SUBSTITUTION- SHIFTING- FOLDING CIPHER ALGORITHM WITH DYNAMIC SYMMETRIC ENCRYPTION KEY

Dr.NuhaJameel Ibrahim[1], Assist. Lecturer Farah TawfiqAbd El-Hussien[1]
[1]Computer Science department / University of Technology
Nuha_alzubedy@yahoo.com , farah.tawfiq@yahoo.com

ABSTRACT

In modern security models, cryptography plays a fundamental role in protecting data integrity and confidentiality in information systems. However, cryptography itself is subject to cryptanalysis attacks. To reduce the cryptanalysis attack risk Encryption/Decryption application is presents in this paper. Encryption involves several processes which is implemented in reverse order in decryption , this method ensure make hard to intruder to guess the true sequences to solve encrypted message .The algorithm involves substitution ,shifting , and folding , these process will be implemented in reverse order in decryption causes a confusion for intruder who does not know the right sequence of the algorithm. Encryption key is dynamic and generated independently for each text depending on the length of the message to be encrypted and Practical because there is no need to exchange encryption keys between sender and receiver cause the receiver knowing how to generate them. As a result, the proposed system diffusion is accomplished by using folding algorithm which rearrange the character of the message after encryption in such away that the frequency of characters will not be appear clearly. Confusion also is performed by using several keys for the same message each key should consist of 2 digits then each digit is used alone with single letter of plaintext then the remaining encryption keys used sequentially according to their generating sequence. For a small amount of data this algorithm will work very smoothly and quickly.

Keywords: Substitution cipher, shifting, folding Dynamic symmetric key.

خوارزمية تشفير الاستبدال و النقل و الطي مع مفتاح تشفير ديناميكي متماثل

المدرس الدكتور نهى جميل ابراهيم[١] ،المدرس المساعد فرح توفيق عبد الحسين[١]
[١]قسم علوم الحاسوب / الجامعة التكنولوجية ، بغداد ، العراق

الخلاصة

في النماذج الأمنية الحديثة،التشفير يلعب دور مهم في حماية سلامة وسرية البيانات في انظمة المعلومات، على أية حال ، التشفير نفسه خاضع لهجمات تحليل الشفرة ولتقليل خطرالهجوم طريقة مقترحة للتشفير و فك الشفرة تعرض في هذا البحث . عملية التشفير تتضمن مجموعة من الخطوات التي سوف يتم تطبيقها بتسلسل معكوس عند فك الشفرة ، بهذه الطريقة نضمن تصعيب تخمين تسلسل العمليات المتبعة في التشفير و فك الشفرة على أي دخيل يحاول كسرها . هذه الخوارزمية تتضمن عمليات الاحلال ، التحريك ، و الطوي ، حيث يتم تطبيقها بتسلسل معكوس عند فك الشفرة مما يسبب الارباك لأي دخيل لا يعرف التسلسل الصحيح للخوارزمية . مفتاح التشفير متغير و غير ثابت و يتم توليده بشكل مستقل لكل نص يراد تشفيره بالاعتماد على طول النص .كنتيجة،الانتشار في النظامِ المُقتَرَحِ يتحقق باستخدام طي الخوارزميةِ الذي يرتب احرف الرسالة بعد التشفير بحيث ترتيب الاحرف لا يظهر بشكل واضح. التشويش أيضاً ينجز باستخدام عدة مفاتيح لنفس الرسالة كل مفتاح يجِب أن يشمل رقمين و كل رقم يستخدم لوحده في الرسالة الواحدة وبقية مفاتيح التشفير تستخدم بتسلسل طبقاً لتسلسل التوليد.لكمية قليلة من البيانات الخوارزمية تعمل بسهولة وسرعة.

1. **Introduction And Related Work**

The cryptography in computer science is a method of transmit and save the data in such a way that only the people you know can read and understand for processing. It is a science of protecting information by encoding it into an unreadable format. The cryptography protect the information from un authorized persons. Most of the cryptography algorithm in computer science can be broken and the attacker detect the information if owns the time, wanting and sources[1].

The data encryption standard (DES) is a Feistel-type Substitution-Permutation The rounds number in the algorithm depends on the length of the key[2]. Another symmetric key encryption method is the TSFS algorithm, that is a symmetric-key algorithm using transposition and substitution techniques which are important in diffusion and confusion. This algorithm uses three keys and then widens into twelve sub-keys to give higher security, twelve rounds and two different keys in each round are used in this algorithm to increase the security[3].

2. **Generating encryption keyspace :**

In encryption process , some or all parameters is appointed by the secret key. The encryption and decryption algorithms use the same secret key. The modern cipher methods use different key for encryption and decryption, and one of them is placed in the public domain. This method called asymmetric key encryption, public key cryptography, etc[4].

For the proposed system generating encryption keys is the same in both sides sender and receiver and consist the following :

a. Encryption key is chosen depending on the length of the plaintext for example if the length is (20) characters then the first number larger than length and represent the root square of an integer in case of L= 20 then the first key = 25 .
b. number of encryption keys are generated by dividing the length of the plaintext by 2 , No. of key = length div 2.
c. encryption keys are set of numbers ,the distance between them is decided by choosing the first prime number less than length in this case its (17) .

example :

Length = 14
First encryption key = 16
no. of keys =14 div 2 = 7
set of encryption keys = (16, 29, 42 , 55 , 68 , 81, 94)

3. **Substitution Cipher**

The Substitution technique is the process of replacing one letter from the plaintext with another letter to produce the cipher text. Julius Caesar propose the simplest substitution cipher[5]. Caesar replace each alphabet letter

Network (SPN) cipher, specified in FIPS PUB 46. The DES algorithm uses a 56-bit key that can be broken by using brute-force methods, use a 16 cycle Feistel system, with an overall 56-bit key permuted into 16 48-bit subkeys, in each cycle [2]. Because of the key size, the DES considered unsecure where the key size too small[3]. Another encryption method is AES, it is a symmetric-key size can be works in high speed until on small devices. The AES provides high security because of the large block size and the long key size. AES uses 128 bit fixed block size andworks with 128, 192 and 256 bit keys,

from the plaintext with another letter shifted three places[6]. Another technique is mono-alphabetic Cipher uses the random substitution. The Polygram substitution cipher technique replace block of letter from plain text with another block to produce the cipher text depending on the key. Poly alphabetic Substitution method uses a set of related mono alphabetic substitution rules depending on the encryption key[7] .

The proposed algorithm uses substitution , shifting , folding and XOR function with dynamic key (in length and content) in order to increase the complexity on cryptanalysis process .

The Encryption is an efficient method in the data security. The Encryption process glossing the contextual of the plaintext where the cardinal information is retrieved through a decryption process only. The goal of the Encryption process is to protect the data from un authorized people. Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations[8].

4. **Folding**

The cipher text is represented in a matrix which has equal number of rows and columns ,folding transformation change onedata matrix elements with another to the same entered data. In folding, the data matrix is folded horizontally, vertically and diagonally. In the horizontal, the first row is replaced with the last row. In the vertical, the first column is replaced with the last column. In the diagonal the inner cells, the upper-left cell is replaced with the down-right cell and the upper-right cell with the down-left cell [2,3].

For the proposed system folding can be represented as following

5. **Diffusion and confusion**

If the frequency distribution is knew the plaintext message uses the known words, this information can be used in cryptography for braking the cipher algorithms. A cryptanalysis can use this information to break a cryptographic algorithm. If the statistical plaintext structure are dissipate this process called diffusion. The Data Encryption Standard (DES) use the permutations of the data to get the cipher text for achieving diffusion. The confusion process complicates the use of the key, although the statistic are known for the attacker, the conclusion of the key sill difficult. [10].

6. **Differential cryptanalysis**

The differential cryptanalysis uses highly probability for plaintext differences occurred and the differences in the last round of cipher. The plaintext attack can be selected by differential cryptanalysis, so that the attacker is able to choose the inputs and test the output for key driving[11].

7. **Proposed system algorithms :**

This section describe algorithms in encryption and decryption phases which consist key generation alg., encryption alg, folding alg.decryption alg.,and folding after decryption As follow:

Key generation algorithm :

Input :plaintext length (L)

Output : encryption keys

- Begin
- Compute plaintext length (L)
- Compute number of encryption keys (key space(n)) such that (no. of keys = L/2) if (L mod 2 <> 0) then (no. of keys = (L+1)/2)
- Compute k1 (first encryption key)
- Compute prime number (p) such that : p first prime number < L
- Generating encryption keys
- For I = 1 to n
- Compute $K_{i=} k_{i-1} + p$

- If $k_i < 99$ then goto 11
- $K_i = k_i$ div 11
- next
- End

Encryption algorithm :

Input: plaintext (P), key space (encryption keys), plaintext length (L), number of key space (N)

Output : ciphertext

- Begin
- Convert all the letters of p to ASCII then convert each on to binary
- For each encryption key :
- Separate numerical value into two digits such that :
- X_1 = ki div 10
- X_2 = ki mod 10
- Convert both X_1 and X_2 TO ASCII then to binary value
- Counter =0
- While i < L
- Compute C[i] = a[i] XOR X_1
- Increment Counter
- If counter mod 2 <> 0 then
  Shift left one bit with rotation
  Else
  Shift right one bit with rotation
  end if
- Compute C[i+1] = a[i+1] XOR X_2
- Increment Counter
- If counter mod 2 <> 0 then
  Shift left one bit with rotation
  Else
  Shift right one bit with rotation
  end if
- End
- End

Encryption process could be expressed as linear equation as follow:

$$Ci = \begin{cases} << (Pi \oplus Ki) \ , \ I \bmod 2 <> 0 \\ >> (Pi \oplus Ki) \ , \ I \bmod 2 = 0 \end{cases} \quad \text{..... (1)}$$

Where :
Pi = plaintext character
Ki = encryption key character
Ci = ciphertextcharacter
I = position

Folding Algorithm (after encryption)

Input : ciphertext

Output : folded ciphertext

- Begin
- Convert **ciphertext** to matrix such that row = column by addind stars"*" as much as needed.
- Exchange first row with last row
- Exchange first column with last column
- Exchange main diagonal with secondary diagonal
- End

Then the encrypted message will be sent as stream of characters.

Decryption algorithm

- Start
- Convert all the letters of C to ASCII then convert each on to binary
- For each encryption key :
- Separate numerical value into two digits such that :
- X_1 = ki div 10
- X_2 = ki mod 10
- Convert both X_1 and X_2 TO ASCII then to binary value
- Counter =0
- While i < L
- If counter mod 2 <> 0 then
  - Shift left one bit with rotation
  - Else
  - Shift right one bit with rotation
    end if
- C[i] = a[i] XOR X_1
- Increment Counter

- If counter mod 2 <> 0 then
  - Shift right one bit with rotation
  - Else
  - Shift left one bit with rotation
  - end if
- C[i+1] = a[i+1] XOR X_2
- Increment Counter
- End
- End

Encryption process could be expressed as linear equation as follow:

$$Pi = \begin{cases} (<<Ci,\ I \bmod 2 = 0) \oplus Ki \\ (>>Ci,\ I \bmod 2 <> 0\ ) \oplus Ki \end{cases} \quad \text{..... (2)}$$

Where :
Pi = plaintext character
Ki = encryption key character
Ci = ciphertextcharacter
I = position

Folding Algorithm (After Decryption)

Input :folded ciphertext
Output : ciphertext

- Begin
- Convert ciphertext to matrix
- Exchange main diagonal with secondary diagonal
- Exchange first column with last column
- Exchange first row with last row
- End

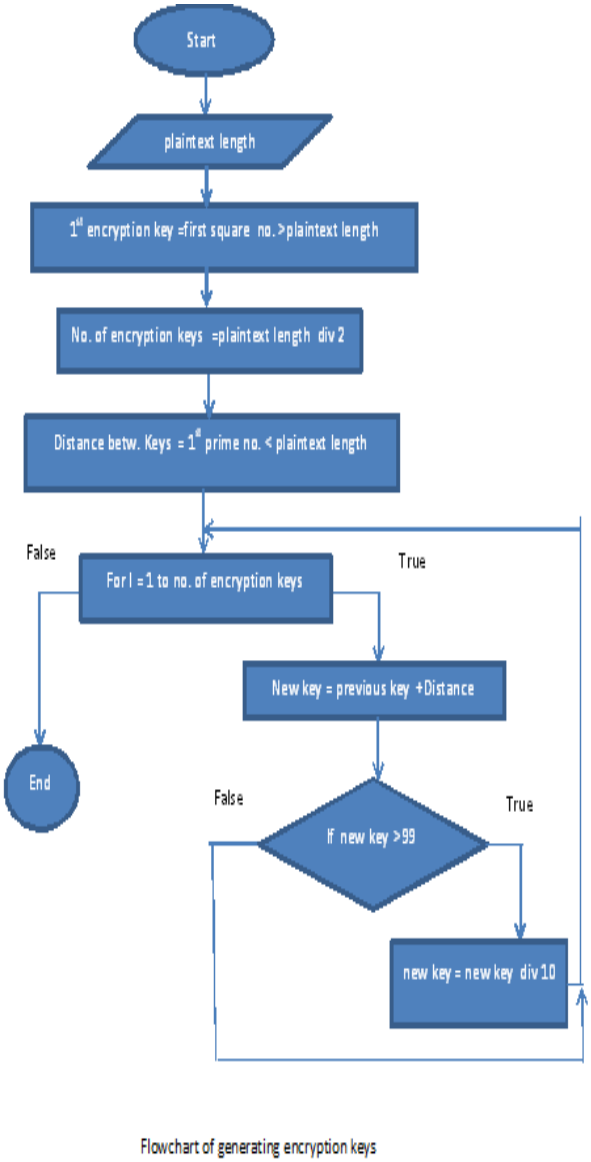


Fig No.(1) generating encryption key

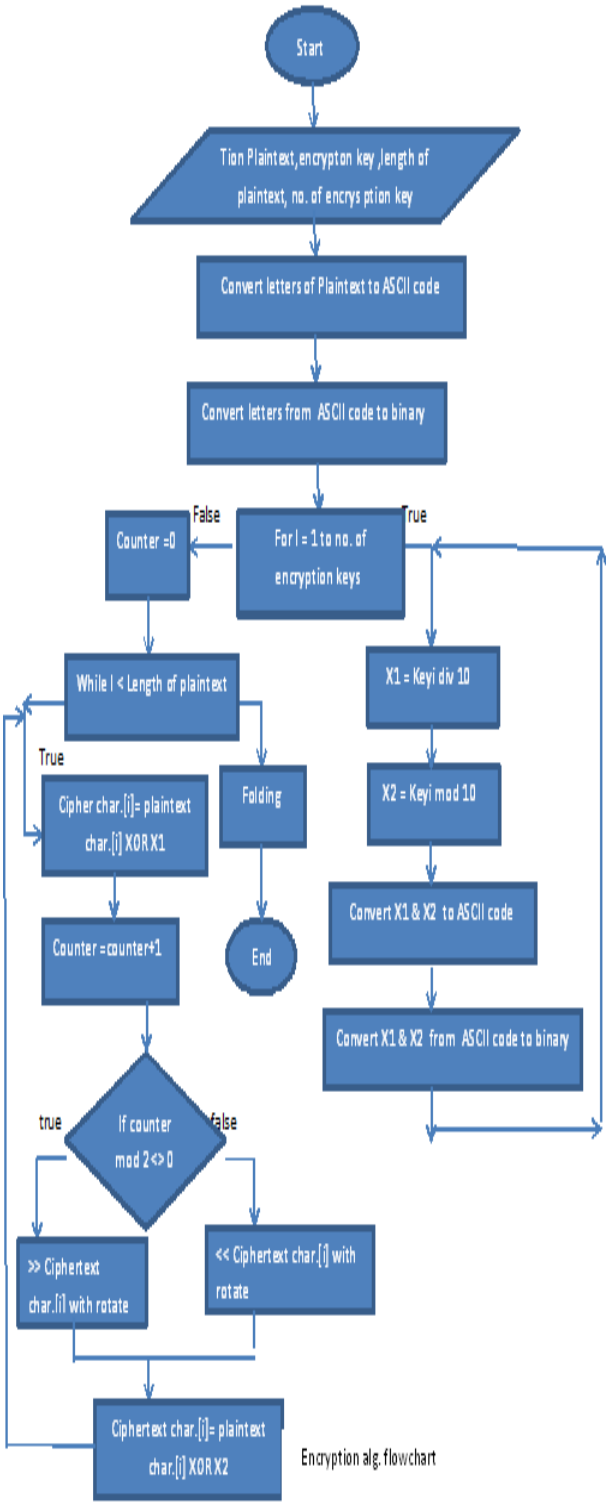
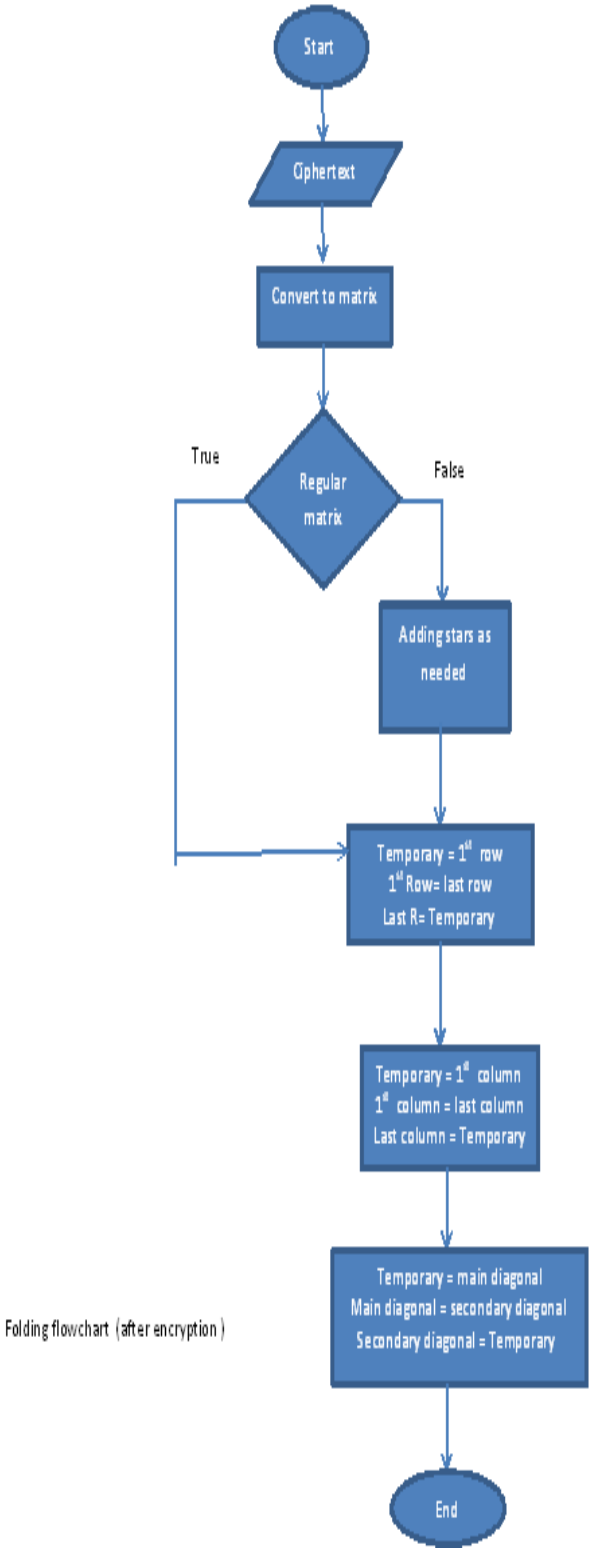


Fig No.(2) Encryption Alg.



Folding flowchart (after encryption)

Fig.(3) Folding Alg. After encryption

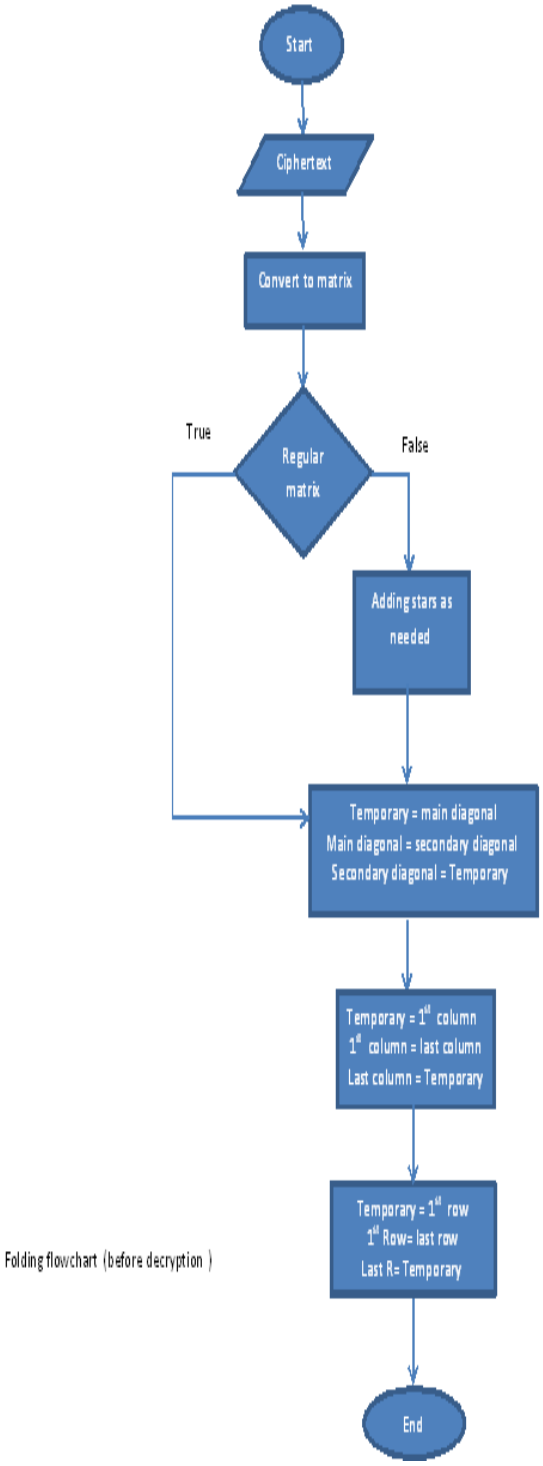


Fig.(4) Folding Alg. Before Decryption

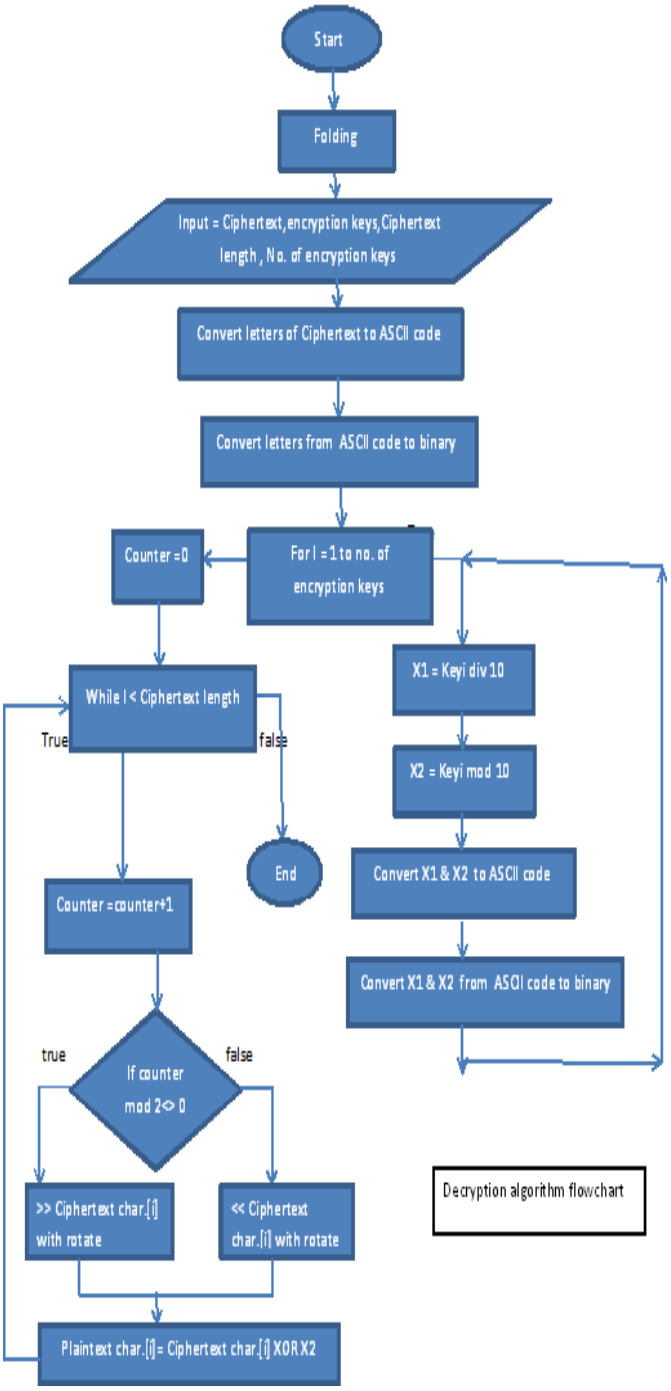


Fig.(5) Decryption Alg.

8 Experimental results:

8.1 Example of key generation

Table number (1) represent the way of generating key space for several messages of different lengths.

1	Message : I am fine needing your help			
	Length of text	**First key**	**Number of keys**	**Space between keys**
	22	25	22/2 =11	19
2	Message :go to the airport			
	Length of text	**First key**	**Number of keys**	**Space between keys**
	14	16	14/2=7	13
3	Message :submit your report to the boss			
	Length of text	**First key**	**Number of keys**	**Space between keys**
	26	36	26/2=13	23
4	Message : the first date should be secret and amaze			
	Length of text	**First key**	**Number of keys**	**Space between keys**
	34	36	17	31

Table no. (1) The way of generating key space

For example number 1 encryption keys will be generated as follows:
K1 = 25
K2= 25 + 19 =44
K3 =44 + 19 = 63
K4= 63 + 19 = 82
K5 = 82 +19 = 101 div 10 = 10
K6 = 101 +19= 120 div 10 = 12
K7= 120+19=139 div 10 = 13
K8 = 139+19=158 div 10 = 15
K9= 158 + 19= 177 div 10 =17
K10= 177 +19=196 div 10 = 19
K11= 196+19=215 div 10 =21

For example number 2 encryption keys will be generated as follows:
K1 = 16
K2= 16 + 13 = 29
K3 =29 + 13 = 42
K4= 42 + 13 = 55
K5 = 55 + 13 = 68
K6 = 68 + 13 = 81
K7= 81 + 13 = 94

For example number 3 encryption keys will be generated as follows:
K1 = 36
K2= 36 + 23 = 59
K3 =59 + 23 = 82
K4= 82 + 23 = 105 div 10 = 10
K5 = 105 + 23 =128 div 10 = 12
K6 = 128 + 23 = 151 div 10 = 15
K7= 151 + 23 = 174 div 10 = 17
K8 = 174 +23=197 div 10 = 19
K9= 197 + 23= 220 div 10 =22
K10= 220 +23=243 div 10 = 24
K11= 243+23=266 div 10 =26
K12= 266 + 23 = 289 div 10 = 28
K13 = 289 + 23 = 312 div 10 = 31

For example number 4 encryption keys will be generated as follows:
K1 = 36
K2= 36+31 = 67
K3 = 67 + 31 = 98
K4= 98+ 31= 129 div 10 =12
K5 = 129 +31 = 160 div 10 = 16
K6 = 160 +31= 191 div 10 = 19
K7= 191+31=222 div 10 = 22
K8 = 222+31=253 div 10 = 25
K9= 253 + 31= 284 div 10 =28
K10= 284 +31=315 div 10 = 31
K11= 315+31=346 div 10 =34
K12= 346+31=377 div 10 =37
K13 = 377 + 31 = 408 div 10 = 40

K14 = 408 + 31 = 439 div 10 = 43
K15 = 439 + 31 = 470 div 10 = 47
K16 = 470 + 31 = 501 div 10 = 50
K17 = 501 + 31 = 532 div 10 = 53

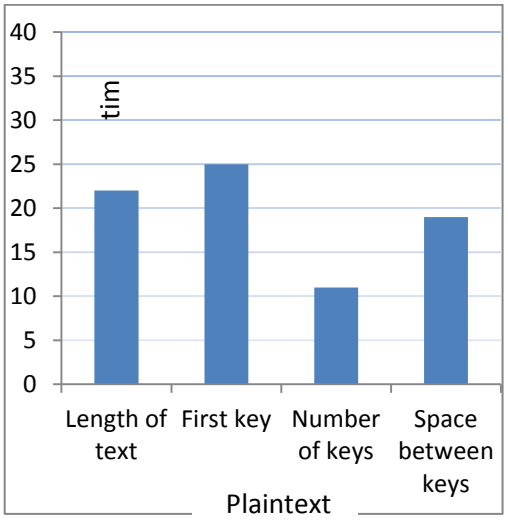


Fig no.(6)encryption keys for the message "I am fine needing your help"

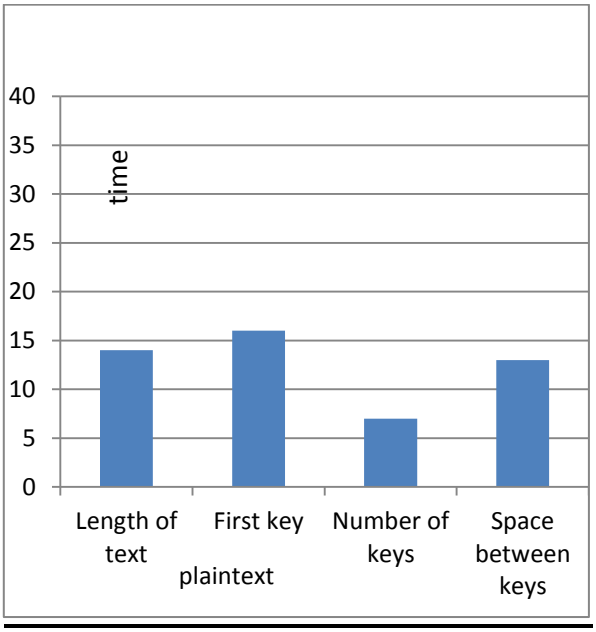


Fig. no.(7)encryption keys for the message "go to the airport"

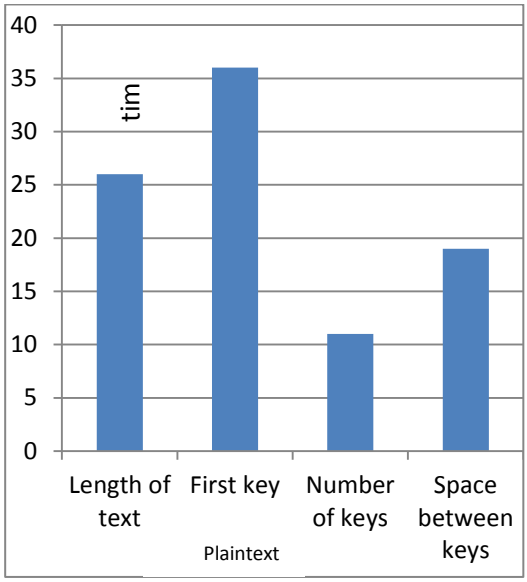


Fig. no.(8)encryption keys for the message "submit your report to the boss"

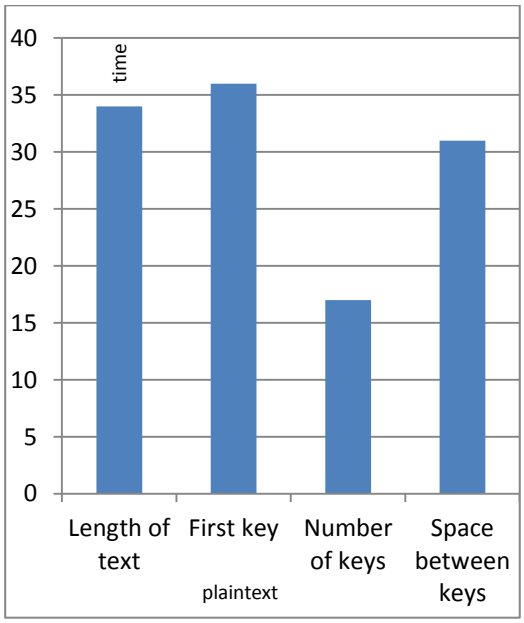


Fig no.(9)encryption keys for the message "the first date should be secret and amaze"

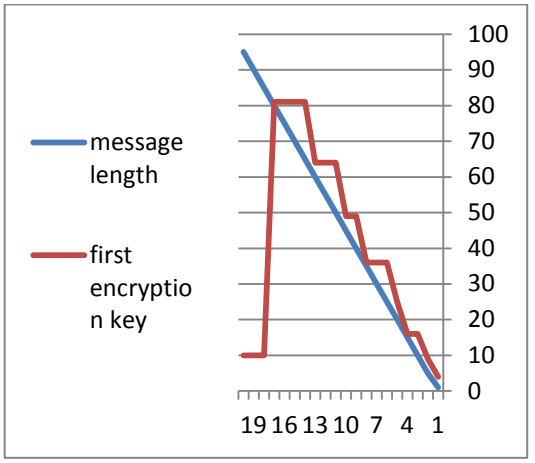


Fig. no.(10) comparing the value of first encryption key according to the message length

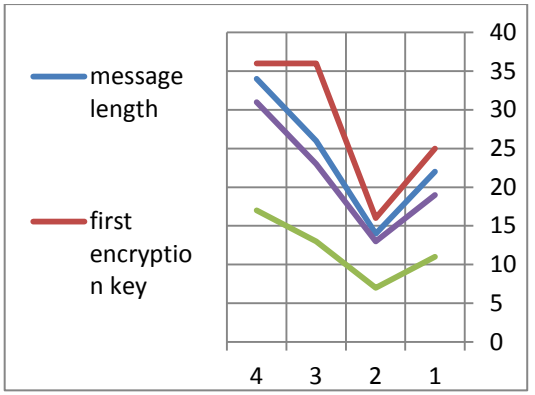


Fig no.(11) showing the distribution values of encryption keys according to table no.(1)

Example no.	Key generation	Ciphering time	Folding process	Total time
1.	10	12	15	37
2.	8	9	13	30
3.	10	12	15	37
4.	12	14	16	42

Table no.(2) Ciphering time requirement in meliseconds for examples in table no.(1)

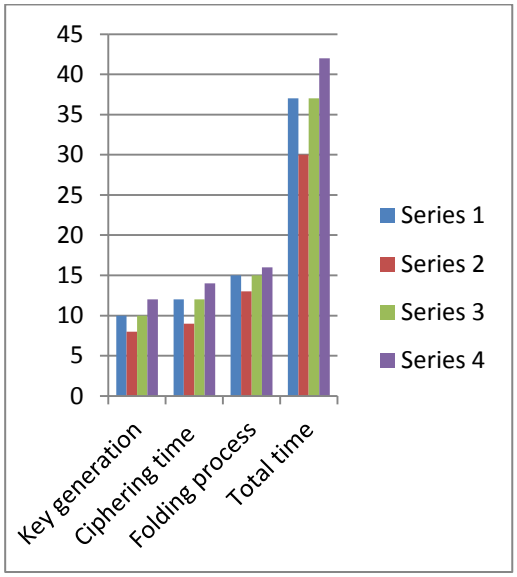


Fig no.(12) Ciphering time requirement in seconds for examples in table no.(1)

9.2 Example of encryption :

The following message should be encrypted " GO TO THE AIRPORT "

- Choosing encryption key : the first encryption key larger than text length is (16) then first key (K1 =16) which has root square = 4 then the matrix which is used to represent the text for folding process is 4*4 matrix .
- number of encryption keys= length of text (L) / 2 = 7 keys , if the length of the key is 3 character then L/ 3 the number that dividing (L) = length of the first key .
- the rest of the keys are generated by deciding the first prime number smaller than (L) in this case its (13) then the next keys are :

K2 = K1+ 13 = 16 +13 = 29

K3 = K2 + 13 = 29 + 13 = 42

K4 = K3+ 13 = 42 +13 = 55

K5 = K4 + 13 = 55 + 13 = 68

K6 = K5+ 13 = 68 +13 = 81

K7 = K6 + 13 = 81 + 13 = 94

- If the (L) is odd then for example 15 when dividing by 2 the result will be fractions

No. keys = 7.5 = 8

- convert to ASCII code then to binary

G= 71 $_{ASCIIcode}$=01000111_2

1= 49 $_{ASCIIcode}$ = 00110001_2

-XOR

G = 01000111

1 = 00110001 XOR

01110110

-Shifting

G position in the text is odd Then :

01110110 = 00111011 = 59 = " ; " = cipher text character , G = ;

- O = 79 = 0100 1111 XOR

6 = 54 = 0011 0110

01111001

since O position in the text is even then shift right with Rotation

01111001 = 11110010 = 242 = ò

O = ò

- T = 48 = 01010100 XOR

2 = 50 = 00110010

01100110 =

00110011= 51 = 3 odd shift left with rotation

T = 3

- O = 79 = 0100 1111 XOR

9 = 57 = 00111001

0 1110110

= 11101100= 236 = ì even shift right with rotation

O = ì

- T = 48 = 01010100 XOR

4 = 52 = 00110100

01100000

= 00110000 = 48 = 0 odd shift left with rotation

- H = 72 = 0100 1000 XOR

2 = 50 = 00110010

01111010 = 11110100 =

244 =ô

even shift right with rotation

H = ô

- E = 69 = 01000101 XOR

5 = 53 = 00110101

01110000 =

00111000 = 56 = 8

E = 8

And so on , so the result of encryption is

GO TO THE AIRPORT = ; ò 3 ì 0 ô8 è¿ Ô4 üµ À

- Folding

The result of encryption is converted to an equal matrix in this case a 4*4 matrix has been choosing , L of the text = 14 which means that the last two position of the matrix

will be empty to solve this proplem always the remaining empty positions are filled with stars "*" as many as needed

;ò 3 ì
0 ô8 è
¿ Ô4 ü
µ À**

→ the first row with the last one →

µ À**
0 ô8 è
¿ Ô4 ü
;ò 3 ì

the first column withthe last one →

* À* µ
è ô80
ü Ô4¿
ì ò3;

→ the inner diagonal with outer one →

µÀ**
è8ô0
ü4Ô¿
;ò3ì

the result is = " µ À ** è 8ô 0 ü 4Ô¿ ; ò3 ì"

9.3 Example of decryption process:

For the previous cipher text getting the original text as follows :

- Representing in matrix and folding

µÀ**
è8ô0
ü4Ô¿
;ò3ì

→ the inner diagonal with outer one →

* À* µ
è ô80
ü Ô4¿
ì ò3;

the first column with the last one →

µ À**
0 ô8 è
¿ Ô4 ü
;ò 3 ì

→ the first row with the last one →

;ò 3 ì
0 ô8 è
¿ Ô4 ü
µ À**

The cipher text is = " ; ò 3 ì 0 ô8 è¿ Ô4 üµ À**"
deleting stars =" ; ò 3 ì 0 ô8 è¿ Ô4 üµ À "

- Converting to ascii code then to binary then XOR with the keys

; = 59 = 00111011=
01110110 ,

Since position is odd then shift right with rotation

01110110
1 = 00110001 XOR

01000111 = 71 = G

ò= 242 = 11110010 =01111001,

Since position is even then shift left with rotation

01111001
6 = 54 = 0011 0110 XOR

0100 1111 = 79 = O ,
and so on for the rest of the cipher text

10 The Proposed System Limitations:

1) The encryption keys length for each one should not exceeding two digits which means that first encryption keys values would be limited between square of (2) and square of (9) and the difference will be in the values of key spaces depending on the length of the message .
2) In folding process when adding stars to perform a matrix such that row=column at the receiver side these stars should be removed and one or more of them could be of the original encrypted text which may affect on choosing the value of first encryption key.
3) The proposed system is perfect for small texts that not

exceeding 99 characters thus if the text is longer it should be portioning for more than one message to be sent .

11 .Comparison between the proposed system and one time pad system

Table (3) comparisonwith one time pad system

Sq	One time pad system	Proposed system
1.	Each key works only once	First encryption key may work with different texts of different sizes
2.	Works with fixed length messages	Works with different length messages
3.	Key length = message length	Generation of encryption keys depends on message length
4.	Not very practical	Practical because there is no need to exchange encryption keys between sender and receiver cause the receiver knowing how to generate them

12 Conclusions:

1. For the proposed system diffusion is accomplished by using folding algorithm which rearrange the character of the message after encryption in such away that the frequency of characters will not be appear clearly (hiding the statistical features of the encrypted message). Also for each message there will be several encryption keys such that encountering them depends on the length of each message then generating the remaining encryption keys.

2. Confusion is performed by using several keys for the same message each key should consist of 2 digits then each digit is used alone with single letter of plaintext then the remaining encryption keys used sequentially according to their generating sequence .

3. For the proposed system it will be strong against Differential cryptanalysis

13 References

[1] Kak Avi, "**Classical Encryption Techniques** ", January 12, 2017

[2] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani***,"New Comparative Study Between DES, 3DES and AES within Nine Factors"***, JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010,

[3] Hanan A. Al-Souly, Abeer S. Al-Sheddi, Heba A. Kurdi , " **Lightweight Symmetric Encryption Algorithm for Secure Database**", (IJACSA),Special Issue on Extended Papers from Science and Information Conference 2013.

[4] Rizza J. M. ,"**Computer Network Security**", 2005.

[5] Zaeniah, Bambang Eka Purnama, **"AN Analysis Of Encryption And Decryption Application By Using One Time Pad Algorithm "**, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, 2015

[6] AtulKahate, **"Cryptography and Network Security"**, Second Edition, Tata McGraw-Hill Edition 2008.

[7]Sourabh Singh1, Anurag Jain2**,** "**An Enhanced Text to Image Encryption Technique using RGB Substitution and AES**", *International Journal of Engineering Trends and Technology (IJETT)* - Volume4Issue5- May 2013.

[8] Majdi Al-qdah, Lin Yi Hui**,"** ***Simple Encryption/Decryption Application",International Journal of Computer Science and Security***, Volume (1) : Issue (1), 2008 .

[9] Kenneth Haugland , " **Finding prime numbers** ",14 Mar 2013 .

[10] William Stallings, "***Cryptography and Network Security***",3rd Edition, Prentice Hall, 2003.

[11] Howard M. Heys," **A Tutorial on Linear and Differential Cryptanalysis**",Electrical and Computer Engineering Faculty of Engineering and Applied Science Memorial University of Newfoundland, Canada,2006.