Volume 3, No. 12, December 2012

Journal of Global Research in Computer Science

RESEARCH PAPER

Available Online at www.jgrcs.info

ISSN-2229-371X

MAGIC SQUARE AND CRYPTOGRAPHY

Meenu Sahni[*1] and D.B. Ojha[2]
[*1] Research Scholar Mewar University, Chittorgarh, Rajasthan, India
mnu.sahni@rediffmail.com[1]
[2] Mewar University, Chittorgarh, Rajasthan, India
ojhabrat@gmail.com[2]

***Abstract*: :** An 8 order magic square is 8×8 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 the help of 8×8 Magic Square, the process established a new platform to generate key and encrypt the data using ORDES.

***Keywords*:** Magic Square, Ordeal Random Data Encryption Standard, Cryptography, Random Number.

INTRODUCTION

ORDES is a technique of Encryption/Decryption. 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]. ORDES 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], ORDES generate 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 utilise the Required Sum of Magic square [5, 6, 7, 8, 9, 10] to generate an encryption key for ORDES.

Data Encryption Standard (DES) symmetric key cryptosystem, which was the natural choice, given that this cryptosystem had been around since 1976 and adopted by the US government in 1977, is the US government's secret-key data encryption standard and is widely used around the world in a variety applications.

The input message is also known as "plaintext" and the resulting output message as "ciphertext". The idea is that only recipients who know the secret key can decrypt the ciphertext to obtain the original message. DES uses a 56-bit key, so there are 256 possible keys [2].

Due to its importance, DES has received a great deal of cryptanalytic attention. However, besides using the complementation property, there were no short-cut attacks against the cipher until differential cryptanalysis was applied to the full DES in 1991 [3, 4, 11].

In [12], Chaum and Evertse presented several meet-in-the-middle attacks on reduced variants of DES.

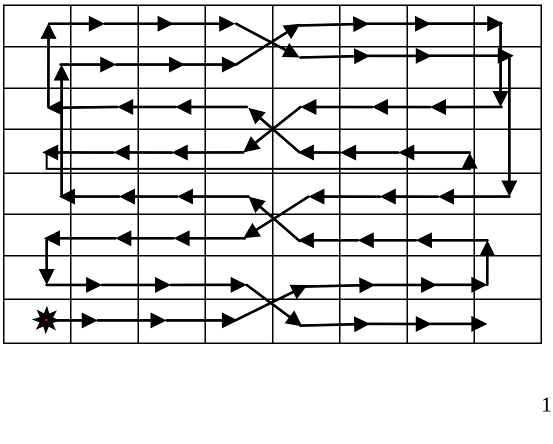
In 1987 Davies described a known plaintext attack on DES [13]. In [14] these results were slightly improved but still could not attack the full DES faster than exhaustive key search.

In 1994 Biham and Biryukov [15] improved the attack to be applicable to the full DES. A chosen ciphertext variant of the attack is presented in [16]; it has a data complexity of 245 chosen plaintexts. The first attack on DES that is faster than exhaustive key search was presented in [17]. In [18] another attack on DES is presented, linear cryptanalysis. This attack was later improved in [19] by exploiting nonlinear relations as well. The improved attack has a data complexity of 242.6 known plaintexts. Using chosen plaintexts, Knudsen and Mathiassen reduced the data complexity in by a factor of 2.

Even after DES was theoretically broken, RSA published a plaintext and its ciphertext encrypted using DES under some unknown key, and offered a prize of several thousand US dollars for whoever finds the secret key [20]. The first exhaustive key search took about 75 days and the key was found using 14,000–80,000 computers over the Internet [21]. In 1997 the Electronic Frontier Foundation (EFF) built a special purpose machine that costs 250,000 US dollars which retrieved the key in 56 hours by means of exhaustive key search [22]. The approach of treating reduced-round DES as an algebraic equation was also suggested in [23, 24].

METHODOLOGY

Magic Square Generalized Figure:



ORDES Approach:

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

PLAUSIBLE KEYING have the property to make various key for various block of message.

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

In ORDES, 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, new $K_{\text{new i}}$ 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.

$C_i = E_{K \text{ new i}} \{m_i\}$ and $D_{k \text{ new i}} \{c_i\}$where $1 \leq i \leq n$

Cipher Text $C = C_1, C_2, C_3, \cdots$ and

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

Sender Initial Phase:

a. Sender choose a required total sum S & difference d and send it to the reciever.
b. Then calculate the first no. using the formula 8a +252d = sum required, where a is first no. and d is difference.
c. Then calculate the sixteen numbers $n_n = n_{n-1} + d$, where d chooses already.
d. Then arrange these sixteen numbers with the help of suggested geometrical figure.
e. Now Sender takes the centre no. and uses this rather than random no.

Reciever Initial Phase:

a. Reciever recieves required total sum S & difference d.
b. Then calculate the first no. using the formula 8a +252d = sum required, where a is first no. and d is difference.
c. Then calculate the sixteen numbers $n_n = n_{n-1} + d$, where d gets already.
d. Then arrange these sixteen 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, Centre no.} = Knew i

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.
6.Result is Knew i.

RESULT AND DISCUSSION

Security Analysis:

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

Mathematically, this is expressed as $\mathrm{H(M)} = \mathrm{H(M|C)}$, here where $\mathrm{H(M)}$ is the entropy of plain text and is the conditional entropy of the plain text given by cipher text $\mathrm{H(M|C)}$ is the conditional entropy of the plain text given by cipher text C.

Perfect secrecy is a strong notion of cryptanalytic difficulty.

ORDES has some advantage in practice:

a. ORDES perfectly like a random one-time pad.
b. 2.ORDES provides secure generation and exchange of the key.

CONCLUSION

In ORDES key is used to control the complete operation i.e. Encryption and Decryption both. Key itself a tool to encrypt plain text and decrypt cipher text. A key size should be large enough that a brute force attack against ORDES may be infeasible. It is necessary for the key length to be only used once like one time pad algorithm. To manage a long key is not an easy task. So, ORDES follows the majestic approach to regenerate a new key every time rather than a long key.

REFERENCES

[1]. Richard Poisel: Modern Communications Jamming Principles & Techniques, Second Edition, 2011.

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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.

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

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

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

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

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

[11]. 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.

[12]. Eli Biham, Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer, 1993.

[13]. David Chaum, Jan-Hendrik Evertse, Cryptanalysis of DES with a Reduced Number of Rounds: Sequences of Linear Factors in Block Ciphers, Advances in Cryptology, proceedings of CRYPTO ’85, Lecture Notes in Computer Science 218, pp. 192–211, Springer, 1986.

[14]. Donald W. Davies, Investigation of a Potential Weakness in the DES Algorithm, private communications, 1987.

[15]. Donald W. Davies, Sean Murphy, Pairs and Triplets of DES S-Boxes, Journal of Cryptology, Vol. 8, No. 1, pp. 1–25, Springer, 1995.

[16]. Eli Biham, Alex Biryukov, An Improvement of Davies’ Attack on DES, Journal of Cryptology, Vol. 10, No. 3, pp. 195–206, Springer, 1997.

[17]. Sebastien Kunz-Jacques, Frederic Muller, New Improvements of Davies-Murphy Cryptanalysis, Advances in Cryptology, proceedings of ASIACRYPT 2005, Lecture Notes in Computer Science 3788, pp. 425–442, Springer, 2005.

[18]. Kunz-Jacques, S., Muller, F.: New Improvements of Davies-Murphy Cryptanalysis.In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 425–442. Springer, Heidelberg (2005)

[19]. Mitsuru Matsui, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology, proceedings of EUROCRYPT ’93, Lecture Notes in Computer Science 765, pp. 386–397, Springer, 1994.

[20]. Takeshi Shimoyama, Toshinobu Kaneko, Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES, Advances in Cryptology, proceedings of CRYPTO ’98, Lecture Notes in Computer Science 1462, pp. 200–211, Springer, 1998.

[21]. CNET News.com, Users take crack at 56-bit crypto. Available on-line at http://news.com.com/2100-1023-278658.html?legacy=cnet, 1997.

[22]. RSA Data Security, Team of Universities, Companies and Individual Computer Users Linked over the Internet Crack RSA’s 56-Bit DES Challenge. Available on-line at: http://www.rsasecurity.com/news/pr/970619-1.html, 1997.

[23]. Electronic Frontier Foundation, Cracking DES, Secrets of Encryption Research, Wiretap Politics & Chip Design, O’reilly, 1998.

[24]. Nicolas T. Courtois, Gregory V. Bard, Algebraic Cryptanalysis of the Data Encryption Standard. Available on-line at: http://eprint.iacr.org/2006/402.pdf, 2006.