Malaya Journal of Matematik, Vol. 8, No. 3, 1138-1141, 2020

https://doi.org/10.26637/MJM0803/0069

On an efficient RSA public key encryption scheme

S.C. Gupta [1] and Manju Sanghi[2*]

Abstract

RSA is the most widely used public key scheme for secure communication. Aboud et.al [1], proposed an improved version of original RSA scheme. They generalized it so that it can be implemented in the general linear group on the ring of integers mod n. In the proposed scheme the original message and the encrypted message are $h \times h$ square matrices with entries in Z_n as against the original RSA scheme which involves integer values. However, we identified a shortcoming of that scheme and proposed a new and efficient RSA public key encryption scheme. We also propose a digital signature scheme based on the new scheme.

Keywords

Public key cryptosystem, RSA, General linear group, Digital signatures.

AMS Subject Classification

94A60.

[1] *Department of Applied Mathematics, Central Institute of Plastics Engineering & Technology, Raipur-492003, Chhattisgarh India.*
[2] *Department of Applied Mathematics, Rungta College of Engineering and Technology, Bhilai-490024, Chhattisgarh, India.*

[*]**Corresponding author**:manjusanghi13@gmail.com
Article History: Received **10** February **2020**; Accepted **18** June **2020**

Contents

1. Introduction

Advancement of technology has increased the communication of data and other information over the internet. These advancements have led to the consequences of security of data, speed of transfer and storage space. Cryptography plays an important role in overcoming these consequences [8]. The fundamental objective of cryptography is to enable two persons to communicate securely over an insecure channel. In 1976, Diffie and Hellman [2] brought the revolutionary concept of public key cryptosystem in the field of cryptography. RSA, is the first and the most widely used public key system which was introduced by Rivest, Shamir and Adleman [5]. The security of RSA is based on the difficulty of factorization of integer modulus which is the product of two large and distinct prime numbers, which is an intractable mathematical problem. Several variants of RSA [3, 4, 6, 7] have been proposed by various researchers to strengthen the security, increase the speed of transfer and overcome the problem of storage space.

Recently, Aboud et al., [1] gave an improved version of the original RSA scheme by using matrix in place of integers. In their proposed scheme the original message and the encrypted message are represented as h x h square matrices (as claimed) with entries in Z_n indicated via (h,Z_n). They generalized the RSA scheme in order to be implemented in the general linear group on the ring of integers mod n and claimed to be efficient, scalable and flexible. However, we demonstrate a short coming of the scheme. Further, we suggest a new scheme to overcome the shortcomings. We also propose a new digital signature based on the new scheme.

The rest of the paper is organized as follows. In Section 2 we present the efficient RSA public key encryption scheme as given by Abound et al. In Section 3 we highlight the shortcomings of the scheme by an example. Proposed new scheme and proposed digital signature are discussed in Sections 4 and 5. Finally, the paper is concluded in Section 6.

2. Efficient RSA public key encryption scheme

This scheme was given by Aboud et al., [1] in which the original message and the encrypted message are hxh square matrices with entries in Z_n as against the integer entries in the original RSA scheme.

Key generation

To generate the keys each User A and B performs the following operations.
1. Randomly chooses 2 large prime numbers p and q.
2. Compute the modulus n = p.q
3. Compute g = (h, Z_n) where g is calculated using

$$g = (p^h - 1)(p^h - p)(p^h - p^{h-1}) + \dots$$
$$+(q^h - 1)(q^h - q)(q^h - q^{h-1})..$$

4. Choose a random integer e where gcd $(e, g) = 1$.
5. Compute the inverse d where e.d $\cong$ 1 mod g.

Public and Private key pairs are therefore (n, e) and (g, d).

Encryption

To encrypt the message User B performs the following steps.
1. Obtain A's public key (n, e).
2. Represent the message M as a $h \times h$ matrix.
3. Compute the cipher text C = M^e mod n.

Decryption

1. To recover the message from cipher text, User A computes M = C^d mod n.

Example 1

Key generation

P = 43, q = 47, n = p.q = 2021
g = (432-1) (432- 43) + (472-1) (472-47) = 8111184
e = 17 since gcd (17, 8111184) = 1
d = 954257 since 17 x 954257 $\cong$ 1 mod 8111184
public key pair is (2021, 17)
private key pair is (8111184, 954257)

Encryption

Here message is taken as an integer M = 741
C = M^e mod n = 74117 mod 2021 = 1471

Decryption

M = C^d mod n = 1471954257 mod 2021 = 741

3. Shortcomings of the scheme

As claimed, if the message is represented as a $h \times h$ matrix, the scheme fails.

A simple example in support of our comments

Example 2

Suppose the message M = 741 is represented as a 2×2 matrix in the form M= $\begin{bmatrix} 7 & 4 \\ 0 & 1 \end{bmatrix}$, the rest of the values being the same we have,
$p = 43, q = 47, n = p.q = 2021$.

$$g = (p^2 - 1)(p^2 - p) + (q^2 - 1)(q^2 - q)$$
$$= (432 - 1)(432 - 43) + (472 - 1)(472 - 47) = 8111184.$$

e = 17, since gcd $(17, 8111184) = 1$.
d = 954257, since 17 x 954257$\cong$ 1 mod 8111184.

Encrypted message

$$C = M^e mod\, n = \begin{bmatrix} 7 & 4 \\ 0 & 1 \end{bmatrix}^{17} mod\, 2021 = \begin{bmatrix} 1 & 1647 \\ 917 & 1666 \end{bmatrix}$$

Decrypted message

$$= C^d mod\, n = \begin{bmatrix} 1 & 1647 \\ 917 & 1666 \end{bmatrix}^{954257} mod\, 2021 = \begin{bmatrix} 1673 & 1544 \\ 386 & 992 \end{bmatrix}$$

which is not the same as the original matrix M.

The method applies if the message is represented in the form of an integer but fails if it is represented as a matrix.

4. Proposed Scheme

In this Section we propose a new and efficient RSA public key encryption scheme. In the proposed scheme the plain text message M is represented as a $h \times h$ matrix such that the determinant of the matrix is relatively prime to modulus n = p.q. The exponentiation modulus is computed by using the formula N =$(p^h - 1)(q^h - 1)$ which is similar to $\phi(n)$ in the original RSA.

Key generation

To generate the keys User A performs the following operations.
1. Randomly chooses 2 large distinct prime numbers p and q and compute the modulus n = p.q.
2. Compute the exponentiation modulus N =$(p^h - 1)(q^h - 1)$
3. Choose a random integer e where gcd $(e, N) = 1$.
4. Compute inverse d such that e.d $\cong$ 1 mod N.

Public and Private key pairs are therefore (n, e) and (N, d).

Encryption

To encrypt the message User B performs the following steps.
1. Obtain A's public key (n, e).
2. Represent the message in the form of a hxh matrix with all the entries under modulo n such that the determinant of M is relatively prime to n. i.e gcd $(|M|, n) = 1$
3. Using public key compute the cipher text C = M^e mod n.

Decryption
To recover the message from cipher text User A uses private key and computes M = C^d mod n.

Example 3
Let the message be represented in the form of a 2 x 2 matrix as M = $\begin{bmatrix} 7 & 4 \\ 0 & 1 \end{bmatrix}$

Key generation
Let p = 43, q = 47, n = p.q = 2021
$|M|$ = -4, Also, gcd (-4, 2021) = 1

N = $(p^2-1)(q^2-1)$ = (432-1) (472-1) = 4080384
e = 17 since gcd (17, 4080384) = 1.
d = e^{-1} mod N = 1200113, since (17).(1200113) ≅ 1 mod 4080384.

Public key pair is (n, e) = (2021, 17).
Private key pair is (N, d) = (4080384, 1200113). **Encryption**

Message is encrypted using the public key as

$$C = M^e mod\, n = \begin{bmatrix} 7 & 4 \\ 0 & 1 \end{bmatrix}^{17} mod\, 2021 = \begin{bmatrix} 1 & 1647 \\ 917 & 1666 \end{bmatrix}$$

Decryption

Private key is used to recover the message from cipher text.

$$C^d mod\, n = \begin{bmatrix} 1 & 1647 \\ 917 & 1666 \end{bmatrix}^{1200113} mod\, 2021 = \begin{bmatrix} 7 & 4 \\ 0 & 1 \end{bmatrix} = \text{M}$$

It can be easily seen that the decrypted message is same as the original message M.

5. Proposed Digital signature scheme based on matrices

In this section, we propose a new variant of RSA digital signature scheme based on matrices. We represent the initial plain text message in the form of a square matrix of order $h \times h$ and select the modulus n such that the determinant of the matrix is relatively prime to n. Also, the exponentiation modulus is calculated by using the relation $N = (p^h - 1)(q^h - 1)$ which is similar to $\phi(n)$ in the original RSA scheme and is used for generating public and private keys. Private key is used to sign the message and public key is used to verify it.

The scheme involves the following steps:
Key generation

1. Randomly select two large primes p, q which are nearly equal and compute the modulus n = p.q.
2. Compute $N = (p^h - 1)(q^h - 1)$ which gives the number of matrices that are relatively prime to n.
3. Select random integer e, $1 < e < N$ such that e and N are relatively prime ie. gcd(e, N) =1.
4. Compute $d = e^{-1} mod N$ where $1 < d < N$ and ed≅ 1 mod N.
5. Public and private keys are now e and d respectively.

Signature generation

1. Represent the message M in the form of a square matrix of order h x h with all the entries under mod n where n = pq and the determinant of M is relatively prime to n, gcd $(|M|, n)$ = 1.
2. Using private key compute the Signature S = $M^d mod n$.

Signature Verification

1. Using public key, verify V = $S^e mod n$ = M mod n.

Example 4.
Suppose the Signer wants to digitally sign the message " SKY IS BLUE" . He represents it in the form of a square matrix of order suppose 3 x 3. Assigning each letter with its position in the alphabets as A = 1, B = 2 and so on, we get M = $\begin{bmatrix} 19 & 11 & 25 \\ 9 & 19 & 2 \\ 12 & 21 & 5 \end{bmatrix}$
Let p = 7, q = 11, n = pq = 77
$|M|$ = -199 and gcd (199, 77) = 1
N = $(p^3-1)(q^3-1)$ = (73 -1) (113 -1) = 454860
e = 17 since gcd (17, 454860) = 1
d = $17^{-1} mod 454860$ = 53513.
Public and Private keys are therefore e = 17 and d = 53513.
Signature is computed by using the private key 'd' as

$$\text{S} = M^d mod n = \begin{bmatrix} 19 & 11 & 25 \\ 9 & 19 & 2 \\ 12 & 21 & 5 \end{bmatrix}^{53513} mod\, 77 = \begin{bmatrix} 69 & 22 & 5 \\ 37 & 32 & 9 \\ 31 & 24 & 9 \end{bmatrix}$$

Signature is verified by using the public key 'e'

$$\text{Verification V} = S^e \text{mod n} = \begin{bmatrix} 69 & 22 & 5 \\ 37 & 32 & 9 \\ 31 & 24 & 9 \end{bmatrix}$$

$$\text{mod } 77 = \begin{bmatrix} 19 & 11 & 25 \\ 9 & 19 & 2 \\ 12 & 21 & 5 \end{bmatrix} = \text{M mod n}$$

6. Conclusion

In this paper we highlight the short comings of an efficient RSA public key encryption scheme proposed by Aboud et al. [1] by an example. We also propose a new and efficient RSA public key encryption scheme. In the proposed scheme the original message is represented as a $h \times h$ matrix such that the determinant of the matrix is relatively prime to modulus n. The exponentiation modulus is computed by using the formula N $=(p^h-1)(q^h-1)$ which is similar to $\phi(n)$ in the original RSA. A new variant of RSA digital signature scheme based on matrices is also proposed.

References

[1] S. J. Aboud, M.A. Al-Fayoumi, M. Al-Fayoumi and H.S. Jabber, An Efficient RSA Public Key Encryption Scheme, *Fifth International Conference on Information Technology: New Generations*, (2008), 127–130.

[2] W. Diffie and M. Hellman, New Direction in Cryptography, *IEEE Transaction on Information Theory*, 22(6)(1976), 644–654.

[3] T. Okamoto and S. Uchiyama, A New Public Key Cryptosystem as Secure as Factoring, *In Proceedings of Europcrypt'98, LNCS 1403*, (1998), 308–318.

[4] D. Pointcheval, New Public Key Cryptosystem Based on the Dependent-RSA Problem, *In proceedings of Euorcrypt'99, LNCS 1592*, (1999), 239–254.

[5] R. Rivest, A. Shamir and L. Adelman, A Method for Obtaining Digital Signature and Public Key Cryptosystems, *Communications of the ACM*, 21 (1978), 120–126.

[6] N. Rakesh and P. Jayaram, NTRU Digital signature scheme-A matrix approach, *International Journal of Advanced Research in Computer Science*, 2(1)(2011), 1–10.

[7] P. Sahadeo, On DRSA Public Key Cryptosystem, *The International Arab Journal of Information Technology*, 3(4)(2006), 334–336.

[8] B. Schneier, *Applied Cryptography*, John Wiley & Sons, 1996.

⋆⋆⋆⋆⋆⋆⋆⋆⋆

ISSN(P):2319 – 3786

Malaya Journal of Matematik

ISSN(O):2321 – 5666

⋆⋆⋆⋆⋆⋆⋆⋆⋆