International Journal on Emerging Technologies **12**(1): 76-79(2021)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Matrix Modification of RSA Public Key Cryptosystem and its Variant

S.C. Gupta[1] and Manju Sanghi[2]
[1]Assistant Professor, Department of Mathematics,
Central Institute of Plastics Engineering & Technology, Raipur, Chhattisgarh, India.
[2]Professor, Department of Mathematics,
Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India.

(Corresponding author: Manju Sanghi)
(Received 09 September 2020, Revised 22 December 2020, Accepted 19 January 2021)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: RSA cryptosystem is one of the most practical public key cryptosystems. 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. The size of the modulus is atleast 1024 bits currently which needs to be increased with the development of factoring technology. However, with the increase in size their arises the problem of minimising the storage space and increasing the speed of transfer. In this paper, modification of RSA public key cryptosystem using square matrices of order h x h is proposed. Also, a variant of RSA using modulus of the form p^rq is proposed along with its matrix modification.

Keywords: Public key cryptosystem, RSA General Linear group

I. INTRODUCTION

The most striking development in the history of Cryptography came in 1976 when whitfield Diffie and Martin Hellman [1] introduced the revolutionary concept of public key cryptosystem that facilitates secure communication over an insecure channel. These Public key cryptosystems are based on encryption/decryption of data using keys whose security lies on the difficulty of hard mathematical problems which are intractable in polynomial time. The security of public key cryptosystem by Diffie and Hellman relies on the difficulty of discrete logarithms. Since then many PKC's have been proposed and have become more and more important in modern communication systems. These PKC's ensure confidentiality and authentication of transferred data and messages.

In 1978, Rivest, Shamir and Adleman discovered the first practical and most widely usedpubic key cryptosystem RSA [2]. The security of RSA is based on the difficulty of factorization of integer modulus 'n' which is the product of two large and distinct prime numbers, which is an intractable mathematical problem. According to the current technology the minimum size of modulus required for secure communications is atleast 1024 bits [3] which needs to be increased with the development of new technologies for factoring of large integers. However, with the increase in size the required time and storage to implement the RSA cryptosystem will be a big hurdle which needs to overcome.

One of the reasons of RSA being the most popular cryptosystem is that it does not require any complex calculations. RSA requires only one modular exponentiation for both encryption and decryption of data. Several variants have been proposed to increase the efficiency of the implementation of RSA cryptosystem through various approaches. One of the approaches is to vary the modulus of the RSA cryptosystem. The most general form of modulus n is

$$n = p_1^{e_1} p_2^{e_2} \ldots\ldots p_m^{e_m}, \quad e_i \geq 1 \quad 1 \leq i \leq m$$

where p_i 's are all distinct prime numbers of nearly the same size. Takagi proposed the RSA cryptosystem using modulus of the form $n = p^rq$ for $r \geq 2$ [4]. The encryption process of Takagi's system is the same as RSA but for decryption he used the method of p-adic expansion [5] to achieve speedy decryption. Lim et al. gave a generalised form of Takagi's cryptosystem [6] with modulus of the form p^rq^s with r,s being relatively prime positive integers. For encryption they used the same process as RSA multi prime technology and Takagi's system but for decryption they applied p-adic expansion to the factor p^r and q-adic expansion to the factor q^s in Takagi's scheme.

The main limitation of RSA cryptosystem is that it cannot be applied if the size of the plain text message is greater than the modulus n. In such a case the message is broken into different blocks m_1, m_2,....m_i such that the size of each block m_i is smaller than n. Each block m_i is then encrypted/decrypted separately using RSA as a result of which the time complexity as well as the storage space for RSA cryptosystem increases. This problem can be resolved if the plain text message (after converting into integers) is represented in the form of a matrix [8, 9, 10, 11]. Motivated by this, matrix modifications for RSA cryptosystem and its variant using different modulus as suggested by Takagi is proposed in this paper.

The rest of the paper is organised as follows. In Section II we describe the RSA cryptosystem along with an example. In Section III we demonstrate the matrix modification of RSA cryptosystem. Section IV covers the variant of RSA cryptosystem with modulus of the form p^rq and its matrix modification. Finally the paper is concluded in Section V.

II. THE RSA CRYPTOSYSTEM

RSA public key cryptosystem is used for sending and receiving of secret messages. It uses 2 different keys, public key for encryption of messages and private(secret) key for decryption. It involves the following 3 algorithms for key generation, encryption and decryption.

Key Generation

To generate the keys both Sender and Receiver perform the following operations.

1. Generate 2 large random prime numbers p and q of nearly the same size.
2. Compute the modulus n = p.q and Euler's totient function $\varphi(n)$ = (p-1) (q-1).
3. Select a random integer e where 1 < e < $\varphi(n)$ such that gcd (e, $\varphi(n)$) = 1
4. Compute integer d, 1 < d < $\varphi(n)$ using the extended Euclidean algorithm such that ed ≡ 1 mod $\varphi(n)$.
5. Public and private keys are therefore (n,e) and (p, q, d) respectively.

Encryption

To encrypt the message, Sender performs the following steps.

1. Obtain Receiver's public key (n, e)
2. Represent the plain text message as a positive integer M such that size of M ≤ n, else break M into different blocks m_1, m_2,....$m_i$such that the size of each block m_i ≤ n.
3. Compute the cipher text C = M^e mod n.

Decryption

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

Example 1:

Key generation

Let p = 43, q = 47 be 2 random primes.
Computing the modulus n = p.q = 43.47 = 2021
Euler's function $\varphi(n)$ = (p-1) (q-1) = (43-1) (47-1) = 1932
Since gcd (17, 1932) = 1 and 1 < 17 < 1932, public key e = 17.
Also since 17. 341 ≡ 1 mod 1932, private key d = 341.
Public and private keys are therefore (2021, 17) and (43, 47, 341) respectively.

Encryption

Let the plain text message be represented in the form of an integer as

M = 741 < n (= 2021).

Ciphertext is computed as

C = M^e mod n = 741^{17} mod 2021 = 1471

Decryption

Plaintext is recovered from the cipher text by using the decryption algorithm

C^d mod n = 1471^{341} mod 2021 = 741 = M

III. MATRIX MODIFICATION

We propose modification to the RSA cryptosystem by representing the plain text message as a h x h matrix. This modification still utilises the modulus as n = p.q, p, q being different primes but replaces the blocks of the plain text message as a h x h matrix. Instead of relying on the Euler's function $\varphi(n)$ = (p-1) (q-1) it relies on the exponentiation modulus N = (p^h-1) (q^h -1) which is obtained by using the concept of general linear groups of order h [12].

Definition.

Let F be a field. Then the general linear group $Gl_n(F)$ is the group of invertible n x n matrices with entries in F under matrix multiplication.

Aboud *et al.* proposed this method for all square matrices using the exponentiation modulus g = (p^h -1) (p^h –p) .....(p^h –p^{h-1}) + (q^h -1) (q^h –q) .....(q^h –q^{h-1}) where g is the general linear group of h x h matrices over Z_n the ring of integers mod n. However we find that their method is error prone and does not work out if the message is represented as a matrix may be of any order [7].

Andrew Pangia in their unpublished paper proposed the method by modifying the exponentiation modulus as g = (p^h -1) (p^h –p) .....(p^h –p^{h-1}).(q^h -1) (q^h –q) .....(q^h –q^{h-1})by using the product of the orders of the general linear groups of degree h over Z_p and Z_q instead of sum as proposed in [7]. They found that the method is effective and works for all the messages represented as a 2 x 2 matrix except for a plain text matrix whose determinant is zero modulo n and the sum of the cross elements is a multiple of one of the factors of n.

Motivated by this we propose the method by using the exponentiation modulus as

N = (p^h-1) (q^h -1) where h represents the order of the matrix, p and q being primes and modulus n = p.q. The method is effective for all plain text messages M represented in the form of a h x h matrix and whose determinant is relatively prime to modulus n.

Following steps are involved for encryption and decryption of messages by the proposed method.

Key generation

1. Randomly choose 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) where h represents the order of the matrix.
3. Choose a random integer e , 1 < e < N such that gcd (e, N) = 1
4. Compute inverse d, 1 < d < N such that e.d ≡ 1 mod N.
5. Public and Private key pairs are therefore (n, e) and (N, d) respectively.

Encryption

To encrypt the message, Sender performs the following steps.

1. Obtain Receiver's public key (n, e)
2. Represent the message in the form of a h x h matrix with all the entries under modulo n such that the determinant of M is relatively prime to n. i.egcd (|M|, n) =1
3. Using the public key computes the cipher text C = M^e mod n.

Decryption

To recover the message from cipher text, Receiver uses private key and computes $M = C^d$ mod n.

Example 2:

Suppose the Sender wishes to send the message "CRYPTOGRAPHY" to the Receiver.
Representing the message in the form of an integer, assigning each letter with its position in the English alphabets as A = 01, B= 02 and so onwe get the plaintext message
M = 031825162015071801160825.
Taking random primes p =503 q = 499
Computing n = p.q = 503.499 = 250997
As the size of M > n we break the message M into sub messages as
m_1= 031825, m_2 =162015, m_3 = 071801 and m_4 = 160825 such that each m_i< n , i = 1, 2..4.
Use of general RSA cryptosystem results in encrypting and decrypting each sub message separately which definetly increases the time as well as the space complexity.
By the proposed method representing the message in the form of a 2 x 2 matrix we get

$$M = \begin{bmatrix} 31825 & 162015 \\ 71801 & 160825 \end{bmatrix}$$

Also, |M| = -6514583390, gcd(6514583390, 250997) =1 ie. |M| and n are relatively prime.
Computing the exponentiation modulus Nsimilar to Euler's function in RSA, we get
N = $(p^h-1)(q^h-1)$ = $(503^2-1)(499^2-1)$ = 62998992000
Finding integer e, 1 < e < N,gcd (e, N) = 1, we take e = 241
Also, 1< d < N and e.d ≡ 1 mod N gives d = 34244265361
To send the message, Sender computes the cipher text using
$C = M^e \bmod n$ =

$$\begin{bmatrix} 31825 & 162015 \\ 71801 & 160825 \end{bmatrix}^{241} \bmod 250997$$

$$= \begin{bmatrix} 153377 & 104497 \\ 76449 & 55902 \end{bmatrix}$$

Receiver recovers the message using C^d mod n

$$= \begin{bmatrix} 153377 & 104497 \\ 76449 & 55902 \end{bmatrix}^{3424426536\,1} \bmod 250997$$

$$= \begin{bmatrix} 31825 & 162015 \\ 71801 & 160825 \end{bmatrix} = M$$

which is same as the plaintext message M.
We have given an example taking a 2 x 2 matrix. However, it can be expanded to higher order matrices also.
As claimed by Andrew Pangia let us suppose take the plain text message as a matrix whose sum of the cross elements is a multiple of one of the factors of n.

Suppose $M = \begin{bmatrix} 251 & 200 \\ 303 & 252 \end{bmatrix}$ such that 251 + 252 = 200 + 303 = 503 = p where n = p.q
Taking the same values as above
P = 503, q = 499 n = p.q = 250997
Public key e = 241, private key d = 34244265361
But in this case |M| =2652 ≠ 0, so gcd (|M| , n) = 1
Hence by our proposed method
Cipher text $C = M^e \bmod n$ =

$$\begin{bmatrix} 251 & 200 \\ 303 & 252 \end{bmatrix}^{241} \bmod 250997 =$$

$$\begin{bmatrix} 60102 & 115272 \\ 13999 & 90798 \end{bmatrix}$$

However, on decrypting
$C^d \bmod n$ =

$$\begin{bmatrix} 60102 & 115272 \\ 13999 & 90798 \end{bmatrix}^{3424426536\,1} \bmod 250997 =$$

$$\begin{bmatrix} 251 & 200 \\ 303 & 252 \end{bmatrix}$$

which is same as the plain text message M .
Hence, proposed method can be applied to all messages represented as a square matrix with the determinant of the matrix being relatively prime to the modulus n.

IV. VARIANT OF RSA USING MODULUS OF THE FORMp^rq AND IT'S MATRIX MODIFICATION

In this section we describe the RSA cryptosystem modulus p^rq and demonstrate its matrix modification. In [4] Takagi proposed the system using the same method for encryption as in RSA but for decryption he used the method of p-adic expansion. We modify it by using the same method as in RSA for both encryption and decryption and give its matrix modification along with an example.

Algorithm

Key generation

1. Generate 2 random primes p, q and compute n = $p^r.q$, r≥ 2
2. Compute Euler's function $\varphi(n) = p(p-1)(q-1)$
3. Select integer e, 1 < e < $\varphi(n)$ such that gcd (e, $\varphi(n)$) = 1
4. Compute d such that e.d ≡ 1 mod $\varphi(n)$

Encryption

Cipher text is computed by using $C = M^e \bmod n$

Decryption

The message is recovered by using $M = C^d \bmod n$.

Matrix modification

The plain text message M is represented as a h x h matrix with all the entries under modulo n= p^rq, p, q being random primes such that the determinant of M is relatively prime to n. Computing the exponentiation

modulus using $N = p^h(p^h-1)(q^h-1)$, selecting integer e such that gcd (e, N) =1 and finding d such that $e.d \equiv 1 \bmod N$. Cipher text is computed using $C = M^e \bmod n$ and the message is recovered by $M = C^d \bmod n$.

Example 3:

Suppose the sender wants to send the message "SOLUTION" to the Receiver.

Representing the message in the form of an integer as in the above example, we get the plaintext message M = 1915122120091514.

Breaking it into sub messages as

m_1= 1915, m_2 = 1221, m_3 = 2009 and m_4 = 1514

such that each sub message is less than the modulus.

Representing it in the form of a 2 x 2 matrix we get M = $\begin{bmatrix} 1915 & 1221 \\ 2009 & 1514 \end{bmatrix}$

Generating random primes p= 43, q = 47

Computing modulus $n = p^2.q$ (taking r = 2), we get n = 86903

Also, |M| = 446321, and determinant of M is relatively prime to n ie. gcd(|M|, n) =1

Computing the exponentiation modulus $N = p^h (p^h-1) (q^h-1)$ = 7544630016.

Selecting public key e such that gcd (e, N) =1, we take e = 17

Finding d such that $e.d \equiv 1 \bmod N$ gives d = 1331405297

Cipher text is computed using $C = M^e \bmod n$

$$= \begin{bmatrix} 1915 & 1221 \\ 2009 & 1514 \end{bmatrix}^{17} \bmod 86903 = \begin{bmatrix} 11686 & 37609 \\ 60315 & 64316 \end{bmatrix}$$

Plain text message is recovered using

$C^d \bmod n =$

$$\begin{bmatrix} 11686 & 37609 \\ 60315 & 64316 \end{bmatrix}^{1331405297} \bmod 86903 = \begin{bmatrix} 1915 & 1221 \\ 2009 & 1514 \end{bmatrix} = M$$

V. CONCLUSION

In this paper we have proposed matrix modifications of RSA public key cryptosystem and variant of RSA using modulus of the form p^rq. Representation of a plain text message in the form of a square matrix of order h x h especially when the size of the message M > n (modulus), saves the time for encryption and minimises the storage space. Also, the use of exponentiation modulus in matrix notation which is vastly larger than $\phi(n)$ complicates the brute force attack.

FUTURE SCOPE

Modification of public key cryptosystems based on discrete logarithms using matrices.

Conflict of Interest: We do not have any conflict of interest.

REFERENCES

[1]. Diffie W. and Hellman, M. (1976). "New Direction inCryptography, *IEEE Transaction on Information Theory*, *IT-22*(6): 644-654.

[2]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

[3]. Lenstra, A. K., & Verheul, E. R. (2001). Selecting cryptographic key sizes. *Journal of cryptology*, *14*(4), 255-293.

[4]. Takagi, T. (1998, August). Fast RSA-type cryptosystem modulo p k q. In *Annual International Cryptology Conference* (pp. 318-326). Springer, Berlin, Heidelberg.

[5]. Takagi, T. (1997, August). Fast RSA-type cryptosystems using n-adic expansion. In *Annual International Cryptology Conference* (pp. 372-384). Springer, Berlin, Heidelberg.

[6]. Seongan Lim, Seungjoo Kim, IkkwonYie, and Hongsub Lee (2000). A GeneralizedTakagi-Cryptosystem with a Modulus of the Form p^rq^sINDOCRYPT 2000, LNCS 1977, pp. 283–294.

[7]. Aboud, S. J., AL-Fayoumi, M. A., Al-Fayoumi, M., & Jabbar, H. S. (2008, April). An efficient RSA public key encryption scheme. In *Fifth International Conference on Information Technology: New Generations (itng 2008)* (pp. 127-130). IEEE.

[8]. Alvarez, R., Martinez, F. M., Vicent, J. F., & Zamora, A. (2007). A new public key cryptosystem based on matrices. *WSEAS Information Security and Privacy*, *3639*.

[9]. Eftekhari, M. (2017, May). Cryptanalysis of some protocols using matrices over group rings. In *International Conference on Cryptology in Africa* (pp. 223-229). Springer, Cham.

[10]. Sweta Jain & Vineet Richhariya (2017). Kerberos based Enhanced Authentication Protocol for Cloud Computing Environment. *International Journal of Theoretical & Applied Sciences*, *9*(2), 25-30.

[11]. P.L. Sharma, S. Kumar &M. Rehan (2014). On Construction of Hadamard Codes UsingHadamard matrices, *International Journal of Theoretical & Applied Sciences, 6*(1), 102-113.

[10]. Darafsheh, M. R. (2005). Order of elements in the groups related to the general linear group. *Finite Fields and Their Applications*, *11*(4), 738-747.

How to cite this article: Gupta, S.C. and Sanghi, M. (2021). Matrix Modification of RSA Public Key Cryptosystem and its Variant. *International Journal on Emerging Technologies, 12*(1): 76–79.