American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
© Global Society of Scientific Research and Researchers
http://asrjetsjournal.org/

A New Modification of RSA Cryptosystem Based on The Number of The Private Keys

Hayder Raheem Hashim*

Department of Mathematics, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq
Email: Hayderr.almuswi@uokufa.edu.iq

Abstract

The need of the privacy for each person has encouraged cryptologists to create and modified cryptosystems. However, the RSA cryptosystem is a secure public key cryptosystem, this paper focuses on modifying RSA cryptosystem by increasing the number of private keys. This modification can be applied over plaintext messages, plain matrices, however in this paper, I focuse on applying it particulary on matrices which are the corresponding matrices of images. A public key and private key are contained in this secure cryptosystem, and the security of its private key depends on the integer factorization problem. But, this only private key might be found by inspection. Therefore, this new modification gives the RSA cryptosystem a higher security, because it suggests a "k" number of distinct private keys. Therefore, this new modification makes the RSA cryptosystem more secure and a confidential public key cryptosystem.

Keywords: Cryptography; public key cryptosystem; RSA cryptosystem.

1. Introduction

The area of Number Theory is one of the pure branches of mathematics that has many applications in information security such as cryptography. Since long eras, many uses of cryptography has occurred such as hiding messages and data that being sent between two different parties [10]. Traditionally, there are two well-known types of cryptography, which are symmetric cryptography and asymmetric cryptography. When the same key being used in the encryption and decryption procedures, this cryptosystem called symmetric cryptosystem [10]. However, in the asymmetric cryptosystem two different keys are used in these procedures; the public key should be announced to everyone and the corresponding private key has to be secret. There are many models of the symmetric and asymmetric cryptosystems [2].

----

* Corresponding author.

Substitution cipher , Hill Cipher, Caesar Cipher, Vigenere Cipher, Affine Cipher, block cipher are examples of the symmetric cryptography, whereas ElGamal, Diffie–Hellman key exchange, RSA, Rabin are associated with the latter cryptography. However, the security of RSA cryptosystem is relied on the prime factorization conjecture, a new modification of the RSA cryptosystem is presented in details in this article to give the RSA cryptosystem a higher security [1].

2. Literature Review

The RSA cryptosystem is the first public key cryptosystem for performing encryption and decryption of data, which was invented in 1977 by Ron Rivest, Adi Shamir, and Len Adleman. The authors in [1] proposed a very simple modification using some mathematical logic and two public key pairs rather than transmitting the value of the public key directly. In [2], the author suggested a modification of the RSA cryptosystem based on changing the value of n=p.q by constructing a large set of prime numbers from which the users can select alternative values of either one of the prime numbers or both that are used for changing the value of n. Moreover, the authors in [3] used two key pair, a small size key pair for encrypting data and another large size key pair to encrypt n of small size key pair. In addition, the article in [4], the authors presented a modified approach to data security using the concept of genetic algorithm and RSA cryptosystem to encrypt and decrypt these data. In [5] the authors suggested a modification of RSA cryptosystem to increase the security of it based on additive homomorphic properties. In [6], the authors tried to speed up the implementation of the algorithms of RSA over networks by enhancing its algorithms and giving a modified form for its algorithms with using of the third prime number in the structure of modulo n, which is very hard to decompose by any attacker. The authors in [7] modified the RSA cryptosystem by modifying the Subset-Sum over RSA cryptosystem, which is secure against Mathematical and brute-force attacks on RSA. On the other, in [8] the authors used Short Range Natural Number Algorithm to modify the RSA cryptosystem using two natural numbers in pair of the public and private keys to increase the security. In 2012, the authors in [9] modified the RSA cryptosystem by increasing the number of the primes, which are composed n, to k given prime numbers. This technique gives the RSA cryptosystem a higher security because it is not easily to decompose n to ‘k’ prime numbers. However, there are different authors have done other modifications, the private key of the RSA cryptosystem might be found by inspection. Therefore, this paper suggests a new modification of RSA cryptosystem by increasing the number of the private keys from one key to "k" chosen private keys. This modification gives RSA cryptosystem a higher security and makes it one of the most secure public key cryptosystem.

3. RSA cryptosystem

There are two keys in RSA cryptosystem, one is public that should be available to everyone and the other is private, which is kept secret by the creator. The public and private keys are used for encryption and decryption procedures respectively [11].

3.1. The key generation of RSA cryptosystem [11]

- Two very large prime numbers **p & q** are selected by every user to from **n=pq**.

- Everyone computes the Euler Phi function such that **φ(n) = φ(pq) =(p-1)(q-1)**.
- Two positive integers w_1 & s_1 are chosen such that s_1 is an inverse of w_1 modulo **φ (n)** with 1< w_1, s_1 < φ (n), gcd(w_1, φ (n))=1
- The pair **(w_1, n)** is announced publicly, and the creator must keep **(s_1, n)** secret.

3.2. The encryption procedure of RSA cryptosystem [11]

- The announced recipient's public key **(w_1, n)** being used to encrypt a plaintext block M; corresponding numerical equivalents of a plaintext message block P.
- E (M) =Y≡ M^{w_1} (mod n) is computed by the sender.
- The ciphertext is transmitted as a list of blocks.

3.3. The decryption procedure of RSA cryptosystem [11]

- The receiver's private key **(s_1, n)** being used by the receiver to decrypt Y.
- D(Y) =M≡ Y^{s_1} (mod n) is computed on every single block.

3.4. The security of the RSA cryptosystem [11]

The RSA cryptosystem has a very good security, because its security depends on the computational hardness of factoring a large integer. However, for RSA keys' size, which is normally1024-or 2048-bits long, cryptologists think that 1024-bit keys might be hacked or cracked easily in future, which is why government has been trying to minimize the length of the key length to 2048-bits. Many studies showed that it is not easy to factor n if n is a large number with approximately 300 decimal digits however in the computer time millions of years are needed to factor n using the fastest factorization [12].

3.5. An example of RSA cryptosystem

Suppose that Ahmed wants to encrypt and send a matrix T = $\begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}$, which is a partition of an image matrix, to Mike whose public key and private key are **(w_1,** n**)** = (7, 143) and (s_1, n)= (103, 143) respectively.

***Encryption Procedure**:* Mike's public key **(w_1,** n**)** = (7, 143) is used by Ahmed to encrypt the matrix

T = $\begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}$ using the encryption algorithm as the following;

- $$\text{E (T) =Y} \equiv T^{w_1} \text{ (mod n)} = \begin{bmatrix} (20)^7 & (02)^7 & (08)^7 & (25)^7 \\ (05)^7 & (11)^7 & (04)^7 & (28)^7 \\ (11)^7 & (22)^7 & (09)^7 & (08)^7 \\ (06)^7 & (12)^7 & (23)^7 & (10)^7 \end{bmatrix} (\text{mod } 143)$$

$$\equiv \begin{bmatrix} 136 & 128 & 57 & 64 \\ 47 & 132 & 82 & 63 \\ 132 & 22 & 48 & 57 \\ 85 & 12 & 23 & 10 \end{bmatrix}.$$

- The cipher matrix will be transmitted to Mike as, $Y = \begin{bmatrix} 136 & 128 & 57 & 64 \\ 47 & 132 & 82 & 63 \\ 132 & 22 & 48 & 57 \\ 85 & 12 & 23 & 10 \end{bmatrix}.$

Decryption Procedure: Mike uses his private key (s_1, n) = (103, 143) to decrypt Y using the following decryption algorithm;

$$\text{D(Y) = T} \equiv (Y)^{s_1} \text{ (mod n)} = \begin{bmatrix} (136)^{103} & (128)^{103} & (57)^{103} & (64)^{103} \\ (47)^{103} & (132)^{103} & (82)^{103} & (63)^{103} \\ (132)^{103} & (22)^{103} & (48)^{103} & (57)^{103} \\ (85)^{103} & (12)^{103} & (23)^{103} & (10)^{103} \end{bmatrix} (\text{mod } 143)$$

$$\equiv \begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}.$$

4. The New Proposed Modification

This modification increases the confidence of using the asymmetric cryptography, RSA cryptosystem, since it increases its security to be with a very high secrecy. Increasing the number of the private keys to "k" private keys, this what this modification has focused on. In this paper, this modification is being applied over matrices, and it can be applied over gray and color images.

4.1. The key generation of this modification

- Two very large prime numbers **p & q** are selected by RSA's user to from **n=pq**.
- Everyone computes **φ(n) ; φ(n) = φ(pq) =(p-1)(q-1)**.
- Choose a positive integer k such that $w_1, w_2, w_3, \dots, w_k$ & $s_1, s_2, s_3, \dots, s_k$ are chosen such that s_h is an inverse of w_h modulo **φ (n)** with 1< w_h , s_h < φ (n), gcd(w_h, φ (n)) =1, for 1≤h ≤ k.
- **(**$w_1, w_2, w_3, \dots, w_k$**,** n**)** will be announced as the public key, and **(**$s_1, s_2, s_3, \dots, s_k$**,** n**)** must be kept secret as the corresponding private key.

4.2. The encryption procedure of this modification

- The announced receiver's public key ($\boldsymbol{w_1}, \boldsymbol{w_2}, \boldsymbol{w_3}, \dots, \boldsymbol{w_k}$, n) being used by a sender to encrypt a plain matrix $\boldsymbol{T_{ij}} = \begin{bmatrix} \boldsymbol{t_{11}} & \boldsymbol{t_{12}} & \cdots & \boldsymbol{t_{1j}} \\ \boldsymbol{t_{21}} & \boldsymbol{t_{22}} & \cdots & \boldsymbol{t_{2j}} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{t_{i1}} & \boldsymbol{t_{i2}} & \cdots & \boldsymbol{t_{ij}} \end{bmatrix}$.

- $w_1, w_2, w_3, \dots, w_k$ should be formed in the encryption key matrix W_{ij} such that W_{ij} has the same size of the plain matrix T_{ij}, and $w_1, w_2, w_3, \dots, w_k$ should be organized respectively in columns so that (k=i*j), which as the following;

$$W_{ij} = \begin{bmatrix} w_1 & w_2 & \cdots & w_j \\ w_{j+1} & w_{j+2} & \cdots & w_{2*j} \\ \vdots & \vdots & \vdots & \vdots \\ w_{(i-1)*j+1} & w_{(i-1)*j+2} & \cdots & w_{i*j=k} \end{bmatrix}.$$

Moreover, if k < i*j; $w_1, w_2, w_3, \dots, w_k$ should be repeated to form W_{ij} as the following;

$w_1, w_2, w_3, \dots, w_k, w_1, w_2, \dots, w_g$ where g is equivalent to i*j and $1 \le g \le$ k , or,

$$W_{ij} = \begin{bmatrix} w_1 & w_2 & \cdots & w_j \\ w_{j+1} & w_{j+2} & \cdots & w_{2*j} \\ \vdots & \vdots & \vdots & \vdots \\ w_k & w_1 & \cdots & w_g \end{bmatrix}.$$

- The matrix T_{ij} will be encrypted using the following defined algorithm:

$$C_R = W_{ij} ® T_{ij} (mod\, n) \equiv \begin{bmatrix} w_1 & w_2 & \cdots & w_j \\ w_{j+1} & w_{j+2} & \cdots & w_{2*j} \\ \vdots & \vdots & \vdots & \vdots \\ w_{(i-1)*j+1} & w_{(i-1)*j+2} & \cdots & w_{i*j=k} \end{bmatrix} ® \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1j} \\ t_{21} & t_{22} & \cdots & t_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ t_{i1} & t_{i2} & \cdots & t_{ij} \end{bmatrix}$$

$$(\text{mod n}) \equiv \begin{bmatrix} {t_{11}}^{w_1} & {t_{12}}^{w_2} & \cdots & {t_{1j}}^{w_j} \\ {t_{21}}^{w_{j+1}} & {t_{22}}^{w_{j+2}} & \cdots & {t_{2j}}^{w_{2*j}} \\ \vdots & \vdots & \vdots & \vdots \\ {t_{i1}}^{w_{(i-1)*j+1}} & {t_{i2}}^{w_{(i-1)*j+2}} & \cdots & {t_{ij}}^{w_k} \end{bmatrix} (\text{mod n}) \equiv \begin{bmatrix} c_{r11} & c_{r12} & \cdots & c_{r1j} \\ c_{r21} & c_{r22} & \cdots & c_{r2j} \\ \vdots & \vdots & \vdots & \vdots \\ c_{ri1} & c_{ri2} & \cdots & c_{rij} \end{bmatrix}$$

- The cipher matrix will be transmitted to a sender as $C_R = \begin{bmatrix} c_{r11} & c_{r12} & \cdots & c_{r1j} \\ c_{r21} & c_{r22} & \cdots & c_{r2j} \\ \vdots & \vdots & \vdots & \vdots \\ c_{ri1} & c_{ri2} & \cdots & c_{rij} \end{bmatrix}$.

4.3. The decryption procedure of this modification

- The receiver's private key ($\boldsymbol{s_1}, \boldsymbol{s_2}, \boldsymbol{s_3}, \dots, \boldsymbol{s_k}$, n) must be used to decrypt $\boldsymbol{C_R}$ after using them to form the corresponding decryption key matrix $\boldsymbol{S_{ij}}$ so that $\boldsymbol{S_{ij}}$ has the same size of the cipher matrix $(\boldsymbol{C_R})_{ij}$, and $\boldsymbol{s_1}, \boldsymbol{s_2}, \boldsymbol{s_3}, \dots, \boldsymbol{s_k}$ should be organized in columns so that (k=i*j), which as the following;

$$S_{ij} = \begin{bmatrix} s_1 & s_2 & \cdots & s_j \\ s_{j+1} & s_{j+2} & \cdots & s_{2*j} \\ \vdots & \vdots & \vdots & \vdots \\ s_{(i-1)*j+1} & s_{(i-1)*j+2} & \cdots & s_{i*j=k} \end{bmatrix}$$

Moreover, if k < i*j; $s_1, s_2, s_3, \dots, s_k$ should be repeated to form S_{ij} as the following;

$$S_{ij} = \begin{bmatrix} s_1 & s_2 & \cdots & s_j \\ s_{j+1} & s_{j+2} & \cdots & s_{2*j} \\ \vdots & \vdots & \vdots & \vdots \\ s_k & s_1 & \cdots & s_g \end{bmatrix}$$ where g is equivalent to i*j and $1 \leq g \leq$ k .

- The matrix $C_R = \begin{bmatrix} c_{r11} & c_{r12} & \cdots & c_{r1j} \\ c_{r21} & c_{r22} & \cdots & c_{r2j} \\ \vdots & \vdots & \vdots & \vdots \\ c_{ri1} & c_{ri2} & \cdots & c_{rij} \end{bmatrix}$ can be decrypted to obtain the plain matrix T_{ij} using the following defined algorithm:

$$T_{ij} = S_{ij} \circledR C_R (mod\ n)$$

$$\equiv \begin{bmatrix} s_1 & s_2 & \cdots & s_j \\ s_{j+1} & s_{j+2} & \cdots & s_{2*j} \\ \vdots & \vdots & \vdots & \vdots \\ s_{(i-1)*j+1} & s_{(i-1)*j+2} & \cdots & s_{i*j=k} \end{bmatrix} \circledR \begin{bmatrix} c_{r11} & c_{r12} & \cdots & c_{r1j} \\ c_{r21} & c_{r22} & \cdots & c_{r2j} \\ \vdots & \vdots & \vdots & \vdots \\ c_{ri1} & c_{ri2} & \cdots & c_{rij} \end{bmatrix} (\text{ mod n})$$

$$\equiv \begin{bmatrix} (c_{r11})^{s_1} & (c_{r12})^{s_2} & \cdots & (c_{r1j})^{s_j} \\ (c_{r21})^{s_{j+1}} & (c_{r22})^{s_{j+2}} & \cdots & (c_{r2j})^{s_{2*j}} \\ \vdots & \vdots & \vdots & \vdots \\ (c_{ri1})^{s_{(i-1)*j+1}} & (c_{ri2})^{s_{(i-1)*j+2}} & \cdots & (c_{rij})^{s_k} \end{bmatrix} (\text{mod n})$$

$$\equiv \begin{bmatrix} ({t_{11}}^{w_1})^{s_1} & ({t_{12}}^{w_2})^{s_2} & \cdots & ({t_{1j}}^{w_j})^{s_j} \\ ({t_{21}}^{w_{j+1}})^{s_{j+1}} & ({t_{22}}^{w_{j+2}})^{s_{j+2}} & \cdots & ({t_{2j}}^{w_{2*j}})^{s_{2*j}} \\ \vdots & \vdots & \vdots & \vdots \\ ({t_{i1}}^{w_{(i-1)*j+1}})^{s_{(i-1)*j+1}} & ({t_{i2}}^{w_{(i-1)*j+2}})^{s_{(i-1)*j+2}} & \cdots & ({t_{ij}}^{w_k})^{s_k} \end{bmatrix} (\text{mod n})$$

$$= \begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1j} \\ t_{21} & t_{22} & \cdots & t_{2j} \\ \vdots & \vdots & \vdots & \vdots \\ t_{i1} & t_{i2} & \cdots & t_{ij} \end{bmatrix} = T_{ij}.$$

4.4. An Illustration Of This New Modification Over Matrices

Suppose that Ahmed wants to encrypt and send a matrix T = $\begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}$, which is a partition of an image matrix, to Mike whose public key is **(**w_1,w_2,w_3,w_4,w_5**,** n**)** = (7, 11,13,23,53, 143) and corresponding private key (s_1,s_2,s_3,s_4,s_5,n)= (103,11,37,47,77, 143).

Encryption Procedure*:* Mike's public key **(**w_1,w_2,w_3,w_4,w_5**,** n**)** = (7, 11,13,23,53, 143) is used by Ahmed to encrypt the matrix T_{4x4} = $\begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}$as the following;

- Mike's public key **(**w_1,w_2,w_3,w_4,w_5**,** n**)** = (7, 11,13,23,53, 143) should be used to form the encryption key matrix W_{4x4} such that W_{4x4} = $\begin{bmatrix} 07 & 11 & 13 & 23 \\ 53 & 07 & 11 & 13 \\ 23 & 53 & 07 & 11 \\ 13 & 23 & 53 & 07 \end{bmatrix}$.
- The following defined encryption algorithm is used to encrypt T_{4x4}:

$$C_R = W_{4x4} \text{ ® } T_{4x4} (mod\ 143) \equiv \begin{bmatrix} 07 & 11 & 13 & 23 \\ 53 & 07 & 11 & 13 \\ 23 & 53 & 07 & 11 \\ 13 & 23 & 53 & 07 \end{bmatrix} \text{®} \begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}$$

$$= \begin{bmatrix} (20)^{7} & (02)^{11} & (08)^{13} & (25)^{23} \\ (05)^{53} & (11)^{07} & (04)^{11} & (28)^{13} \\ (11)^{23} & (22)^{53} & (09)^{07} & (08)^{11} \\ (06)^{13} & (12)^{23} & (23)^{53} & (10)^{07} \end{bmatrix} (\text{mod}\,143) \equiv \begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix}.$$

- The cipher matrix will be transmitted to Mike as, $C_R = \begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix}$.

Decryption Procedure: Mike uses his private key (s_1,s_2,s_3,s_4,s_5,n)= (103,11,37,47,77, 143) to decrypt C_R after using s_1,s_2,s_3,s_4,s_5 =103,11,37,47,77 to form the corresponding decryption key matrix S_{4x4} so that ,

$$S_{4x4} = \begin{bmatrix} 103 & 11 & 37 & 47 \\ 77 & 103 & 11 & 37 \\ 47 & 77 & 103 & 11 \\ 37 & 47 & 77 & 103 \end{bmatrix}.$$

- The matrix $C_R = \begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix}$ can be decrypted to obtain the plain matrix T_{4x4}using the following defined algorithm: $T_{4x4} = S_{4x4} \circledR C_R(mod\ n)$

$$T_{4x4} = S_{4x4} \circledR C_R(mod\ 143) = \begin{bmatrix} 103 & 11 & 37 & 47 \\ 77 & 103 & 11 & 37 \\ 47 & 77 & 103 & 11 \\ 37 & 47 & 77 & 103 \end{bmatrix} \circledR \begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix}$$

$$= \begin{bmatrix} (136)^{103} & (46)^{11} & (138)^{37} & (38)^{47} \\ (70)^{77} & (132)^{103} & (114)^{11} & (106)^{37} \\ (110)^{47} & (55)^{77} & (48)^{103} & (96)^{11} \\ (84)^{37} & (12)^{47} & (56)^{77} & (10)^{103} \end{bmatrix} (\text{mod } 143) \equiv \begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}.$$

5. Discussion And Comparison

The RSA cryptosystem is one of the most secure public key cryptosystems, which has one public key ($\boldsymbol{w_1}$, n) and one private key ($\boldsymbol{s_1}$, n). Hacking or cracking this cryptosystem relies on the knowledge of the private key ($\boldsymbol{s_1}$, n), which relies on finding the Euler phi function of n (φ(n)). Finding φ(n) depends on factoring n into the product of two prime numbers p & q, and that is very difficult and needs thousands of years. However, identifying the private key ($\boldsymbol{s_1}$, n) by a hacker or cracker is being impossible; this private key might be found by inspection. As it is shown at the example of RSA cryptosystem above, whole the encrypted plain matrix will be cracked or hacked easily by knowing the private key. Then, the plain matrix will be identified easily. Therefore, this paper suggests a new modification for the RSA cryptosystem based on increasing the number of the private keys to "k" private keys, which leads to "k" public keys. This suggestion solves the lack of identifying ($\boldsymbol{s_1}$, n) by anyone other than the recipient and sender and gives the RSA cryptosystem a higher security. For instance, the above illustration of this modification shows that the encrypted matrix cannot be decrypted by finding one or (k-1) private keys. Anyone other than the sender and intended receiver can decrypt this matrix only by knowing the "k" private keys, which is very impossible because identifying (k) private keys by inspection is very difficult especially with large prime numbers.

6. Conclusion

This paper has proposed a new modification of the RSA cryptosystem based on increasing the number of the private keys and corresponding public keys. RSA cryptosystem is a very secure public key cryptosystem that has only one private key and its corresponding public key; however, this paper focuses on discussing and solving a lack in the RSA cryptosystem, which is the ability of hacking or cracking this cryptosystem throughout identifying its only private key by inspection. Therefore, this paper has proposed a solution for this problem by increasing the number of the private keys to "k" distinct keys, and this modification gives the RSA cryptosystem a higher security and makes it impossible to be hacked or cracked by any attacker.

Acknowledgements

I would like to thank my family, my friends, and my colleagues at Department Of Mathematics, who have supported me to make this article possible and a magnificent experience for me.

References

[1] Ayele, A. A., & Sreenivasarao, V.“ A Modified RSA Encryption Technique Based on Multiple public keys”. International Journal of Innovative Research in Computer and Communication Engineering, vol.1, 2013.

[2] Hussain, A. K. “A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm”. IJISET-International Journal of Innovative Science, Engineering & Technology, vol. 2, 2015.

[3] Abudin, J., Keot, S. K., Malakar, G., Borah, N. M., & Rahman, M. “Modified RSA PublicKey Cryptosystem Using Two Key Pairs”. International Journal of Computer Science and Information Technologies,vol. 5, pp. 3548-3550, 2014.

[4] Hassan, A. K. S., Shalash, A. F., & Saudy, N. F. “MODIFICATIONS ON RSA CRYPTOSYSTEM USING GENETIC OPTIMIZATION”. International Journal of Research and Reviews in Applied Sciences, vol. 19, 2014.

[5] Dhakar, R. S., Gupta, A. K., & Sharma, P.“Modified RSA encryption algorithm (MREA) ”. Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012.

[6] Patidar, R., & Bhartiya, R. “ Modified RSA cryptosystem based on offline storage and prime number”. In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference, IEEE, 2013.

[7] Sharma, S., Sharma, P., & Dhakar, R. S. “RSA algorithm using modified subset sum cryptosystem. In Computer and Communication Technology (ICCCT) ”, 2011 2nd International Conference , IEEE, 2011.

[8] Sharma, S., Yadav, J. S., & Sharma, P. “ Modified RSA public key cryptosystem using short range natural number algorithm”. International Journal, vol. 2, 2012.

[9] Ivy, B. P. U., Mandiwa, P., & Kumar, M. “A modified RSA cryptosystem based on ‘n’ prime numbers”. International Journal Of Engineering And Computer Science, vol. 1, pp.63-66, 2012. mathematical cryptography. New York: springer, 2008.

[11] Damgård, I., & Koprowski, M.“Practical threshold RSA signatures without a trusted dealer”. International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2001.

[12] Rosen, K.H. Elementary Number Theory and Its Applications,5th Edn. United State of America, Boston: Addison Wesley, 2005.