such that gcd (e, n) = 1.
- Find d such that $ed \equiv 1 \pmod{\phi(n)}$. The correct value of d = 23.
- Public key is (n, e) = (187, 7) and private key is (n, d) = (187, 23).

In order to encrypt a message m = 88, using the above steps the corresponding ciphertext $c = 88^7 \pmod{187} = 40867559636992 \pmod{187} = 11$.

To decrypt the ciphertext c, we need to calculate m as $m = 11^{23} \pmod{187} = 8954902432552372246531 \pmod{187} = 88$.

4. Building Blocks Of The Propsed Scheme

In this section we present some mathematical preliminaries related to our proposed Rebalanced Elatrash RSA Public-Key Cryptosystem. The proposed scheme uses a general linear group, the group of non-singular matrices, of square matrices of order k with entries taken form the ring Z_n, where n is a product of two large primes as in the case of classical RSA.

Consider the multiplicative group G of non-singular matrices of order k over Z_n. In general the calculation of the order of G is complicated. However, we calculate the order of G using the following theorem.

Theorem [5]: If n = pq be the product of two primes p and q, and the general linear group $G = GL(k, Z_n)$ of k×k matrices over Z_n. Then the order of the group G is

$$|G| = (p^k-1)(p^k-p)\ldots(p^k-p^{k-1})(q^k-1)(q^k-q)\ldots(q^k-q^{k-1}).$$

Proof: Every matrix $m \in G$ reduced to be two matrices m_p and m_q, where m_p and m_q are matrices over Z_p and Z_q respectively; also $m_p = m \pmod p$ and $m_q = m \pmod q$. Since m is non-singular iff both m_p and m_q are non-singular. In fact, the mapping

$\theta : GL(k, pq) \to GL(k, p) \otimes GL(k, q)$, is

is omorphism of two rings, because θ is both additive and multiplicative homomorphism, one-to-one follows from CRT and also onto. Hence the order of the GL (K, pq) is same as the order of $GL(k, p) \otimes GL(k, q)$. But the order of $GL(k,p) = (p^k-1)(p^k-p)\ldots(p^k-p^{k-1})$ and $GL(k,q) = (q^k-1)(q^k-q)\ldots(q^k-q^{k-1})$. Hence $|G| = (p^k-1)(p^k-p)\ldots(p^k-p^{k-1})(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})$.

5. Proposed Scheme

(Rebalanced Elatrash RSA Public-key Cryptosystem)

In this section we propose a variant of Elatrash RSA scheme,called Rebalanced Elatrash RSA Public-Key Cryptosystem, which employs a general linear group GL (k, Z_n). In this scheme the plaintext and ciphertext messages are k×k matrices with parameters in Z_n. The

proposed scheme consists of the following three algorithms. We suppose that the entity A wants to send a message m to entity B.

Key generation algorithm:

- Entity B generates two distinct large primes p, q and computes n = pq, $\phi(n)$= (p-1)(q-1).
- Choose d_p, d_q such that gcd (d_p, p-1) = 1, gcd (d_q, q-1) = 1 and $d_p = d_q \pmod 2$.
- Find d such that $d=d_p \pmod{p-1}$, $d = d_q \pmod{q-1}$.
- Compute an integer e such that $e \equiv 1 \pmod{|G|}$, where G = GL (k, Z_n).
- Entity B publishes his public key (n, k, e) and keeps private key (n, k, d, d_p, d_q) as secret.

Encryption Algorithm: In order to encrypt a message m for B; A should do the following.

- Obtain B's public key (n, k, e).
- Represent the message m as a k×k non-singular matrix.
- Compute the ciphertext C as a k×k non-singular matrix as $C = m^e \pmod n$.
- Send the ciphertext C to B.

Decryption Algorithm: In order to decrypt the ciphertext matrix C received from A; B should do the following.

- Compute $m_p = C^{dp} \pmod{dp}$ & $m_q = C^{dq} \pmod{dq}$.
- Use CRT [9] to compute $m \in GL(k, Z_n)$ such that $m=m_p \pmod{dp}$ and $m=m_q \pmod{dq}$. Note that $m=C^d \pmod n$. Hence the resulting is a proper decryption of the ciphertext C.

Example

Key generation: Select two primes p = 5, q = 7 such that gcd of (p-1, q-1) = 2.

Find n=pq = 35. Choose dp = 3, dq = 5 such that $d = 3 \pmod 4$, $d = 5 \pmod 6$. Apply CRT to find d. Here the correct value of d = 11.

Compute = $(p^2-1)(p^2-p)(q^2-1)(q^2-q) = 967680$. Find an integer e such that $ed \equiv 1 \pmod{}$, where G = GL (2, Z_{35}); the correct value of e = 87971.

Public key (n, k, e) = (35, 2, 87971) and private key (n, k, d,d_p,d_q) = (35, 2, 11,3,5).

Encryption: Take the plaintext as

$$m = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \in GL(2, Z_{35}).$$

Then the ciphertext for m is $C = m^e \pmod n$ =

$$\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}^{87971} \pmod{35} = \begin{pmatrix} 0 & 1 \\ 18 & 17 \end{pmatrix}.$$

Decryption: To recover the plaintext, first compute

$$m_p = C^{dp} = \begin{pmatrix} 0 & 1 \\ 18 & 17 \end{pmatrix}^3 \bmod 5 = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \text{and}$$

$$m_q = C^{dq} = \begin{pmatrix} 0 & 1 \\ 18 & 17 \end{pmatrix}^5 \bmod 7 = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$ Apply CRT to recover the plaintext as $m = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$.

Advantages of the proposed scheme:

1. The key space of the proposed scheme is large when compared to classical RSA.
2. The hardness of factorization of n remains the same as in RSA.
3. We have used a k×k matrix m instead of an integer as in the RSA, this is not a disadvantage. Infact, it is an advantage, since the RSA is a block cipher. We take k^2 blocks and set them in a matrix and calculate whatever needed, so it is more complex than one block to one block cipher.
4. Digital signature can be embedded in the matrix as an entry. So our scheme supports digital signature scheme.
5. For k = 1, our scheme reduces to the rebalanced RSA scheme [13].
6. Our scheme can also be used with a sub group of G not only the full group G.

7. With our scheme, we perform the fast decryption when compared to Elatrash RSA scheme.

6. Conclusions

In this paper, we proposed an RSA type public-key cryptosystem, called Rebalanced Elatrash RSA, which is an extension of Elatrash RSA public-key encryption scheme. In our scheme, the original and encrypted messages are in GL (k, Z_n), i.e., k×k non-singular matrices with values in Z_n. The security of the proposed scheme is based on the intractability of Integer Factorization Problem. In our scheme, we can encrypt or decrypt k^2 blocks at a time. We use Chinese Remainder Theorem (CRT) to calculate m from m_p and m_q. This is approximately four times as fast as evaluating $C^d \bmod n$ directly [6, p. 613]. So, the decryption process in our proposed Rebalanced Elatrash RSA scheme is approximately four times faster than the decryption in Elatrash RSA scheme. This behavior i.e. fast decryption is particularly useful in some applications as discussed in Section 2.

References

[1] Collins.T, Hopkins.D, Langford.S and Sabin.M, *"Public Key Cryptographic Apparatus and Method"*, US Patent #5,848,159. Jan. 1997.

[2] Diffie.W and Hellman.M, *"New Direction in Cryptography"*, IEEE Transactions on Information Theory, Vol.22, PP. 644-654, 1976.

[3] Fiat. A, *"Batch RSA"*, In G. Brassard, ed., Proceedings of CRYPTO- 1989, Vol. 435, LNCS, PP. 175–185. Springer-Verlag, Aug. 1989.

[4] Fayik Ramadan EL-Naowk, *"A Generalization of the RSA Elatrash Scheme"*, Journal of Applied Sciences, 7(13): 1824-1826, 2007.

[5] Gabe Cunningham. The General Linear Group. See: www-math.**mit.edu**/~dav/genlin.pdf.

[6] Menezes.A, Van Oorschot. P and Vanstone.S. *"Handbook of Applied Cryptography"*, CRC Press, 1997.

[7] Okamoto. T and Uchiyama. S, *"A New Public Key Cryptosystem as Secure as Factoring"*, in Proceedings of EUROCRYPT-98, LNCS 1403, Springer- Verlag, PP. 308-318, 1998.

[8] Pointcheval.D, *"New Public Key Cryptosystem Based On the Dependent-RSA Problem"*, in proceedings of EUROCRYPT - 99, LNCS 1592, Springer-Verlag, PP.239 -54,1999.

[9] Quisquater J. J. and Couvreur. C, *"Fast decipherment algorithm for RSA public key cryptosystem,"* Electronic Letters, Vol. 18, PP.905-907, 1982.

[10] Rabin.M, *"Digitalized Signature Scheme and Public key Functions as intractable as factorization"*, Technical Report, MIT/LCS-TR, MIT Lab, Computer Science, Cambridge, Jan 1979.

[11] Rivest .R, Shamir.A and Adleman.L, *"A Method for obtaining Digital Signatures and Public key Cryptosystem"*, Communication of the ACM, Vol. 1, No. 2, PP.120-126, 1978.

[12] Shimada. M, *"Another Practical Public Key Cryptosystem"*, Electronic Letters, 5th November, Vol.28, No.23, 1992.

[13] Takagi.T, *"Fast RSA-type Cryptosystem Modulo $p^k q$."*, In H. Krawczyk, ed., Proceedings of CRYPRO-1998, Vol. 1462 of LNCS, PP. 318–326. Springer-Verlag, Aug. 1998.

[14] Wiener. M, *"Cryptanalysis of Short RSA Secret Exponents"*, IEEE Trans. Information Theory , 36(3):553–558. May 1990.

[15] William. S, *"Cryptography and Network Security"*, Person Education, Inc. 2003.

Author's Biography

Dr. P. Vasudeva Reddy received M.Sc (Mathematics), PhD (Cryptography) from S.V. University, Tirupati, India. He is currently working as an Associate professor in the department of Engineering Mathematics, College of Engineering, Andhra University, Visakhapatnam, India. His field of interests includes Algebra & Number theory Applications, secret sharing, and Cryptography.

Dr. B. Muniswamy received M. Sc,Ph.D (Statistics) from S.V. University, Tirupati, India. He is currently working as an associate professor in the department of Statistics, Andhra University, Visakhapatnam, India. His fields of interests include Statistical computing and Econometrics.

B.Umaprasada Rao received M. Sc in mathematics from Andhra University. He is working as research scholar in the department of Engineering Mathematics, Andhra University, A.P. India. His field of research is cryptography.

K. Venkata Rao received degree in Computer Science & Engineering from Andhra University and holds M. Tech in Computer Science & Technology from Andhra University. At present, he is working as an Associate professor in the dept. of Computer Science & Systems Engineering. Also he is WEB MASTER and in charge of online examinations of Andhra University. He has 13 years of teaching and two years of industrial experience. He conducted four National level conferences. His research interests include Image processing, Web Technology and Security.

T. Gowri received B.Tech from Nagarjuna University and M. Tech from Jawaharlal Nehru Technological University. She is currently working as an Associate professor in the department of Electronics and Communication Engineering, AudiSankara College of Engineering and Technology, Gudur, A.P, India. Her research interests include Digital systems and computer electronics, Digital Image Processing, Wireless Communications and Information Security.