A note on matrix algebra for cryptography settings and applications

A note on matrix algebra for cryptography settings and applications

A. O. Ayo-Aderele[1], S. O. Edeki[1], V. O. Udjor[2], O. Ugbenu[3]

[1]Department of Mathematics, Covenant University, Ota, Nigeria
[2]SBU, Covenant University Ota, Nigeria
Directorate of Research, National Institute for Policy and Strategic Studies, Kuru, Nigeria

Contact Emails: adediwura.ayo-aderele@stu.cu.edu.ng; soedeki@yahoo.com

Abstract: Cryptography is an interdisciplinary topic that adopts concepts from several disciplines. In today's environment, cryptography makes important use of computer science and mathematics, especially discrete mathematics. This study aims to discuss the daily use of matrices in cryptography. Globally, secure text communication is critical while various cryptosystems exist to accomplish this security. Hence, with regard to the cryptosystem, the key matrix from the plane's equation is considered by determining the orthogonal matrix that implements reflection. This method boosts encryption security by making it more arduous to locate a secret key matrix. In order to produce encryptions, the approach uses the orthogonal matrix transform characteristics. The suggested encryption method's simplicity enables it to be adapted to other circumstances requiring secret communication transmission

Keywords: cryptography, coding, algorithm, matrix algebra

1. Introduction

The term ‘matrix’ is simply a rectangular array of data (numbers, variables, symbols, and expressions) arranged in the form of rows and columns. The individual items contained in any matrix are called entries or elements of the matrix.

One of the numerous applications of matrices is in the field of Cryptography. Cryptography is the science of securing information by modifying it into an unintelligible form known as ciphertext via a procedure known as encryption. Modern cryptography encompasses the intersection of various fields of computer science, applied mathematics, electrical engineering, physics and communication science. The most common areas of mathematics largely used in cryptography include algebra, number theory, and probability.

Data/information encryption has become a thing of necessity with the rise of sensitive data being stored and transmitted via computers. A matrix can be used as a cipher to encrypt a message [1]. Matrices provide a security advantage; that is, the embedding degree is tied to the size of the matrix [2].

Information security has become a very crucial aspect of modern computing systems. With the global emergence and, consequently, the acceptance of the Internet, most, if not all, computers in the world are connected to each other. No doubt, this has created immense productivity and unprecedented

opportunities in the world in which we operate; it has also given way to new fears and threats for the users of these computers for fear of threats from intruders in the form of hackers, crackers, unauthorized users, etcetera who use a variety of techniques and tools at their disposal to break into computer systems, steal/pilfer information, tamper with data and cause various other havoc. If no security measures are taken, there is no doubt that such data and additional sensitive information will continuously be falsified, altered, and formatted by the system intruders [3].
Matrices have been proven to have a particular distinctive substantial concept and are easy to comprehend. It is only logical that the idea of matrix algebra is utilized as an efficient technique of encrypting and storing information. The encryption system uses a matrix to keep the information inputted by the sender in the form of their positions, by using an algorithm to encrypt these said values [4].
Therefore, the aim of this study is to propose a simple method for the encryption and decryption of information by generating encryption keys using matrix operation and Hill Ciphers; and use the generated encryption keys for information encoding and decoding.

1.1 Preliminaries and basic terms

Matrix and Matrix Notation

A matrix can be denoted by uppercase boldface letters and is written in either square brackets or enclosed in parentheses. We shall display a matrix $\boldsymbol{X}$ of dimension $\boldsymbol{a}\times\mathbf{b}$ as:

$$\boldsymbol{X}=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1b} \\ x_{21} & x_{22} & \cdots & x_{2b} \\ \vdots & \vdots & \ddots & \vdots \\ x_{a1} & x_{a2} & \cdots & x_{ab} \end{pmatrix}$$

The matrix $\boldsymbol{X}$ can be abbreviated to $\boldsymbol{X}=\left(\boldsymbol{x_{ij}}\right)_{\boldsymbol{a}\times\boldsymbol{b}}$. This expression will be taken to mean that $\boldsymbol{X}$ is the $\boldsymbol{a}\times\mathbf{b}$ matrix whose $\left(i,\ j\right)-th$ element is $\boldsymbol{x_{ij}}$.

Hermitian and Nature of Hermitian Matrix: A square matrix $\boldsymbol{X}$ is said to be a Hermitian matrix whenever $\boldsymbol{X}=\boldsymbol{X}^{*}$. That is, whenever $\boldsymbol{a_{ij}}=\bar{\boldsymbol{a}}_{\boldsymbol{ji}}$, where $\boldsymbol{X}^{*}$ is the conjugate transpose of $\boldsymbol{X}$. This is the complex analog of symmetry. A square matrix $\boldsymbol{X}$ is said to be a skew Hermitian matrix whenever $\boldsymbol{X}=-\boldsymbol{X}^{*}$. That is, whenever $\boldsymbol{a_{ij}}=-\bar{\boldsymbol{a}}_{\boldsymbol{ji}}$, where $\boldsymbol{X}^{*}$ is the conjugate transpose of $\boldsymbol{X}$. This is the complex analog of skew symmetry.
Cryptography: Cryptography is the science of encrypting information (plaintext) into secret codes and decrypting information (ciphertext) written in secret codes [5]. It is a process that centers on achieving the information security goals of confidentiality, integrity, authentication, and non-repudiation via storing and transmission of data in a form that can only be accessed by the predetermined recipient [6]. Figure 1 shows the classes of cryptography in applications.

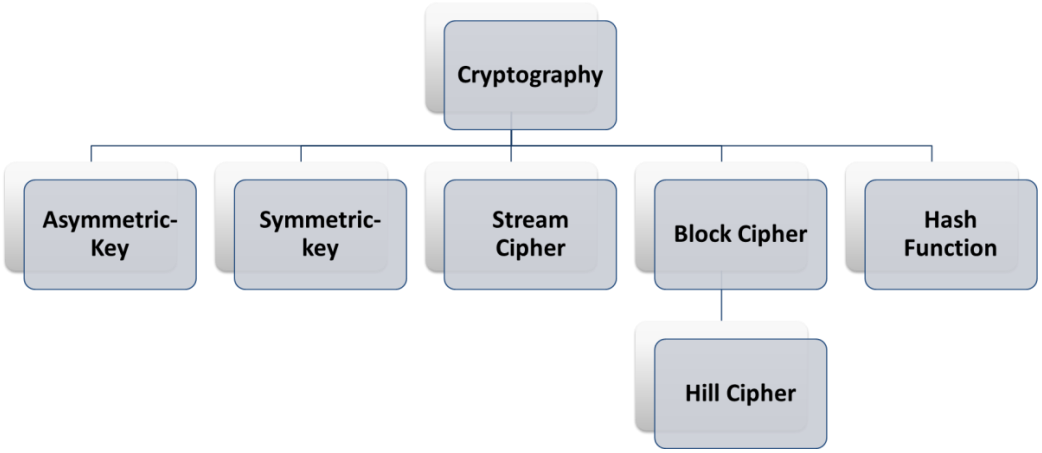

Figure 1: *Types of Cryptography*

Secret Key Cryptography: Secret key cryptography or symmetric key encryption (used interchangeably) refers to algorithms for cryptography that make use of a single cryptographic key for the process of encrypting the plaintext message and decrypting of ciphertext [7]. The key being used is referred to as a secret key or a symmetric key. In this method of cryptography, all parties concerned have to know the key to decrypt the ciphertext when it is received and encrypt the plaintext to be sent. The key is a shared secret as it is available to the parties concerned but is privy to third parties [8].

Public Key Cryptography: Asymmetric cryptography, often known as public-key cryptography, is a cryptosystem that employs a pair of keys: public keys that may be shared with the public and private keys that are kept private by the owner. To build one-way functions, cryptographic procedures based on mathematical problems are used to generate both keys. Only the private key must be kept safe for adequate security. Without posing any security issues, the public key may be made accessible to anybody [9-11].

Hash Functions: These are mathematical procedures that convert data of any size defined as the message to a fixed-size bit array called hash value [12].

Cipher: A cipher is an algorithm for encrypting or decrypting data in cryptography. It is a set of stages with clear instructions that may be followed as a process.

Plaintext: Text that has not been computationally tagged, particularly formatted, or written in code is referred to as plaintext.

Ciphertext: The ciphertext is the result of an encryption process done on plain text through a cipher algorithm [13] in cryptography. Encrypted/encoded data is another name for ciphertext.

Encryption: Encryption is a kind of cryptography in which plaintext is scrambled into ciphertext. Encryption is the cornerstone of security mechanisms such as digital signatures, digital certificates, and the Public Key Infrastructure, which uses these technologies to safeguard computer interactions [14].

Decryption: Decryption takes ciphertext and converts it back into plaintext that an individual or a computer can read and comprehend [15].

Cryptographic Key: A cryptographic key or a key is a string of characters incorporated into an encryption algorithm to alter data to appear random. Much like a physical key, it locks data (encryption) so that only an individual in possession of the right key can unlock the data (decryption) (Learning: Cloudflare).

Symmetric and Asymmetric Keys: Symmetric keys are a shared secret that may be used to maintain a confidential information relationship between two or more people. It's a cryptographic key that may be used to encrypt and decrypt data [16]. The cornerstone of Public Key Infrastructure (PKI) is asymmetric keys, a cryptographic system that requires two keys, one to encrypt the plaintext and the other to decipher the ciphertext. Neither key has the ability to do both duties. The public key is made public, while the private key is kept secret. If the encryption key is made public, the system allows for

private communication between the public and the decryption key owner. If the decryption key is the same as the one uploaded, the system acts as a signature verification.

Private and Public Keys: A secret key, also widely recognized as a private key, is a long, randomly generated number that is difficult to guess. It is cryptographic key that is used to encrypt and decrypt data using an algorithm. Because secret keys are only shared with the key generator, they are extremely secure. Secret keys play a crucial role in public-key cryptography, secret-key cryptography, and cryptocurrencies [17]. Public keys refer to cryptographic keys that are accessible to everyone to encrypt information intended for a particular recipient in such a way that the encrypted messages can be decrypted only via another key available only to the recipient.

Block and Hill Ciphers: This type of encryption method that makes use of a deterministic algorithm in line with a symmetric key to encrypt an entire block of text. The ciphertext generated via block ciphers can only be accessed using decryption algorithms and private keys. Hill ciphers refer to a type of block cipher that operates based on the principle that the ciphertext character that substitutes a specific plaintext character in the encryption depends on the subsequent plaintext characters. The encryption is concluded via matrix algebra.
A lot of researchers have worked on matrices, algebra, cryptography, network analysis, security, steganography, cyber systems, and so on [18-34].
This study looks at providing algorithms to secure confidential and sensitive information in-store or transit via unsecured means from the hands of cybercriminals and snoops by the encryption of the data into an unintelligible series of letters and decryption via a series of matrix operations in concurrence with the principles of the Hill Cipher.
.

2. Basi Matrix Operations and Applicability in Cryptography

2.1 Matrix Addition

The sum of two $\boldsymbol{a}\times\boldsymbol{b}$ matrices $\boldsymbol{X}=[\boldsymbol{x}_{ij}]$ and $\boldsymbol{Y}=[\boldsymbol{y}_{ij}]$ is the $\boldsymbol{a}\times\boldsymbol{b}$ matrix $\boldsymbol{Z}=[\boldsymbol{z}_{ij}]$, where $\boldsymbol{z}_{ij}=\boldsymbol{x}_{ij}+\boldsymbol{y}_{ij}$ for every $i=1,2,\ldots,a$ and every $j=1,2,\ldots,b$.
In other words, the sum/addition of two matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ is done by simply adding elements in corresponding positions.
The sum $\boldsymbol{Z}$ of matrices $\boldsymbol{X}$ and $\boldsymbol{Y}$ exists only when $\boldsymbol{X}$ and $\boldsymbol{Y}$ have the same dimension.

2.2 Orthogonal Matrix

An $\boldsymbol{n}\times\boldsymbol{n}$ square matrix $\boldsymbol{X}$ with real entries/elements is said to be orthogonal if and only if $\boldsymbol{X}^{\boldsymbol{T}}=\boldsymbol{X}^{-1}$. Since $\boldsymbol{X}\boldsymbol{X}^{-1}=\boldsymbol{I}=\boldsymbol{X}^{-1}\boldsymbol{X}$, it follows that an orthogonal matrix $\boldsymbol{X}$ satisfies the relation $\boldsymbol{X}\boldsymbol{X}^{\boldsymbol{T}}=\boldsymbol{X}^{\boldsymbol{T}}\boldsymbol{X}=\boldsymbol{I}$. Where $\boldsymbol{I}$ is an identity matrix and $\boldsymbol{X}^{\boldsymbol{T}}$ is the transpose of $\boldsymbol{X}$.
Orthogonal matrices are ideal for cryptography than any other matrix because they provide more security for information. Only the sender and recipient know that the key matrix is designed to be an orthogonal matrix that executes reflection on the given plane $\boldsymbol{R}^{\boldsymbol{n}}$.

2.3 Properties of Orthogonal Matrix

I. Any orthogonal matrix is invertible, that is $\boldsymbol{X}^{\boldsymbol{T}}=\boldsymbol{X}^{-1}$. If $\boldsymbol{X}$ is orthogonal, then $\boldsymbol{X}^{\boldsymbol{T}}$ and $\boldsymbol{X}^{-1}$ are orthogonal.
II. The reciprocal matrix of every orthogonal matrix is also orthogonal, as is the resulting matrix from the multiplication of two orthogonal matrices.
III. For an orthogonal matrix, the determinant is 1 or -1.
IV. The orthogonal transformation preserves angles and lengths while leaving the parallelepiped's volume unchanged. We may deduce from these facts that the orthogonal transformation entails a rotation..

2.4 Reflection and Rotation in a Plane (Orthogonal Matrix)

Informally, an orthogonal $\boldsymbol{n}\times\boldsymbol{n}$ matrix is the n-dimensional equivalent of the rotation matrices $\boldsymbol{R}_{\theta}$ in $\boldsymbol{R}^2$.

An orthogonal transformation of $\boldsymbol{R^n}$ is a rotation if it has a determinant 1, a reflection if it has a determinant -1.

Any vector $\boldsymbol{v} \in \boldsymbol{R}^3$ can be written as the sum of its orthogonal projections on $\boldsymbol{L}$ and on the given plane $\boldsymbol{L}^{\perp}$: $\boldsymbol{v} = \boldsymbol{v}, \boldsymbol{uu} + \boldsymbol{w}, \boldsymbol{w} = \boldsymbol{v} - \langle \boldsymbol{v}, \boldsymbol{u} \rangle \boldsymbol{u} \in \boldsymbol{L}^{\perp}$

The reflection $\boldsymbol{T}$ flips $\boldsymbol{u}(\boldsymbol{Tu} = -\boldsymbol{u})$ and fixes every $\boldsymbol{w} \in \boldsymbol{L}^{\perp}$ (that is, $\boldsymbol{Tw} = \boldsymbol{w}$).

By linearity of $\boldsymbol{T}$:

$\boldsymbol{T}_v = \langle \boldsymbol{v}, \boldsymbol{u} \rangle \boldsymbol{Tu} + \boldsymbol{Tw} = \boldsymbol{v} - 2\langle \boldsymbol{v}, \boldsymbol{u} \rangle$

2.5 Hill Cipher Plaintext Characters

A number modulo 26 is assigned to each letter. This simple scheme known as alphabetical encoding is often used, even though it is not a vital feature of the cipher. References are made to Tables 1 to 3.

Table 1: *Alphabetical Encoding Scheme*

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

2.6 Generation of key matrix for encryption

In cryptography, a matrix must satisfy two conditions in order to be used as a key matrix. The conditions include:

I. The matrix must be invertible.

II. The matrix must be composed of random integers.

2.7 Generation of key matrix for encryption

We derive the key matrix using the equation of a plane by finding the orthogonal matrix that implements reflection on the plane.

Given an equation of a plane $R^n : a_1x_1 + a_2x_2 + \ldots + a_nx_n$, we will need to find the orthogonal matrix in standard basis which applies reflection on the plane $\boldsymbol{R^n}$ with the given equation. The following unit vector spans the orthogonal line $\boldsymbol{L}$

$$\boldsymbol{u} = \frac{1}{\sqrt{\left(\boldsymbol{a}_1^{\,2} + \boldsymbol{a}_2^{\,2} + \ldots + \boldsymbol{a}_n^{\,2}\right)}} .$$

Using the general formula for the reflection on a plane with unit normal $\mathbf{u}$, $\boldsymbol{Tv} = \boldsymbol{v} - 2\langle \boldsymbol{v}, \boldsymbol{n} \rangle$, we have that :

$$\boldsymbol{Tv} = \boldsymbol{v} - 2\boldsymbol{v}, (\boldsymbol{a}_1 + \boldsymbol{a}_2 + \ldots + \boldsymbol{a}_n)(\boldsymbol{a}_1 + \boldsymbol{a}_2 + \ldots + \boldsymbol{a}_n)$$

$$\boldsymbol{T}_1 = \boldsymbol{e}_1 - 2\boldsymbol{va}_1(\boldsymbol{a}_1 + \boldsymbol{a}_2 + \ldots + \boldsymbol{a}_n)$$

$$\boldsymbol{T}_2 = \boldsymbol{e}_2 - 2\boldsymbol{va}_2(\boldsymbol{a}_1 + \boldsymbol{a}_2 + \ldots + \boldsymbol{a}_n)$$

$$\vdots$$

$$\boldsymbol{T}_n = \boldsymbol{e}_n - 2\boldsymbol{va}_n(\boldsymbol{a}_1 + \boldsymbol{a}_2 + \ldots + \boldsymbol{a}_n)$$

Note: The matrix of reflection is the $\boldsymbol{n} \times \boldsymbol{n}$ identity matrix. For instance, the matrix of reflection takes the form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ for $\boldsymbol{R}^3$. Likewise for $\boldsymbol{R^n}$. $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ represents each row of the reflection matrix.

This series of calculations result in the columns of the matrix of $\boldsymbol{T}$ in the standard form/basis. This becomes our key matrix $\boldsymbol{K}$.

2.8 Algorithm for encryption of plaintext using hill cipher

I. Divide the information to be encoded (plaintext) into equal parts such that the length of each part is equal to the length of the given equation.
II. Derive the initial ciphertext of the plaintext using the ordinary hill cipher procedure (alphabetical encoding).
III. Step II will result in a series of numbers. Combine these numbers into a matrix $\boldsymbol{X}$.
IV. Multiply the matrix $\boldsymbol{X}$ by the known key matrix $\boldsymbol{K}$. That is, $\boldsymbol{Y}=\boldsymbol{KX}$ or $\boldsymbol{Y}=\boldsymbol{XK}$ depending on the dimension of the matrices.
V. Convert that the resulting matrix $\boldsymbol{Y}$ to $\boldsymbol{mod}\,26$.
VI. Dissolve matrix $\boldsymbol{Y}$ by concatenating the rows of $\boldsymbol{Y}$ into a sequence of integers.
VII. Replace each integer with its corresponding letter using alphabetical encoding once again.
VIII. In general, the process of encryption of plaintext can be summarized as $\boldsymbol{Y}=\boldsymbol{KX}(\boldsymbol{mod}\,26)$ or $\boldsymbol{Y}=\boldsymbol{XK}(\boldsymbol{mod}\,26)$ depending on the dimension of the matrices, where $\boldsymbol{X}$ is the plaintext message, $\boldsymbol{Y}$ is the resulting ciphertext message and $\boldsymbol{K}$ is the key matrix.

2.9 Algorithm for decryption of ciphertext using hill cipher

I. Assign each letter with its corresponding integer using alphabetical encoding.
II. Combine the resulting numbers into a matrix $\boldsymbol{Y}$.
III. Multiply the matrix $\boldsymbol{Y}$ with the inverse of the key matrix. That is, $\boldsymbol{K}^{-1}$. Note that since $\boldsymbol{K}$ is an orthogonal matrix, $\boldsymbol{K}^{-1}=\boldsymbol{K}^{\boldsymbol{T}}$. Therefore, we will perform the operation $\boldsymbol{X}=\boldsymbol{K}^{-1}\boldsymbol{Y}$ or $\boldsymbol{X}=\boldsymbol{YK}^{-1}$ depending on the dimension of the matrices.
IV. Convert the resulting matrix $\boldsymbol{X}$ to $\boldsymbol{mod}\,26$.
V. Dissolve matrix $\boldsymbol{X}$ by concatenating the rows of $\boldsymbol{X}$ into a sequence of integers.
VI. Replace each integer with its corresponding letter using alphabetical encoding.

In general, the process of encryption of plaintext can be summarized as an operation $\boldsymbol{X}=\boldsymbol{K}^{-1}\boldsymbol{Y}(\boldsymbol{mod}\,26)$ or $\boldsymbol{X}=\boldsymbol{YK}^{-1}(\boldsymbol{mod}\,26)$ depending on the dimension of the matrices, where $\boldsymbol{X}$ is the plaintext message, $\boldsymbol{Y}$ is the resulting ciphertext message and $\boldsymbol{K}^{-1}$ is the inverse of the key matrix. Encryption and Decryption processes are showed in Figure 2.

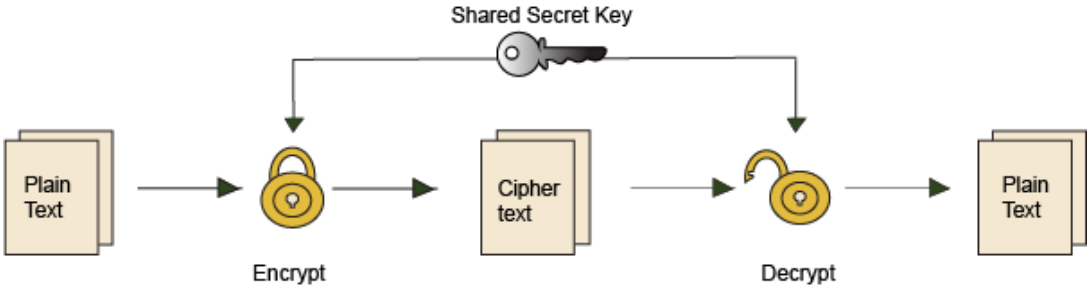

Figure 2: *Encryption and Decryption Process*

3. Overview of the Study and Discussion of Results

The fundamental concept of cryptography is that information can be encoded via an encryption scheme and decoded only by the individuals privy to the scheme. Various kinds of encryption schemes exist, ranging from uncomplicated to very complicated. The majority of such schemes are mathematical in nature. In this particular study, the Hill Cipher is the encryption scheme, the encoder is a matrix, and the decoder is the inverse of the same matrix.

3.1 Example encryption using matrices

We will consider a message to be sent: **SEND HELP NOW**

We will use the Hill Cipher alphabetical encoding scheme instead of the ASCII encoding scheme used in some similar studies. According to the alphabetical encoding scheme, the letters in the message corresponding to the following numbers:

Table 2: *Alphabetical Encoding Scheme for message to be encrypted*

LETTER	S	E	N	D	H	L	P	O	W
NUMER	19	5	14	4	8	12	16	15	23

The message will be sent using the predetermined secret key privy to only those concerned.

At this point, it is necessary to state the requirements of a square matrix of integers $\boldsymbol{K}$ for it to be a suitable key for a Hill cipher. For the decryption process to be effective, $\boldsymbol{K}$ needs to be invertible in modulo 26, which means that the determinant of $\boldsymbol{K}$ must satisfy $\boldsymbol{gcd}\left(\left|\boldsymbol{K}\right|,26\right)=1$.

Suppose the secret key is $\boldsymbol{K}=\begin{bmatrix} 9 & 18 & -18 \\ 18 & 9 & 18 \\ -18 & 18 & 9 \end{bmatrix}$.

Using the conversion table above (alphabetical encoding), the plaintext message is represented as
19 5 14 4 8 5 12 16 14 15 23

We will now break up this sequence lengthwise into rows of length 3 (the dimension of $\boldsymbol{K}$). This step will result in a matrix $\boldsymbol{X}$ as shown below:

$$\boldsymbol{X}=\begin{bmatrix} 19 & 5 & 14 \\ 4 & 8 & 5 \\ 12 & 16 & 14 \\ 15 & 23 & ? \end{bmatrix}$$

For the encryption to proceed, the "?" that appears in the last row must be addressed. The easiest way is to replace it with a value that also represents a plaintext letter that will be be viewed as extraneous when the information is decrypted. In this calculation, we will use the integer 6, the representative of the letter "F". We form a matrix from the resulting four rows:

$$\boldsymbol{X}=\begin{bmatrix} 19 & 5 & 14 \\ 4 & 8 & 5 \\ 12 & 16 & 14 \\ 15 & 23 & 6 \end{bmatrix}$$

Now we encrypt the message by performing the operation of matrix multiplication thus:

$$\boldsymbol{Y}=\boldsymbol{XK}$$

$$\boldsymbol{Y}=\begin{bmatrix} 19 & 5 & 14 \\ 4 & 8 & 5 \\ 12 & 16 & 14 \\ 15 & 23 & 6 \end{bmatrix}\times\begin{bmatrix} 9 & 18 & -18 \\ 18 & 9 & 18 \\ -18 & 18 & 9 \end{bmatrix}$$

$$\boldsymbol{y}_{11}=\left(19\times 9\right)+\left(5\times 18\right)+\left(14\times -18\right)$$

$$\boldsymbol{y}_{12}=\left(19\times 18\right)+\left(5\times 9\right)+\left(14\times 18\right)$$

$$\boldsymbol{y}_{13}=\left(19\times -18\right)+\left(5\times 18\right)+\left(14\times 9\right)$$

$$\boldsymbol{y}_{21}=\left(4\times 9\right)+\left(8\times 18\right)+\left(5\times -18\right)$$

$$y_{22} = (4\times 18)+(8\times 9)+(5\times 18)$$
$$y_{23} = (4\times -18)+(8\times 18)+(5\times 9)$$
$$y_{31} = (12\times 9)+(16\times 18)+(14\times -18)$$
$$y_{32} = (12\times 18)+(16\times 9)+(14\times 18)$$
$$y_{33} = (12\times -18)+(16\times 18)+(14\times 9)$$
$$y_{41} = (15\times 9)+(23\times 18)+(6\times -18)$$
$$y_{42} = (15\times 18)+(23\times 9)+(6\times 18)$$
$$y_{43} = (15\times -18)+(23\times 18)+(6\times 9)$$

$$\boldsymbol{Y} = \begin{bmatrix} (171)+(90)+(-252) & (342)+(45)+(252) & (-342+90+126) \\ (36)+(144)+(-90) & (72)+(72)+(90) & (-72)+(144)+(45) \\ (108)+(288)+(-252) & (216)+(144)+(252) & (-216)+(288)+(126) \\ (135)+(414)+(-108) & (270)+(207)+(108) & (-270)+(414)+(54) \end{bmatrix}$$

$$\boldsymbol{Y} = \begin{bmatrix} 9 & 639 & -126 \\ 90 & 234 & 117 \\ 144 & 612 & 198 \\ 441 & 585 & 198 \end{bmatrix}$$

For every entry y_{ij} that does not satisfy $0 \le y_{ij} \le 25$, we replace y_{ij} with the integer $y_{ij}^{*} \in \{0,...,25\}$ such that $y_{ij}^{*} \equiv y_{ij} \pmod{26}$.

This gives:

$$\boldsymbol{Y} = \begin{bmatrix} 9 & 15 & 4 \\ 12 & 0 & 13 \\ 14 & 14 & 16 \\ 25 & 13 & 16 \end{bmatrix} mod\, 26$$

Now concatenate the rows of $\boldsymbol{Y}$ to get 9 15 4 12 0 13 14 14 16 25 13 16 and replace each integer with its corresponding letter according to alphabetical encoding to obtain the ciphertext **IODLZMNNPYOP**.

3.2 Example decryption using matrices

We will consider a ciphertext to be decrypted: **IODLZMNNPYMP**

According to the Hill Cipher alphabetical encoding scheme, we will make use of as opposed to the ASCII encoding scheme, the letters in the ciphertext correspond to the following numbers:

Table 3: *Alphabetical Encoding Scheme for message to be decrypted*

LETTER	I	O	D	L	Z	M	N	P	Y
NUMER	9	15	4	12	0	13	14	16	25

The message will be decrypted using the predetermined secret key privy to only those concerned. Suppose the secret key is $\boldsymbol{K} = \begin{bmatrix} 9 & 18 & -18 \\ 18 & 9 & 18 \\ -18 & 18 & 9 \end{bmatrix}$.

We will now break up this sequence lengthwise into rows of length 3 (the dimension of $\boldsymbol{K}$). This step will result in a matrix $\boldsymbol{Y}$ **,** as shown below:

$$\boldsymbol{Y} = \begin{bmatrix} 9 & 15 & 4 \\ 12 & 0 & 13 \\ 14 & 14 & 16 \\ 25 & 13 & 16 \end{bmatrix}$$

Now we decrypt the message by performing the operation of matrix multiplication thus:

$$\boldsymbol{X} = \boldsymbol{Y}\boldsymbol{K}^{-1}$$

$$\boldsymbol{K}^{-1} = \begin{bmatrix} 9 & 18 & -18 \\ 18 & 9 & 18 \\ -18 & 18 & 9 \end{bmatrix}$$

$$\boldsymbol{X} = \begin{bmatrix} 9 & 15 & 4 \\ 12 & 0 & 13 \\ 14 & 14 & 16 \\ 25 & 13 & 16 \end{bmatrix} \times \begin{bmatrix} 9 & 18 & -18 \\ 18 & 9 & 18 \\ -18 & 18 & 9 \end{bmatrix}$$

$$\boldsymbol{x}_{11} = (9\times 9)+(15\times 18)+(4\times -18)$$
$$\boldsymbol{x}_{12} = (9\times 18)+(15\times 9)+(4\times 18)$$
$$\boldsymbol{x}_{13} = (9\times -18)+(15\times 18)+(4\times 9)$$
$$\boldsymbol{x}_{21} = (12\times 9)+(0\times 18)+(13\times -18)$$
$$\boldsymbol{x}_{22} = (12\times 18)+(0\times 9)+(13\times 18)$$
$$\boldsymbol{x}_{23} = (12\times -18)+(0\times 18)+(13\times 9)$$
$$\boldsymbol{x}_{31} = (14\times 9)+(14\times 18)+(16\times -18)$$
$$\boldsymbol{x}_{32} = (14\times 18)+(14\times 9)+(16\times 18)$$
$$\boldsymbol{x}_{33} = (14\times -18)+(14\times 18)+(16\times 9)$$
$$\boldsymbol{x}_{41} = (25\times 9)+(13\times 18)+(16\times -18)$$
$$\boldsymbol{x}_{42} = (25\times 18)+(13\times 9)+(16\times 18)$$
$$\boldsymbol{x}_{43} = (25\times -18)+(13\times 18)+(16\times 9)$$

$$\boldsymbol{X} = \begin{bmatrix} 81+270-72 & 162+135+72 & -162+270+36 \\ 108+0-234 & 216+0+234 & -216+0+117 \\ 126+252-288 & 252+126+288 & -252+252+144 \\ 225+234-288 & 450+117+288 & -450+234+144 \end{bmatrix}$$

$$\boldsymbol{X} = \begin{bmatrix} 279 & 369 & 144 \\ -126 & 450 & -99 \\ 90 & 666 & 144 \\ 171 & 855 & -72 \end{bmatrix}$$

For every entry x_{ij} that does not satisfy $0 \le x_{ij} \le 25$, we replace x_{ij} with the integer $x_{ij}^* \in \{0,...,25\}$ such that $x_{ij}^* \equiv x_{ij} \left(\boldsymbol{mod} 26\right)$.

This gives:

$$\boldsymbol{X} = \begin{bmatrix} 19 & 5 & 14 \\ 4 & 8 & 5 \\ 12 & 16 & 14 \\ 15 & 23 & 6 \end{bmatrix} mod\, 26$$

We concatenate the rows of $\boldsymbol{X}$ to get $19\ 5\ 14\ 4\ 8\ 5\ 12\ 16\ 14\ 15\ 23\ 6$ and replace each integer with its corresponding letter according to alphabetical encoding to obtain the plaintext message **SENDHELPNOWP** from which we deduce that the actual message is **SEND HELP NOW P**.

This is one way that matrices can be used for encrypting messages. The security of the encryption method can be improved by using a different encoding scheme apart from the direct substitution for the alphabet, that is, alphabetical encoding schemes such as the ASCII encoding scheme and several others. Also, the size of the matrix can be increased to make the decoding process more strenuous.

When choosing matrices in modulo 26, it has to be noted that not all matrices have inverses in modulo 26. It is wiser to choose a different basis, perhaps even a larger one to be included symbols and punctuation marks. All in all, matrices are very useful for encoding messages.

The use of the orthogonal matrix, gotten from the equation of the plane, has made the encryption process relatively more secure. The orthogonal matrices are, in turn, used to create a key matrix of classical Hill cipher to improve the security of communication text.

The advancement of computers and technology rendered the Hill Cipher incredibly vulnerable. Figuring out the encryption key was no longer a cumbersome process as computers can iterate through thousands of keys in relatively short periods, making it possible to find the correct key in minutes.

However, in recent times, the use of Hill Cipher for encryptions has declined significantly because of its vulnerability but has become a building block for various other encryption schemes.

An alternative form of encryption that is also widely used and provides the practical security required in today's world is the RSA encryption. The principle behind the RSA encryption is the use of extremely large prime numbers as keys. Today these keys are about 2048 bits long. That is, the keys can have approximately 617 digits. The fact that no known method can effectively factor such huge numbers is the foundation of RSA encryption. Both the sender and the receiver have a public and a private key in RSA encryption. Anyone, including those who may desire to intercept the encoded communication, has access to the public key. The private key, on the other hand, is known only by its owner, as one would expect. A communication is encrypted using the sender's public key, and it can only be decoded with the intended recipient's private key, which is only known to them.

4. Conclusion and Remarks

Data encryption and data decryption algorithm to secure information using a secret key passed between a sender and a receiver has been discussed in this paper. The following conclusions have been drawn based on the results obtained from this study:

I. Modern Mathematical Cryptography has its foundation in many aspects of Mathematics such as Number theory, Algebra, Probability, Statistics, and Information theory, and as such, the role of Mathematics in Cryptography is a very crucial one because difficult mathematical problems form the foundation of asymmetric key cryptography.
II. The algorithm in this paper provides a method of sending messages securely and secretly and is considered a good one because it uses mathematical techniques. The encrypted message can only be decrypted if the sender and receiver know the key matrix and congruence modulo.
III. The simplicity and availability of the encryption and decryption algorithms discussed in this paper prove that problem-solving tools can be developed with no resort to expensive software from the market. Although the algorithms are not as efficient as more widely known modern-day encryption algorithms, they can be used ad building blocks for better algorithms.
IV. Cryptography is necessary to secure digital communications, software, and other digital property. The security of communications and commerce in this digital age depends on the modern incorporation of the pre-historic technique of codes and ciphers.
V. Reduction of the amount of storage space and computational overhead consumed is possible with data encryption because the data owner can harness the advantage of message splitting into smaller words.

4.1 Recommendation

Cyclic square matrices can be used in place of orthogonal matrices because they provide an efficient approach suitable for any number of words having significantly more characters. Cryptosystems that eliminate the need for key sharing are more secure because they reduce the risks of an attack. One of such cryptosystems involves the use of block matrices with a generalized Fibonacci sequence. This cryptosystem should be studied with reference to asymmetric key cryptography because they provide for increased efficiency and security.

The security of the Hill cipher is often compromised due to its linearity. This issue can be addressed via modifications using a bit-level permutation that would make the Hill Cipher non-linear in addition to matrix transformation as well as matrix multiplication.

Cryptosystems/Cryptography algorithms should focus not only on security but also on the time complexity. That is, the algorithms should be made computationally less intensive to reduce the amount of CPU time and space they consume at the time of encryption.

Acknowledgment

The authors thank the CUCRID section of Covenant University for supporting this research.

References

[1] David, M., Diego, P., & Daniel, L. A. (n.d.). Cryptography and Linear Algebra.
[2] Ayan, M. (2013). Are Matrices Useful in Public-Key Cryptography? International Mathematical Forum, 8(39), 1.
[3] Peter, B. Z., & Wajiga, G. (2011). Cryptographic Algorithm Using Matrix Inversion. Journal of ICT, 68.
[4] Yamuna, M., Rohith, S. R., Pramodh, M., & Avani, G. (2013, March). Text Encryption Using Matrices. International Journal of Application or Innovation in Engineering & Management, 2(3), 1.
[5] Chua, B. L. (2006). Harry Potter and the Cryptography with matrices. Nanyang Technological University, Singapore, Singapore.

[6] Mani, D. K., & Begam, A. B. (2019, October). Generation Of Keymatrix For Hill Cipher Encryption Using Quadratic Form. International Journal of Scientific & Technology Research, 8(10), 964-968.
[7] Kartit, Z., Azoughahge, A., Idrissi, H. .., Marraki, M. E., M.Hedabou, & Belkasmi, M. (2017). Applying Encryption Algorithm for Data Security in Cloud Storage. Mohammed V University , Morocco , Faculty of Sciences , Rabat.
[8] Lander, S. (2017). Advantages & Disadvantages of Symmetric Key Encryption: https://itstillworks.com/advantages-disadvantages-symmetric-key-encryption-2609.html
[9] Stallings, W. (2005). Cryptography and Network Security Principles and Practices (4th ed.). Upper Saddle River, New Jersey, United States of America: Pearson Prentice Hall.
[10] Blumenthal, M. (2010). Encryption: Strengths and Weaknesses of Public-Key Cryptography. Villanova University, Department of Computing Sciences , Villanova.
[11] Miller, B. (2016, August 6). More: Green Garage Blog. Retrieved July 1, 2020, from Green Garage Blog: https://greengarageblog.org/8-pros-and-cons-of-asymmetric-encryption
[12] Dang, Q. (2009). Randomized Hashing for Digital Signatures. National Institute of Standards and Technology , Department of Commerce.
[13] Gaines, F. H. (1939). Cryptanalysis: A study of ciphers and their solution (1st ed.). New York, New York, United States of America: Dover Publications, Inc
[14] Shinder, D. L., & Cross, M. (2008). Understanding Cybercrime Prevention (2nd ed.). (A. Doyle, Ed.) United States of America: Syngress Publishing Inc.
[15] Hope, C. (2017, April 26). Dictionary D-Definitions: ComputerHope. Retrieved July 1, 2020, from ComputerHope: https://www.computerhope.com/jargon/d/decrypti.
[16] Delfs, H., & Knebl, H. (2007). Introduction to Cryptography: Principles and Applications (2nd ed.). Lausanne, Switzerland: Springer.
[17] Rouse, M. (2019, May). Retrieved July 1, 2020, from Search Security: https://searchsecurity.techtarget.com/definition/private-key
[18] Davidson, L. (2010). Applications of Linear Algebra in Economics: Input-Output and Inter-Industry Analysis
[19] Kotas, W. A. (2000). A Brief History of Cryptography. Honors Thesis Projects, University of Tennessee , Computer Science, Knoxville.
[20] Hamed, A. B., & Albudaw, I. O. (2017). Encrypt and Decrypt Messages Using Invertible Matrices. American Journal of Engineering Research (AJER), 6(6), 212.
[21] Thiagarajan, K., P, B., Nagaraj, J., & Padmashree, J. (2018). Encryption and decryption algorithm using algebraic matrix approach. IOP Conf. Series: Journal of Physics. pp. 70-73
[22] McAndrew, A. "Using the Hill cipher to teach cryptographic principles," International Journal of Mathematical Education in Science & Technology, vol 38. No. 7, 2008, pp. 967-979.
[23] Thiruchelvi,M Application of Linear Algebra in Cryptography, International Conference on Information and Image Processing (ICIIP-2014), ISBN 978-93-83459-16-2 © 2014 Bonfring
[24] Mokhtari, M. and Naraghi, H "Analysis and Design of Affine and Hill Cipher," Journal of Mathematics Research, vol. 4, no. 1, 2012, pp. 67-77.
[25] Meyer, C. D. (2000). Matrix Analysis and Applied Linear Algebra. (K. Thomas, Ed.) SIAM.
[26] Diffiem W and Hellman, M. E. "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, 1976, pp. 644-654Richard, B., & Gabriel, B. C. (2009). MATRIX METHODS: Applied Linear Algebra (3rd Edition ed.). San Diego, California, United States of America: Academic Press.
[27] Odun-Ayo, I., Alagbe, O., Yahaya, J. 2021, A systematic mapping study of security, trust and privacy in clouds Bulletin of Electrical Engineering and Informatics, 10(3), pp. 1598-1610.
[28] Afolabi, I.T., Ayo, A., Odetunmibi, O.A. 2021, Academic Collaboration Recommendation for Computer Science Researchers Using Social Network Analysis, Wireless Personal Communications, 121(1), pp. 487-501