Journal homepage www.jzs.univsul.edu.iq
Journal of Zankoy Sulaimani
Part-A- (Pure and Applied Sciences)

Selective Multi Keys to Modify RSA Algorithm

Maiwan Bahjat Abdulrazzaq

Dept. of Computer Science, Faculty of Science, University of Zakho, Kurdistan Region – Iraq.
E-mail:maiwan.abdulrazzaq@uoz.edu.krd

Article info

Original: 3 November 2018
Revised: 10 January 2019
Accepted: 17 February 2019
Published online: 20 June 2019

Key Words:
Cryptography, public key cryptography, RSA algorithm, asymmetric key, symmetric key.

Abstract

The use of the internet and communication technology noticeably contributes to development in all branches of science. The data that is transferred to communication channel are unsecured. Cryptography including security and integrity is a domain that provides policies for having privacy of the data. Protection of the data transferred through the internet is very important since such data when transferred through an unprotected channel may be attacked by a third party. RSA represents one of the public key cryptography methods that generate the modulus using two primes. These two primes represent the weakness of RSA benefited from and used by attackers. This paper proposes a new modified RSA method using selective multi keys encryption and decryption for the same modulus instead of using two keys, one for encryption and the other for decryption. This new method guarantees and increases the security of RSA.

I. Introduction

The development of network and communication technology stands behind the revolution of information technology. Security is one of the problems that permanently exist in network and communication technology. This problem calls for and simultaneously demands the development of a new strong cryptography method. Cryptography falls into two main types, namely symmetric key and asymmetric key. In symmetric cryptography, the same key is used for encryption and decryption, while in asymmetric cryptography the key used for encryption differs from that used for decryption. The concept of asymmetric key encryption cryptosystem is also called public key cryptography was introduced by Whitfield Diffe and Martin Hellman in 1976[1]. Many methods of public key cryptography have been developed, viz. Rabin cryptosystem[2], Elagmal cryptosystem [3], ECC [4]. The most common one in use is RSA which was introduced in 1978 by (Rivest Shamir Adleman) [5]. The encryption key **e** and the modulus **n** are quite public in RSA. The Privacy in RSA is represented by the decryption key **d** with the Euler function. Currently RSA is the safest technique and the most effective method, yet has certain drawbacks represented mainly by the possibility of coming under Discrete Logarithm, Cycle, Brute Force, Mathematical, and Timing attack [6, 7]. The RSA cryptosystem protocol involves two prime numbers to produce the modulus n. These two prime numbers weakness form the source of the weakness of RSA. The larger prime number gives higher security of the algorithm. The attacker's main goal is to break the security of this algorithm. Such a break can be done by factorizing the modulus which takes place exponential time. This operation can be adopted in order to discover the value of the modulus [8]. There are many researchers work in deferent ways to modified RSA the following papers some of them:

R. S. Dhakar et al. (2012) presented a new cryptography algorithm depending on the properties of the additive homomorphic. The new method is called Modified RSA Encryption Algorithm (MREA). MREA is secure for both the decisional composite residuosity, i.e. the intractability hypothesis assumptions as well as

factoring problem compared to RSA. The additive homomorphism cryptosystem scheme public-key of m1 and m2, can compute the encryption of m1 + m2 to improves the security [9].

K. Somsuk (2016) proposed a new method, namely d-RSA to reduce the computation of the decryption process. The method uses a new private key not the traditional inverse. The new private key must have low Hamming weight. Also, the result of the multiplication between public key and private key modulo Euler function must be small. It is worthy to note that the decryption process of d-RSA is more efficient than RSA when the size of n is large [10].

P. Chaudhury, et al. (2017) proposed a modified RSA cryptosystem algorithm called "Asymmetric key based Cryptographic Algorithm using Four Prime numbers to secure message communication (ACAFP)" to handle four prime numbers used to generate the modulus and the Euler function. ACAFP can solve the factorization problem of RSA by including smallest prime numbers and hence the scheme becomes more advanced as far as memory consumption and computational speed are concerned [11].

I. G. Amalarethinam and H. Leena (2017) proposed the Enhanced RSA (ERSA) algorithm that uses two additional prime numbers in the Standard RSA algorithm. The four prime numbers are used to generate (N1, N2). N1 is used with encryption key e, while N2 is used with decryption key d. This idea was raised the high Speed and security RSA algorithm which use two random prime numbers for the key generation process[12].

A. Goel (2017) proposed algorithm use double encryption and decryption that's mean use double private and double public keys for dual modulus to provide security against Brute-force attacks. The basic motivation behind the carrying out of this research is that can factor modulus (n) into its prime numbers in conventional RSA algorithm, to generate a private key. As such, to remove this weakness, the dual modulus and substantially improve the security of the system [13].

I. Yakymenko et al. (2018) developed the scheme of modular multiplication and modular exponentiation algorithms. This was done by replacing the multiplication operation with the addition operation. Consequently, the process of encryption / decryption of information were accelerated. The developed method also reduced the temporal complexity of modular exponentiation in comparison with the classical one and increased the speed of the RSA algorithm[14].

As shown the goal of the researchers is to increase the security and the complexity of the RSA algorithm. The researchers aim is to complicate the mission of decipher the message from the hackers. Some of them increased the number of primes that generate the modulus. Other goes though the multiplication or raising the power of the keys for encryption and decryption. The methodology of this paper tries another way through using multi key encryption and decryption as much as the numbers of message blocks that can be selected from the candidate keys.

The remaining of this paper is organized as follows. In Section II, RSA algorithm is presented. In Section III, light is shed on the modified RSA key selective. Section IV puts forward the results of the key generations. Finally, Section V presents the conclusions.

II. RSA ALGORTHM

The RSA algorithm can be comprises three main steps, namely key generation, encryption and decryption[15]:

1. Key generation
   i. Select two large prime p and q
   ii. Compute the modulus
   $$n = p * q$$
   iii. Calculate the Euler function as:
   $$\varphi(n) = (p - 1) * (q - 1)$$
   iv. Choose the public key 'e' according to
      a. $0 < e < \varphi(n)$
      b. $\gcd(e, \varphi(n)) = 1$
   v. Find private key d such that:

$e * d = 1 \bmod \varphi(n)$

vi. The public (e, n) and the privet $(e, d, p, q, \varphi(n))$

2. Encryption
   i. The message M, coded to integer such that:
      $0 < M < n$
   ii. Cipher the message by $C = M^e \bmod n$
3. Decryption
   i. Recover the message by $M = C^d \bmod n$

III. PROPOSED SELECTIVE MULTI KEYS FOR MODIFYING RSA ALGORTHEM

Selective Multi Keys for modifying RSA Algorithm consists of three steps, namely key generation, encryption and decryption:

1. Key generation
   i. Select two large prime p and q
   ii. Compute the modulus $n = p * q$
   iii. Calculate the Euler function as: $\varphi(n) = (p - 1) * (q - 1)$
   iv. Put all primes less than $\varphi(n)$ in candidate vector (CK) :

```
for i = 1: size(CK) ; {
    if(gcd((CK_i), φ(n)) = 1
        Ke_i = CK_i ;
        Kd_i = CK_i ;
    end
end
```

   v. Finding the encryptions and decryptions keys:

```
k = 1;
for i = 1: size(Ke_i)
    for j = 1: size (Kd_j)
        if(mod((Ke_i * Kd_i), φ(n)) = 1
            E_k = Ke_i;
            D_k = Kd_j;
            k = k + 1;
        end
    end
end
```

   vi. The Public keys are (E_k, n).
   vii. The Private keys are $(D_k,\ p,\ q,\ \varphi(n))$
2. Encryption:
   i. Split the messages (M) to blocks, which each block (M_x) is coded to integer less than n
   ii. Select randomly number of keys (e_x) from (E_k) and (d_x) from (D_k) equal to the number of (M_x).
   iii. for $i = 1: \text{size}(M_x)$
      $C_i = M_i^{e_i} \bmod n$; , d_x)
3. Decryption:
   for $i = 1: \text{size}(M_x)$
   $M_i = C_i^{d_i} \bmod n$

Example1 of Selective Multi Keys RSA Algorithm

1. Key generation

   i. Let p = 7 and q = 13
   ii. Compute the modulus $n = 7 * 13 = 91$
   iii. Calculate the Euler function $\varphi(n) = (7 - 1) * (13 - 1) = 72$

iv. CK= (2 ,3 ,5 ,7 ,11 ,13 ,17 ,19 ,23 ,29 ,31 ,37 ,41 ,47 ,53 ,59 ,61 ,67 ,71).

v. The keys (E_x, D_x) that satisfy the condition from the candidate keys (CK) are :

1) $E_1 = 5 \;\; ; D_1 = 29$
2) $E_2 = 7 \;\; ; D_2 = 31$
3) $E_3 = 11 \; ; D_3 = 59$
4) $E_4 = 13 \; ; D_4 = 61$
5) $E_5 = 23 \; ; D_5 = 47$

vi. Public keys are (5, 7, 11, 13, 23), 91) and Private keys are (29, 31, 59, 61, 47), 72)

2. Encryption

i. Divide the messages(GO) to blocks; each block code less than (91), then G =07 and O =15

ii. Select any two keys (e_3, e_5) which they are (11, 47) from the public key sequence, and the inverse of them are (d_3, d_5) which they are (23, 47) .

1) $C_1 = 7^{11} \; mod \; 91 = 28$
2) $C_2 = 15^{23} \; mod \; 91 = 85$

3. Decryption

1) $M_1 = 28^{59} \; mod \; 91 = 7$
2) $M_2 = 85^{47} \; mod \; 91 = 15$

The number of primes that can be consider as candidate keys (CK) are 19 which there values less than φ (n)= 72. From these 19 primes, the numbers that satisfy the conditions in this example are 10. They are split into two groups. Group1: in (E_x) consists of five prime's (5, 7, 11, 13, and 23) they will be use for encryption selecting. Group 2: in (D_x) which also consists of five primes (29, 31, 59, 61, and 47) they will be use for decryption. The decryption keys selection depends on the encryption key selection. For encrypting the messages, (GO) should be divided into two blocks. Then, each block is coded to integer. The message block length has to be less than (91). Accordingly, G will be (7) and O will be (15). Because they are two blocks, two keys need to be chosen for encryptions. Let be (e_3, e_5) and in the same sequence for decryption (d_3, d_5). These keys are then used to apply the encryption and decryption processes.

Example 2 of Selective Multi Keys for modifying RSA Algorithm

1. Key generation

i. Let p = 1009 and q = 1901

ii. Compute the modulus $n = 1009 * 1901 = 1918109$

iii. Calculate the Euler function $\varphi(n) = (1009 - 1) \; * \; (1901 - 1) = 1915200$

iv. CK= (2 ,3 ,5 ,7 ,11 ,13 ,17 ,19 ,23 ,29 ,31 ,…, 1915163 ,1915183).

v. The encryption and decryption keys are:

1) $e_1 = 13$; $d_1 = 1767877$
2) $e_2 = 23$; $d_2 = 582887$
3) $e_3 = 43$; $d_3 = 1247107$

⋮ ⋮

48819) $e_{48819} = 1915019$; $d_{48819} = 687779$

48820) $e_{48820} = 1915183$; $d_{48820} = 1239247$

vi. Public keys are ((13, 23, 43… 1915019, 1915183), 1918109).

vii. Private keys are ((1767877, 582887, 1247107,…, 687779, 1239247), 1009 , 1901, 1915200)

2. Encryption

i. Divide the messages (SEND HELP SOON) to blocks; each block code length is less than (n= 1918109). The message becomes four blocks

SEN=180513, DHE=30704, LPS=111518, OON=141423.

ii. Select any four keys $(e_{2270}, e_{2602}, e_{26922}, e_{32686})$ from the public key sequence with values (66643, 77773, 1000003, 1915183) used for cipher the message and the inverse of selected keys are $(d_{2270}, d_{2602}, d_{26922}, d_{32686})$ with values (66643, 77773, 1000003, 1915183) used for decipher the message:

1) $C_1 = 180513^{66643} \; mod \; 1918109 = 321850$
2) $C_2 = 30704^{77773} \; mod \; 1918109 = 1098671$
3) $C_3 = 111518^{1000003} \; mod \; 1918109 = 7484448$
4) $C_4 = 141423^{1915183} \; mod \; 1918109 = 503402$

3. Decryption

1) $M_1 = 321850^{1569307} \; mod \; 1918109 = 180513$
2) $M_2 = 1098671^{60037} \; mod \; 1918109 = 30704$
3) $M_1 = 7484448^{1252267} \; mod \; 1918109 = 111518$
4) $M_1 = 503402^{1239247} \; mod \; 1918109 = 141423$

The number of primes that can be consider as candidate keys (CK) are 143082 which there values are less than φ (n)= 1915200. Prime numbers that satisfy the conditions in the example are 48820. They are split into two groups. Group 1 consists of (71541) primes (13, 23, 43… 1915019, 1915083) that are used for encryption. Group 2 also comprises (71541) primes (1767877, 582887, 1247107, 687779, and 1239247) which used for decryption. The decryption keys selection depends on the encryption keys selection. For encrypting the messages, (SEND HELP SOON) is divided into blocks; each block code length is less than (n) which is value equal to (1918109), then SEN=180513, DHE=30704, LPS=111518, ON=141423. The numbers of blocks are four. This means that for encryptions, four keys need to be selected (66643, 77773, 1000003, and 1915183). This enforces the choice of the decryption keys (1569307, 60037, 1252267, and 1239247). These keys are then used for the application of the encryption and decryption processes.

V. RESULTS OF KEY GENERATION

Selecting the two prime numbers p and q is very important for RSA. The two primes will determine the size of the modulus (n) and Euler function φ (n).The modulus will determine the size of the message blocks, while the Euler function will determine the number and size of the keys. The last raw in table 1 shows that the values of selecting **p** equal to 1129, **q** equal to 8887 determine the value of the Euler function to be equal 10023408.The number of primes they can be consider as candidate keys are 666045.The keys that satisfy the condition from candidate keys are 135454 as shown in Table1.can select keys from them for encryption and decryption as much as the block messages have.

Table-1: The number of keys produced from selecting (p and q).

p	q	φ (n)	n-primes	n-keys
7	13	72	20	10
17	43	672	121	64
79	97	7488	948	388
223	433	95904	9242	2694
353	929	326656	28137	25392
1901	1009	1915200	143082	48800
1129	8887	10023408	666045	135454

The relationship between the digit number of Euler function and the number of keys is increasing as shown in Figure 1.

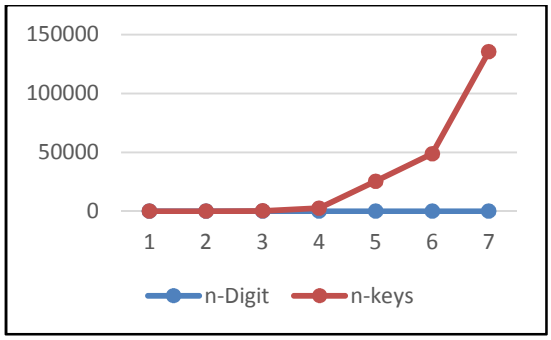

Figure-1: The number of Euler function digit and number of keys.

VI. CONCLUSIONS

The original RSA algorithm process depends of using two keys. The first key called public key which is use for ciphering the blocks of the messages. The second key which is the privet key is use for recovering the ciphered blocks of the messages. That is mean this algorithm depend on only one key for deciphering the message. As known there are many methods used for attacking RSA algorithm. Therefore the solution that RSA is used to solve this problem is by increasing the number of the digits of the keys and the modulus. This solution raises the difficulty to be attacked easily. The current paper presents proposes method for modifying RSA cryptography algorithm that depends on using multi keys, instead of using only one key for decryption. Each block of the message uses its own selected key. The key will use exactly one time. Even finding one privet key from the attacker will not recover all messages but only recover that block, that is mean increasing the security. The chosen of the two large prime's p and q gives a larger Euler function that leads to a larger numbers of the keys that used for encryption and decryption; as a result led to increase the complexity. It is very difficult for any hackers to guess the numbers of the keys have been used for encryption with the size of the block also which keys have been selected and in any sequence they used. The limitation of the proposed method is the calculation time. Which will increase depends on (p, q) and the numbers of selected keys (e, d).

References:

[1] A. K. Mishra and S. G. Samaddar, *"Generation of symmetric sharing key using ABC conjecture",* International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 144-150. (2017).

[2] M. Elia, M. Piva, and D. Schipani, *"The Rabin cryptosystem revisited",* Applicable Algebra in Engineering, Communication and Computing. Vol. 26, pp. 251-275. (2015).

[3] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, *"An ElGamal-like cryptosystem for enciphering large messages",* IEEE Transactions on Knowledge and Data Engineering. Vol. 14, pp. 445-446. (2002).

[4] M. Rosing, *"Implementing elliptic curve cryptography"*, Manning Greenwich, (1999).

[5] S. J. Aboud, M. A. AL-Fayoumi, M. Al-Fayoumi, and H. S. Jabbar, *"An efficient RSA public key encryption scheme",* in Information Technology: New Generations 2008. Fifth International Conference on, 2008, pp. 127-130. (2008).

[6] F. F. Moghaddam, S. D. Varnosfaderani, I. Ghavam, and S. Mobedi, "*A client-based user authentication and encryption algorithm for secure accessing to cloud servers based on modified Diffie-Hellman and RSA small-e",* in Research and Development (SCOReD), IEEE Student Conference on, 2013, pp. 175-180. (2013).

[7] V. Shende and M. Kulkarni, *"FPGA based hardware implementation of hybrid cryptographic algorithm for encryption and decryption"*, in Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), International Conference on, 2017, pp. 416-419. (2017).

[8] M. Lakkadwala and S. Valiveti, *"Parallel generation of RSA keys—A review",* in Cloud Computing, Data Science & Engineering-Confluence, 7th International Conference on, 2017, pp. 350-355. (2017).

[9] R. S. Dhakar, A. K. Gupta, and P. Sharma, *"Modified RSA encryption algorithm (MREA)",* Second International Conference on Advanced Computing & Communication Technologies, 2012, pp. 426-429. (2012).

[10]K. Somsuk, *"The improving decryption process of RSA by choosing new private key",* in Information Technology and Electrical Engineering (ICITEE), 8th International Conference on, 2016, pp. 1-4. (2016).

[11]P. Chaudhury, S. Dhang, M. Roy, S. Deb, J. Saha, A. Mallik, et al., *"ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm",* in Industrial Automation and Electromechanical Engineering Conference (IEMECON), 8th Annual, 2017, pp. 332-337. (2017).

[12]I. G. Amalarethinam and H. Leena, *"Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud",* in Computing and Communication Technologies (WCCCT), World Congress on, 2017, pp. 172-175. (2017).

[13]A. Goel, *"Encryption algorithm using dual modulus",* in Computational Intelligence & Communication Technology (CICT), 3rd International Conference on, 2017, pp. 1-4. (2017).

[14]I. Yakymenko, M. Kasianchuk, S. Ivasiev, A. Melnyk, and Y. M. Nykolaichuk, *"Realization of Rsa cryptographic algorithm based on vector-module method of modular exponention",* in Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 14th International Conference on, 2018, pp. 550-554. (2018).

[15]T. C. Segar and R. Vijayaragavan, *"Pell's RSA key generation and its security analysis",* in Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference on, 2013, pp. 1-5. (2013).