Unitary Type - I Matrices and Its Applications in Cryptosystems

*Yamuna A, #Afshan Nifasath A Z

*Assistant Professor, #Scholar, PG & Research Department of Mathematics, A.V.C. College (Autonomous), Mannampandal, Mayiladuthurai, Tamil Nadu, India.

*dr.a.yamuna.avc@gmail.com, #afshanzahirudeen@gmail.com

Abstract: The secure transmission of text information is critical all around the world. One of the approaches for achieving security in communication is cryptography. This paper proposes new type of matrices called Unitary Type-I Matrices for developing new algorithm in cryptographic communication systems. Also, this paper develops some properties of Unitary Type-I Matrices and produces importance in the field of creating complex encryptions. The proposed algorithm using Unitary Type-I Matrices helps to encrypt and decrypt the secured communication of text information.

Keywords: Determinants, Eigen values, Inner product, Unitary Matrix, Encryption, Decryption.

I. INTRODUCTION

Cryptography, the science of encrypting and deciphering messages written in secret codes, has played a vital role in securing information since ancient times [3]. Julius Caesar employed what has become known as the Caesar shift cipher when encoding messages to communicate with his generals. Under this form of encryption technique, each letter in a message is substituted with the letter that was a certain number of places further down the alphabets. Caesar used a shift of three places and so A is replaced by D, B is replaced by E, and so on.

In the modern history, the Nazis continued to use the presumably highly sophisticated Enigma machine to encrypt their messages when they communicated, still unaware that three polish mathematicians had already cracked the unbreakable codes of the Enigma machine and had provided the allied forces with the means to gain access to their top secrets.

More recently, with millions of financial transactions conducted over the internet daily, Cryptography has become more important than ever. Companies have begun to make online transactions more secure by installing encryption software to prevent sensitive information such as credit card numbers falling into wrong hands.

Due to great need of security for passing sensitive data from one individual to another or from one association to another through electronic technology, there is requirement for cryptography as an answer to this issue. Due to big problem of plain text attack, this research will try to solve this problem by employing use of Unitary type-I matrices in the cryptography mechanism [7, 10].

Unitary type-I matrix is a generalization of an unitary matrix [9] which has lot of applications in many fields such as Cryptography, Artificial Intelligence, IOT(Internet Of Things) and other emerging coding fields.

This paper will help to understand an insight of unitary matrices [4, 5] which is considered as most powerful tool in matrices. The influence of matrices in mathematical world spreads important base to many of the principles and practices of cryptosystem. The main aim of this paper is to develop encrypting and decrypting the plain text using Unitary type-I matrices which strengthen the complexity of the cryptography process. Also, the break of encrypted text is more complicated using Unitary type-I matrices than other cryptography process.

II. PRELIMINARIES

Matrix: A matrix [6, 8] may define as an orderly arrangement of some number or symbols in certain rows and columns enclosed by parenthesis / brackets, subscribe by the magnitude of its order and denoted by some capital letter.

Unitary matrix: A square matrix A is said to be an Unitary matrix if $AA^{*} = A^{*}A = I$.

Cryptography: Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Secret key: Secret key or a private key is a piece of information that is used to encrypt and decrypt message in a symmetric manner.

Encoding: This is the process of converting data from one form to another form.

Decoding: This is a conversion of a coded message into intelligible language.

DOI : 10.35291/2454-9150.2022.0492

III. RESULTS AND PROPOSITIONS

Definition 3.1:

A Complex square matrix $C_{n\times n}$is called an **unitary type-I matrix** if

$C^p(C^*)^p = I_n \quad ((C^*)^p C^p = I_n)$, for some $p \in \mathbb{N}$.

Example: $X = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{-i\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & \frac{i\sqrt{2}}{2} \end{bmatrix}$ *and* $Y = \begin{bmatrix} 1 & 1-i \\ 0 & -1 \end{bmatrix}$ are unitary type-I matrices.

Definition 3.2:

Let C be an unitary type-I matrix. The smallest positive integer p with $C^p(C^*)^p = I_n$ is called the index of C.

In such a case, we say that C is an unitary type-I matrix of index p or p-index unitary type-I matrix and it is denoted by $ind(C)$.

Example:

$C = \begin{bmatrix} 1 & 1-i \\ 0 & -1 \end{bmatrix}$is a 2-index unitary type-I matrix.

$$p = 1, C(C^*) = \begin{bmatrix} 3 & -1+i \\ -1-i & 1 \end{bmatrix}$$
$$p = 2, C^2(C^*)^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$p = 3, C^3(C^*)^3 = \begin{bmatrix} 3 & -1+i \\ -1-i & 1 \end{bmatrix}$$
$$p = 4, C^4(C^*)^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$p = 5, \mathrm{C}^5(\mathrm{C}^*)^5 = \begin{bmatrix} 3 & -1+\mathrm{i} \\ -1-\mathrm{i} & 1 \end{bmatrix}$$
$$p = 6, \quad C^6(C^*)^6 \ = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Here, for $p = 2,4,6,8, \ldots$

$C^p(C^*)^p = I_2$. Hence, the index of C is 2 where 2 is the smallest positive integer among the index.

Proposition 3.3:

Every unitary matrix is a unitary type-I matrix and the converse is not true. Obviously, it is of index 1.

Illustration:

The unitary matrix $C = \frac{1}{2}\begin{bmatrix} 1 & -i & -1+i \\ i & 1 & 1+i \\ 1+i & -1+i & 0 \end{bmatrix}$ is an unitary type-I matrix of index 1.

$$p = 1, C(C^*) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$p = 2, C^2(C^*)^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$p = 3, C^3(C^*)^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$p = 4, C^4(C^*)^4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Here, for $p = 1,2,3,4 \ldots$

$C^p(C^*)^p =$. Hence, the index of C is 1 where 1 is the smallest positive integer among the index.

Proposition 3.4:

If C is an unitary type-I matrix of index p, then $|\det(C^p)| = 1$.

Proof:

Let C be an unitary type-I matrix of index p then,

$$C^p(C^*)^p = I_n$$
$$\Rightarrow \det(C^p(C^*)^p) = \det(I_n)$$

DOI : 10.35291/2454-9150.2022.0492

$$\Longrightarrow \det(C^p(C^*)^p) = 1$$
$$\Longrightarrow \det(C^p)\, det(C^*)^p = 1$$
$$\Longrightarrow \det(C^p)\, \overline{\det(C^T)^p} = 1$$
$$\Longrightarrow \det(C^p)\, \overline{\det(C^p)} = 1$$
$$\Longrightarrow |\det(C^p)| = 1$$

Theorem 3.5:

If C is an unitary type-I matrix of index p, then it is invertible with $C^{-1} = C^{p-1}(C^*)^p$

Proof:

From Proposition 3.4,

We know that $\det(C) \neq 0$, hence C is invertible.

For some $p \in \mathbb{N}$,

$C^p(C^*)^p = I_n$,

$\Longrightarrow (C^*)^p = (C^p)^{-1}$

$\Longrightarrow (C^*)^p = (C^{-1})^p$

$\Longrightarrow (C^*)^p = (C^{-1})^{p+1-1} = (C^{-1})^{P-1}(C^{-1})$

$\Longrightarrow (C^*)^p = (C^{-1})^{P-1}(C^{-1})$

$\Longrightarrow C^{-1} = C^{p-1}(C^*)^p$

Proposition 3.6:

Let $C \in \mathbb{C}_{n\times n}$ matrix, then the following statements are equivalent:

(1) C is an unitary type-I matrix
(2) C^{-1} is an unitary type-I matrix
(3) C^T is an unitary type-I matrix
(4) $\overline{C}$ is an unitary type-I matrix
(5) C^* is an unitary type-I matrix

Proof:

(1) $\Longrightarrow$ (2):

Suppose that C is an unitary type-I matrix, then

$$C^p(C^*)^p = I_n, \text{ for some } p \in \mathbb{N}$$
$$\Longrightarrow (C^p(C^*)^p)^{-1} = (I_n)^{-1}$$
$$\Longrightarrow (C^p)^{-1}((C^*)^p)^{-1} = I_n$$
$$\Longrightarrow (C^{-1})^p((C^{-1})^*)^p = I_n$$

Thus, C^{-1} is an unitary type-I matrix.

(2) $\Longrightarrow$ (3):

Suppose that C^{-1} is an unitary type-I matrix, then

$$(C^{-1})^p((C^{-1})^*)^p = I_n, \text{ for some } p \in \mathbb{N}$$
$$\Longrightarrow ((C^{-1})^p((C^{-1})^*)^p)^{-1} = (I_n)^{-1}$$
$$\Longrightarrow ((\overline{(C^{-1})^T})^p)^{-1}((C^{-1})^p)^{-1} = I_n$$
$$\Longrightarrow (\overline{C^T})^p(C^p) = I_n$$
$$\Longrightarrow ((C^*)^p(C^p))^T = (I_n)^T$$
$$\Longrightarrow (C^T)^p((C^T)^*)^p = I_n$$

Hence, C^T is an unitary type-I matrix.

(3) $\Longrightarrow$ (4):

Suppose that C^T is an unitary type-I matrix, then

$$(C^T)^p((C^T)^*)^p = I_n, \text{ for some } p \in \mathbb{N}$$
$$\Longrightarrow ((C^T)^*)^p(C^T)^p = I_n$$
$$\Longrightarrow (((C^T)^*)^p(C^T)^p)^T = (I_n)^T$$
$$\Longrightarrow ((C^T)^T)^p((\overline{(C^T)^T})^T)^p = I_n$$

DOI : 10.35291/2454-9150.2022.0492

$$\Longrightarrow C^p((\overline{C})^T)^p = I_n$$
$$\Longrightarrow \overline{C^p((\overline{C})^T)^p} = \overline{I_n}$$
$$\Longrightarrow (\overline{C})^p((\overline{C})^*)^p = I_n$$

Hence, $\overline{C}$ is an unitary type-I matrix.

(4) $\Longrightarrow$ (5):

Suppose that $\overline{C}$ is an unitary type-I matrix, then

$$(\overline{C})^p((\overline{C})^*)^p = I_n, \text{ for some } p \in \mathbb{N}$$
$$\Longrightarrow ((\overline{C})^p((\overline{C})^*)^p)^T = (I_n)^T$$
$$\Longrightarrow (((\overline{C})^*)^p)^T((\overline{C})^p)^T = I_n$$
$$\Longrightarrow ((\overline{C^T})^*)^p(\overline{C^T})^p = I_n$$
$$\Longrightarrow ((C^*)^*)^p(C^*)^p = I_n$$

Hence, C^* is an unitary type-I matrix.

(5) $\Longrightarrow$ (1): Suppose that C^* is an unitary type-I matrix, then

$$((C^*)^*)^p(C^*)^p = I_n, \text{ for some } p \in \mathbb{N}$$
$$\Longrightarrow (((C^*)^*)^p(C^*)^p)^* = (I_n)^*$$
$$\Longrightarrow C^p(C^*)^p = I_n$$

Hence, C is an unitary type-I matrix.

Theorem 3.7:

If $C_{n\times n}$ and $D_{n\times n}$are commute unitary type-I matrices, then CD is an unitary type-I matrix.

Proof:

Let C and D be the unitary type-I matrices with the same index p,then

$C^p(C^*)^p = I_n$ and $D^p(D^*)^p = I_n$.Thus,

$$\Longrightarrow (CD)^p((CD)^*)^p$$
$$\Longrightarrow (CD)^p(D^*C^*)^p$$
$$\Longrightarrow C^p\,(D^p(D^*)^p)(C^*)^p$$
$$\Longrightarrow C^p(C^*)^p$$
$$\Longrightarrow I_n$$

Hence, CD is an unitary type-I matrix.

Corollary 3.8:

If C and D have different indices, we have the following:

Let C and D be unitary type-I matrices with indices p_1 and p_2 respectively. Then, $(CD)^p((CD)^*)^p = I_n$, where p is the least common multiple of p_1 and p_2.

Where $ind\,(CD) = lcm\big(ind(C), ind(D)\big)$.

Theorem 3.9:

The matrix C is an unitary type-I matrix of index p if and only if C^m is an unitary type-I matrix of index p for each $m \in \mathbb{N}\backslash\{1\}$.

Proof:

Since C is an unitary type-I matrix, then

$$C^p(C^*)^p = I_n, \text{ for some } p \in \mathbb{N}$$
$$\Longrightarrow (C^p(C^*)^p)^m = (I_n)^m$$
$$\Longrightarrow (C^p)^m((C^*)^p)^m = I_n$$
$$\Longrightarrow (C^m)^p((C^m)^*)^p = I_n$$

Hence, C^m is an unitary type-I matrix.

We know that,

$$ind(C^m) = lcm\{ind(C), ind(C), \dots, ind(C) \dots (m\ times)\}$$
$$= lcm\{p, p, \dots, p \dots (m\ times)\} = p$$

Now, we suppose that C^m is an unitary type-I matrix for each m∈ $\mathbb{N}\backslash\{1\}$, especially, each of C^2 and C^3 is unitary type-I matrix of index p.

$$\text{So,} I_n = C^3((C^3)^*)^p$$

$$= (C^p)(C^2)^p((C^2)^*)^p(C^*)^p$$

$I_n = C^p(C^*)^p$, for C^2 is an unitary type-I matrix

Hence, C is an unitary type-I matrix of index p.

Theorem3.10:

If C is an unitary type-I matrix of index$p$, then for each of C^T,C^*,C^{-1},$\overline{C}$ are unitary type-I matrix of index p.

Proof:

Since, C is an unitary type-I matrix of index p, then

$(i)C^T$ is an unitary type-I matrix with $ind(C^T) \le p$

Now, suppose that $ind(C^T) = p - r, 1 \le r \le p$

Then$(C^T)^{p-r}((C^T)^*)^{p-r} = I_n$

$$((C^T)^*)^{p-r}(C^T)^{p-r} = I_n$$

Taking conjugate, we have,

$$((C^*)^*)^{p-r}(C^*)^{p-r} = I_n$$

$$\Longrightarrow C^{p-r}(C^*)^{p-r} = I_n$$

Thus, $ind(C) = p - r,$ which is a contradiction.

Hence, $ind(C^T) = p.$

(ii) From Proposition 3.6, we know that,C^* is an unitary type-I matrix with $ind(C^*) \le p$

Suppose that $ind(C^*) = p - r, 1 \le r \le p$

Then, $(C^*)^{p-r}((C^*)^*)^{p-r} = I_n$

$$C^{p-r}(C^*)^{p-r} = I_n$$

Thus, $ind(C) = p - r,$which is a contradiction.

Hence, $ind(C^*) = p.$

(iii)From Proposition 3.6, we know that,C^{-1} is an unitary type-I matrix with $ind(C^{-1}) \le p$

Suppose that $ind(C^{-1}) = p - r, 1 \le r \le p$

Then, $(C^{-1})^{p-r}((C^{-1})^*)^{p-r} = I_n$

$$((C^{-1})^{p-r}((C^{-1})^*)^{p-r})^{-1} = (I_n)^{-1}$$

$$(C^*)^{p-r}C^{p-r} = I_n$$

Thus, $ind(C) = p - r,$which is a contradiction.

Hence, $ind(C^{-1}) = p.$

(iv) From Proposition 3.6, we know that, $\overline{C}$ is an unitary type-I matrix with $ind(\overline{C}) \le p$

Suppose that $ind(\overline{C}) = p - r, 1 \le r \le p$

Then, $(\overline{C})^{p-r}((\overline{C})^*)^{p-r} = I_n$

Taking Transpose, we get,

$$((C^*)^*)^{p-r}(C^*)^{p-r} = I_n$$

$$C^{p-r}(C^*)^{p-r} = I_n$$

Thus, $ind(C) = p - r,$which is a contradiction.

Hence, $ind(\overline{C}) = p.$

Theorem 3.11:

If λ is an Eigen value of an unitary type-I matrix C with index p,

then λ is of modulus 1.

Proof:

Let C be an unitary type-I matrix with index p, then $C^p(C^*)^p = I_n$

$\Longrightarrow (C^p)^{-1} = (C^*)^p = (C^p)^T$

Since, λ is an Eigen value of C, then λ^p is an Eigen value of C^p and ${}^{1}/_{\lambda^p}$ is an Eigen value of $(C^p)^{-1}$.

DOI : 10.35291/2454-9150.2022.0492

Since C^p and $(C^p)^{-1}$ have the same Eigen values, then

$\lambda^p = {}^{1}/_{\lambda^p}$

$\therefore (\lambda^p)^2 = 1$

Then, $|(\lambda^p)^2| = |\lambda||\lambda| \dots |\lambda| \dots (2p\ times) = 1$

Since, $|\lambda| > 0$, and real number, then we must have $|\lambda| = 1$.

Theorem 3.12:

If $C_{n\times n}$ is an unitary type-I matrix ,then it preserves the inner product in the Eigen vector subspace.

Proof:

Let λ be an Eigen value of C and x and y be Eigen vectors corresponding to λ.

Then $Cx = \lambda x$ and $Cy = \lambda y$

$$\begin{aligned} \text{So, } < Cx, Cy > &= < \lambda x, \lambda y > \\ &= \lambda\bar{\lambda} < x, y > \\ &= |\lambda|^2 < x, y > \\ &= < x, y > \end{aligned}$$

Corollary 3.13:

If $C_{n\times n}$ is an unitary type-I matrix then, it preserves the length in the Eigen vectors subspace.

Proof:

Let λ be an Eigen value of C and x be an Eigen vector corresponding to λ.

Then, $< Cx, Cx > = < x, x >$

So,$\|Cx\|^2 = \|x\|^2$.

Hence, $\|Cx\| = \|x\|$.

IV. APPLICATION OF UNITARY TYPE-I MATRICES IN CRYPTOSYSTEM

4.1 Algorithm:

According to [1, 2], use of matrix multiplication Hill Cipher acts on groups of letters, where plaintext is divided into groups of letters of a fixed size, and each group is transformed into different group of letters. Hiller Cipher applies matrices to cryptography. Ciphers are methods for transforming a secret message called plaintext into a particular form so that only those for whom it is intended and know the key can read and process it. A common way to send coded messages is to assign numerical values from 1-26 to the alphabet and send a message to a string of integers .The problem with this is that these codes are easily broken using an analysis of frequency of numbers that appears in the coded messages.

Alphanumeric message is been encrypted [3] using matrix by the following procedures:

1) Convert alphanumeric message to numbers
2) Generate a matrix from this numbers
3) Generate a secret key
4) Use a secret key to decode the message
5) To decode the encoded message multiply decoded message by inverse of secret key.

4.1.1 Encrypting process:

Step 1: Split the message text into n segments $S_1, S_2, \dots, S_n$, each segment contains one word from the message.

Step 2: Turn the message text to be encoded into different numbers $h_1, h_2, \dots, h_{m_i}, m_i = \#(S_i), i = 1,2, \dots, n$, for each character of the alphabet according to our numbering way.

Step 3: For each segment $S_i, i = 1,2, \dots, n$, select a unitary type-I matrix U_i of index p_i and take the matrix ${U_i}^{p_i - 1}$ of size $m_i \times m_i$ which is also a unitary type-I matrix.

Step 4: Apply the following code to obtain encrypted text

$en_i = ({U_i}^{p_i+1})^{-1} \exp(D_i) {U_i}^{p_i+1} A_i$, for $p_i = 1,2$

$en_i = ({U_i}^{p_i-1})^{-1} \exp(D_i) {U_i}^{p_i-1} A_i$, for $p_i > 2$

DOI : 10.35291/2454-9150.2022.0492

$$A_i = \begin{bmatrix} h_1 \\ h_2 \\ . \\ . \\ . \\ h_{m_i} \end{bmatrix}_{m_i \times 1} \quad \text{, Where } i = 1,2,\dots,n$$

4.1.2 Decrypting Process:

Multiplying the encrypted text $en_i$by the respective unitary type-I matrix such that

$de_i = U_i^{p_i+1} \times en_i$, for $p_i = 1,2$

$de_i = U_i^{p_i-1} \times \ en_i$, for $p_i > 2$

Because the encryption using the matrix $U_i^{p_i-1}$ and its inverse, some values is negative, in such case we shall use the absolute value.

The secret keys for UPPERCASE, lowercase and some other symbols are as follows:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**a**	**b**	**c**	**d**	**e**	**f**
17	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**
G	**H**	**i**	**J**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**
33	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**
W	**X**	**y**	**Z**	**@**	**?**	**&**	**$**	**’**	*****	**#**	**/**	**!**	**|**	\	**,**
49	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**	**64**

The following illustration explains how to encrypt the message:

The encrypt message is “***No Man’s Land***”.

This idiom was originally used on maps to indicate burial grounds. Today, the term is used colloquially for people who are wandering or are caught in the wrong place at the wrong time.

The message contain 3 words, then according to the algorithm we must arrange the message into 3 segments such that $n =$ 3.Every segment need to be a unitary type-I matrix of index p_i.

$\boldsymbol{S_1}$: "***No***"

$h_1: N = 14, h_2: o = 41$

Now, select an unitary type-I matrix

$U_1 = \begin{bmatrix} 1 & 1 \\ 0 & i \end{bmatrix}$ of size 2× 2 and $p_1 = 4$

$en_1 = ({U_1}^3)^{-1} \exp(D_1) {U_1}^3 A_1$

Here,$U_1{}^3 = \begin{bmatrix} 1 & i \\ 0 & -i \end{bmatrix}$,$({U_1}^3)^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & i \end{bmatrix}$

$$en_1 = \begin{bmatrix} 1 & 1 \\ 0 & i \end{bmatrix} \begin{bmatrix} e^{14} & 0 \\ 0 & e^{41} \end{bmatrix} \begin{bmatrix} 1 & i \\ 0 & -i \end{bmatrix} \begin{bmatrix} 14 \\ 41 \end{bmatrix}$$

$$en_1 = \begin{bmatrix} 14e^{14} + i41e^{14} - i41e^{41} \\ 41e^{41} \end{bmatrix}$$

$\boldsymbol{S_2}$: "***Man's***"

$h_1: M = 13 \,, h_2: a = 27 \,, h_3: n = 40 \,, h_4: ' = 57, h_5: s = 45$

Now, select an unitary type-I matrix

$U_2 = \begin{bmatrix} -5 & 8 & 0 & 0 & 0 \\ 3 & 5 & 0 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & -i \end{bmatrix}$ of size 5×5 and $p_2 = 2$

$en_2 = ({U_2}^3)^{-1} \exp(D_2) {U_2}^3 A_2$

DOI : 10.35291/2454-9150.2022.0492

Here, $U_2{}^3 = \begin{bmatrix} -5 & -8 & 0 & 0 & 0 \\ 3 & 5 & 0 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 0 & i \end{bmatrix}, (U_2{}^3)^{-1} = \begin{bmatrix} -5 & -8 & 0 & 0 & 0 \\ 3 & 5 & 0 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & -i \end{bmatrix}$

$$en_2 = \begin{bmatrix} -5 & -8 & 0 & 0 & 0 \\ 3 & 5 & 0 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 0 & -i \end{bmatrix} \begin{bmatrix} e^{13} & 0 & 0 & 0 & 0 \\ 0 & e^{27} & 0 & 0 & 0 \\ 0 & 0 & e^{40} & 0 & 0 \\ 0 & 0 & 0 & e^{57} & 0 \\ 0 & 0 & 0 & 0 & e^{45} \end{bmatrix} \begin{bmatrix} -5 & -8 & 0 & 0 & 0 \\ 3 & 5 & 0 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 0 & i \end{bmatrix} \begin{bmatrix} 13 \\ 27 \\ 40 \\ 57 \\ 45 \end{bmatrix}$$

$$en_2 = \begin{bmatrix} 1405e^{13} - 1392e^{27} \\ -843e^{13} + 870e^{27} \\ -281e^{13} + 348e^{27} - 27e^{40} \\ 57e^{57} \\ 45e^{45} \end{bmatrix}$$

$\boldsymbol{S_3}$: "***Land***"

$h_1: L = 12,\ h_2: a = 27,\ h_3: n = 40\ , h_4: d = 30$

Now, select an unitary type-I matrix

$U_3 = \begin{bmatrix} i & 1 & 0 & 0 \\ 2 & -i & 0 & 0 \\ 0 & 0 & 1 & 1+i \\ 0 & 0 & 0 & -i \end{bmatrix}$ of size 4×4 and $p_3 = 4$

$en_3 = (U_3{}^3)^{-1}\exp(D_3)U_3{}^3A_3$

Here, $U_3{}^3 = \begin{bmatrix} i & 1 & 0 & 0 \\ 2 & -i & 0 & 0 \\ 0 & 0 & 1 & 1-i \\ 0 & 0 & 0 & i \end{bmatrix}, (U_3{}^3)^{-1} = \begin{bmatrix} i & 1 & 0 & 0 \\ 2 & -i & 0 & 0 \\ 0 & 0 & 1 & 1+i \\ 0 & 0 & 0 & -i \end{bmatrix}$

$$en_3 = \begin{bmatrix} i & 1 & 0 & 0 \\ 2 & -i & 0 & 0 \\ 0 & 0 & 1 & 1+i \\ 0 & 0 & 0 & -i \end{bmatrix} \begin{bmatrix} e^{12} & 0 & 0 & 0 \\ 0 & e^{27} & 0 & 0 \\ 0 & 0 & e^{40} & 0 \\ 0 & 0 & 0 & e^{30} \end{bmatrix} \begin{bmatrix} i & 1 & 0 & 0 \\ 2 & -i & 0 & 0 \\ 0 & 0 & 1 & 1-i \\ 0 & 0 & 0 & i \end{bmatrix} \begin{bmatrix} 12 \\ 27 \\ 40 \\ 30 \end{bmatrix}$$

$$en_3 = \begin{bmatrix} (27+12i)ie^{12} + (24-27i)e^{27} \\ (27+12i)2e^{12} - i(24-27i)e^{27} \\ (70-30i)e^{40} + 30i(1+i)e^{30} \\ 30e^{30} \end{bmatrix}$$

Using the decrypted process, to decrypt the cipher-segment message as follows:

$\boldsymbol{S_1}$:

$de_1 = (U_1)^{p_1 - 1} \times en_1$

$de_1 = (U_1)^3 \times en_1$

$$= \begin{bmatrix} 1 & i \\ 0 & -i \end{bmatrix} \begin{bmatrix} 14e^{14} + i41e^{14} - i41e^{41} \\ 41e^{41} \end{bmatrix}$$

$$de_1 = \begin{bmatrix} (14 + i41)e^{14} \\ -41ie^{41} \end{bmatrix}$$

Taking the absolute values to the negative values.

$(14 + i41)e^{14}$:The number 14 indicate the character “N”.

$41ie^{41}$:The number 41 indicate the character “o”.

$\boldsymbol{S_2}$:

$de_2 = (U_2)^{p_2 + 1} \times en_2$

$de_2 = (U_2)^3 \times en_2$

$$de_2 = \begin{bmatrix} -5 & -8 & 0 & 0 & 0 \\ 3 & 5 & 0 & 0 & 0 \\ 1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 0 & i \end{bmatrix} \begin{bmatrix} 1405e^{13} - 1392e^{27} \\ -843e^{13} + 870e^{27} \\ -281e^{13} + 348e^{27} - 27e^{40} \\ 57e^{57} \\ 45e^{45} \end{bmatrix}$$

DOI : 10.35291/2454-9150.2022.0492

$$de_2 = \begin{bmatrix} -281e^{13} \\ 174e^{27} \\ 27e^{40} \\ -57ie^{57} \\ 45ie^{45} \end{bmatrix}$$

Taking the absolute values to the negative values.

$281e^{13}$:The number 13 indicate the character “M”.

$174e^{27}$:The number 27 indicate the character “a”.

$27e^{40}$:The number 40 indicate the character “n”.

$57ie^{57}$:The number 57 indicate the character “ ′”.

$45ie^{45}$: The number 45 indicate the character “s”.

$\boldsymbol{S_3}$:

$de_3 = (U_3)^{p_3-1} \times en_3$

$de_3 = (U_3)^3 \times en_3$

$$de_3 = \begin{bmatrix} i & 1 & 0 & 0 \\ 2 & -i & 0 & 0 \\ 0 & 0 & 1 & 1-i \\ 0 & 0 & 0 & i \end{bmatrix} \begin{bmatrix} (27+12i)ie^{12} + (24-27i)e^{27} \\ (27+12i)2e^{12} - i(24-27i)e^{27} \\ (70-30i)e^{40} + 30i(1+i)e^{30} \\ 30e^{30} \end{bmatrix}$$

$$de_3 = \begin{bmatrix} (27+12i)e^{12} \\ (24-27i)e^{27} \\ (70-30i)e^{40} \\ 30ie^{30} \end{bmatrix}$$

Taking the absolute values to the negative values.

$(27+12i)e^{12}$:The number 12 indicate the character “L”.

$(24-27i)e^{27}$:The number 27 indicate the character “a”.

$(70-30i)e^{40}$:The number 40 indicate the character “n”.

$30ie^{30}$: The number 30 indicate the character “d”.

V. CONCLUSION

With the increasingly rise of cipher text cracking, it is important to employ the use of the crypto mechanism using matrices to generate a secret key to encrypt message safely. The effectiveness of the encryptions and advancements are developed with the help of Unitary type-I matrices in this paper. Unitary type-I matrices are a generalization of the unitary matrices. These matrices are invertible and its eigenvalues are of modulus 1.Because of its index, it realize that every unitary type-I matrix C of index p induces a set of unitary matrices $\{C^{np}\}_{n\in N}$. The efficacy of Unitary type-I matrices in Cryptography is explained elaborately with suitable models.

This paper elucidates the generation of secret key using Unitary type-I matrices to improve the complexity of symmetric cipher mechanism. It is inevitable to employ the generation of the secret key to encrypt the messages safely due to the rise of cipher text cracking. Also, this paper helps to develop more cryptography mechanism using Unitary type-I matrices in further studies.

REFERENCES

[1] Chattaroy, S. K., Majhi, J., & Rath, G. S. Encryption by Hill cipher and by a novel method using Chinese remainder theorem in Galois field. International Journal of Signal and Imaging Systems Engineering, 6(1), 38-45, (2013).

[2] Chefranov A.G., “Secure Hill Cipher Modification SHC-M” Proc. Of the First International conference on Security of Information and Network (SIN2007), Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing, Canada, 2008: pp 34-37, (2007).

[3] Elder, Timo hanke, An introduction to cryptography, (2018).

[4] Fuzhen Zhang, “Matrix Theory”, *Springer Int. Edn.*, Delhi, (2010).

[5] Horn, Roger A, Topics in matrix analysis Cambridge University, (1991).

[6] Meyer, C. D Matrix analysis and applied linear algebra (Vol. 71). Siam, (2000).

[7] Mukhesh Kumar Singh *Public key Cryptography with Matrices*, Proceedings of the IEEE Workshop on Information Assurance, United states Military Academy, West Point, NY 10-11 June (2004).

[8] Richard Bronson, “Matrix Methods an Introduction”, *Elsevier Publications*, Delhi, (2006).

[9] Shanti Narayan, Mittal P. K, “A text book of Matrices”, *S Chand Publications*, Delhi, (2006).

[10] Yeh YS, Wu TC, Chang CC, Yang WC. “A New Cryptosystem Using Matrix Transformation”. 25th IEEE International Carnahan Conference on Security Technology, 131-138, (1991).

DOI : 10.35291/2454-9150.2022.0492