A PROPOSED METHOD FOR TEXT ENCRYPTION USING SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEMS

Hayder Raheem Hashim[1], Mohammed Abdul Hameed Jasem Alkufi [2]

Faculty of Computer Science and Mathematics, University of Kufa, Iraq[1], Department of Islamic education , University of Kufa , Iraq[2]

[1]hayderr.almuswi@uokufa.edu.iq
[2]mohammeda.alkufi@uokufa.edu.iq

Publication date – August 24, 2017

Abstract— *This proposed method focuses on encrypting texts that are written in English or Arabic language using symmetric and asymmetric cryptosystems respectively. The symmetric and asymmetric cryptosystems presented by Vigenere Cipher and RSA Cryptosystem respectively. Therefore, a plaintext encrypted using Vigenere Cipher, then the obtained ciphertext must be encrypted again using RSA Cryptosystem in a way that makes this method programmed using MATLAB. Therefore, this suggested method has a higher level of security than either Vigenere Cipher or RSA Cryptosystem since its security relies on the hardness of factoring the product of two large prime numbers, the factoring problem and on the secrecy of the keyword of the Vigenere Cipher. Therefore, this method gives us the confidence of using Vigenere cipher over text messages as a part of asymmetric cryptography and suggests a new method for encrypting text messages.*

Keywords: Vigenere Cipher, RSA Cryptosystem, Encryption, Decryption, MATLAB.

I. INTRODUCTION

Number theory was one of the "purest" branches of mathematics, but it has been really useful and applicable especially in a security of computers. For example, number theory helps to protect sensitive messages and information such as banking card numbers when we shop online, and protecting messages when we send them through insecure networks [16]. Therefore, one of the most important applications of number theory used for this matter is cryptography [1]. Traditionally, the need of cryptography in exchanging messages secretly has occurred in diplomacy and military affairs. Nowadays, cryptography has become an important tool in the electronic communication. It gives a great deal of interest in the techniques of making messages and data unintelligible to everyone except the intended receiver [2]. There are two kinds of cryptosystems which are symmetric and asymmetric cryptosystems. In symmetric cryptosystem, a sender and a receiver share the same key in the encryption and decryption procedures [12]. On the other hand, in the asymmetric cryptosystem, every single sender or receiver has two different keys called private and public keys. The public key should be fairly available to anyone, so that the private key must be kept secretly by every person[9].There many examples of symmetric and asymmetric cryptosystems. Caesar Cipher, Hill Cipher, Vigenere Cipher, Affine Cipher are examples of former, whereas RSA, ElGamal, Rabin are associated with the latter [12]. In this article, we focus on encrypting an Arabic or English text message using one of the symmetric cryptosystems – Vigenere cipher was invented by a French diplomat and cryptologist, Blaise de Vigenere in 1553. The Vigenere Cipher is a method of encrypting alphabetic texts. Then, the obtained ciphertext will be encrypted again using asymmetric cryptosystem, RSA cryptosystem. In addition, MATLAB program is used to create the encryption and decryptions algorithms of this method. The security of RSA cryptosystem is based on the factoring problem which depends on the difficulty of factoring a product of two large prime numbers [4],[15]. This new method of encrypting a plaintext message using Vigenere Cipher and RSA cryptosystem has a higher level of security and is stronger than both the classical Vigenere Cipher and RSA cryptosystem since the security of this proposed approach depends on the security of both RSA and Vigenere Cipher. However, the security of Vigenere Cipher depends on the privacy of keeping the exchanged keyword secretly [11]. Therefore, this method has the same public and private keys that are used in the RSA cryptosystem and has the same secret keyword used in Vigenere Cipher. This method is really secure because it has security as much as both RSA cryptosystem and Vigenere Cipher have.

II. LITERATURE REVIEW

In this section, two different cryptosystems which are Vigenere Cipher and RSA cryptosystem will be considered in details. Vigenere Cipher is traditional cryptosystem that requires a single key in encryption and decryption procedures. However, The RSA cryptosystem is a public key cryptosystem that has two different corresponding keys a public key and a private key.

A. *Vigenere Cipher*

Vigenere Cipher was named after French cryptologist Blaise de Vigenere in 1553 [2]. It is a very simple cipher that is moderately difficult for any unintended parties to decipher. It is kind of like shift cipher (C ≡ P+K (mod

26) where P is a plaintext block and K is a particular key which is a positive number), but in Vigenere Cipher, K is changed with every letter[11]. The key of Vigenere Cipher consists of an English keyword $L_1, L_2, \ldots L_S$ that should be exchange between the sender and the receiver. Assume that the numerical equivalents of letters $L_1, L_2, \ldots L_S$ are k_1 $k_2 \ldots k_S$ respectively .Also, suppose that the numerical equivalents of the letters of the plaintext are $p_1\ p_2 \ldots p_j$. Note that, if the number of the numerical equivalents of the letters of the keyword may not be equal to the number of the numerical equivalents of letters of the plaintext, they should be repeated to be equal to the number of the numerical equivalents of the letters of English plaintext[5].

To encrypt an English plaintext message, a sender has to do the following:

- Translate the letters of the plaintext and keyword into their numerical equivalents $p_1\ p_2 \ldots p_j$ and $k_1\ k_2 \ldots k_S$ respectively(s and j are positive integers) using **Table(1)** [2]:

Table(1) :The numerical equivalents of letters

Letter	A	B	C	D	…	X	Y	Z
Numerical equivalent	00	01	02	03	...	23	24	25

- If the number of the numerical equivalents for the keyword $k_1\ k_2 \ldots k_S$ less than to the number of the numerical equivalents for the plaintext letters $p_1\ \ p_2 \ldots p_j$, they should be repeated as $k_1, k_2 \ldots k_S\ \ k_1\ \ k_{2..}\ k_j$ so that their numbers are equal.
- Apply the following encryption algorithm on every p_i: $c_i :\equiv p_i + k_i \pmod{26}$ where c_i is corresponding ciphertext for $p_i : i = 1, 2, \ldots, j$[10].

To decrypt a ciphertext, a receiver has to do the following:

- Translate the letters of the ciphertext into its numerical equivalents $c_1\ c_2 \ldots c_j$.
- If $s < j$, then of the numerical equivalents for the key word $k_1\ k_2 \ldots k_S$ should be repeated such $k_1\ k_2 \ldots k_S\ k_1\ k_{2..}\ k_j$.
- Apply the following decryption algorithm on every c_i : $p_i : \equiv c_i - k_i \pmod{26}$ [2], [10].

Example: Use the Vigenere cipher with encrypting key "SECRET" to obtain the ciphertext of the message "MATHEMATICS"**,** then decrypt the ciphertext to produce the original plaintext**.**

Encryption Procedure: The sender has to do the following:

- Translate the letters of the message "MATHEMATICS " into "$p_1\ p_2\ p_3\ p_4\ p_5\ p_6\ p_7\ p_8\ p_9\ p_{10}\ p_{11}$" = " 12 00 19 07 04 12 00 19 08 02 18".
- Translate the letters of the keyword" SECRET" into "$k_1\ k_2\ k_3\ k_4\ k_5\ k_6$ "= "18 04 02 17 04 19".
- The numerical equivalents for the keyword "$k_1\ k_2\ k_3\ k_4\ k_5\ k_6$ "= "18 04 02 17 04 19" should be repeated as" $k_1\ k_2 \ldots k_S\ \ k_1\ k_{2.}\ k_j = k_1\ k_2 \ldots k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}$" = "18 04 02 17 04 19 18 04 02 17 04".
- Apply the encryption algorithm of Vigenere Cipher with the specified key to get the ciphertext as follows:
- Apply the following encryption algorithm on every p_i: $c_i :\equiv p_i + k_i \pmod{26}$ for $i = 1, 2, \ldots, 11$ to get the following ciphertext in its numerical equivalents:

"$c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8\ c_9\ c_{10}\ c_{11}$" = "04 04 21 24 08 05 18 23 10 19 22 "**.**

- Translate the numerical equivalents of the ciphertext into letters "EEVYIFSXKTW"**.**

Decryption Procedure: The intended receiver has to do the following:

- Translate the letters of the ciphertext into its numerical equivalents "$c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8\ c_9\ c_{10}\ c_{11}$" = "04 04 21 24 08 05 18 23 10 19 22 " and use the key in its numerical equivalents " $k_1\ k_2 \ldots k_6\ k_7\ k_8\ k_9\ k_{10}\ k_{11}$" = "18 04 02 17 04 19 18 04 02 17 04".
- Apply the following decryption algorithm on every c_i: $p_i :\equiv c_i - k_i \pmod{26}$ to get numerical equivalents of the plaintext "$p_1\ p_2\ p_3\ p_4\ p_5\ p_6\ p_7\ p_8\ p_9\ p_{10}\ p_{11}$" = " 12 00 19 07 04 12 00 19 08 02 18" which is " MATHEMATICS".

B. RSA CRYPTOSYSTEM

The RSA cryptosystem is a public key cryptosystem, invented by Ron Rivest, Adi Shamir, and Len Adleman in 1970s [9]. RSA is the most commonly used cryptosystem in our modern life. For instance it is used in commercial, Web servers, browsers to secure Web traffic, authenticity of e-mail, and electronic credit card payment systems [6]. The RSA cryptosystem has two corresponding keys that are a public key, that should be fairly available to everyone, and a private key, that should be kept secret by its creator. Plaintexts that are encrypted with the public key can only be decrypted using the private key.

The following shows how the RSA's keys can be generated by users [7]:

- Two very large primes p and q are chosen by every user to form the product N=pq.
- Compute $\varphi(N) = \varphi(\ pq) = \varphi\ (\ p)\ \varphi\ (q) = (\ p-1)(q-1)$. (where $\varphi(N)$ is the Euler's phi-function, and it is the number of integers between 1 and (N-1),which are relatively prime to N) [14].
- Pick a positive integer e such that $1<e < \varphi\ (N)$ and $\gcd(e, \varphi\ (N))=1$.
- Compute d such that $ed \equiv 1 \pmod{\varphi(N)}$.
- Announce her public key that is the pair (e, N) and keep the corresponding private key (d, N) secret.

The following is the encryption process of RSA[9]:

- A sender uses the intended receiver's public key (e, N) to encrypt a plaintext message (in particular).
- After translating letters into their numerical equivalents and forming plaintext blocks, P_i , such that a nonnegative integer $P_i < N$ and i is positive. The sender uses the following encryption algorithm to encrypt P_i : $E(P_i) = C \equiv\ P_i^{\,e} \pmod{N}$. This C_i is the ciphertext of the plaintext P_i, that should be submitted to the intended receipt.

The following is the decryption process of RSA[9] :

- To decrypt the ciphertext block C_i, the receiver uses the following decryption algorithm $D(C_i) = P_i \equiv (C_i)^d \pmod{N}$.

The Security Of RSA Cryptosystem

The RSA cryptosystem is very secure cryptosystem since its security relies on the integer factorization problem[15]. Breaking this cryptosystem depends on knowing the private key (d, N). To find the private key (**d**, N) by anyone other than the sender and the receiver, he/she has to obtain the factors p and q of N[13]. Then, it is easy to find φ (N) and since **e** is known. But this has been really difficult, because it is quite hard to obtain the prime factors of N if N is a large composite number. Thus, breaking RSA by factoring N is mathematically difficult. Also, there might be other ways to obtain d by finding φ(N) from N, so that $\varphi(N)= \varphi(pq)= \varphi(p)\ \varphi(q)=(p-1)(q-1)$. Then p and q, that factorize N, can be found easily. But, finding φ(N) is not easier that factoring N. Moreover, when p and q both have approximately 100 decimal digits, then n=pq has approximately 200 decimal digits. To factor an integer of this size using the fastest factorization algorithm known, we need millions of years of computer time [2].

Example: Show the encryption and decryption procedures of RSA cryptosystem when a receiver's public key is (e, N) = (7, 33) and her private key is (d, N)= (3, 33) with the English plaintext " GOOD"

Encryption Procedure: The sender has to do the following:

- Translate the letters of the plaintext into their numerical equivalents: "$P_1P_2P_3P_4$"= "06141403"
- Form blocks of largest possible size(with an even number of digits) such that $P_i< N=33$:
  "P_1 P_2 P_3 P_4"= "06 14 14 03" .
- Use the receiver's public key(e, N)= (7, 33).
- Apply the encryption algorithm on every P_i: $C_i=E(P_i)\equiv P_i^e \pmod N$ for i=1,2, 3, 4 to get the ciphertext "C_1 C_2 C_3 C_4 " = "30 20 20 09".

Decryption procedure: The receiver has to do the following*:*

- Use her private key (d, N)= (3, 33).
- Apply the decryption algorithm on every C_i: $D(C_i)= P_i \equiv (C_i)^d \pmod N$ for i=1, 2, 3, 4 to get the numerical equivalents of the plaintext
  " $P_1P_2P_3P_4$"= "06141403".
- Translate the plaintext into letters to get " GOOD".

III. A Proposed Method For Text Encryption

This method gives us the confidence of using Vigenere Cipher in the public key cryptography since Vigenere Cipher has not been very secure to be used in encrypting messages since the coming of asymmetric cryptosystems. It focuses on applying the algorithms of RSA over the text message that is being encrypted using Vigenere Cipher in a way that increases the security and the efficiency of the Vigenere Cipher. Therefore, this method of text encryption using Vigenere Cipher and RSA cryptosystem could be considered as a public key (asymmetric) cryptosystem that has a better security than the classical Vigenere Cipher, because its security is based on the secrecy of the exchanged keyword of Vigenere Cipher and on the secrecy of the private key d of the RSA cryptosystem, that can be found by factoring N which is composed of a product of very large primes, which requires thousands of years as explained in the RSA cryptosystem. Therefore, this method has the exchanged key word of Vigenere Cipher and the RSA public key and private key[16].

The following shows the key generation, encryption algorithm, the decryption algorithm, and finally an illustration of this new proposed method for encrypting an English plaintext using Vigenere Cipher and RSA cryptosystem.

A. *The Key Generation Procedure*

- Select an English keyword such that this keyword may consist of one word, sentence, paragraph, or any different characters, and it should be exchanged secretly between the sender and the receiver. It is better to be used once in every encryption procedure.
- Choose two distinct prime numbers *p* and *q*. For security purposes, the primes *p* and *q* should be of similar bit-length and chosen randomly. Also , p and q should have the following forms: $p=2f +1$ *and* $q = 2r + 1$, where f and r large primes [4].
- Compute N = pq .
- Compute Euler's phi- function $\varphi(N)=(p- 1)(q – 1)$
- Pick a positive integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(N)) = 1$.
- Compute d such that $d \equiv e^{-1} \pmod{\varphi(N)}$ or $ed\equiv1 \pmod{\varphi(N)}$.
- Publish the pair (e, N) as the public key, and keep d as the private key that must be kept secret by the creator.

Therefore, this new method for text encryption using Vigenere Cipher and RSA Cryptosystem in the public key cryptography has a secret exchanged keyword, a public key (e, N) that should be fairly available to everyone, and a private key d that must be secret by each user.

B. *The Encryption Procedure*

The encryption algorithm of this proposed method is quite different from the normal algorithms of the symmetric and asymmetric cryptosystems, because encrypting a plaintext "message" using this method, two different encrypting algorithms are used over that message respectively with the use of the "keyword" and receiver's public key (e, N). The procedure is as followed,

Step 1: Use **Table(2)** below to translate the letters of the plaintext "message" and "keyword" into their numerical equivalents.

Table (2): The numerical equivalents of letters for the proposed method

Letters	A "a"	B "b"	C "c"	D "d"		X "x"	Z "z"	Space
Numerical equivalent	1	2	3	4		25	26	27

Step 2: Put the numerical equivalents of the plaintext "message" into an n x m matrix "M" by specifying the number of the rows (n). For instance, if we let the numerical equivalents of a "message" are "p_1 p_2 p_3 p_4 p_5 p_6 p_7… p_j" and n=4, then

$$M_{4xm} = \begin{bmatrix} p_1 & p_5 & \cdots\cdots.. & p_{j-3} \\ p_2 & p_6 & \cdots\cdots\cdots & p_{j-2} \\ p_3 & p_7 & \cdots\cdots\cdots & p_{j-1} \\ p_4 & p_8 & \cdots\cdots\cdots & p_j \end{bmatrix}.$$

Note that, if the last column of the matrix "M" is not completed, we use the number "27" in the end of it to form a completed matrix.

Step 3: Divide the M $_{n\ x\ m}$ matrix into **m** columns such that every column (say P) is an n x 1 matrix. So that the above matrix M_{4xm} can be divided into $P_1=\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix}$, $P_2=\begin{bmatrix} p_5 \\ p_6 \\ p_7 \\ p_8 \end{bmatrix}$,…, $P_m=\begin{bmatrix} p_{j-3} \\ p_{j-2} \\ p_{j-2} \\ p_j \end{bmatrix}$

Step 4: Put the numerical equivalents of the "keyword" into an n x m matrix" K_{nxm}". So that, If the number of the numerical equivalents for the "keyword" that are" k_1 k_2 …$k_{S"}$ less than to the number of the numerical equivalents for the plaintext letters p_1p_2 p_3 …$p_{j\,,}$ they should be repeated as k_1 k_2 …k_S $k_1k_{2..}$ k_j, so that their numbers are equal. Otherwise, there is no problem. If we suppose that the numerical equivalents for the keyword are" k_1 k_2 k_3 k_4 k_5 k_6" , then key matrix " K_{nxm}" for "M_{4xm}" will be ,

$$K_{4xm} = \begin{bmatrix} k_1 & k_5 & k_3 & \cdots\cdots \\ k_2 & k_6 & k_4 & \cdots.. \\ k_3 & k_1 & k_5 & \cdot\cdot\ . \\ k_4 & k_2 & k_6 & .\,\ldots \end{bmatrix}$$

Step 5: Divide the " K_{nxm}" matrix into **m** columns such that every column (say K) is an n x 1 matrix. So that the above matrix K_{4xm} can be divided to $K_1=\begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{bmatrix}$, $K_2=\begin{bmatrix} k_5 \\ k_6 \\ k_1 \\ k_2 \end{bmatrix}$, $K_2=\begin{bmatrix} k_3 \\ k_4 \\ k_5 \\ k_6 \end{bmatrix}$…, $K_m=\begin{bmatrix} \vdots \\ . \\ . \end{bmatrix}$

Step 6: Apply the encryption algorithm of Vigenere Cipher on every P_i (i =1, 2,…, m) to compute Vigenere ciphertext as: $C_{Vi} \equiv P_i + K_i$ (mod 27) .

Step 7: Apply the encryption algorithm of RSA on every C_{Vi} (i =1, 2,…, m) to compute the RSA ciphertext as:

$C_{Ri} \equiv (C_{Vi})^e$ (mod N) .

The final ciphertext will be sent as the columns: $C_{R1}, C_{R2,\ldots\ldots,} C_{Rm}$ or as a matrix formed from combining those columns. Once the matrix or $C_{R1}, C_{R2,\ldots\ldots,} C_{Rm}$ reaches the intended receiver, it must be decrypted.

C. The Decryption Procedure

When the receiver gets the ciphertext as $C_{R1}, C_{R2,\ldots\ldots,} C_{Rm}$, she has to decrypt it as the following with the use of the "keyword" and (d, N):

Step1: Apply RSA decryption algorithm on every C_{Ri} (i =1, 2,…, m) to produce the Vigenere ciphertext as:

$C_{Vi} \equiv (C_{Ri})^d$ (mod N) .

Step 2: Do the same as of Step 4 and Step 5 in the encryption procedure for the numerical equivalents of the keyword and ciphertext.

Step 3: Apply Vigenere decryption algorithm on every C_{Vi}(i =1, 2,…,m) to compute plaintext(P_i) in its numerical equivalents as: $P_i \equiv C_{Vi} - K_i$ (mod 27) .

Step 4: Translate P_1, P_2,…, P_m in to their equivalent letters respectively.

Step5: Obtain the original "message".

D. An Illustration Of This Method Using MATLAB

Suppose that Mohammed wants to encrypt the text " A New Method For Text Encryption Using Vigenere Cipher and RSA Cryptosystem" and sends it to Hayder using this method with the exchanged keyword " Mohammed And Hayder". Also, Hayder's public key (e, N) = (3, 33) and private key(d, N) = (7, 33) that can be generated using the keys generation algorithm preformed by MATLAB by inputting two distinct primes p= 3, and q= 11 in particular.

Encryption Procedure

Mohammed has to encrypt the message using the programmed algorithm preformed by MATLAB with inputting the following:

- The number of the rows (n) in the matrix M_{nxm}. For instance, he chooses n= 8.
- The message " A New Method For Text Encryption Using Vigenere Cipher and RSA Cryptosystem".
- The keyword" Mohammed And Hayder".
- Hayder's public key (e, N)= (3 , 33).

Then, he obtains the ciphertext in the following matrix form:

5	**14**	**31**	**4**	**0**	**19**	**4**	**5**	**13**	**26**	**10**
9	**3**	**21**	**18**	**22**	**17**	**30**	**26**	**28**	**17**	**76**
22	**8**	**23**	**18**	**18**	**23**	**30**	**5**	**4**	**19**	**10**
18	**17**	**30**	**29**	**19**	**5**	**3**	**22**	**4**	**5**	**0**
3	**0**	**14**	**18**	**5**	**26**	**24**	**28**	**14**	**19**	**0**
19	**5**	**0**	**22**	**9**	**24**	**31**	**3**	**9**	**19**	**0**
24	**4**	**26**	**14**	**1**	**26**	**26**	**1**	**28**	**26**	**0**
3	**4**	**5**	**24**	**14**	**0**	**26**	**16**	**16**	**31**	**0**

Decryption Procedure

When Hayder gets the ciphertext which is the matrix above, he has to decrypt it using the programmed algorithm with inputting the following:

- His private key (d, N)= (7, 33).
- The keyword" Mohammed And Hayder".

Then, he would obtain the original plaintext" A New Method For Text Encryption Using Vigenere Cipher and RSA Cryptosystem". Note that, the decryption program that is preformed using MATLAB produced the original message in small letter form.

IV. DISCUSSION AND RESULTS

In this paper, we suggested an interesting method for encrypting Arabic or English text messages in a way that gives us the confidence of using the symmetric cryptosystem, Vigenere Cipher, in the modern cryptography. On the other hand, it gives a new method for encrypting messages using Vigenere cipher and RSA cryptosystem. It turned out that this new method has a higher level of security than the mentioned cryptosystems. Also, it encrypts any Arabic or English plaintext message, which could be a word, phrase, sentence, or paragraph to an unintelligible ciphertext. This ciphertext is formed in a numerical matrix. The RSA cryptosystem is used in this method because it is a very secure cryptosystem since its security depends on the factorization problem, so it is not easy to break this method with using RSA cryptosystem. Also, the RSA cryptosystem works very well on this method especially when we transform the plaintext message into a matrix. Moreover, this method produces a quite unique cryptosystem for many reasons such as:

- It encrypts and decrypts a message using two well-known cryptosystem respectively.
- It has a exchanged keyword, a public key and private key.
- It has a higher level of security than the Vigenere Cipher and RSA cryptosystem since its security depends on the security of RSA cryptosystem and Vigenere Cipher.
- It deals with capital and small English letters in the same way. However, it has a treatment to these messages with spaces. When we test this proposed algorithm with the text in the Fig.1 written in English language, the decrypted text comes out to be the same as the original plaintext.

This suggested method is much more secure than the Vigenere Cipher or RSA Cryptosystem since its security relies on the hardness of factoring the product of two large prime numbers, the factoring problem. On the other hand, it depends on the secrecy of the keyword of the Vigenere Cipher. Therefore, this method gives us the confidence of using Vigenere Cipher over text messages as a part of asymmetric cryptography. Then, we have concluded that this method produces a new strategy to reactivate a symmetric cryptosystem called Vigenere Cipher to be used in the modern cryptography especially over electronic messaging.

Figure 1: English plaintext

- It also deals with Arabic language, when we test its algorithms with long key almost equal to the size of plaintext written in Arabic language (**Fig. 2)** to prove the possibility of using these algorithms with Arabic language; the decrypted text comes out to be the same as the original plaintext

النص الذي استخدم في التشفير هو "ان صلة الرحم تعتبر مفتاحا سماويا يقع في متناول الانسان لفتح ابواب الجنه ويجب علينا الفوز بهذا المفتاح الثمين والسهل المنال لان صلة الرحم ممكن ان تنال ولو بالتزاور بين الارحام على اقل تقدير. وان الكثير من الايات القرئانية والاحاديث النبوية الكريمه تشير الى ان صلة الرحم تنزل الخير والبركات على من فاز بهذا المفتاح السماوي. ان الله سبحانه وتعالى قد خلق الخلق وفطره على العيش الجمعي ورزق الخلق من خيرات السماوات والارض بما يكفيهم ان يعيشوا عيشا كريما. لذلك يجب علينا ان نراقب بعضنا البعض ونتناصح فيما بيننا لان الدين عند الله النصيحة والنصيحه هي ضرب من ضروب الامر بالمعروف والنهي عن المنكر التي تعتبر من اهم اعمدة الدين حيث جاء في حديث لامير المؤمنين علي بن ابي طالب(ع) "(اذا تركتم الامر بالمعروف والنهي عن المنكر ابتلاكم الله بغلاء الاسعار وخسران التجار ومسك السماء وشحة الماء وسلط عليكم شرار خلقه يسومونكم سوء العذاب)" ونسأل الله عز وجل ان يجعلنا من عبادة اللذين يأمرون بالمعروف والاحسان وينهون عن المنكر ".

Figure 2: Arabic plaintext

- Using MATLAB Program in the encryption and decryption procedures of this proposed symmetric and asymmetric cryptosystem showed that it has good accuracy standards as the following and it is shown in Table (3) and fig(3):

- The accuracy standards between the matrix of numerical values for the original text and numerical values for,
  - values after decryption:
    - MSE (mean squared error)= 0.
    - PSNR (peak signal-to-noise ratio)= infinity.
    - Mean error = 0
    - Correlation Coefficient = 1.
  - values for encryption matrix:
    - Correlation Coefficient = -1.
    - NPCR (The number of changing pixel rate)=100 %
- UACI (Unified Average Change Intensity)= 0 % **.**

- The encryption and decryption times were reasonable, and the throughput is also determined. These results are shown in **Table(3)**. Where, the throughput can be calculated as the following:

$$\text{Throughput} = \frac{\text{The size of the encrypted text in Megabyte}}{\text{The time required for encryption in seconds}}$$

Table 3: Encryption and decryption time and throughput.

Plaintext	number of text characters	Size of text K.B.	Experiences	Enc. time m.sec	throughput of encryption	Dec. time m.sec	throughput of decryption
English	200	12.6	1	75	0213	66	0.661
			2	50	0.341	26	0.877
			3	44	0.312	35	0.341
			4	55	0.374	52	1.365
	400	12.8	1	65	0.301	40	0.314
			2	51	0.365	44	0.403
			3	65	0.258	45	0.521
			4	50	0.323	35	0.525
	600	12.9	1	66	0.303	41	0.458
			2	65	0.302	38	0.444
			3	58	0.222	40	0.847
			4	55	0.363	45	0.441
	800	13	1	50	0.548	31	0.419
			2	52	0.276	45	0.867
			3	47	0.321	41	0.763
			4	49	0.257	44	0.851
Arabic	200	12.7	1	55	0.333	44	0.412
			2	52	0.387	42	0.542
			3	51	0.362	44	0.845
			4	58	0.357	52	0.652
	400	12.9	1	55	0.321	52	0.258
			2	50	0.318	54	0.369
			3	51	0.319	51	0.430
			4	56	0.541	59	0.859
	600	13	1	59	0.384	51	0.489
			2	51	0.562	59	0.746
			3	49	0.341	49	0.459
			4	71	0.652	59	0.652
	800	13.1	1	49	0.658	37	0.589
			2	48	0.856	51	0.596
			3	54	0.852	52	0.623
			4	58	0.598	54	0.612

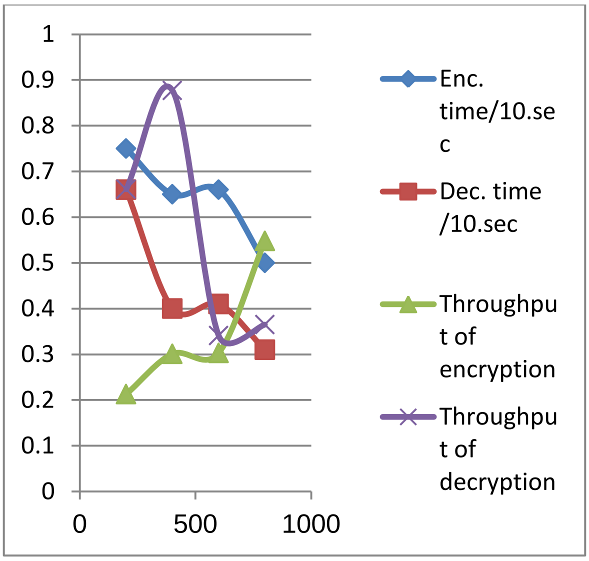

Figure 3: Encryption and decryption time and throughput's chart

.

V.CONCLUSION

This proposed new method for text encryption using two of the symmetric and asymmetric cryptosystems, which are Vigenere Cipher, and RSA cryptosystem, has been considered to be a public key cryptosystem since it has a public key that should be announced publicly and a private key that should be kept secret. Moreover, it has a secret exchanged key. Also, It gives a new way for encrypting text messages written in Arabic or English Languages using those symmetric and asymmetric cryptosystems respectively. In addition, it has a better security than either RSA or Vigenere Ciphers since its security depends on secrecy of the exchanged key and the factorization problem. Moreover, MATLAB Program is used to perform the keys generation and encryption and decryption procedures. Moreover, we have concluded that this method produces a new strategy to reactivate the symmetric cryptosystem called Vigenere Cipher to be used in the modern cryptography especially over electronic messaging. Although, the encryption and decryption times of this method were reasonable and can be reduced with faster computers.

ACKNOWLEDGMENT

We would like to thank all of our colleagues, at the department of Mathematics: Faculty of Computer Science and Mathematics, who have encouraged us to keep it up in the scientific research and made this search possible and an unforgettable experience for our authorship.

REFERENCES

[1] B Kaliski.(2006).The Mathematics of the RSA Public-Key Cryptosystem. RSA Laboratories.

[2] K.H.Rosen, "Inroduction to Cryptography," in Elementary of Number Theory and Its Applications, 5th ed. Boston, United State of America, 2005, ISBN-10: 0201870738.

[3] J.Buchman, " Introduction to cryptography," United State of America, Springer Science & Business Media, 2013.

[4] T.Okamoto, and S. Uchiyama.(1998).A new public-key cryptosystem as secure as factoring. In *Advances in Crypto log*.Springer Berlin Heidelberg.

[5] R. S. Douglas" Cryptography," in Theory and Practice: Discrete Mathematics and Its Applications, United State Of America, Taylor and Francis Group, 2006.

[6] D.Boneh.(1999).Twenty years of attacks on the RSA cryptosystem. Notices of the AMS. 46(2), pp. 203- 213.

[7] J. Hoffstein, J. Pipher, and J.H. Silverman," An Introduction to Mathematical Cryptography,"New York, United State of America, Springer, Science +Business, Media, LLC, 233,2008.

[8] Damgård, Ivan, and Maciej Koprowski.(2001). Practical threshold RSA signatures without a trusted dealer. Springer Berlin Heidelberg.

[9] Z. Kartit, and M. El Marraki. (2015). Applying Encryption Algorithm to Enhance Data Security in Cloud Storage.Engineering Letters. 23(4).

[10] Goyal, Dinesh, and Vishal Srivastava.(2012).RDA Algorithm: Symmetric Key Algorithm. International Journal Of Information and Communication Technology Research. 2(4).

[11] W. Trappe, and L.C. Washington," Introduction to Cryptography with Coding Theory," 2nd ed. New Jersey, United State of America, Prentice Hall, 2002.

[12] M. G. AL-Saidi, Nadia and Md. Said, Mohamad Rushdan and M. Ahmed, Adil . (2011). *Efficiency analysis for public key systems based on fractal functions.* Journal of Computer Science, 7 (4). pp. 526-532.

[13] Ali, Zulkarnain M., Nawara MA Makhzoum, and Alhassan Makhzoum. (2012). Computation of private key based on Divide-By-Prime for luc cryptosystems. Journal of Computer Science 8 (4).

[14] Ismail, Eddie Shahril, and S. Baharudin. (2012). Secure hybrid mode-based cryptosystem. American Journal of Applied Sciences 9(3).

[15] H.R.Hashim (2014). H-Rabin cryptosystem. J. Math. Stat., 10: 304-308.DOI: 10.3844/jmssp.2014.304.308.

[16] P. S.Narkhede, S.M. Ajabe,and Dandage, P. B. Zope," A Review of Public Key Cryptography for Secure Communication Using RSA," presented at the National Conference "CONVERGENCE", 2015.