ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 8 , August 2017

Cryptosystem Using New Strategy for Generating Key

Saad AbdualAzize. Al_ani,Zaid AbassFadahl Al-haboobi

Associate prof. Dr.,Department of Computer Science,Al_Mamon University College, Baghdad, Iraq
Assistant Lecturer, Department of Computer Science, Baghdad College of Economic Science University, Baghdad, Iraq

ABSTRACT: Data security and transmission methods became an essential aspects with the vast improvements in communications technology. Cryptography is one of the most important methods used to secure data and information to prevent hacking on both private and public networks; this paper produce a new cryptosystem depends on generating random numbers, select a magic square to create a key;the plain text encrypted with the initial key then a logical XOR gate will be used to generate a new key; then GF (2^8) function will be used to create another key; so three keys are used with each plaintext to produce cipher text.

KEYWORD: Random number, Magic square, Vernam, GF (2^8), logicalXOR

I. INTRODUCTION

During last decade, there has been increasing dependence of both organizations and individuals on computing systems and public internet for business applications and social networking. While this dependence has enhanced the operational efficiency and ease of communications, the security associated with the exchange of information has become crucial. [1]

During the last two decades, the public internet and computers have revolutionized our life styles, business styles, modes of our social interactions, education and entertainment. This change also saw emergence of new set adversaries who are now constant threat to secure communications and information infrastructure essential for change life styles [2].

Ciphers are arguably the corner stone of cryptography. In general, a cipher is simply just a set of steps (an algorithm) for performing both an encryption, and the corresponding decryption [3].

The impressive challenge the data that approved and stored over the network is make these data being protection and disclosed to illegitimate users. And the use of computer networks - particularly during the last decade – has grown significantly. For this reason, create and build up the security systems and encryption techniques should take large focus in the field of information security [4].

II. PSEUDO – RANDOM NUMBER

Pseudo-random number generators (PRNGs) are algorithms that can mechanically generate alarge runs of numbers with excellent random properties but ultimately the sequence repeats (or the memory usage grows without bound). The string of values generated by such algorithms is normally determined by a fixed number called a seed. One of the most common PRNG is the linear congenital generator, which uses the repetition

$$X_{n+1} = (aX_n + b) \bmod m$$

To generate numbers. The maximum number of numbers the formula can produce is the modulus, m.What makes this technique interesting is its ease of implementation.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 8 , August 2017

III. MAGIC SQUARE

Calculate the magic constant by:

The magic constant = [n * (n2 + 1)] / 2,

Wheren = the number of boxes per side. [5]

IV. VERNAM CIPHER

As an article on cryptography that outlines the use of the Vernam Cipher to encrypt text by hand; the Vernam Cipher is the only known method of encryption that is proven to be unbreakable when implemented/used correctly.[6]

In simple terms, each character from a text, known as plaintext, is encrypted by modular arithmetic with a character from a secret random key of the same length as a plaintext. What results is a cipher text. If the key is truly random and as large as the original text and has never been used then the cipher text will be impossible to decrypt without knowing the key.[7]

V. PROPOSED WORK

The proposed method has two parts: encryption and decryption; the encryption part has two phases and three functions, as follows:

Encryption Algorithm

Phaseone: plain text

1- Convert the plain text to equivalent sequence number depending on table 1.

2- Arrange the first (d,d) number in a matrix **pm1**(d,d).

Phase two: generate key

1-Use the equation $X_{n-1} = (aX + b) \bmod m$ to generate **m** number (a,b,m seed number)

2-Select a number from m to satisfy magic square equation to generate key1(d,d).

Where magic square equation:[n * (n^2 + 1)] / 2], where n = the number of elements per side.

3- Rotate counter clock wise the matrix to get key2.

4-Shift each row in key2 to get key3.

F1 function

- For the first elements of **pm1** and **key1** , separate tens from individuals as :
  - Ten_imp1 = pm1/10
  - Indv_mp1 = pm1 mod 10

  - Ten_key1 = pm1/10
  - Indv_ket1 = pm1 mod 10

- Apply Vernam mod 10 on both.
  - Vten = (ten_mp1 + ten_key1) mod 10
  - Vindv = (indv_mp1 + indv_key1) mod 10
- Concatenate to get pm2 = concatenate (vten ,vindv)

F2 function

- Take the first element of pm2 and key2, separate ten from individual (ten_mp2, individual _mp2 and ten_key2, individual _key2).
- Convert each to 4-bits (bin1-mp2 ,bin2-mp2,bin3-mp2,bin3-mp2 and bin1-key2 ,bin2-key2,bin3-key2,bin3-key2)
- Apply logical XOR on binary bits like the following :
  Bmp3= mp2(bin1…bin4) $\oplus$key(bin1…bin4)
  t-mp3= bin-mp3 (1:4) D1-mp3 =decimal(t-mp3)
  I-mp3= bin-mp3 (5:8) D2-mp3 =decimal (I-mp3)
  Mp3= concatenate (D1-mp3, D2-mp3)

F3- function

For each element from both (mp3 and key3) apply the following:

- Produce a polynomial of power x using GF(8)
- Apply XOR between both polynomials.
- Convert the result to binary then decimal.
- Repeat (1) on all the elements of mp3 and key3 to get the cipher text (mp4).

char	code	Char	code	char	Code	char	Code
0	0	A	10	K	20	U	30
1	1	B	11	L	21	V	31
2	2	C	12	M	22	W	32
3	3	D	13	N	23	X	33
4	4	E	14	O	24	Y	34
5	5	F	15	P	25	Z	35
6	6	G	16	Q	26		
7	7	H	17	R	27		
8	8	I	18	S	28		
9	9	J	19	T	29		

Table 1: weight of the character

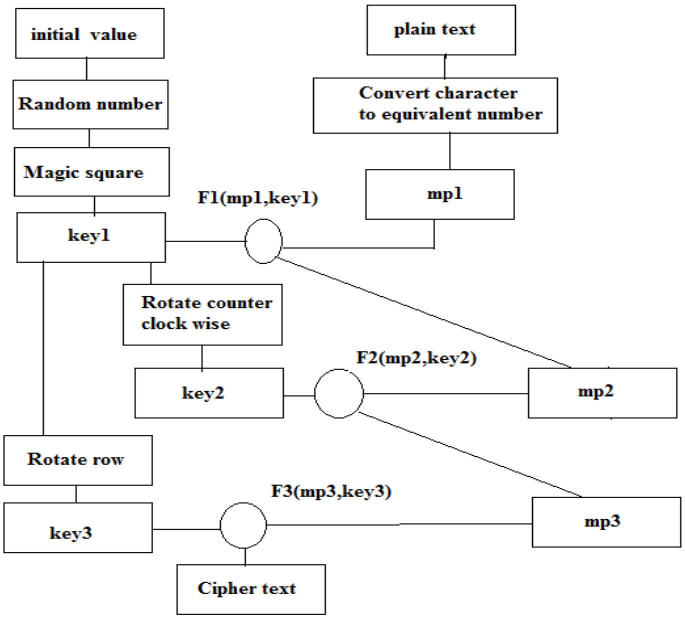
Encryption

1- Apply phase one
2- Apply key generation
3- Apply F1 function
4- Apply F2 function
5- Apply F3 function

Decryption

1- Apply key generation
2- Apply F3 function
3- Apply F2 function
4- Apply F1 function

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 8 , August 2017



Flow chart for key generation and encryption

VI. IMPLEMENTATION AND RESULTS

1- Plain text =”Most public key cryptographic “
2- Convert the plain text to equivalent sequence number

Char	Char	Char	Char	char	Char
M=22	P=25	I=18	Y=34	P=25	R=27
O=24	U=30	C=12	C=12	T=29	A=10
S=28	B=11	K=20	R=27	O=24	P=25
T=29	L=21	E=14	Y=34	G=16	H=17

3- mp

22	25	18	34
24	30	12	12
28	11	20	27
29	21	14	34

4- The equation $\boldsymbol{X_{n-1} = (aX + b) mod\ m}$ arrange number randomly
X_0=3, a= 3, b=3, m=31
X=1,6,21,4,15,17,23,10,2,9,30,0,3,12,8,27,22,7,24,13,11,5,18,26,29,19,28,25,16,20
5- To find the magic constant = [n * (n^2 + 1)] / 2
Mc=[3*(3^2 +1)]/2 =[3*10]/2=15

8	1	6
3	5	7
4	9	2

Magic square

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 8 , August 2017

6- Apply Vernam mod 10 (between mp1 and key1).

22	29	11
24	25	21
28	30	18

Mp1

8	1	6
3	5	7
4	9	2

Key1

08 + 22= 2 ,10 mod 10 =0== 20
01 + 29 = 2 , 10 mod 10 = 0== 20
06 + 11= 1 , 7 mod 10 = 7 == 17
03 +24 = 2 , 7 mod 10 = 7 == 27

05+25 = 2, 10 mod 10 =0 ==20
07+ 21= 2,8 mod 10 = 8 == 28
04 + 28= 2 , 12 mod 10 =22
09 + 30 = 3, 9 mod 10 = 39
02 + 18 = 1 , 10 mod 10 = 0 ==10

7- Xor key2 with mp2

01	06	07
08	05	02
03	04	09

Key2

20	20	17
27	20	28
22	39	10

mp2

01 ⊕20= 00000001⊕ 00100000=00100001=21
06 ⊕ 20=26
07 ⊕ 17 =10

08 ⊕ 27 = 23
05 ⊕ 20 =25
02 ⊕ 28 =2A
03⊕ 22 = 21
04 ⊕ 39 =3D
09 ⊕ 10 =19

8- Apply XOR between both polynomials

21	26	10
23	25	2A
21	3D	19

mp3

01	06	08
05	07	03
09	04	02

Key3

21+ 01 = x^5 +1 ⊕1 = x^5=10
26+ 06 = x^5 +x^2 +x ⊕ x^2 + x = x^5=20
10 + 08 = x^4⊕ x^3= x^4 + x^3=18
23+05 = x^5 + x +1 ⊕ x^2 + 1 = x^5 + x^2 +x =23
25+07 = x^5 + x^2 +1 ⊕ x^2 + x +1 = x^5 + x=22

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 8 , August 2017

$2A + 03 = x^5 + x^3 + x \oplus x+1 = x^5 + x^3 + 1=29$
$21+09 = x^5 + 1 \oplus x3 +1 = x^5 + x^3=28$
$3D + 04 = x^5 + x^4 + x^3 + x^2 +1 \oplus x^2 = = x^5 + x^4 + x^3 +1 =39$
$19 + 02 = x^4 + x^3 + 1 \oplus x = = x^4 + x^3 + x + 1 =2B$

10	20	18
23	22	29
28	39	2B

Cipher text

After applying the encryption process to the whole plain text, a cipher text is produced and send to the receiver;the receiver will apply the decryption process and retrieve the original plaintext.

VII. CONCLUSION

The proposed method uses many powerful functions in a new way that make a full use of the strength points of each function; random function give a sequence of random numbers which maximize the complexity of the proposed method; also the use of magic square and module function, all that increase the complexity and robustness of the proposed method. Using XOR function was useful in keeping the number of 1's and 0's fairly distributed. With all the strength previous points, simplicity was preserved by using Vernum encryption method.

REFERENCES

[1]. Alexander Stanoyevitch, "INTRODUCTION TO CRYPTOGRAPHY WITH MATHEMATICAL FOUNDATIONS AND COMPUTER IMPLEMENTATIONS", California State University Carson, California, U.S.A.
[2]. William Stallings, Prentice Hall, "CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE FIFTH EDITION". FIFTH EDITION 2011.
[3]. Behrouz A.Forouzan,"Cryptography and Network security", Publishing Company Limited. McGraw-Hill Education, 2007.
[4]. Rob Curley, “Cryptography: Cracking Codes”, Britannica Educational Publishing, Jun, 2013.
[5]. B. Raman, "Cryptography & Network Security," *IIT Kanpur, May*, 2005.
[6]. A. Kahate, *Cryptography and network security*: Tata McGraw-Hill, Education, 2013.
[7]. Y. Dodis, *et al.*, "Security analysis of pseudo-random number generators with input: /dev/random is not robust," in *Proceedings of the 2013ACM SIGSAC conference on Computer & communications security*, 2013, pp. 647-658.
[8]. M. François, *et al.*, "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science and Numerical Simulation,* vol. 19, pp. 887-895, 2014.
[9]. M. Beck and A. Van Herick, "Enumeration of 4× 4 magic squares," *Mathematics of Computation,* vol. 80, pp. 617-621, 2011.
[10]. U. E. Standard, "Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition method, Satyaki Roy, NavajitMaitra, JoyshreeNath, Shalabh Agarwal and AsokeNath," in Proceedings of IEEE sponsored National Conference on Recent Advances in Communication, Control and Computing Technology-RACCCT, 2012, pp. 29-30.
[11]. S. Dey, *et al.*, "An Integrated Symmetric Key Cryptographic Method-Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation and Reversal Method: SJA Algorithm," International Journal of Modern Education and Computer Science, vol. 4, p. 1, 2012.
[12]. F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE transactions on information forensics and security,* vol. 6, pp. 307-322, 2011.