Songklanakarin J. Sci. Technol.
43 (5), 1237-1243, Sep. - Oct. 2021

http://www.sjst.psu.ac.th

Original Article

Alternative matrix in cryptography with Hadamard matrix

Nilobol Kamyun[1], Supannee Sompong[2], Nichakan Kamtalang[1],
Mongkoltong Sroypachr[1], and Kannika Khompungson[1*]

[1] *Division of Mathematics, School of Science,*
University of Phayao, Mueang, Phayao, 56000 Thailand

[2] *Department of Mathematics and Statistics, Faculty of Science and Technology*
Sakon Nakhon Rajabhat University, Mueang, Sakon Nakhon, 47000 Thailand

Received: 15 June 2020; Revised: 9 September 2020; Accepted: 5 October 2020

Abstract

This paper aims to describe the methods that were used in order to construct the Hadamard matrix and its basic properties and how it is applied in Cryptography. Moreover, this matrix was used to construct a new algorithm in cryptography.

Keywords: Hadamard matrix, orthogonal matrix, cryptography

1. Introduction

The basic concept of Cryptography study primarily consists of two parts: encryption and decryption. Both of these parts have a myriad of methods for the construction of an algorithm when it comes to cryptography.

As present, cryptography is usually classified into two major categories, symmetric and asymmetric. To more specific, both the sender and the receiver utilize the same key for encryption and decryption. However, in asymmetric cryptography, two different keys are used. In the English Language, the alphabet consist of 26 letters; therefore, the main idea of Hill Cipher, is to assign a numerical value to each letter of the words, thus Hill Cipher works on modulo 26 (Abedal-Hamza & Baneen, 2017a). In 2017, Abdulaziz B.M. Hamed and Ibrahim O.A. Albudawe proposed to solve the problem of cryptographic messages by utilizing the invertible matrices (modulo 27) instead of the Hill Cipher method. In detail, the messages have been encrypted and decrypted perfectly using secret key matrices along with congruence modulo, relative prime and inverse multiplication (modulo 27) relations corresponding to English alphabetic letter plus space.

The Hadamard matrix is well-known matrix with a wide range of applications in mathematics especially in communication system digital and image processing. This paper aims to describe the processes and the methods that we used to construct the Hadamard matrix as well as its basic properties, which are then applied to the cryptographic problems in using the Hill Cipher method (modulo 27). It is important to note, as it was stated above that there are many methods of constructing an algorithm in cryptography. An entirely new algorithm was constructed with the use of this matrix.

2. Hadamard Matrix

A real square matrix H_m is said to be a real Hadamard matrix if all entries are +1 or -1 and all rows of H_m are mutually orthogonal ($H_m H^t_m = mI_m$)

For example, for $m = 2 : \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$

$$m = 4 : \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Moreover, we have the following properties,

*Corresponding author
Email address: kannika.kh@up.ac.th

If H_m is a Hadamard matrix then $H^t_m H_m = H_m H^t_m$.
If H_m is symmetric Hadamard matrix then $H^2_m = mI_m$.

Next, let us provide the useful theorem that makes it easy to use software to check whether a matrix is a Hadamard matrix (Horadam, 2007a).

Theorem 2.1 Let $H_m = [h_{ij}]_m$ be an $m \times m$ real matrix whose entries satisfy $|h_{ij}| \le 1$ for all i, j then $\det(H_m) \le m^{\frac{m}{2}}$. Moreover, $\det(H_m) = m^{\frac{m}{2}}$ if and only if H_m is the Hadamard matrix.

Theorem 2.2 If m is the order of a Hadamard matrix and $m \ne 1, 2$ then it necessary that m should be divisible by 4.

There are many methods of construction of Hadamard matrices. Let us begin as the following:

Theorem (Sylvester's Construction) If $m = 2^k$ for some $k \in \mathbb{N}$ then

$$H_{2m} = \begin{bmatrix} H_m & H_m \\ H_m & -H_m \end{bmatrix}$$

is a Hadamard matrix where H_m is a Hadamard matrix.

For example, It is easy to see that $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is a Hadamard matrix and by the above theorem we obtain the Hadamard matrix as follows:

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Moreover, if H_m is a symmetric matrix then we observe that H^2_{2m} is a diagonal matrix.

Next, let us mention the methods of construction of Hadamard matrices by tensor product of two Hadamard matrices, which is useful (Neha & Sachin, 2014). First, let us introduce the definition of the tensor product. Let A and B be a matrix of order m and n respectively.

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \vdots & \vdots & \dots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mm}B \end{bmatrix}$$

Theorem 2.3 The tensor product of two Hadamard matrices is a Hadamard matrix.

Let $A = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ be a Hadamard matrix. We have the Hadamard matrix as the following.

$$A \otimes B = \begin{bmatrix} -B & B \\ B & -B \end{bmatrix} = \begin{bmatrix} -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$

To this end, let us add some observation. Let A be a 2 x 2 Hadamard matrix. If A is not a symmetric matrix, $a_{12} \ne a_{21}$, then we observe that A^2 is an anti diagonal matrix (the (i, j) element is zero $\forall i, j \in \square_n$ ($i + j \ne n+1$)). That is, we have $a_{12}a_{21} = -1$ and

$$A^2 = \begin{bmatrix} a_{11}^2 + a_{12}a_{21} & a_{11}a_{12} + a_{12}a_{22} \\ a_{21}a_{11} + a_{22}a_{21} & a_{22}^2 + a_{21}a_{12} \end{bmatrix}$$
$$= \begin{bmatrix} 0 & a_{11}a_{12} + a_{12}a_{22} \\ a_{21}a_{11} + a_{22}a_{21} & 0 \end{bmatrix}$$

Furthermore, if A, B are 2 x 2 Hadamard matrices but not a symmetric matrices then we point out that $(A \otimes B)^2$ is anti diagonal matrix. To this end, let us consider as the following:

$$(A \otimes B)^2 = \begin{bmatrix} (a_{11}^2 + a_{12}a_{21})B^2 & (a_{11}a_{12} + a_{12}a_{22})B^2 \\ (a_{21}a_{11} + a_{22}a_{21})B^2 & (a_{22}^2 + a_{21}a_{12})B^2 \end{bmatrix}$$
$$= \begin{bmatrix} 0 & (a_{11}a_{12} + a_{12}a_{22})B^2 \\ (a_{21}a_{11} + a_{22}a_{21})B^2 & 0 \end{bmatrix}$$

As we describe the above two methods, Williamson's approach is also one of the important methods and requires a computer to search for the construction of higher order of Hadamard matrices (Manjhi & Arjun, 2018).

Theorem 2.4 Suppose there exist *m x m* matrices *A, B, C,* and *D* that satisfy the following properties:

1. *A, B, C,* and *D* are symmetric matrices having entries ±1;
2. The matrices *A, B, C,* and *D* commute;
3. $A^2 + B^2 + C^2 + D^2 = 4nI_n$.

Then there is a Hadamard matrix of order 4*n* given by

$$H_{4n} = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

Theorem 2.5. If A is an *n x n* matrix with the property $3A^2 = -nJ + 4nI_n$, then the following matrix.

$$H = \begin{bmatrix} J & A & A & A \\ -A & J & A & -A \\ -A & -A & J & A \\ -A & A & -A & J \end{bmatrix}$$

where J is all 1 matrix of order n, is a Hadamard matrix of order 4*n* (Abedal-Hamza & Hussein, 2015).

For example, let $A=\begin{bmatrix}-1 & 1 & 1\\ 1 & -1 & 1\\ 1 & 1 & -1\end{bmatrix}$ and it is easy to check that

A is a symmetric matrix of order 3 and $3A^2 = -nJ + 4nI_n$, then the Hadamard of order 12 is obtained by using theorem 2.5.

We end this section by using the *h-transpose* to construct the Hadamard matrix (Horadam, 2007b).

Definition 2.6 Let *A* be a *n* square matrix. The *h-transpose* of the matrix *A* is defined by $A^h=[a_{ij}^h]=[a_{(n+1-j)(n+1-i)}]$ where $i,j=1,2,3,...,\mathrm{n}$. For example, if $A=\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}$ then $A^h=\begin{bmatrix}4 & 2\\ 3 & 1\end{bmatrix}$.

Theorem 2.7 Let *A* and *B* be a *n* square matrix, then

1. $(A^h)^h = A$
2. $(A^t)^h = (A^h)^t$
3. $(AB)^h = B^h A^h$
4. $\det(A)=\det(A^h)$

Theorem 2.8 If H_m is a Hadamard matrix then $H^h{}_m$ is the Hadamard matrix.

Proof. Suppose that H_m is a Hadamard matrix. That is, $H_m H^t{}_m = mI_m$.

Let us consider as the following:

$$(H_m^h)(H_m^h)^t=(H_m^h)(H_m^t)^h=(H_m^tH_m)^h=mI_m\,.$$

Therefore, $H^h{}_m$ is the Hadamard matrix.

For example, if $H_2=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}$ is the Hadamard matrix then $H_m^h=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}$ is the Hadamard matrix.

The following result may be proved in much the same way as in theorem 2.8

Theorem 2.9 If H_m is a Hadamard matrix then $(H^h{}_m)^t$ is the Hadamard matrix.

For example, if $H_2=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}$ is a Hadamard matrix then $(H_m^h)^t=\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}$ is the Hadamard matrix.

As we known that $H_4=\begin{bmatrix}-1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1\\ 1 & 1 & -1 & -1\\ -1 & 1 & 1 & -1\end{bmatrix}$ then we obtain that $(H_4^h)^t=\begin{bmatrix}-1 & 1 & 1 & -1\\ -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1\\ 1 & 1 & -1 & 1\end{bmatrix}$ is also the Hadamard matrix.

2.1 Cryptography using Hadamard matrix

The method of Cryptography consists of two parts: Encryption and Decryption.

Plaintext means data that can be read and understandable easily. The process of hiding or masking in the information such as plain text, for example, is called encryption, which turns into unreadable text, also known as cipher text. On the other hand, the process of converting cipher text to its original is called decryption. Currently, various methods can be used for construction of encryption and decryption processes. This section concentrates on providing two specific methods of secretly sending messages. For our first method, we utilized the *Hadamard* key matrices congruent modulo 27 instead of using congruent modulo 26, which were introduced by Hill Cipher to encrypt and decrypt messages. To be more specific, the key matrix and congruence modulo must be known by both the sender and the receiver. Hill Cipher was used in order to encrypt and decrypt messages, which is described below in detail. At this moment, let us recall the definition and theorem of the inverse of an integer a to modulo m.

Definition 3.1 Two numbers a and b are relatively prime if their prime factorization have no factors in common, such that $\gcd(a,b)=1$.

Definition 3.2 Inverse of an integer a to modulo *m* is a^{-1} such that $aa^{-1}\equiv 1(\operatorname{mod} m)$, where is called the inverse of a.

Theorem 3.3 Let $m\geq 2$. If a and m are relative prime then there exists a unique integer a^* such that $aa^*\equiv 1(\operatorname{mod} m)$

Before we describe our first algorithm, let us prepare the table for alphabets and its corresponding positive and negative integers value.

2.1.1 Encrypting process 1

Step 1: divide the message text into *n* blocks $B_1,B_2,...,B_n$, each block contains the same number, *m*, of the alphabet which includes space.

Step 2: choose the Hadamard matrix H_m as an encryption key

Table 1. Illustrating English Alphabetic letters and its corresponding numerical integer value modulo 27.

Alphabetic	A	B	C	D	E	F	G	H	I
Number	1	2	3	4	5	6	7	8	9
	-26	-25	-24	-23	-22	-21	-20	-19	-18
Alphabetic	J	K	L	M	N	O	P	Q	R
Number	10	11	12	13	14	15	16	17	18
	-17	-16	-15	-14	-13	-12	-11	-10	-9
Alphabetic	S	T	U	V	W	X	Y	Z	space
Number	19	20	21	22	23	24	25	26	27
	-8	-7	-6	-5	-4	-3	-2	-1	0

Step 3: convert the message text to be encoded into different numbers $l_1, l_2, ..., l_m$ for each block. That is, we defined $P^i = \begin{bmatrix} l_1^i \\ l_2^i \\ \vdots \\ l_m^i \end{bmatrix}$ which is represented the plaintext for B_i.

Step 4: compute matrices multiplication

$$\begin{bmatrix} c_1^i \\ c_2^i \\ \vdots \\ c_m^i \end{bmatrix} \equiv \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1m} \\ h_{21} & h_{22} & \cdots & h_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ h_{n1} & h_{n2} & \cdots & h_{mm} \end{bmatrix} \begin{bmatrix} l_1^i \\ l_2^i \\ \vdots \\ l_m^i \end{bmatrix} (\text{mod } 27)$$

for all $i = 1, 2, ..., n$ or we can express as the following:

$$c_1^i \equiv (\sum_{k=1}^{n} h_{1k} l_k^i) \text{ mod } 27$$
$$\vdots$$
$$c_m^i \equiv (\sum_{k=1}^{n} h_{nk} l_k^i) \text{ mod } 27$$

where *C* is column vectors of length *m*, representing the ciphertext respectively and *H_m* is a matrix, which must be known for both Sender and Receiver.

2.1.2 Decrypting process 1

Multiplying the encrypted text by the inverse key Hadamard matrix H_m.

Since we known that $\det(H_m) = m^{\frac{m}{2}}$, we see that $\det(H_m)$ and *m* are relatively prime then there exists a unique integer a^* such that $\det(H_m)(\det(\text{H}_m))^* \equiv 1(\text{mod } m)$.

$$\begin{bmatrix} l_1^i \\ l_2^i \\ \vdots \\ l_m^i \end{bmatrix} = \frac{1}{\det(H_m)} adj(H_m) \begin{bmatrix} c_1^i \\ c_2^i \\ \vdots \\ c_m^i \end{bmatrix} (\text{mod } 27)$$

$$= \det(H_m)^* adj(H_m) \begin{bmatrix} c_1^i \\ c_2^i \\ \vdots \\ c_m^i \end{bmatrix} (\text{mod } 27)$$

Example 3.1 Use the key matrix

$$B = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Let us show how to encrypt the message "HELP HIM". According to the algorithm we must sort the message into 2 blocks and *m* = 4. That is, we have that

$$B_1 : \text{"HELP"} \Rightarrow X_1 = \begin{bmatrix} 8 \\ 5 \\ 12 \\ 16 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 14 \\ 1 \\ 15 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \\ 12 \\ 16 \end{bmatrix} (\text{mod } 27)$$

which means $B_1 : \text{"HELP"} \Rightarrow \text{NAOG}$.

$$B_2 : \text{"\_HIM"} = \begin{bmatrix} 27 \\ 8 \\ 9 \\ 13 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 3 \\ 12 \\ 14 \\ 23 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 27 \\ 8 \\ 9 \\ 13 \end{bmatrix} (\text{mod } 27)$$

That is, $B_2 : \text{"\_HIM"} \Rightarrow \text{CLNW}$. Therefore, the message “HELP HIM” encrypted to cipher text as “NAOR CLNW”.

To decrypt the message “NAOR CLNW” to the original one, we use the inverse of a key matrix, such that

$$B^{-1} = \frac{1}{\det(B)} adj(A)(\bmod 27) = \frac{1}{16}\begin{bmatrix}4 & -4 & -4 & 4\\ 4 & 4 & -4 & -4\\ 4 & -4 & 4 & -4\\ 4 & 4 & 4 & 4\end{bmatrix}(\bmod 27)$$

$$= 22\begin{bmatrix}4 & -4 & -4 & 4\\ 4 & 4 & -4 & -4\\ 4 & -4 & 4 & -4\\ 4 & 4 & 4 & 4\end{bmatrix}(\bmod 27) \;= \begin{bmatrix}7 & 20 & 20 & 7\\ 7 & 7 & 20 & 20\\ 7 & 20 & 7 & 20\\ 7 & 7 & 7 & 7\end{bmatrix}$$

To decrypt the cipher-block message, we use the decrypted process

$$\begin{bmatrix}l_1^i\\ l_2^i\\ \vdots\\ l_m^i\end{bmatrix} = \det(H_m)^* adj(H_m)\begin{bmatrix}c_1^i\\ c_2^i\\ \vdots\\ c_m^i\end{bmatrix}(\bmod 27)$$

$$\Rightarrow \begin{bmatrix}8\\ 5\\ 12\\ 16\end{bmatrix} = \begin{bmatrix}7 & 20 & 20 & 7\\ 7 & 7 & 20 & 20\\ 7 & 20 & 7 & 20\\ 7 & 7 & 7 & 7\end{bmatrix}\begin{bmatrix}14\\ 1\\ 15\\ 18\end{bmatrix}(\bmod 27)$$

That is, we have cipher-block message $B_1 : \text{"HELP"}$. Similarly, we also have cipher-block message $B_2 : \text{"}NEED\text{"}$.

We end this section by presenting the new algorithm in cryptography system with the key Hadamard matrix *Hm*. Specifically, our algorithm is achieved by improving the algorithm proposed by Abedal-Hamza and Baneen. Let us mention this briefly.

Definition 3.2 A square matrix *A* is called an orthogonal of type I matrix if $A^k(A^t)^k = I_n$ and $(A^t)^k A^k = I_n$ for some $k \in \mathbb{N}$

If *k* is the smallest positive integer such above equations holds then we say that *A* is an orthogonal of type I of period *k* and we denote it by *ind(A)*. Moreover, let us point that if A is an orthogonal of type I matrix of index k, then $\det(A^k) = \pm 1$. Clearly, $\frac{1}{\sqrt{m}} H_m$ is an orthogonal of type I of period 1. According to Abedal-Hamza and Baneen (Abedal-Hamza & Baneen, 2017b), we apply the following code to obtain encrypted text $en = (C^{k+1})^{-1}\exp(D\ )C^{k+1}X$ for $k = 1, 2$

where $X \ = \begin{bmatrix}l_1\\ l_2\\ \vdots\\ l_m\end{bmatrix}$ which is represented the plaintext for *Bi* and

$$\exp(D\ ) = \begin{bmatrix}e^{l_1} & 0 & 0 & 0\\ 0 & e^{l_2} & 0 & 0\\ \vdots & & \vdots & \vdots\\ 0 & 0 & 0 & e^{l_n}\end{bmatrix}$$

To decrypt the cipher-block message, we use the decrypted process:

$$de \ = (C^3)en$$

Let us report some cases that might make a mistake between the sender and the receiver. Let choose the word "NEED" and the orthogonal of type I matrix of index 2 as follows:

$$C = \begin{bmatrix}-5 & 6 & 0 & 0\\ -4 & 5 & 0 & 0\\ 0 & 0 & -5 & 6\\ 0 & 0 & -4 & 5\end{bmatrix} \Rightarrow C^3 = \begin{bmatrix}-5 & 6 & 0 & 0\\ -4 & 5 & 0 & 0\\ 0 & 0 & -5 & 6\\ 0 & 0 & -4 & 5\end{bmatrix} \Rightarrow$$

$$(C^3)^{-1} = \begin{bmatrix}-5 & 6 & 0 & 0\\ -4 & 5 & 0 & 0\\ 0 & 0 & -5 & 6\\ 0 & 0 & -4 & 5\end{bmatrix}$$

and $B : \text{"NEED"} \Rightarrow X = \begin{bmatrix}14\\ 5\\ 5\\ 4\end{bmatrix}$. That is, we have that

$$en = (C^3)^{-1}\exp(D)C^3X \ = \begin{bmatrix}-186e^5 + 290e^{14}\\ 160e^{14} - 155e^5\\ 125e^5 - 120e^5\\ 100e^5 - 24e^5\end{bmatrix}$$

where the matrix $\exp(D)$ is given by $\begin{bmatrix}e^{14} & 0 & 0 & 0\\ 0 & e^5 & 0 & 0\\ 0 & 0 & e^5 & 0\\ 0 & 0 & 0 & e^4\end{bmatrix}$.

According to the decrypted process, it's easy to see that *e⁴* is missing. That is, the receiver will missing the *e⁴* which corresponding the alphabet "D"

$$de \ = (C^3)en \ = \begin{bmatrix}-5 & 6 & 0 & 0\\ -4 & 5 & 0 & 0\\ 0 & 0 & -5 & 6\\ 0 & 0 & -4 & 5\end{bmatrix}\begin{bmatrix}-186e^5 + 200e^{14}\\ 160e^{14} - 155e^5\\ 5e^5\\ 4e^5\end{bmatrix}$$

As we described above, we then improve and propose the new algorithm cryptography system as shown below.

2.2 Algorithm 2

2.2.1 Encrypting process 2

Step 1: divide the message text into n blocks $B_1, B_2, ..., B_n$, each block contains the same number, m, of the alphabet.

Step 2: choose the Hadamard matrix *H* for each *B*ᵢ for all $i \in \mathbb{N}$

Step 3: construct $C_i \equiv HX_i (\bmod 27)$ and

$$E_i = C_i + \begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix}_{n\times 1} \quad \text{where } X_i = \begin{bmatrix} l_1\\ l_2\\ \vdots\\ l_{m_i}\end{bmatrix} \text{ and } i = 1,2,...,\text{n}.$$

Step 4: Apply the following code to obtain encrypted text

$$en_i = H^T \exp(D_i)\,\mathrm{E}_i$$

2.2.2 Decrypting process 2

Multiplying the encrypted text en_i by Hadamard matrix *H* such that $dn_i = Hen_i$

Example 3.2 Use the key Hadamard matrix

$$B = \begin{bmatrix} 1 & 1 & 1 & 1\\ -1 & 1 & -1 & 1\\ -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1\end{bmatrix}$$

Let us show again how to encrypt the message "HELP HIM" We must sort the message into two blocks with *m* = 4. According to example 3.1, we obtain the following matrix

$$B_1:\text{"HELP"} \Rightarrow X_1 = \begin{bmatrix}8\\5\\12\\16\end{bmatrix} \Rightarrow \begin{bmatrix}14\\1\\15\\7\end{bmatrix} + \begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \begin{bmatrix}15\\2\\16\\8\end{bmatrix} = E_1$$

$$en_1 = H^T \exp(D_1)\,\mathrm{E}_1$$

$$en_1 = \begin{bmatrix} 1 & -1 & -1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & 1 & -1\\ 1 & 1 & 1 & 1\end{bmatrix}\begin{bmatrix} e^8 & 0 & 0 & 0\\ 0 & e^5 & 0 & 0\\ 0 & 0 & e^{12} & 0\\ 0 & 0 & 0 & e^{16}\end{bmatrix}\begin{bmatrix}15\\2\\16\\8\end{bmatrix}$$

$$= \begin{bmatrix} -2e^5 + 15e^8 - 16e^{12} + 8e^{16}\\ 2e^5 + 15e^8 - 16e^{12} - 8e^{16}\\ -2e^5 + 15e^8 + 16e^{12} - 8e^{16}\\ 2e^5 + 15e^8 + 16e^{12} + 8e^{16}\end{bmatrix},$$

which is the message “HELP HIM” encrypted to cipher text.

To decrypt the cipher-block message, we use the decrypted process:

$$dn_1 = Hen_1$$

$$dn_1 = \begin{bmatrix} 1 & 1 & 1 & 1\\ -1 & 1 & -1 & 1\\ -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1\end{bmatrix}\begin{bmatrix} -2e^5 + 15e^8 - 16e^{12} + 8e^{16}\\ 2e^5 + 15e^8 - 16e^{12} - 8e^{16}\\ -2e^5 + 15e^8 + 16e^{12} - 8e^{16}\\ 2e^5 + 15e^8 + 16e^{12} + 8e^{16}\end{bmatrix} = \begin{bmatrix}60e^8\\ 8e^5\\ 64e^{12}\\ 32e^{16}\end{bmatrix}$$

$60e^8$ the number 8 represents the character"H"

$8e^5$ the number 5 represents the character"E"

$64e^{12}$ the number 12 represents the character"L"

$32e^{16}$ the number 16 represents the character"P"

Similarly, for $B_2:\text{"\_HIM"} = \begin{bmatrix}27\\8\\9\\13\end{bmatrix}$ we have

$$E_2 = \begin{bmatrix}3\\12\\14\\23\end{bmatrix} + \begin{bmatrix}1\\1\\1\\1\end{bmatrix} = \begin{bmatrix}4\\13\\15\\24\end{bmatrix}$$

$$en_2 = \begin{bmatrix} 1 & -1 & -1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & 1 & -1\\ 1 & 1 & 1 & 1\end{bmatrix}\begin{bmatrix} e^{27} & 0 & 0 & 0\\ 0 & e^8 & 0 & 0\\ 0 & 0 & e^9 & 0\\ 0 & 0 & 0 & e^{13}\end{bmatrix}\begin{bmatrix}4\\13\\15\\24\end{bmatrix}:$$

$$= \begin{bmatrix} 4e^{27} - 13e^8 - 15e^9 + 24e^{13}\\ 4e^{27} + 13e^8 - 15e^9 - 24e^{13}\\ 4e^{27} - 13e^8 + 15e^9 - 24e^{13}\\ 4e^{27} + 13e^8 + 15e^9 + 24e^{13}\end{bmatrix}$$

To decrypt the cipher-block message, we use the decrypted process:

$$dn_2 = Hen_2$$

$$dn_2 = \begin{bmatrix} 1 & 1 & 1 & 1\\ -1 & 1 & -1 & 1\\ -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1\end{bmatrix}\begin{bmatrix} 4e^{27} - 13e^8 - 15e^9 + 24e^{13}\\ 4e^{27} + 13e^8 - 15e^9 - 24e^{13}\\ 4e^{27} - 13e^8 + 15e^9 - 24e^{13}\\ 4e^{27} + 13e^8 + 15e^9 + 24e^{13}\end{bmatrix} = \begin{bmatrix}16e^{27}\\ 52e^8\\ 60e^9\\ 96e^{13}\end{bmatrix}$$

$16e^{27}$ the number 27 represents the character"_"

$52e^8$ the number 8 represents the character"H"

$60e^9$ the number 9 represents the character"I"

$96e^{13}$ the number 13 represents the character"M"

3. Conclusions

In this paper, we are only constructed a new algorithm in cryptography by using the available material from the Hadamard matrix but also improved the algorithm proposed by Abedal-Hamaza.

Acknowledgements

The author is supported by School of Science University of Phayao under Grant No. Sc04/2563.

References

Abedal-Hamza, M. H., & Baneen, K. I. (2017). Orthogonal of type I matrices with application. *Applied Mathematical Sciences, 11*(40), 1983-1994.

Abedal-Hamza, M. H., & Hussein, H. A. (2015). Construction new types of matrices. *International Journal of Mathematics Trends and Technology, 24*(2), 84-91.

Abdulaziz, B. M. H., & Ibrahim, O. A. A. (2017). Encrypt and decrypt messages using invertible matrices modulo 27. *American Journal of Engineering Research, 6*(6), 212-217.

Horadam, K. J. (2007). *Hadamard matrices and their applications*. Princeton, NJ: Princeton University Press.

Manjhi, P. K., & Arjun, K. (2018). On the construction of Hadamard matrices. *International Journal of Pure and Applied Mathematics, 120*(1), 51–58.