Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

8th International Conference
on Electrical Engineering
ICEENG 2012

New Encryption Method Based on Using The Kharaghani Array of Order 8

By

Manal A. Shehab Noha O. Korany *

Abstract:

This paper suggests a new encryption method based on using the form and the properties of an orthogonal Hadamard array called the Kharaghani array of order 8. In this method; the used encryption key, the plaintext and the ciphertext values should be integers less than 256 to be presented in the form of the 8-bit binary representation.

There are some constrains that restrict the chosen value for the encryption key, these constrains lead to have only 126 available values for the encryption key. The 126 encryption keys were checked on the available plaintext values and some concluded notes and results were presented.

The suggested encryption method has the advantage of being easy to implement because the construction of the Hadamard array is easy.

Keywords:

Encryption, Hadamard and Kharaghani array

---

* Electrical Engineering Department, Faculty of Engineering, Alexandria University- Egypt

1. Introduction:

Securing sensitive data during its transmission is very important, using encryption is one way to achieve that. The paper suggests a new encryption method that is denoted by E1 for simplicity [1]. E1 is based on using one of the Hadamard arrays called the Kharaghani array of order 8.

The Hadamard Array H [h, k, λ] based on the indeterminates x1, x2, . . . , xk, with k ≤ h, is an h × h matrix with entries chosen from {±x1, ±x2, . . . ,±xk} in such a way that; in any row there are λ entries ±x1, λ entries ±x2,. . . , λ entries ±xk, and similarly for the columns regarding that the rows and columns are (formally) pairwise orthogonal, respectively [2].

The Hadamard array H [h, k, λ] with h = k = 8, λ = 1 and indeterminants A through H is an orthogonal Hadamard array H [8, 8, 1] known as the Kharaghani array of order 8 and it has the following form [2]& [3]:

H [8, 8, 1] = X =

$$\left[\begin{array}{cccc|cccc} A & B & C & D & E & F & G & H \\ -B & A & D & -C & F & -E & -H & G \\ -C & -D & A & B & G & H & -E & -F \\ -D & C & -B & A & H & -G & F & -E \\ -E & -F & -G & -H & A & B & C & D \\ -F & E & -H & G & -B & A & -D & C \\ -G & H & E & -F & -C & D & A & -B \\ -H & -G & F & E & -D & -C & B & A \end{array}\right]. \quad (1)$$

$X^T X = K I_8$, where I_8 is the 8 × 8 identity array, X^T is the transpose of X and (2)

$K = A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2$. (3)

The next section describes the E1 encryption method, then section 3 evaluates the suggested method. Finally; section 4 summarizes the conclusions.

2. New Suggested Encryption Method (E1) Based on Using the Kharaghani Array of Order 8:

The E1 method uses an encryption key that could be presented in the form of the 8-bit binary representation to form the Kharaghani array of order 8 that is defined in equation (1). Sections 2.1 and 2.2 describe the encryption and the decryption algorithms respectively, then section 2.3 presents the conditions of the used encryption key.

2.1 The Encryption Algorithm of the E1 Method:

The Encryption algorithm of the E1 method is defined as follows:

1- Let the plaintext P be the 1× 8 array whose sequenced elements are the 8-bits binary representation of the ASCII code of the covert character, so P = [p_7 p_6 p_5 p_4 p_3 p_2 p_1 p_0].

2- The chosen encryption key e should be less than 256 to be able to convert to the 8-bit binary representation that would be denoted as [e_7,: : , e_1 ,e_0]. The conditions of selecting the value of e will be presented in section 2.3.

3- The 8 bits of the encryption key would be distributed in the form of the orthogonal Kharaghani array of order 8 which is presented as the X array in equation (1) where;

A = e_0, B = e_1, C = e_2, D = e_3, E = e_4, F = e_5, G = e_6 and H = e_7. (4)

So the resulting array **X** that would be used to encrypt the plaintext would be:

$$X=\begin{bmatrix} e0 & e1 & e2 & e3 & e4 & e5 & e6 & e7 \\ -e1 & e0 & e3 & -e2 & e5 & -e4 & -e7 & e6 \\ -e2 & -e3 & e0 & e1 & e6 & e7 & -e4 & -e5 \\ -e3 & e2 & -e1 & e0 & e7 & -e6 & e5 & -e4 \\ -e4 & -e5 & -e6 & -e7 & e0 & e1 & e2 & e3 \\ -e5 & e4 & -e7 & e6 & -e1 & e0 & -e3 & e2 \\ -e6 & e7 & e4 & -e5 & -e2 & e3 & e0 & -e1 \\ -e7 & -e6 & e5 & e4 & -e3 & -e2 & e1 & e0 \end{bmatrix} \quad (5)$$

4- The 8-bit binary representation of the ciphertext C could be presented in the form of 1 × 8 array [c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0] that would be obtained from multiplying the plaintext P and the Kharaghani array X, then calculating the modular of modulus 2 for each element of the resulted array to limit the C elements in 0 and 1 values. The resulting ciphertext is defined by the following equation:

$$C \equiv P\ X \pmod 2 \qquad (6)$$

Then $[c_7\ c_6\ c_5\ c_4\ c_3\ c_2\ c_1\ c_0] \equiv$

$$[p_7\ p_6\ p_5\ p_4\ p_3\ p_2\ p_1\ p_0] \begin{bmatrix} e0 & e1 & e2 & e3 & e4 & e5 & e6 & e7 \\ -e1 & e0 & e3 & -e2 & e5 & -e4 & -e7 & e6 \\ -e2 & -e3 & e0 & e1 & e6 & e7 & -e4 & -e5 \\ -e3 & e2 & -e1 & e0 & e7 & -e6 & e5 & -e4 \\ -e4 & -e5 & -e6 & -e7 & e0 & e1 & e2 & e3 \\ -e5 & e4 & -e7 & e6 & -e1 & e0 & -e3 & e2 \\ -e6 & e7 & e4 & -e5 & -e2 & e3 & e0 & -e1 \\ -e7 & -e6 & e5 & e4 & -e3 & -e2 & e1 & e0 \end{bmatrix} \pmod 2$$

5- Optionally convert the ciphertext to its decimal according to the decided re-presentation form.

2.2 The Decryption Algorithm of the E1 Method:

The decryption algorithm of the E1 method is defined as follows:

1- The ciphertext C array is presented in the form of 1×8 array as $[c_7\ c_6\ c_5\ c_4\ c_3\ c_2\ c_1\ c_0]$.

2- The 8 elements of the encryption key is used to construct the X^{-1} array which is the inverse of the Kharaghani array X by referring to equations (2), (3), (4) and (5) as follows:

I- Calculate the factor K using equations (3) and (4);

$$K = e^2_0 + e^2_1 + e^2_2 + e^2_3 + e^2_4 + e^2_5 + e^2_6 + e^2_7 \qquad (7)$$

II- Calculate X^{-1} by multiply both sides of equation (2) by X^{-1} as;

$$X^T X X^{-1} = K * I_8 X^{-1}$$

$$X^T I_8 = K\ I_8 X^{-1}$$

This means that;

$$X^{-1} = (1 / K) X^T \qquad (8)$$

3- The plaintext P could be obtained from multiplying both sides of equation (6) by X^{-1}, then calculating the modular of modulus 2 for each element of the resulted array to limit the values of the elements of the P array in 0 and 1 values. So;

$C\ X^{-1} \equiv P\ X\ X^{-1} \pmod 2$

i.e. $C\ X^{-1} \equiv P\ I_8 \pmod 2$ then;

$C\ X^{-1} \equiv P \pmod 2$ (9)

Substitute by the value of X^{-1} from equation (8) in equation (9) to get the plaintext P:

$(1/K)\ C\ X^{T} \equiv P \pmod 2$

$C\ X^{T} \equiv P\ K \pmod 2$ (10)

While the elements of P are either 0 or 1 which return themselves when modulus 2 is calculated to them, then:

$P \equiv P \pmod 2$ (11.a)

K must be odd as modulus 2 of an odd value returns 1. K must not be even as modulus 2 of an even value returns 0; the matter which prevents retrieving the plaintext in the deciphering process.

So for the odd values of K; $K \pmod 2 \equiv 1$ (11.b)

Substituting from 11.a and 11.b in 10, then for odd values of k:

$P \equiv C\ X^{T} \pmod 2$ (12)

2.3 Conditions of the Used Encryption Key in the E1 Encryption Method:

The used encryption key e in the E1 method should be selected according to the following conditions:

1- The encryption key e should be less than 256 to be presented in the 8-bit binary form.

2- The number of 1s in the 8-bit binary representation of the used encryption key e in the E1 encryption method should be odd. Practical calculated sample shows that $K \pmod 2 = 0$ when the number of 1s in the 8-bit binary representation of e is even which agrees with equation (7), and therefore the plaintext couldn't be retrieved back from equation (10).

3- The following notes restrict the chosen value of the encryption key within $2 \leq e \leq 253$:
(I) $e \neq 1$ as it returns C = P.
(II) $e \neq 254$ as for $1 \leq P \leq 255$; it returns 127 values for which C = P, and 128 values for which C = 255 - P.

4- From the above points 2 and 3; the number of the available values of the encryption key for the E1 encryption method is 126.

3. Evaluation of the E1 Encryption Method:

The E1 encryption method has the advantage of using one key for the encryption and the decryption operations. While the elements of the 8-bits binary representation of the encryption key are the indeterminates of the Kharaghani Hadamard array X and the construction of X is easy, then the E1 encryption is quite easy to implement. The main disadvantage of the E1 method is having only 126 available values for the used encryption key.

Some general results from applying the E1 encryption method:

1- For the same value of e;
- If P = a returns C = b, then C = a when P = b.
- If P = e, then C = 1. So; it's not recommended to use the E1 method to encrypt the plaintext when it equals e.
- If P = 255, then C = 255.

2- For each value of e;
- There is an R set of the plaintext values where each P within the R set has C = P.
- There is an S set of the plaintext values where each P within the S set has C = 255 - P.

3- The 126 available values for the encryption key could be presented into 21 T sets (from T_1 to T_{21}) as shown in table 1, so that all the keys within the same T_i set have the same R_i and S_i sets for $1 \leq i \leq 21$.

T_i	Included keys within the T_i set	Number of keys in T_i	Number of elements in R_i	Number of elements in S_i
T_1	{2, 13, 49, 62, 193, 206, 242, 253}	8	15	16
T_2	{4, 11, 81, 94,161,174, 244, 251}	8	15	16
T_3	{7, 8, 97, 110, 145, 158, 247, 248}	8	15	16
T_4	{14, 241}	2	63	64
T_5	{16, 35, 69, 118, 137, 186, 220, 239}	8	15	16
T_6	{19, 32, 73, 122, 133, 182, 223, 236}	8	15	16
T_7	{21, 41, 64, 124, 131, 191, 214, 234}	8	15	16
T_8	{22, 42, 76, 112, 143, 179, 213, 233}	8	15	16
T_9	{25, 37, 67, 127, 128, 188, 218, 230}	8	15	16
T_{10}	{26, 38, 79, 115, 140, 176, 217, 229}	8	15	16
T_{11}	{28, 47, 70, 117, 138, 185, 208, 227}	8	15	16
T_{12}	{31, 44, 74, 121, 134, 181, 211, 224}	8	15	16
T_{13}	{50, 205}	2	63	64
T_{14}	{52, 59, 82, 93, 162, 173,196, 203}	8	15	16
T_{15}	{55, 56, 98, 109, 146, 157, 199, 200}	8	15	16
T_{16}	{61, 194}	2	63	64
T_{17}	{84, 171}	2	63	64
T_{18}	{87, 88, 100, 107, 148, 155, 167, 168}	8	15	16
T_{19}	{91, 164}	2	63	64
T_{20}	{103, 152}	2	63	64
T_{21}	{104, 151}	2	63	64
Total number of keys		**126**		

Table 1: *The 126 available values for the encryption key of the E1 encryption method presented into 21 T sets so that all the keys within the T_i set have the same R_i and S_i sets for $1 \leq i \leq 21$.*

4- Each T set contains even number of keys act as complement pair(s) (i.e. if a key is located within certain T_i set, then its complement is included also in the same T_i set).

5- Each R set contains odd number of plaintexts which act as complement pairs beside 255, while each S set contains even number of plaintexts which act as complement pairs.

6- There are 14 T sets in which each set includes 8 keys; so that all the 8 keys within the same T set have 15 values in their R set and 16 values in their S set.

7- There are 7 T sets in which each set includes 2 keys only; so that the two keys within the same T set have 63 values in their R set and 64 values in their S set.

Table 2 shows sample results of applying the encryption method E1 to encrypt the capital characters from Q to Z when the encryption key = $(167)_{10}$ = $[1010\ 0111]_2$.

Char.	**ASCII Code in Decimal $(P)_{10}$**	**Plaintext in 8-bit Binary representation $(P)_2$**	**Ciphertext in 8-bit Binary representation $(C)_2$ $C \equiv P \ X \pmod 2$**	**Ciphertext in Decimal $(C)_{10}$**
Q	**81**	0101 0001	0000 0111	**7**
R	**82**	0101 0010	1111 1011	**251**
S	**83**	0101 0011	0101 1100	**92**
T	**84**	0101 0100	0000 1101	**13**
U	**85**	0101 0101	1010 1010	**170**
V	**86**	0101 0110	0101 0110	**86**
W	**87**	0101 0111	1111 0001	**241**
X	**88**	0101 1000	1111 1110	**254**
Y	**89**	0101 1001	0101 1001	**89**
Z	**90**	0101 1010	1010 0101	**165**

***Table (2):** Sample results of the E1 encryption method using $(167)_{10}$ as an encryption key*

It is shown from table 2 that for the used encryption key; each value of P has its own value of C (i.e. there are unrepeated values of C for different values of P).The used key e = 167 resides within the T_{18} set which is shown in table 1. All the keys within the T_{18} set have the same R_{18} and S_{18} sets. R_{18} includes 15 plaintext values defined as R18 = {15, 51, 60, 86, 89, 101, 106, 149, 154, 166, 169, 195, 204, 240, 255}, whereas S_{18} includes 16 plaintext values defined as S18= {3, 12, 48, 63, 85, 90, 102, 105, 150, 153, 165, 170, 192, 207, 243, 252}.

The E1 encryption method could be used with an 8 × 8 plaintext array. In this case; the message is divided into 8-character blocks and the last 8-character block could be padded if it needs that. The 8 character block will be presented in the form of an 8 × 8 plaintext array in which the number of rows is the number of characters in the block, and the sequenced elements of a row are the sequenced elements of the 8-bit binary representation of the ASCII equivalent of the corresponding character.

Example:
If the used e = $(167)_{10}$ = $[1010\ 0111]_2$ and the eight rows of the 8 × 8 plaintext array are the followed 8-bit binary representation of the ASCII characters from A to H.

So, if the plaintext array P = $\begin{bmatrix} 0100\ 0001 \\ 0100\ 0010 \\ 0100\ 0011 \\ 0100\ 0100 \\ 0100\ 0101 \\ 0100\ 0110 \\ 0100\ 0111 \\ 0100\ 1000 \end{bmatrix}$, the ciphertext array C = $\begin{bmatrix} 0111\ 1101 \\ 1000\ 0001 \\ 0010\ 0110 \\ 0111\ 0111 \\ 1101\ 0000 \\ 0010\ 1100 \\ 1000\ 1011 \\ 1000\ 0100 \end{bmatrix}$

4. Conclusions:

This paper suggests a new encryption method E1 that uses the Kharaghani array of order 8 which is an orthogonal Hadamard array H [8, 8, 1]. The encryption algorithm provides ciphertext results bounded by 255 as an upper limit to be able to present the results in the form of the 8-bit binary representation. The encryption key e should be located in the decimal range $2 \le e \le 253$ and the number of 1s in its 8-bit binary representation should be odd. Therefore; the number of available values for the used encryption key in the E1 method is 126. The encryption algorithm of E1 is quite easy to implement because the construction of the Hadamard arrays is easy.

References:

[1] Manal A. Shehab, "New Encryption and Steganographic Methods for Data Hiding in the IP Packets or Their Fragments", Master of Science in Electrical Engineering, Electrical Engineering Department, Faculty of Engineering, Alexandria University, Egypt, October 2011.
[2] Ryan Harkins, Eric Weber, and Andrew Westmeyer, "Encryption Schemes using Finite Frames and Hadamard Arrays", Experiment Math., vol. 14, Issue 4, 423-433, 2005.
http://projecteuclid.org/DPubS/Repository/1.0/Disseminate?view=body&id=pdf_1&handle=euclid.em/1136926973
[3] Georgiou, S, Koukouvinos, C and Seberry, J, Chapter: “Hadamard matrices, orthogonal designs and construction algorithm”, Book: “Further Combinatorial and Constructive Design Theory”, Kluwer Academic Publishers, Norwell, Massachusetts, in Wallis, WD (ed), Designs 2002, 133-205. http://ro.uow.edu.au/infopapers/308

Last access to the web sides was in 14 March 2012.