Thai Journal of Mathematics
Volume 19 Number 4 (2021)
Pages 1671–1683
http://thaijmath.in.cmu.ac.th

ISSN 1686-0209

Encryption Schemes Using Anti-Orthogonal of Type I Matrices

Nilobol Kamyun[1], Krittiya Pingyot[1] and Supunnee Sompong[2,*]

[1] *Department of Mathematics, School of Science, University of Phayao, Thailand*
e-mail : nilobol.ka@up.ac.th (N. Kamyun); Krittiya.pingyot.ingfha@gmail.com (K. Pingyot)

[2] *Department of Mathematics and Statistics, Faculty of Science and Technology, Sakon Nakhon Rajabhat University, Thailand*
e-mail : s_sanpinij@yahoo.com

Abstract Applications of the orthogonal matrix have been applied to many circumstance such as signal processing, image processing, coding theory, cryptology. In this paper, we are not only introduce the new type of matrices, anti-orthogonal and H-anti-orthogonal of type I matrices but also apply these matrices in cryptology.

MSC: 11B99; 11C20; 15A10
Keywords: anti-orthogonal; H-anti-orthogonal; cryptography

Submission date: 28.05.2020 / Acceptance date: 19.03.2021

1. Introduction

Applications of the orthogonal matrix, $AA^T = I_n$, have been applied to many circumstance such as signal processing , image processing, coding theory, cryptology. The highlight of using orthogonal matrices come from the fact that the computation of inverse matrices is avoided, simply by using the transpose of the orthogonal matrix. The orthogonal matrix is often referred as Hadamard matrices that were first defined by Sylvester and extensively studied by Hadamard. The concept of orthogonality has been extended into various circumstances which are relaxed or generalized.

In 2017, A. M. Hamza and B. K.Imran [1] introduced a new type of matrices, we called it orthogonal of type I matrix. That is, a square matrix A is said to be orthogonal of type I matrix if $A^k(A^T)^k = I_n$, for some $k \in \mathbb{N}$. Clearly, it is a generalization of orthogonal matrices. As we said above, the useful fact of these matrices comes from the fact that they are invertible and their inverses are derived by simple calculations. Moreover, this matrix is used to construct a new algorithm in cryptography which consists of two parts: Encryption and Decryption. In detail, encryption is the process of masking in the information such as the plain text. On the other hand, decryption is the process of

[*] Corresponding author.

Published by The Mathematical Association of Thailand.

converting ciphertext to its original. Specifically, the encryption and decryption processes are given the Figure 1.

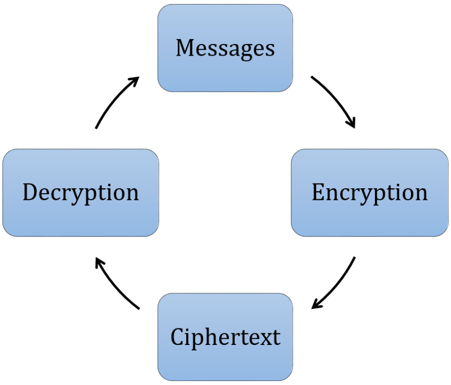

Figure 1. Messages cryptography cycle

Unfortunately, there are some cases that might a mistake between the sender and the receiver. Before we briefly described the algorithm, let us prepare the table for alphabets and numbers and its corresponding positive and negative integers value as shown in Tables 1.1 and 1.2.

Table 1.1 Numeral encryption table

1	2	3	4	5	6	7	8	9	10
1	2	3	4	5	6	7	8	9	0

Table 1.2 Letter encryption table

11	12	13	14	15	16	17	18	19	20	21	22	23
A	B	C	D	E	F	G	H	I	J	K	L	M
24	25	26	27	28	29	30	31	32	33	34	35	36
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Next, let us choose the word BLUE and the othogonal of type I matrix of index 2 as follows:

$$C = \begin{bmatrix} -11 & 6 & 0 & 0 \\ -20 & 11 & 0 & 0 \\ 0 & 0 & -11 & 6 \\ 0 & 0 & -20 & 11 \end{bmatrix},$$

According to A. M. Hamza, we apply the following code to obtain encrypted text

$$en = ((C)^3)^{-1} e^D (C)^3 X,$$

where we have the following:

$$(C)^3 = \begin{bmatrix} -11 & 6 & 0 & 0 \\ -20 & 11 & 0 & 0 \\ 0 & 0 & -11 & 6 \\ 0 & 0 & -20 & 11 \end{bmatrix}, \; X = \begin{bmatrix} 12 \\ 22 \\ 31 \\ 15 \end{bmatrix}$$

$$((C)^3)^{-1} = \begin{bmatrix} -11 & 6 & 0 & 0 \\ -20 & 11 & 0 & 0 \\ 0 & 0 & -11 & 6 \\ 0 & 0 & -20 & 11 \end{bmatrix} \text{ and } e^D = \begin{bmatrix} e^{12} & 0 & 0 & 0 \\ 0 & e^{22} & 0 & 0 \\ 0 & 0 & e^{31} & 0 \\ 0 & 0 & 0 & e^{15} \end{bmatrix}.$$

Therefore, the encryption equation below are created as ciphertext below:

$$en = ((C)^3)^{-1} e^D (C)^3 X = \begin{bmatrix} 12e^{22} \\ 22e^{22} \\ 2,761e^{31} - 2,730e^{15} \\ 5,020e^{31} - 5,005e^{15} \end{bmatrix}.$$

Multiplying the encrypted text en by C^3 as decrypted process.

$$de = (C)^3(en) = \begin{bmatrix} 0 \\ 2e^{22} \\ -251e^{31} \\ -455e^{15} \end{bmatrix}.$$

It clearly to see that e^{12} is missing which means that the receiver will missing the alphabet B.

The paper is organized as follow: in section 3 and 4, we introduce the new type of matrices and they are invertible which simple calculate inverse matrix is achieved. Section 5 concentrates on providing the new method of secretly sending messages by improving the algorithm which proposed by A. M. Hamza as we described above.

2. Preliminaries

In this paper, $A \in M_{n\times n}(\mathbb{C})$ such that $det(A)$, $ind(A)$, $\overline{A}$, A^T, A^*, A^H, $ind_H(A)$ and A^θ means the determinant, index, conjugate, transpose, conjugate transpose, H-transpose, H-index and conjugate H-transpose of matrix A , respectively.

Definition 2.1 ([2]). Let $A_{n\times n}$ be a square matrix, A is said to be orthogonal if $AA^T = I_n$

Definition 2.2 ([3]). Let $A_{n\times n}$ be a square matrix, A is said to be anti-orthogonal if $AA^T = -I_n$

Definition 2.3 ([1]). Let $A_{n\times n}$ be a square matrix, A is said to be orthogonal of type I matrix if $A^k(A^T)^k = I_n$, for some $k \in \mathbb{N}$.

Definition 2.4 ([4]). Let $A_{n\times n}$ be a square matrix. The H-transpose of matrix A is defined by $A^H = [a^H_{ij}] = [a_{(n+1-j)(n+1-i)}]$, where $i, j = 1, 2, 3, ..., n$.

Example 2.5. Let $A = \begin{bmatrix} 0 & -i & 7 \\ 5 & 4 & -2 \\ 1 & 3 & 2+i \end{bmatrix}$, thus $A^H = \begin{bmatrix} 2+i & -2 & 7 \\ 3 & 4 & -i \\ 1 & 5 & 0 \end{bmatrix}$.

Theorem 2.6 ([5]). *Let k be a natural number and $A_{n\times n}, B_{n\times n}$ are square matrix, then:*
1. $(A^H)^H = A$
2. $(A^H)^T = (A^T)^H$
3. $(\overline{A})^H = \overline{(A^H)}$
4. $(AB)^H = B^H A^H$
5. $(A^H)^{-1} = (A^{-1})^H$
6. $(A^k)^H = (A^H)^k$
7. $det(A) = det(A^H) = det(A^T) = det(A^T)^H$
8. A *and* A^H *have the same eigenvalues*
9. $(A^\theta)^\theta = A$
10. $(AB)^\theta = B^\theta A^\theta$
11. $(A^k)^\theta = (A^\theta)^k$

Definition 2.7 ([5]). Let $A_{n\times n}$ be a square matrix, A is said to be H-orthogonal of type I matrix if $A^k(A^H)^k = I_n$, for some $k \in \mathbb{N}$.

3. Anti-Orthogonal of Type I Matrices

In this chapter we present all our results which consist the proof of theorems and examples of anti-orthogonal of type I matrices.

Definition 3.1 ([6]). A square matrix $A_{n\times n}$ is called anti-orthogonal of type I matrix if $A^k(A^T)^k = -I_n$ for some $k \in \mathbb{N}$.

The smallest positive integer k with $A^k(A^T)^k = -I_n$ is called the index of A. We say that A is anti-orthogonal of type I matrix of index k. The index of A is denoted by $ind(A)$.

Remark 3.2. From Definition 3.1, we can see that:

1. $A^k(A^T)^k = -I_n$ if and only if $(A^T)^k A^k = -I_n$.

2. If A is anti-orthogonal of type I matrix then A is orthogonal of type I matrix. Since if $A^k(A^T)^k = -I_n$ for some $k \in \mathbb{N}$, then we have $A^{2k}(A^T)^{2k} = [A^kA^k][(A^T)^k(A^T)^k] = [A^k(A^T)^k][A^k(A^T)^k] = I_n$.

3. If A is orthogonal of type I matrix of index k, where k is odd number, then iA is anti-orthogonal of type I matrix. Since if $A^k(A^T)^k = I_n$ for some odd number $k \in \mathbb{N}$, then we have $(iA)^k((iA)^T)^k = (i)^{2k}A^k(A^T)^k = -I_n$. Therefore, iA is anti-orthogonal of type I matrix.

Example 3.3. 1. Let $A = \begin{bmatrix} -1 & 1+i \\ -1 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -i & 0 \\ i & i & 0 \\ 0 & 0 & i \end{bmatrix}$, $C = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}$, $D = \begin{bmatrix} 1 & -1+i \\ 1 & -1 \end{bmatrix}$, $E = \begin{bmatrix} \sqrt{i} & 0 \\ 0 & \sqrt{i} \end{bmatrix}$ and $F = \begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -1 \end{bmatrix}$.

We have, $A^2(A^T)^2 = -I_n, B^3(B^T)^3 = -I_n, CC^T = -I_n$, $D^2(D^T)^2 = -I_n$ and $E^2(E^T)^2 = -I_n$. Thus, A, B, C, D and E are anti-orthogonal of type I matrices. It follows that $ind(A) = 2, ind(B) = 3, ind(C) = 1, ind(D) = 2$ and $ind(E) = 2$. But F is not anti-orthogonal of type I matrix.

2. From 1, we can see that $AD \neq DA, C(-C) = I_2 = (-C)C$ and $AD, DA, C(-C)$ is not anti-orthogonal of type I matrix. But $E^2 = C$ is anti-orthogonal of type I matrix.

Thus, in general, multiplication of anti-orthogonal of type I matrix need not to be anti-orthogonal of type I matrix.

Theorem 3.4. *If $A_{n\times n}$ is anti-orthogonal of type I matrix of index k, then*

$$det(A^k)=\begin{cases}\pm i, & n \text{ is odd,}\\ \pm 1, & n \text{ is even.}\end{cases}$$

Proof. Let A be anti-orthogonal of type I matrix of index k. Thus, $A^k(A^T)^k = -I_n$, for some $k \in \mathbb{N}$. Next, we observe that $[det(A^k)]^2 = det(A^k)(det(A^T)^k) = det(A^k(A^T)^k) = det(-I_n) = (-1)^n$. Therefore, we can conclude that $det(A^k) = \pm\ 1$ if n is even. Otherwise, $det(A^k) = \pm\ i$. ■

Theorem 3.5. *If $A_{n\times n}$ is anti-orthogonal of type I matrix of index k, then it is invertible with $A^{-1} = -A^{k-1}(A^T)^k$.*

Proof. By Theorem 3.4 we have $det(A) \neq 0$, it implied that A is invertible matrix. Since A is anti-orthogonal of type I matrix, there is $k \in \mathbb{N}$ such that $A^k(A^T)^k = -I_n$.Then, we have that $-A^k(A^T)^k = I_n$. It follows that $A^{-1} = -A^{k-1}(A^T)^k$. The prove is completed. ■

Theorem 3.6. *Let $A_{n\times n}$ be a square matrix , then the following statements are equivalent:*
1. A is anti-orthogonal of type I matrix.
2. A^{-1} is anti-orthogonal of type I matrix.
3. A^T is anti-orthogonal of type I matrix.
4. $\bar{A}$ is anti-orthogonal of type I matrix.
5. A^* is anti-orthogonal of type I matrix.

Proof. (1 ⇒ 2) Suppose that A is anti-orthogonal of type I matrix. Then, there is $k \in \mathbb{N}$ such that $A^k(A^T)^k = -I_n$. From remark 3.2, we can see that $[(A^T)^kA^k]^{-1} = (-I_n)^{-1}$, it follows that $(A^{-1})^k((A^{-1})^T)^k = -I_n$.
Hence A^{-1} is anti-orthogonal of type I matrix.

(2 ⇒ 3) Suppose that A^{-1} is anti-orthogonal of type I matrix. Then, there is $k \in \mathbb{N}$ such that $(A^{-1})^k((A^{-1})^T)^k = -I_n$.

We consider the following $[((A^{-1})^T)^k(A^{-1})^k]^{-1} = (-I_n)^{-1}$. Thus, we have $A^k(A^T)^k = [(A^{-1})^k]^{-1}[((A^{-1})^T)^k]^{-1} = -I_n$. From remark 3.2, we have $(A^T)^k[(A^T)^T]^k = (A^T)^kA^k = -I_n$. Hence, A^T is anti-orthogonal of type I matrix.

(3 ⇒ 4) Suppose that A^T is anti-orthogonal of type I matrix. Then, there is $k \in \mathbb{N}$ such that $(A^T)^k((A^T)^T)^k = -I_n$. From remark 3.2 and conjugate of matrix, we have $(\bar{A})^k((\bar{A})^T)^k = \overline{(A^k)}\ \overline{(A^T)^k} = \overline{A^k(A^T)^k} = \overline{-I_n} = -I_n$. Hence, $\bar{A}$ is anti-orthogonal of type I matrix.

(4 ⇒ 5) Suppose that $\bar{A}$ is anti-orthogonal of type I matrix. Then, there is $k \in \mathbb{N}$ such that $(\bar{A})^k[(\bar{A})^T]^k = -I_n$. Thus, $((\bar{A})^T)^k(\bar{A})^k = -I_n$ and so we have $(A^*)^k((A^*)^T)^k = -I_n$. Hence, A^* is anti-orthogonal of type I matrix.

(5 ⇒ 1) Suppose that A^* is anti-orthogonal of type I matrix. Then, there is $k \in \mathbb{N}$ such that $(A^*)^k((A^*)^T)^k = -I_n$. It follows that $((A^*)^T)^k(A^*)^k = -I_n$. Thus, $A^k(A^T)^k = ((A^*)^*)^k[((A^*)^*)^T]^k = [((A^*)^T)^k(A^*)^k]^* = (-I_n)^* = -I_n$. Hence, A is anti-orthogonal of type I matrix. ■

Theorem 3.7. *If A is anti-orthogonal of type I matrix of index k, then each of A^T, A^{-1}, $\bar{A}$ and A^* are anti-orthogonal of type I matrix of index k.*

Proof. Assume that A is anti-orthogonal of type I matrix of index k, then A^T is anti-orthogonal of type I matrix with $ind(A^T) \leq k$.
Suppose that $ind(A^T) = r, 1 \leq r < k$. Then $(A^T)^r A^r = -I_n$, so by remark 3.2 we have $A^r(A^T)^r = -I_n$. Thus, $ind(A) = r < k$, which is a contradiction. Hence, $ind(A^T) = k$. Similarly with respect to $A^{-1}, \bar{A}$ and A^*. ■

4. H-Anti-Orthogonal of Type I Matrices

In this chapter, we present all our results and examples of H-anti-orthogonal of type I matrices. The proof in section 4 can be obtained similar to the proof of theorem in section 3. So, we shall omit our proof.

Definition 4.1. A square matrix $A_{n\times n}$ is called a H-anti-orthogonal of type I matrix if $A^k(A^H)^k = -I_n$ for some $k \in \mathbb{N}$.

The smallest positive integer k with $A^k(A^H)^k = -I_n$ is called the H-index of A. We say that A is H-anti-orthogonal of type I of H-index k. The H-index of A is denoted by $ind_H(A)$.

Remark 4.2. From Definition 4.1, we can see that:

1. $A^k(A^H)^k = -I_n$ if and only if $(A^H)^k A^k = -I_n$.
2. If A is H-anti-orthogonal of type I matrix, then A is H-orthogonal of type I matrix.
3. If A is H-orthogonal of type I matrix of H-index k, where k is odd number, then iA is H-anti-orthogonal of type I matrix.

Example 4.3. Let $A = \begin{bmatrix} 0 & -i & 0 & 0 \\ i & i & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & i \end{bmatrix}$ and $B = \begin{bmatrix} 0 & -i & 0 \\ i & i & 0 \\ 0 & 0 & i \end{bmatrix}$.

Thus, A is H-anti-orthogonal of type I matrices, but B is not H-anti-orthogonal of type I matrix.

Theorem 4.4. *If $A_{n\times n}$ is H-anti-orthogonal of type I matrix of H-index k, then*

$$det(A^k) = \begin{cases} \pm i, & n \text{ is odd}, \\ \pm 1, & n \text{ is even}. \end{cases}$$

Theorem 4.5. *If $A_{n\times n}$ is H-anti-orthogonal of type I matrix of H-index k, then it is invertible with $A^{-1} = -A^{k-1}(A^H)^k$.*

Theorem 4.6. *Let $A_{n\times n}$ be a square matrix , then the following statements are equivalent:*

1. A is H-anti-orthogonal of type I matrix.
2. A^{-1} is H-anti-orthogonal of type I matrix.
3. A^H is H-anti-orthogonal of type I matrix.
4. $\bar{A}$ is H-anti-orthogonal of type I matrix.
5. A^θ is H-anti-orthogonal of type I matrix.

Theorem 4.7. *If A is H-anti-orthogonal of type I matrix of H-index k, then each of A^H, A^{-1}, $\bar{A}$ and A^θ are H-anti-orthogonal of type I matrix of H-index k.*

To this end let we describe of some relation between anti-orthogonal of type I matrix and H-anti-orthogonal of type I matrix. We observe that anti-orthogonal of type I matrix need not to be H-anti-orthogonal of type I matrix and H-anti-orthogonal of type I matrix need not to be anti-orthogonal of type I matrix in general. We will show in the following example.

Example 4.8. Let a square matrices

$$A = \begin{bmatrix} 1 & -1+i \\ 1 & -1 \end{bmatrix}, \ B = \begin{bmatrix} 0 & -i & 0 \\ i & i & 0 \\ 0 & 0 & i \end{bmatrix} \text{ and } C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

Then, we can see that A is both anti-orthogonal of type I matrix and H-anti-orthogonal of type I matrix. B is anti-orthogonal of type I matrix, but B is not H-anti-orthogonal of type I matrix. C is H-anti-orthogonal of type I matrix, but C is not anti-orthogonal of type I matrix.

5. Cryptography Using Anti-Orthogonal of Type I Matrices

This section concentrates on providing the new method of secretly sending messages by improving the algorithm which proposed by A. M. Hamza as we described in section 1.

1. A person thinks of a secret message that they want to send to another person (someone else). To send a secreted message from one person to the other, the first one needs to think of a secret message. For this purpose as an example, lets choose a message to be ROOM NUMBER 101.

2. Next, the secret message must be divided into blocks with each block representing one word.

3. For each block that represents each word, a suitable anti-orthogonal matrix must be selected.

4. To encrypt the message, the following equation can be used:

$$en_i = ((C_i)^{k_i+1})^{-1} e^{D_i} |(C_i)^{k_i+1}| X_i, \text{ when } k_i = 1, 2$$

$$en_i = ((C_i)^{k_i-1})^{-1} e^{D_i} |(C_i)^{k_i-1}| X_i, \text{ when } k_i > 2$$

$$e^{D_i} = \begin{bmatrix} e^{l_1} & 0 & \cdots & 0 \\ 0 & e^{l_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{l_{m_i}} \end{bmatrix}_{m_i \times m_i} \quad \text{and}$$

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

5. The message can be decrypted by incorporating the result from encryption equation into the following formula:

$$de_i = |(C_i)^{k_i - 1}|(en_i).$$

Example 5.1. For the example lets take **ROOM NUMBER 101** as a secret message: Cryptography can be used to encrypt this three-word message ROOM NUMBER 101

Before proceeding, we must divide this message into three blocks. Each block will represent one word.

[ROOM BLOCK 1; NUMBER BLOCK 2; 101 BLOCK 3]

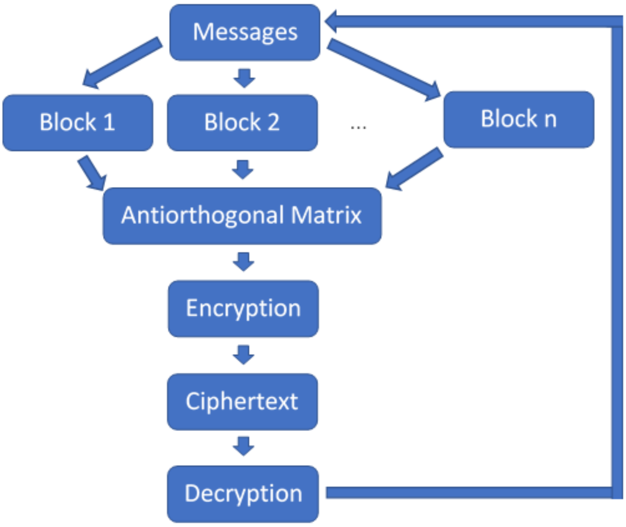

FIGURE 2. Step by Step diagram for encryption and decryption

BLOCK 1 ROOM

1. First, we choose the anti-orthogonal of type I matrix, which is a 4 × 4 matrix that is suitable for using for a four-letter word.

$$C_1 = \begin{bmatrix} 0 & -i & 0 & 0 \\ i & i & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & i \end{bmatrix}, \text{ when } k_1 = 3.$$

2. Second, we utilize anti-orthogonal of type I matrix from step one to calculate $(C_1)^2, |(C_1)^2|, ((C_1)^2)^{-1}, e^{D_1}$ and X_1 are shown as follows:

$$(C_1)^2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \ |(C_1)^2| = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \ X_1 = \begin{bmatrix} 28 \\ 25 \\ 25 \\ 23 \end{bmatrix}$$

$$((C_1)^2)^{-1} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \text{ and } e^{D_1} = \begin{bmatrix} e^{28} & 0 & 0 & 0 \\ 0 & e^{25} & 0 & 0 \\ 0 & 0 & e^{25} & 0 \\ 0 & 0 & 0 & e^{23} \end{bmatrix}.$$

3. The results gathered from step 2 can be incorporated into the encryption equation below to create ciphertext:

$$en_1 = ((C_1)^2)^{-1} e^{D_1} |(C_1)^2| X_1 = \begin{bmatrix} -28e^{25} \\ 53e^{28} + 28e^{25} \\ -25e^{23} \\ 48e^{25} + 25e^{23} \end{bmatrix}.$$

4. Ciphertext received from step 3 can be used to decrypt the secret message by substituting it into the decryption equation below:

$$de_1 = |(C_1)^2|(en_1) = \begin{bmatrix} 53e^{28} \\ -28e^{25} \\ 48e^{25} \\ -25e^{23} \end{bmatrix}.$$

5. Using the numbers of both table 1.1 and table 1.2 for each value, the exponent of exponential can be found to find the value of the plain text. Therefore, for Block 1:
$53e^{28}$: Exponent 28, so, the first letter is R
$-28e^{25}$: Exponent 25, so, the second letter is O
$48e^{25}$: Exponent 25, so, the third letter is O
$-25e^{23}$: Exponent 23, so, the fourth letter is M

BLOCK 2 NUMBER

1. First, we choose the anti-orthogonal of type I matrix, which is a 6 × 6 matrix that is suitable for using for a six-letter word.

$$C_2 = \begin{bmatrix} -1 & 1+i & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1+i & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1+i \\ 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}, \text{ when } k_2 = 2.$$

2. Second, we utilize Anti-orthogonal of type I matrix from step one to calculate $(C_2)^3, |(C_2)^3|, ((C_2)^3)^{-1}, e^{D_2}$ and X_2 are shown as follows:

$$(C_2)^3 = \begin{bmatrix} i & 1-i & 0 & 0 & 0 & 0 \\ i & -i & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 1-i & 0 & 0 \\ 0 & 0 & i & -i & 0 & 0 \\ 0 & 0 & 0 & 0 & i & 1-i \\ 0 & 0 & 0 & 0 & i & -i \end{bmatrix},$$

$$|(C_2)^3| = \begin{bmatrix} 1 & \sqrt{2} & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \sqrt{2} & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \sqrt{2} \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$((C_2)^3)^{-1} = \begin{bmatrix} 1 & -1-i & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1-i & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1-i \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix},$$

$$e^{D_2} = \begin{bmatrix} e^{24} & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{31} & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{23} & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{12} & 0 & 0 \\ 0 & 0 & 0 & 0 & e^{15} & 0 \\ 0 & 0 & 0 & 0 & 0 & e^{28} \end{bmatrix} \text{ and } X_2 = \begin{bmatrix} 24 \\ 31 \\ 23 \\ 12 \\ 15 \\ 28 \end{bmatrix}.$$

3. The results gathered from step 2 can be incorporated into the encryption equation below to create ciphertext:

$$en_2 = ((C_2)^3)^{-1} e^{D_2} |(C_2)^3| X_2 = \begin{bmatrix} -55(1+i)e^{3} + (24+31\sqrt{2})e^{24} \\ -55e^{31} + (24+31\sqrt{2})e^{24} \\ (23+12\sqrt{2})e^{23} - 35(1+i)e^{12} \\ (23+12\sqrt{2})e^{23} - 35e^{12} \\ -43(1+i)e^{28} + (15+28\sqrt{2})e^{15} \\ -43e^{28} + (15+28\sqrt{2})e^{15} \end{bmatrix}.$$

4. Ciphertext received from step 3 can be used to decrypt the secret message by substituting it into the decryption equation below:

$$de_2 = |(C_2)^3|(en_2) = \begin{bmatrix} (24+31\sqrt{2})e^{24} \\ 55e^{31} \\ (23+12\sqrt{2})e^{23} \\ 35e^{12} \\ (15+28\sqrt{2})e^{15} \\ 43e^{28} \end{bmatrix}.$$

5. Using the numbers of both table 1.1 and table 1.2 for each value, the exponent of exponential can be found to find the value of the plain text. Therefore, for Block 2:

$(24 + 31\sqrt{2})e^{24}$: Exponent 24, so, the first letter is N
$55e^{31}$: Exponent 31, so, the second letter is U
$(23 + 12\sqrt{2})e^{23}$: Exponent 23, so, the third letter is M
$35e^{12}$: Exponent 12, so, the fourth letter is B
$(15 + 28\sqrt{2})e^{15}$: Exponent 15, so, the fifth letter is E
$43e^{28}$: Exponent 28, so, the sixth letter is R

BLOCK 3 101

1. First, we choose the anti-orthogonal of type I matrix, which is a 3 × 3 matrix that is suitable for using for a three-letter word.

$$C_3 = \begin{bmatrix} 0 & -i & 0 \\ i & i & 0 \\ 0 & 0 & i \end{bmatrix}, \text{ when } k_3 = 3.$$

2. Second, we utilize anti-orthogonal of type I matrix from step one to calculate $(C_3)^2$, $((C_3)^2)^{-1}$, e^{D_3} and X_3 are shown as follows:

$$(C_3)^2 = \begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \ |(C_3)^2| = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$((C_3)^2)^{-1} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \ e^{D_3} = \begin{bmatrix} e^1 & 0 & 0 \\ 0 & e^{10} & 0 \\ 0 & 0 & e^1 \end{bmatrix} \text{ and } X_3 = \begin{bmatrix} 1 \\ 10 \\ 1 \end{bmatrix}.$$

3. The results gathered from step 2 can be incorporated into the encryption equation below to create ciphertext:

$$en_3 = ((C_3)^2)^{-1} e^{D_3} |(C_3)^2| X_3 = \begin{bmatrix} -e^{10} \\ 11e^1 + e^{10} \\ -e^1 \end{bmatrix}.$$

4. Ciphertext received from step 3 can be used to decrypt the secret message by substituting it into the decryption equation below:

$$de_3 = |(C_3)^2| en_3 = \begin{bmatrix} 11e^1 \\ e^{10} \\ e^1 \end{bmatrix}.$$

5. Using the numbers of both table 1.1 and table 1.2 for each value, the exponent of exponential can be found to find the value of the plain text. Therefore, for Block 3:

$11e^1$: Exponent 1, so, the first letter is 1
e^{10} : Exponent 10, so, the second letter is 0
e^1 : Exponent 1, so, the third letter is 1

As we have above example, let us add some useful observation about this method. According from the process of decryption, we see that the key matrix is not unique in general. Specifically, if anti-orthogonal type I is chosen as the key in this method then there is another matrix which we can use as the key matrix to decrypt the message. An example of this follows next.

Example 5.2. For the example lets take **101** as a secret message.

1. First, we choose the H-anti-orthogonal of type I matrix, which is a 3×3 matrix that is suitable for using for a three-letter word.

$$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -1 \end{bmatrix}, \text{ when } k = 3.$$

2. Second, we utilize H-anti-orthogonal of type I matrix from step one to calculate $C^2, (C^2)^{-1}, e^D$ and X.

3. The results gathered from step 2 can be incorporated into the encryption equation below to create ciphertext:

$$en = ((C)^2)^{-1} e^D |(C)^2| X = \begin{bmatrix} e^1 \\ -10e^{10} \\ e^1 \end{bmatrix}.$$

4. Ciphertext received from step 3 can be used to decrypt the secret message by substituting it into the decryption equation below:

$$de = |(C)^2| en = \begin{bmatrix} e^1 \\ -10e^{10} \\ e^1 \end{bmatrix}.$$

5. Using the numbers of both table 1.1 and table 1.2 for each value, the exponent of exponential can be found to find the value of the plain text. Therefore,

e^1 : Exponent 1, so, the first letter is 1
$-10e^{10}$: Exponent 10, so, the second letter is 0
e^1 : Exponent 1, so, the third letter is 1

Acknowledgements

We would like to thank the referees for their useful comments and suggestions on the manuscript.The first author is supported by the School of Science, University of Phayao under Grant No.Sc01/2563.

References

[1] A.M. Hamza, B.K. Imran, Orthogonal of type I matrices with application, Applied Mathematical Sciences 11 (2017) 1983–1994.

[2] D.C. Lay, S.R. Lay, J.J. McDonald, Linear Algebra and Its Applications, 5th Edition, Pearson, USA, 2016.

[3] J.L. Massey, Orthogonal, antiorthogonal and self-orthogonal matrices and their codes, Communications and Coding 2 (1998) 1–7.

[4] A.M. Hamza, H.A. Hussein, Construction new types of matrices, International Journal of Mathematics Trends and Technology 24 (2015) 84–91.

[5] A.M. Hamza, B.K. Imran, A study of H-orthogonal of type I matrices, International Educational Scientific Reaseach Journal 3 (2017) 86–96.

[6] B.O. Al-Fatlawy, A Study of Certain Types of Orthogonal Matrices with Applications, Master's Thesis, University of Kufa, 2017.