Proposed Method for Text Encryption Using Two Secret Keys and One Secret Mathematical Equation

Qusay M. Jafar Alsadi
Alrafidain University College
Department of Computers Communication Engineering

Abstract

Information security is a vital issue and it needs to continuous developments. This paper focused on developing the concept of encryption by using a proposed method to encrypt text information or may be after some farther processing it is suitable for all types of files. This method used two secret keys (symmetric encryption) and one secret mathematical equation, and there are two levels of encryption; firstly through first secret key (key1) (convolution key); secondly through another secret key (key2) and secret mathematical equation. The cipher text is only real numbers. Also this paper will include some results of encryption and decryption.

Keywords:

Security, Encryption, Convolution key, Secret key, Secret Mathematical equation, and Proposed method.

الخلاصة:

امنية المعلومات هي واحدة من ضمن المواضيع الحيوية والتي تحتاج الى تطوير بشكل مستمر. هذا البحث يركز على تطوير مبدأ التشفير باستخدام طريقة مقترحة لتشفير النصوص والتي بالامكان تطويرها بعد زيادة المعالجة للبيانات لتشمل كافة انواع الملفات. هذه الطريقة تستخدم مفتاحين سريين (التشفير المتناظر) ومعادلة رياضية سرية ايضا، لهذا يوجد مستويين من التشفير، الاول خلال المفتاح الاول (مفتاح الالتفاف) والثاني خلال(المفتاح السري) والمعادلة الرياضية السرية. النص المشفر الناتج هو فقط ارقام حقيقية. وكذلك هذا البحث سوف يشمل بعض النتائج للتشفير وفك التشفير.

1- Introduction

Encryption has primarily been used to prevent the disclosure of confidential information, but can also be used to provide authenticity of the source of the message, verify the integrity of received data, provide the digital equivalent of a handwritten signature, and nonrepudiation. Nonrepudiation assures that a transacting party cannot deny that the transaction took place [3].

Cryptography is the name for the study of procedures, algorithms, and methods to encode and decode information, Where, *Cryptanalysis* is the study of methods and means to defeat or compromise encryption techniques [2]. Encryption usually requires the use of a hidden transformation that requires a *secret key* to encrypt, as well as to reverse the process or decrypt [4].

2- Symmetric and Asymmetric

With some encryption methods, the same key is used to both encrypt and decrypt the information [3]; this paper will used the same idea, This form of encryption is known as *symmetric* encryption, which is also known as *single-key* or *secret-key* encryption [3,8]. Another form of encryption uses two keys:

one key to encrypt and a different key to decrypt. These systems are referred to as *asymmetric* encryption, also referred to as *public-key* encryption, since one of the two keys is publicly known (and the other is kept secret)[1].

Messages or data are referred to as *clear text* or *plain text* before encryption is applied, and *cipher text* to describe text or data that has been encrypted. When the key is used to reverse the process (i.e., transform cipher text back to the original clear text), the decoding process is known as *decryption*[6].

3- Proposed method

The proposed system will include, how the data will be encrypted using convolution key to build the first template of encoding data, and then encryption using secret key and secret mathematical equation to make the file ready for sending , finally this paper will include some results of encryption and decryption to prove the effectiveness of using this method.

Key generation:

One of very important fundamentals in encryption is selection the secret keys, in this proposed system there are two keys of (n) bits, explained as follow:

Convolution key:

In this section we will explain the first one (convolution key). Let this key (key_1) of 9 bits, is represented in a matrix of (3*3) " mask key". The following example will show how the first key encrypts the plain text as a first level of defense in this proposed system:

Ex\ Let $key_1 = (220)_{10}$

Key_1 is convolution key it is selected randomly but it will be known for sender and receiver.

$(220)_{10} = (011011100)_2$

Key_1 mask

0	1	1
0	1	1
1	0	0

If there are two inputs in XOR gate then the output with one of these two inputs it will give the other[5].

This mask will convolute with the matrix of plain text using XOR operation.

Also, let the plain text is the word AHMED:

The ASCII of (A) is 65; (H) is 72 and so on for all the characters of the plain text.

For each character there is an ASCII code, each one of this ASCII codes will be represented as a decimal number and converted to binary according to a table presented by the system.

The matrix of the plain text (AHMED) will be represented in the program as an array of
(N row* M column)
A=65=01000001
H=72=01001000
M=77=01001101 Eight bits is enough to represent any character
E=69=01000101
D=68=01000100

M column

N rows

0	1	0	0	0	0	0	1	0	1
0	0	1	0	0	0	0	1	0	0
1	1	0	1	0	1	0	0	0	1
0	1	0	1	0	0	0	1	0	0

Matrix of the plain text

The first data (3*3)(submatrix) from the plain text matrix is:

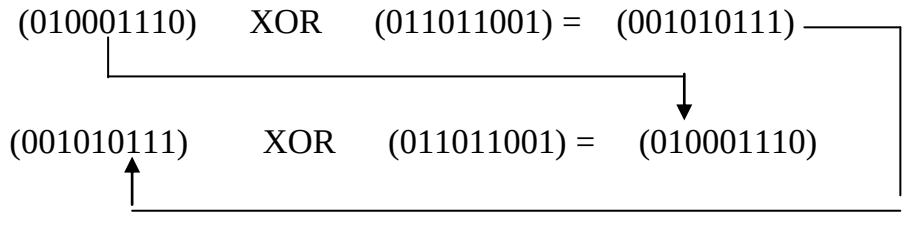
0	1	0
0	0	1
1	1	0

Note: the key1 mask is (3*3), it may be (4*4), (5*5),…., (n*n) according to the number of bits that represent the key1,(9,16,25 bits, ….) ,also the number of rows and columns in key1 mask must equal to the number of rows and columns in submatrix (subarray) extracted from plain text matrix, (A is the array of the plain text =[N,10]).
So,

(010001110) XOR (011011001) = (001010111)
First submatrix key1 first template
9 bits saved in second matrix
(temporary array)

To get the second data (2'nd 9 bits) the sub matrix (data mask) must shift one column right and it will be as follow (100010101), (000100010),…., until last column of the first row, and then shift one row down for the first column (001110010),shift one column right(010101101),…, and so on for all data matrix (bits).

XOR is a very useful for encoding (first level of encryption) and decoding (decryption)



Plain text $\oplus$ key1 = Cipher text

Cipher text $\oplus$ key1 = Plain text

Finally, the cipher text resulted from first level of encryption is (C1).

Secret key:

In this proposed system there is another type of key (secret key (Key_2)), also it will be used for encryption and decryption but it is through a secret mathematical equation. Secret key will be selected as a decimal number and only for sender and receiver will be known. I prefer to select a long decimal number to represent Key_2, and it will stay in a decimal form no need to change it to another form of representation. As shown before the convolution key (Key_1) will be secure between sender and receiver only.

4- Mathematical Equation Representation

The second level of protection (ciphering) is using secret key and secret equation. Secret mathematical equation is the main factor in this proposed method, it is possible to select it randomly using a program to generate a random equation depending on some constraints such as determining the number of variables and then the system composed an equation that will be known for sender and receiver. In this proposed system we select the following equation; Let C_2 is the secret mathematical equation:

$$C_2=\overset{3}{C_1}+1/2K_2+5 \quad \text{….. Eq(1)}$$

Where C_1 is the cipher text from convolution operation between the plain text and convolution key (first secret key (Key_1)) using XOR operation, see section 3-1-1. K_2 is the secret key, see section 3-1-2, (5) is a constant. The result of Eq(1) is the final cipher text. It is possible to select any type of equation but it is a very important to notice that the secret equation must be accepted to be in inverse form i.e:

$$C_2=\overset{3}{C_1}+1/2K_2+5 \quad \text{….. eq(1)}$$

$$\overset{3}{C_1}=C_2-1/2K_2-5$$

$$C_1=\sqrt[3]{C2-1/2Key2-5} \quad \text{….. eq(2)}$$

This proposed system may give the idea of a multi level of encryption.

5- Encryption/Decryption Mechanism and Algorithm

The following diagram explains the proposed system:

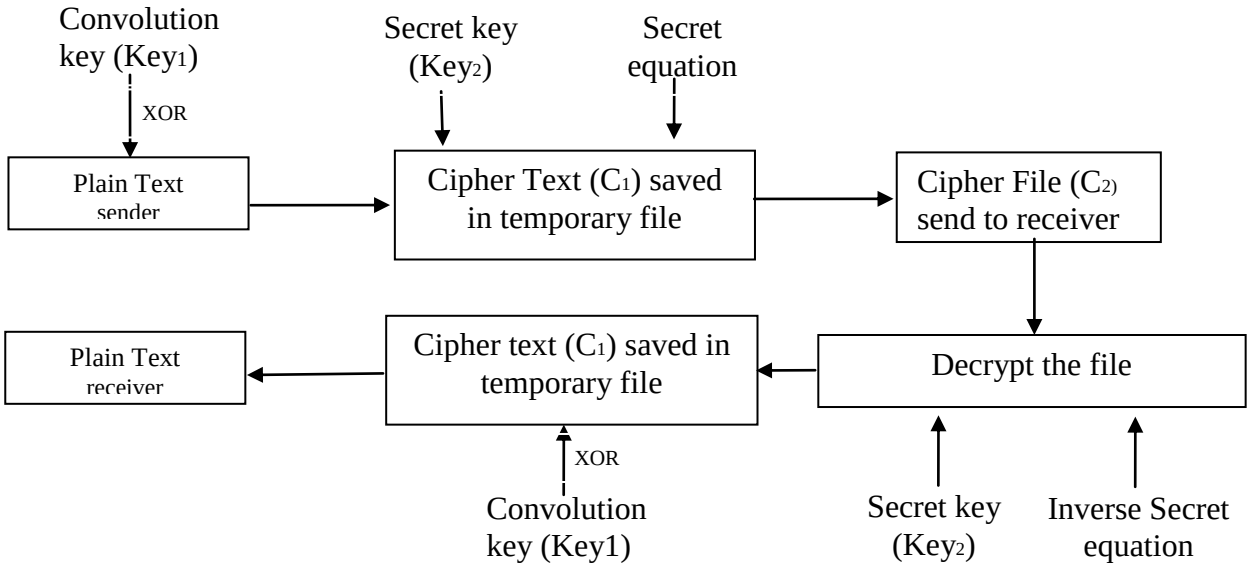


Fig (1) Block diagram of the proposed system

This diagram shows that there are two levels of encryption/decryption (C_1 and C_2).

The Algorithm

The following algorithm will explain the proposed system:

1- preprocessing the plain text will include the following steps:
   a- open the file
   b- Take the ASCII code for each character and deal with it as a decimal number.
   c- Convert each decimal number to binary in order to create a matrix of 0's and 1's only.
2- Select a convolution key (Key_1) (decimal number and convert it to a binary and then represents as a mask of n*n)
3- XOR between Key_1 and plain text (submatrix n*n)to create a temporary template (cipher text (C_1)) using convolution operation.
4- Select a secret key (Key_2) to be a decimal number.
5- Select a secret mathematical equation (MathEq).
6- After converting C_1 to an equivalent decimal number, use Key_2 and MathEq to create a final cipher text (C_2) (MathEq(key_2,C_1) to get C_2), C_2 is real numbers .
7- Send the result of step 6 to the receiver.
   Note: Key_1, Key_2 and MathEq must be known for sender and receiver only.
8- Use the inverse MathEq and Key_2 to get C_1 (Decryption).
9- XOR between Key_1 and C_1 to get the plain text, but notice that it must begin from last real number to the first one (repeat).

Note: you must take in your mind the shifting of rows and columns in Encryption and Decryption (loops). Also, select long decimal number to represent key_1, key_2, and use complex MathEq will make the system more strong to be broken.

6- Computations and Results

6-1 Encryption

Suppose we want to encrypt the following message:

HELLO.SIR

The ASCII code will represent as a decimal and then converted to binary according to the programming codes in the program. Table (1) shows how encoding each character:

Char	ASCII	Binary
H	72	01001000
E	69	01000101
L	76	01001100
L	76	01001100
O	79	01001111
.	46	00101110
S	83	01010011
I	73	01001001
R	82	01010010

Table (1)

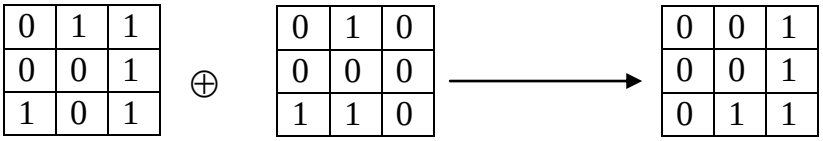
The following matrix represents the message HELLO.SIR:

0	1	0	0	1	0	0	0	0	1
0	0	0	1	0	1	0	1	0	0
1	1	0	0	0	1	0	0	1	1
0	0	0	1	0	0	1	1	1	1
0	0	1	0	1	1	1	0	0	1
0	1	0	0	1	1	0	1	0	0
1	0	0	1	0	1	0	1	0	0
1	0	0	0	0	0	0	0	0	0

The last eight position of the last row will be filled with 0's to complete the matrix.

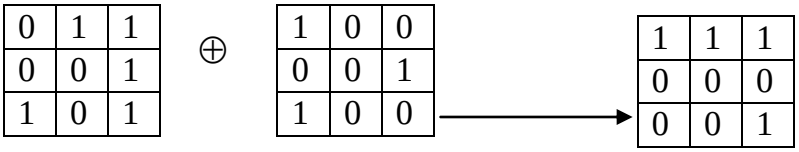
Suppose the convolution key (Key_1) is 205 in binary it is represented as follows 011001101, and then after representation of the convolution key as a matrix (convolution mask) the XOR operation will be done between convolution mask and submatrix of plain text:

Conv key (Key$_1$) | Plain text submatrix (First row second column) | $C_1[1,1]$ (Saved in a temporary array)



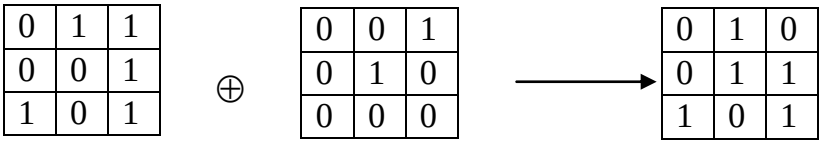
For the next submatrix (shift on column right):

Key$_1$ | next iteration of internal loop (First row third column) | $C_1[1,2]$ (Saved in a temporary array)



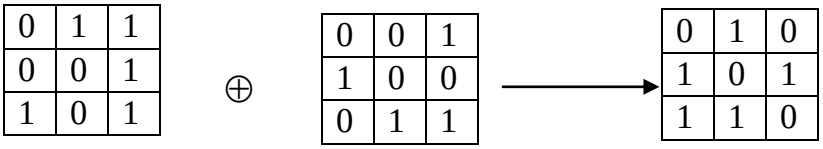
For the next submatrix (shift one column right):

Key$_1$ | next iteration of internal loop (First row fourth column) | $C_1[1,3]$ (Saved in a temporary array)



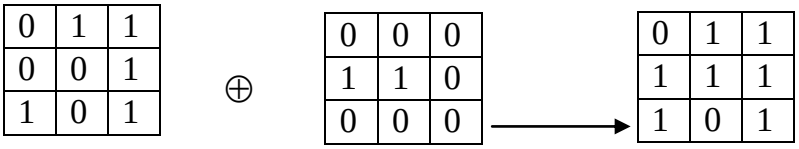
And so on for the next iterations of internal loop until first iteration of internal loop finished.

Key$_1$ | (first row eighth column) | $C_1[1,8]$



For the next row (shift one row down) (increment the external loop by one)

Key$_1$ | (second row second column) | $C_1[2,1]$



Continue with incrementing the internal loop until last column (eighth), and then increment the external loop by one, and so on until the last submatrix.

The final cipher text C_1 using convolution key (key1) as follow:

0010010111110000010100111101…….010101110……..011111101……

This sequence of binary digits (C_1) will be ready to encrypt using secret key (Key_2) and secret mathematical equation (MathEq)

Suppose that the sender and receiver was agreemented about the (MathEq) to be as follow:

$$C_2=\overset{3}{C_1}+1/2Key_2+5 \quad \text{.....eq(1)}$$

C_2 is the result of secret mathematic equation (EathEq) (second level of encryption) using secret key (key_2), C_1 is the result of first level of encryption using convolution key (key_1).

For the first nine bits (001001010) the decimal number is 75(C_1). Note: it is possible to change the strategy of selection the number of rows and columns for ciphering using convolution key, also it is possible to select any number of bits to represent the decimal number in encryption using secret equation and secret key but it needs a programming ability.

Also let key_2 is 188, C_2 is the result of MathEq, so:

$$C_2=\overset{3}{(75)}+90.5+5= 421875+90.5+5$$
$$C_2=421970.5$$

For the second nine bits (111000001) the decimal number is 449, so that C_2=90518944.5 , and so on for all the contents of C_1 matrix(of binary digits and converting to decimal) to get C_2 (file contains only long real numbers), finally C_2's (file) is ready to send to the receiver as an encrypted file.

6-2 Decryption

After all the data (C_2's) was send to the receiver as a file of real numbers only, now the receiver person must know the strategy of decryption this data, this point begins from knowing the MathEq, Key_1, Key_2 to be ready for his/her computation (the program will execute all the necessary processing to extract the original data after input the MathEq, Key_1, Key_2 by an authorized person).

$C_2=\overset{3}{C_1}+1/2Key_2+5$, so the inverse of this equation is:

$$C_1=\sqrt[3]{C2-1/2Key2-5}$$

For the second real number in C_2 file (90518944.5),

$C1=\sqrt[3]{90518944.5 - ((1/2)*181) - 5} = 449$

C1 is the same result of the second nine bits resulted from convolution key with second submatrix.

For the first real number in C_2 file (405319.5),

$C1=\sqrt[3]{421970.5 - ((1/2)*181) - 5} = 75$

C1 is the same result of the first nine bits which result from convolution Key with first submatrix

$(449)_{10} = (111000001)_2$

$(75)_{10} = (001001011)_2$

$C_1 \oplus Key_1 = \text{plain text}$

Key_1 is (205) identified previously,

$$449 \oplus 205$$

$$111000001 \oplus 011001101 = 100001100$$

1	0	0
0	0	1
1	0	0

It is equivalent to the second submatrix (3*3) (first row second column of the plain text matrix), that gives the original data (part of plaintext).

$$74 \oplus 205$$

$$001001011 \oplus 011001101 = 010000110$$

0	1	0
0	0	0
1	1	0

It is an equivalent to the first submatrix (first row first column of the plain text matrix). Continue for all C_2 to get C_1 and then plain text characters.

Note: from the experimental results, we can see that the Decryption of any character depends on the next character and vice versa for Encryption.

7- Conclusion

Security is one of the main issues in information technology, security is very wide field, and there are many methods to protect information in computer, encryption is one of them. In this research an encryption method system was proposed, designed and implemented. This system is known as "two keys one mathematical equation" (***2keys+1MathEq***). We can conclude from the proposed system the following:

1- This proposed system uses two secret keys and one secret mathematical equation, these make the proposed system more strong and difficult to breakthrough because there are three secret things.
2-The main problem of using this method is the size of the cipher text (file), it will need more size to save or send over the net.
3- Using convolution theorem (convolute the first key) is a new manner in encryption.
4- It is possible to use any number of rows and columns to represent the plain text submatrix, this will give a flexibility of selection the strategy of encryption.
5- This proposed system supports the idea of multilevel encryption, also this system needed four seconds to encrypt a file of 450 characters beginning from opening the file, creation a file of long real numbers, and finally saving the file.
6- The encrypted file is only long real numbers and there is no repetition, therefore it is difficult to guess the plaintext, if there is any repetition that does not mean the same symbol.

References:

[1] B. Furht, D. Socek, and A. M. Eskicioglu, ***"Fundamentals of multimedia encryption techniques"*** , in Multimedia Security Handbook, CRC Press, 2004, ch. 3, pp. 93–132.
[2] B. Schneier, ***"Applied Cryptography: Protocols, Algorithms, and Source Code in C"***. John Wiley & Sons, New York, second edition, 1996.
[3] C. Li, X. Li, S. Li, and G. Chen, ***"Cryptanalysis of a multistage encryption system",*** in Proc. IEEE Int. Symposium on Circuits and Systems, 2005, pp. 880–883.
[4] C.Wukmish and J. Kuo, ***"Design of integrated multimedia compression and encryption systems"***, IEEE Trans. Multimedia, vol. 7,no. 5, pp. 828–839, 2005.
[5] Morrisn Mano, "***Digital Design***", Prentice Hall, 2002.
[6] pual.jim, ***" The security of an image encryption method",*** in Proc. IEEE Int. Conference on Image Processing, vol. 2, 2002, pp. 925–928.
[7] Richard E. Smith, **"*Authentication from Password to Public Key*"**, Addison Wesley, 2002.
[8] Yuliang Zheng, ***"Authenticated Public Key Encryption Schemes using Universal Hashing"***, IEEE P1363, 1996.
[9] X.-Y. Zhao, G. Chen, ***"Ergodic matrix in image encryption***", in: Proc. Second International Conference on Image and Graphics, Vol. 4875 of Proc. SPIE, 2002, pp. 394–401.
[10] د. وسيم الحمداني **"*انظمة التشفير*"** ,المكتبة العربية,1997.

طريقة مقترحة لتشفير النصوص باستخدام مفتاحين سريين ومعادلة رياضية سرية واحدة

م.م. قصي محمد جعفر السعدي
كلية الرافدين الجامعة
قسم هندسة اتصالات الحاسبات