Volume 3, No. 12, December 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

SECURE COMMUNICATION SCHEME WITH MAGIC SQUARE

Nitin Pandey*[1] , D.B.Ojha[2]
*[1]Research Scholar, Mewar University, Chittorgarh, Rajasthan, India
npandeyg@gmail.com[1]
*[2]Professor, Mewar University, Chittorgarh, Rajasthan, India
ojhdb@yahoo.co.in[2]

Abstract: An N order magic square is N*N matrix containing integers and addition result of each row, column and diagonally get the same value. We utilize the generalized form of a 8×8 matrix with the help of a special geometrical figure. With help of 8×8 Magic Square, the process establishes a new platform to generate key and encrypt the data using our encryption scheme.

Key word: Magic Square, Encryption, Cryptography, Random Number.

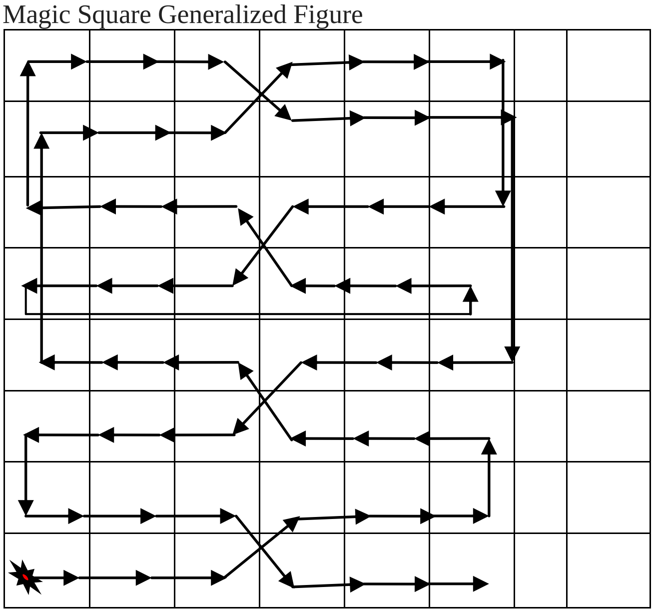
INTRODUCTION

Cryptography is a branch of applied mathematics that aims to add security in the ciphers of any kind of messages. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document [1]. Encryption [2, 3, 4] technique uses random number either generated by PRNG or HRNG.

Using generalization of 8×8 magic square given by Deo Brat ojha and B L Kaul [5], encryption generates a key on the pattern of 8×8 magic square image. A 8×8 matrix filled with the integers in such a way that the sum of the numbers in each row, each column or diagonally also remain same, in which one integer use at once only. This scheme utilize the Required Sum of Magic square [5, 6, 7, 8, 9, 10] to generate an encryption key for the Scheme.

PRELIMINARIES

Magic Square Generalized Figure



Our Approach:

Steps:

a. Fix the required total sum($260 \le S < \infty$), Then there exist two favourable cases
   (i) $S = 8p, p \in I$.
   (ii) $S = 8p + 4, p \in I$.
b. In case (i) Now, We have to decide starting number $n_1 = p - [w = \{\text{Number of blocks}\} - 1]$.

In case (i) Now, We have to decide starting number $n_1 = p - [w = \{\frac{\text{Number of blocks}}{2}\} - 1]$

c. Then calculate the sixteen numbers $n_2 = n_1 + d$, where d is predefined by problem, if not then take $d = 1$, $n_1, n_2, n_3, .,.,..n_{16}$. Later on w may be change after the fixed limit, but it will change in the manner $W = nw + 1, n \in I$.
d. Then arrange these sixteen numbers with the help of suggested geometrical figure.
e. We can find numerous solutions with the help of rotation of suggested figure in clockwise and anticlockwise direction.
f. We can find numerous solutions by defining the suitable d .
g. But in all cases, we find optimized sum required.
h. In case (ii), only d will be even with the same process.

Our Process:

In encryption phase, we take a message block and a new generated key $K_{new...i}$ implement encryption process as per traditional DES.

Now, we have a new key for every block of message. This new key $K_{new...i}$ is applied on each block of message M .

In this approach, New key is also make 16 different key for every round of DES using shifting property as per traditional

DES. For every block of message M , $K_{new...i}$ new makes a new key block for every round of DES to implement in the encryption process.

Decryption Process is the inverse step of encryption process. In decryption, we also use the same key which is used in encryption.

$$C_i = E_{K_{newi}}\{m_i\}\, and\, m_i = D_{K_{newi}}\{c_i\}$$

Where $1 \le i \le n.$

Cipher Text $C = C_1, C_2, C_3, \dots \; \dots \dots \dots \dots \; C_n$ *and*

Plain Text $M = m_1, m_2, m_3, \dots \; \dots \dots \dots \dots \; m_n$

Sender Initial Phase:

a. Sender chooses a required total sum S & difference d and sends it to the receiver.
b. Then calculate the first no. using the formula 2a +7d = sum required, where a is first no. and d is difference.
c. Then calculate the sixty four $n_n = n_{n-1} + d$, where *d* chooses already.
d. Then arrange these sixty four numbers with the help of suggested geometrical figure.
e. Now Sender takes the centre no. and uses this rather than random no.

Receiver Initial Phase:

a. Receiver receives required total sum S & difference d.
b. Then calculate the first no. using the formula 2a +7d = sum required, where a is first no. and d is difference.
c. Then calculate the sixty four numbers $n_n = n_{n-1} + d$, where *d* gets already.
d. Then arrange these sixty four numbers with the help of suggested geometrical figure.
e. Now receiver also takes the centre no. and uses this rather than random no.

Key Generation Phase:

$$F\{K, Center\ no.\} = K_{new\ i}$$

$$\underline{Function F}$$

a. Input the bit value of initial key K (56-bit).
b. Input generated centre no.
c. Convert Rj (centre number) into 56- bit binary number.
d. Now, we have
   Key K = {KB1, KB2, KB3, ..., KB56}
   And Centre no. ={Rb1, Rb2, Rb3, ..., Rb56}
   Where KBr is the bit of Key and Rbr is the bit of centre number.
   Here r =1, 2, 3...............56.
e. Apply condition on K and Centre no.
   IF Rbr = 1 then, Complement (convert 1 to 0 or 0 to 1) of corresponding KBr.
   ANDIF Rbr = 0 then, Retain the same (1 to 1 or 0 to 0) of corresponding KBr.
f. Result is Knew i.

Encryption & Decryption Phase:

$$C_i = E_{K_{newi}}\{m_i\}\, and\, m_i = D_{K_{newi}}\{c_i\}$$

Where $1 \le i \le n.$

Cipher Text $C = C_1, C_2, C_3, \dots \; \dots \dots \dots \dots \; C_n$ *and*

Plain Text $M = m_1, m_2, m_3, \dots \; \dots \dots \dots \dots \; m_n$

Both sender and receiver follow the process and generate separate key using generalized form of 8×8 a matrix with the help of a special geometrical. Every time when, required sum and difference are changed than new generated key also changed. Now, the sender use this newly generated key for encryption and the receiver uses this key for decryption.

SECURITY ANALYSIS

Using Magic Square generalized image and our scheme itself based on random number works like a one-time pad. One time pad has a property termed perfect secrecy, i.e. the cipher text gives no additional information regarding plain text . Thus pre probability of a message M is the same as post of a message M given the resultant cipher text.

Mathematically, the method is expressed in terms as $H(M) = H(M|C)$, here $H(M)$ is the entropy of the plain text and is the conditional entropy of the plain text given by cipher text $H(M|C)$ is the conditional entropy of the plain text given by cipher text C.

Perfect secrecy is a strong notion of cryptanalytic difficulty. Our process has some advantage in practice:

a. It is perfectly like a random one-time pad.
b. It provides secure generation and exchange of the key.

REFERENCES

[1]. Eli Biham, Adi Shamir, Differential Cryptanalysis of the Full 16-Round DES, Advances in Cryptology, proceedings of CRYPTO ’92, Lecture Notes in Computer Science 740, Springer, 1993.

[2]. D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati garg “An Innovative Approach to Enhance the Security of Data Encryption Scheme” International Journal of Computer Theory and Engineering, Vol. 2,No. 3, June, 2010,1793-8201.

[3]. Ramveer Singh, Deo Brat Ojha, An Ordeal Random Data Encryption Scheme (ORDES), The Seventh International

Conference on eLearning for Knowledge-Based Society, 16-17 December 2010, Thailand.

[4]. Ramveer Singh, Deo Brat Ojha, An Ordeal Random Data Encryption Scheme (ORDES), International Journal of the Computer, the Internet and Management Vol.18.No.3 (September - December, 2010) pp 38-50.

[5]. Deo Brat Ojha, B L Kaul, Generalization of 4×4 Magic Square, International Journal of Applied Engineering Research, Dindigul, Volume 1, No 3, 2010.

[6]. Harold M. Stark. An introduction to number theory. MIT Press, Cambridge, Mass., 1978.

[7]. Joseph H. Silverman.The arithmetic of elliptic curves. Springer-Verlag, New York-Berlin, 1986.

[8]. Ezra Brown.Magic squares, finite planes, and points of inflection on elliptic curves. College Math. J., 32(4):260–267, 2001.

[9]. Agnew, Elizabeth H., “Two problems on magic squares,”Mathematics Magazine, 44 (1971),12–15.

[10]. Hanson, Klaus D.,“The magic square in Albrecht D¨urer’s“Melencolia I”:Metaphysical symbol or mathematical pastime,” Renaissance and Modern Studies, 23 (1979), 5–24.

