International Journal For Technological Research In Engineering
Volume 1, Issue 10, June-2014 *ISSN (Online): 2347 - 4718*

A MODIFIED VERSION OF POLYBIUS CIPHER USING MAGIC SQUARE AND WESTERN MUSIC NOTES

Moumita Maity
Department of Computer Science, Vidyasagar University
West Bengal, India.

Abstract: Polybius square is a simple monoalphabetic substitution cipher for fractionating plaintext characters so that they can be represented by a smaller set of symbols. Here, in this paper, a modified version of Polybius cipher is designed using magic square and western music notes. In recreation mathematics, magic square has huge application in mathematical puzzles and games. An N order magic square is NxN square grid of distinct numbers, usually integers, where the numbers in each row, and in each column, and the numbers in the forward and backward main diagonals, all add up to the same number. As magic square has applications in puzzles, here this concept is applied to cryptography. Use of music is not very common in cryptography, music notes is used here for substitution. Here, a 6x6 normal magic square is used to achieve the design along with increasing C major scale C–D–E–F–G–A–B.

Keywords: Encryption, decryption, magic square, music notes, plain text, cipher text

I. INTRODUCTION

Cryptography is all about constructing techniques for secure communication in the presence of third parties. It is the art of protecting information, which is called plaintext, by encrypting it in to a meaningless or unreadable format called cipher text. The reverse process of converting cipher text into a plain text is called decryption. In the process of encryption and decryption, keys and algorithms are involved. [1] Cryptography can be classified into three main categories: Symmetric key ciphers, Asymmetric key ciphers and Cryptographic protocols. [1][2] A symmetric key cipher (also known as shared-key cipher) is one that uses the same (necessarily secret) key to encrypt messages as it does to decrypt messages. Until the invention of asymmetric key cryptography all ciphers were symmetric. Each party to the communication needed a key to encrypt a message; and a recipient needed a copy of the same key to decrypt the message. Asymmetric key ciphers are the one in which encryption and decryption is performed using the different keys: a public key and a private key. It is also known as public-key encryption. Cryptographic protocols deal with the application of cryptographic algorithms. Symmetric and asymmetric algorithms are the building blocks with which applications such as secure internet communication can be established. All Cryptographic algorithms are based on two general principles: [3]

- substitution, in which each element in the plaintext (bit, letter, and group of bits or letters) is mapped into another element and
- Transposition, the elements of the plaintext have simply been re-arranged in different order; their position with relation to each other has been changed.

Magic square has huge application in recreation mathematics like puzzles. So, it also can be applied in cryptography. Here, a modified Polybius square is designed with the help of magic square to change the arrangements of characters. As an order 6 square is taken, it can represent 36 characters. Alphanumeric characters A-Z 0-9 (total 36) can be encrypted in this system in the place of 25 characters of original Polybius square. The normal magic square is used to place all 36 alphanumeric characters in order, according to the arrangements of integers in the magic grid and make them ready for substitution. As it is a grid, rows and columns are indexed with names and each cell is identified by its row and column index. Here the name of rows and columns act as substitution code. So, the character in each cell is substituted by its index. Music notes are used here for indexing rows and columns. As alphanumeric characters A-Z 0-9 can be encrypted, this system can be used for encrypting small text based data.

II. MATERIALS AND METHODS

In this section, a brief introduction is provided on Polybius cipher, western music notes and magic square those are used to design the proposed system.

A. Polybius Cipher

Polybius cipher is a basic form of encryption invented by the ancient Greek historian Polybius in the second century B.C. It is based on fractionating plaintext characters so they can be represented by a smaller set of symbols. In the Polybius cipher, all the letters of the alphabet are written in a 5×5 square, where each letter is identified by its row and column. Encryption is done by replacing each plain letter with its coordinates in the Polybius square. As there are 26 alphabets, I and J placed in one cell to cut down the number to 25.[4]

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fig. 1: Polybius Cipher

Here, every characters is reduced to a pair of digits, like A = 11, X= 53.
For example: Plain text MESSAGE can be encrypted to: 32 15 43 43 11 22 15
Even though the cipher consists of numbers, it can be easily broken.

B. Western Music Notes

In music, the term note means a sign used in musical notation to represent the relative duration and pitch of a sound or pitched sound itself. In traditional music, pitch classes are typically represented by the first seven letters of the Latin alphabet (A, B, C, D, E, F and G). [5]
A scale is any set of musical notes ordered by fundamental frequency or pitch. A scale ordered by increasing pitch is an ascending scale, while descending scales are ordered by decreasing pitch.
For instance, the increasing C major scale is C–D–E–F–G–A–B–[C], with the bracket indicating that the last note is an octave higher than the first note.
Here heptatonic (i.e. 7 notes per octave) increasing C major scale C–D–E–F–G–A–B is used for encryption. [6][7]

C. Magic Square

A magic square is an arrangement of distinct numbers in such way that the numbers in each row, column, and main diagonals, all sum up to the same number, a constant which is called the magic constant or magic sum. Magic squares exist for all values of *n*, with only one exception of order 2.[8][9]

8	1	6	15
3	5	7	15
4	9	2	15
15	15	15	15

Fig. 2: 3x3 Magic square with the magic sum of rows, columns and diagonals

Magic squares can be classified into three types:

- Odd – 3x3, 5x5 etc
- Doubly even (*order 4n*) – 4x4, 8x8 etc
- Singly even (*order 4n+2*) – 6x6, 14x14 etc

Odd and doubly even magic squares are easy to generate. The construction of singly even magic squares is more difficult but several methods exist, including the LUX method, the method of Strachey and Medjig method. [8][9]
A normal magic square means if it is a NxN square then its values are 1 to N^2.

D. Medjig Method To Construct 6x6 Magic Square:

This method is based on a 2006 published mathematical game called medjig by Willem Barink. [8]. The medjig method of constructing a magic square of order 6 is as follows: [8] [10]
1. Take any 3 × 3 magic square

2	9	4
7	5	3
6	1	8

Fig. 3: 3X3 Magic square

2. Divide each of its squares into four quadrants, on which the numbers 0, 1, 2 and 3 are placed in all sequences but with a particular sequence to make all rows, columns and diagonals sum up to make 9

2	3	0	2	0	2
1	0	3	1	3	1
3	1	1	2	2	0
0	2	0	3	3	1
3	2	2	0	0	2
0	1	3	1	1	3

Fig. 4: Medjig square

3. Fill these quadrants by $x+9y$, where x is the original number from 3x3 magic square and y is a number from 0 to 3, following the pattern of the medjig-square.

20	29	9	27	4	22
11	2	36	18	31	13
34	16	14	23	21	3
7	25	5	32	30	12
33	24	19	1	8	26
6	15	28	10	17	35

Fig. 5: 6x6 Magic square

III. PROPOSED ENCRYPTION METHODOLOGY

In the proposed system a unique 6x6 magic square and heptatonic increasing C major scale C–D–E–F–G–A–B is used for encryption. First any unique 6x6 normal magic square is taken which is arranged with integers from 1 to 36. Next all the alphanumeric characters are placed like this: as A is first letter, it is placed in cell with digit 1, second letter B in the cell with digit 2 and so on. A-Z is placed in the cell numbered 1 to 26. Likewise 0-9 is placed in cell with number 27 to 36 respectively. As music notes are used for substitution, all 6 rows of square are marked with notes C–D–E–F–G–A like row1 as C, row2 as D and so on. All columns are also followed the same sequence of notes. B is not used in square substitution. It is left for denoting space between two words and end marker. Now each cell is indexed with row name and column name.

	C	D	E	F	G	A
C	26 Z	35 8	1 A	19 S	6 F	24 X
D	17 Q	8 H	28 1	10 J	33 6	15 O
E	30 3	12 L	14 N	23 W	25 Y	7 G
F	3 C	21 U	5 E	32 5	34 7	16 P

G	31 4	22 V	27 0	9 I	2 B	20 T
A	4 D	13 M	36 9	18 R	11 K	29 2

Fig. 6: 6x6 magic square indexed with music notes and alphanumeric are placed with their order

Now the substitution will be done as follows:
Character in each cell will be substituted with index of that cell.
For example, Q is 17th letter so it is placed in the cell with digit 17. The cell contained Q is indexed as DC, so it will be the code of Q after encryption.
Whenever the arrangement of magic square will be changed, code of Q will be different with the same indexing of grid. Indexing also can be changed by changing sequence of music notes or scale.

IV. ILLUSTRATION

A. Encryption
Plain text: MARY HAD A LITTLE LAMB
MARY= ADCEAFEG
HAD = DDCEAC
A = CE
LITTLE= EDDEGAGAEDFE
LAMB= EDCEADGG
Cipher text:
ADCEAFEGBDDCEACBCEBEDDEGAGAEDFEBEDCE ADGGB

B. Decryption
Cipher text:
GADDFEBEDCEADGGBEFCECFBCFFDAFFEBGAGEB EAGEB
GADDFE = THE
EDCEADGG=LAMB
EFCECF=WAS
CFFDAFFE=SURE
GAGE=TO
EAGE=GO
Plain Text: THE LAMB WAS SURE TO GO

V. CONCLUSION

Each time the arrangements of integers in magic square are changed, the arrangements of characters are also different. Hence for every substitution, each single character would have different types of codes. The order of alphanumeric characters are very difficult to guess as there are 1.77×10^{19} possible 6x6 normal magic squares any of which can be chosen during key selection.[11] Musical notes C–D–E–F–G–A–B are 7 notes where anyone of those can be used as space/end marker and remaining can be used for substitution purpose. Also the scale can be changed. Sender and receiver only have that knowledge of which unique 6x6 square is used and which note is the space/end marker and the sequence of indexing rows and columns. So there are several combination of keys can be made from them. Sender can change keys frequently with the knowledge of receiving end. The huge combinations of keys make guessing or cracking of the keys very much impossible. Security concern of simple Polybius cipher can be overcome with this system. Hence the proposed system is safe for small text based data transfer.

REFERENCES

[1] W. Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall, 2011
[2] B. Schneier, Applied Cryptography Protocols, Algorithms, And Source Code In C, 2nd Edition
[3] S. Vaudenay, A Classical Introduction To Cryptography Applications for Communications Security, Springer, 2006
[4] D. Salomon, Coding for Data and Computer Communications, Springer, 2006
[5] http://en.wikipedia.org/wiki/Note_(music)
[6] http://en.wikipedia.org/wiki/Scale_(music)
[7] J. Procopio, Basic Music Theory, 2010
[8] http://en.wikipedia.org/wiki/Magic_square
[9] W. S. Andrews, Magic Squares and Cubes, Cosimo, Inc., 2004
[10] http://www.perfectmagicsquares.com/ 6x6.html
[11] http://www.trump.de/magic-squares/

