عدد خاص
بالمؤتمر الليبي الدولي للعلوم التطبيقية
و الهندسية
27-28- سبتمبر 2022

# Some Applications of the Multiplicative Inverse of the Matrix in Cryptography

**Asmaa M. Kanan**
Mathematics Department
Science Faculty
Sabratha University, Libya
asmaakanan20@gmail.com

**Nahla alkhtry**
Computer Science Department
Science Faculty
Sabratha University, Libya
alkhtrynahla@gmail.com

**Marwa K. Golek**
Higher Institute of Technical
Water Affairs
Alajelat, Libya
marwajolk@gmail.com

**الملخص**

علم التشفير هو مجال علوم الكمبيوتر والرياضيات الذي يركز على تكنولوجيا الاتصال الآمن بين شخصين أثناء وجود شخص ثالث. إنه يتضمن عمليتي التشفير وفك التشفير.

في هذه الورقة ندرس استخدام المعكوس الضربي للمصفوفة كتطبيق للجبر الخطي فوق حلقة الأعداد الصحيحة مقياس $n$ في التشفير. نحن نناقش استخدامه في التشفير كمفتاح involutory مؤسس على صيغة مصفوفية عامة، وكمفتاح private مؤسس على مصفوفة مربعة غير شاذة، وفي كلا الحالتين نحن نعمل على حلقة الأعداد الصحيحة العامة $\mathbb{Z}_{26}$؛ كما نناقش استخدامه في الحالتين السابقتين اعتماداً على ترميز الآسكي، وفي هذه الحالة نعمل على $\mathbb{Z}_{255}$. نحن نعطي خوارزميات لكل ذلك ونوضحها بأمثلة. باستخدام هذين المفتاحين في التشفير نتحصل على رسائل واتصالات سرية وآمنة.

**Abstract**

Cryptography is a field of computer science and mathematics that focusses on techniques for secure communication between two parties while a third-party is present. It includes an encryption and decryption.

In this paper we study using the multiplicative inverse of the matrix as an application of linear algebra over $\mathbb{Z}_n$ in cryptography. We investigat using it in cryptography as the involutory key based on a general matrix formula, and as private key based on a square non-singular matrix. In both cases, we work on the general ring of integers $\mathbb{Z}_{26}$; as we investigate using it in the last two cases depending on American Standard Code for Information Interchange (ASCII), in this case we work on $\mathbb{Z}_{255}$. We give algorithms for all that and explain them by examples. Using these keys in cryptography we get secure and confidential messages and communications.

**Keywords:** Cryptography, The Multiplicative Inverse of The Matrix, Plain text, Cipher text, Encryption, Decryption, Algorithms.

## 1. Introduction

Cryptography is the science of study of encryption and decryption and uses the mathematics for that. Human in world have a big problem with electronic communication on computer net works. They need a way to ensure that messages and information with electronic communication on computer net works stay confidential. Cryptography gives solutions for this problem. Encryption techniques hav both advantages and disadvantages, but have become the immediate solutions.

Many papers studied the algebraic methods in cryptography. We mean, the algebraic methods which converts a plain message (plain text) into a cipher message (cipher text), these methods are well-known through some papers [5-9] and others. In 2016 [10] Maxrizal and Prayanti introduced Hill cipher in a new method using rectangular matrix. In 2019 [2] Jayanthi worked on ASCII code and developed an algorithm for cryptography using Laplace transforms and corresponding inverse Laplace transforms for encryption and decryption respictively. In 2020 [1] Kanan and Abu Zayd worked on $\mathbb{Z}_{26}$ and introdused a good method in cryptography, they used the rectangular matrix that has full row rank or full column rank or full factorization as a key for encryption, and corresponding Moore-Penrose generalized inverse as a key for decryption.

The aim of this paper is study using the multiplicative inverse of the matrix in cryptography; for that we give a very general matrix formula of a matrix $K$ such that $K = K^{-1}$ [6] to use it in symmetric cryptography (involutory key). As we choose a square matrix $K$ such that the determinant of $K$ is not equal to zero ($|K| \neq 0$), this means that $K$ has the multiplicative inverse $K^{-1}$ [12] (i.e., $K$ is an invertible matrix) and use it in asymmetric cryptography (private key). The modular computations play an important rule in crypyography, so all our computations through this paper depending on the modular 26, and 255 (mod 26, and mod 255). If we will work on $\mathbb{Z}_{26}$, then we can do all computations when $|K|$ is prime to 26, and if we will work on $\mathbb{Z}_{255}$, then we can do all computations when $|K|$ is prime to 255. As we use $K^{-1}$ of the invertible matrix $K$ in cryptography applied on message encoded by ASCII code.

It is well-known that to each of the 26 letters of the alphabet there exists a unique integer from the set 0, 1, 2, 3, …, 25. That means, there is a one-to-one correspondence between the alphabit letters and the last set of numbers, as in the following table.

**Table 1. The alphabetic correspondence**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

| O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

These numerical values are used to construct the matrix of the plain taxt $P$, and the matrix of the cipher taxt $C$. That is any plain text or message can be converted to a unique cipher text by dividing the letters of the plain text into blocks and replacing these letters by numerical values from table (1) to get $P$ which converts to $C$ using the key of encryption $K$, then using table (1) we can replace the entries of $C$ into letters, hence we get the cipher text.

By the converse way, we can decryption the cipher text into the plain taxt using the key of decryption $K^{-1}$ and table (1). We give algorithms for our work in this paper and apply them by examples.

Note that, you can use the Matlab programming to get quick results.

## 2. Preliminaries

In this section, we give important concepts about the multiplicative inverse of the matrix, and cryptography. For more information about these (and other) notions, we refer the reader to $[3, 11, 12]$.

### *2.1. Definitions and Theorems*

**Definition 2.1.1 (The multiplicative invere of a matrix)**

If $A \in M_n(\mathbb{R})$, then $A$ is invertible (non–singular) if there exists a matrix $A^{-1}$ satisfies

$$AA^{-1} = A^{-1}A = I,$$

where $A^{-1}$ is called the multiplicative inverse of $A$, or simply, inverse of $A$. If $A$ is not invertible then $A$ is called a singular.

**Definition 2.1.2 ( Full rank )**

If rank of a matrix $A$ $(of\ size\ m \times n\ )$ equals the smaller of $m\ and\ n$, then $A$ has full rank. Where rank of $A$ is the maximum number of non-zero rows in the row-readuced matrix of $A$.

**Theorem 2.1.1 [3] (Invertibility )**

A matrix is invertible if and only if it is square and full rank.

### *2.2 Computation of The Multiplicative Inverse of a Matrix*

In this section we give one method for finding the multiplicative inverse of a matrix. It is a simple method and given by the following theorem.

**Theorem 2.2.1** If $|A| \neq 0$, then $A$ is invertible and

$$A^{-1} = \frac{1}{|A|}\, adj(A), adj(A) = [cof(A)]^T,$$

where $adj(A)$ denotes the adjoint of $A$, $cof(A)$ denotes the cofactor of $A$.

### *2.3 Types of Cryptography*

**(1) Symmetric (conventional) cryptography**

In this type we use one key for each of encryption and decryption. It depends on the used key which is called the symmetric key or involutory key. Examples for this type:

(i) Caesar cipher.

(ii) Vigener cipher.

(iii) Data Encryption Standard (or DES).

The following figure shows this type.

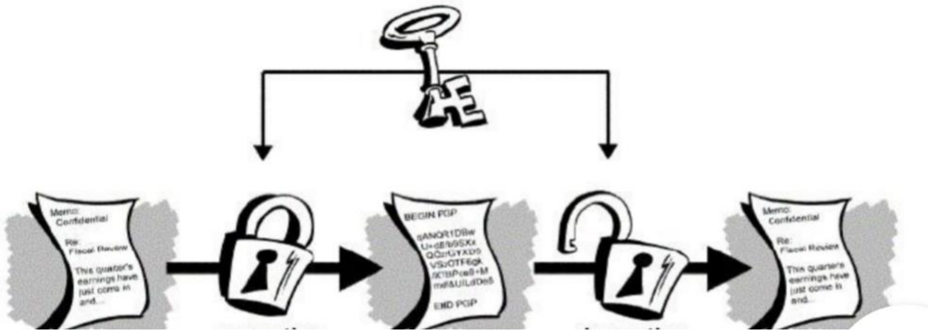

Figure1. [4] Symmetric cryptography

**(2) Asymmetric cryptography**

In this type, we use two keys. One of them uses for encryption to get cipher text, it is called the public key, and the other one uses for decryption to get plain text, it is called privet key and stays only with the recipient. Examples for asymmetric cryptography:

(i) The W-key Drazin inverse encryption [6].

(ii) The V-key Drazin inverse encryption [7].

The following figure shows this type.

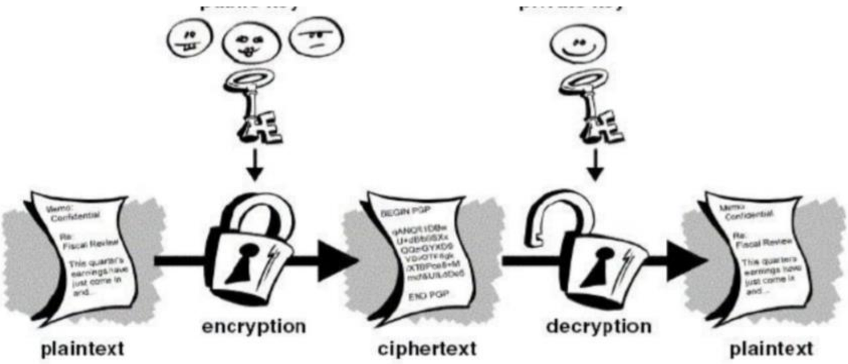


Figure 2. [4] Asymmetric cryptography

## 3. Using The Multiplicative Inverse of a Matrix in Cryptography

In this section we will work on the general ring $\mathbb{Z}_{26}$, and $\mathbb{Z}_{255}$. We will use $K^{-1}$ for the multiplicative inverse of the matrix $K$.

### *3.1 Using $K^{-1}$ as Involutory Key*

We consider an involutory key. In the symmetric cryptography, we can use the matrix $K$ that satisfies $K = K^{-1}$, as a key for each of encryption and decryption. This means $K^{-1}$ or $K$ is an involutory key. In this case, the plain text always can be described, because $KK = I$. Also, the size of the plain text and the cipher text is equal, so there is a one-to-one corresponding between the plain text and the cipher text [10].

In this subsection, we mention a very general formula for involutory matrices [6]. This formula states that the matrix $K$ defined by

$$K = \begin{pmatrix} A_2A_1 - I_S & \vdots & A_2 \\ \dots & \dots & \cdots \\ 2A_1 - A_1A_2A_1 & \vdots & I_r - A_1A_2 \end{pmatrix}_{m\times m},$$

is (in a partition form) always involutory ($K = K^{-1}$ or $K^2 = I\ (mod\ 26)$), where $A_1$ and $A_2$ are arbitrary matrices of size $r \times s$ *and* $s \times r$ respectively, and $r + s = m$.

**Example 3.1.1** If we want the matrix $K$ of size $m \times m$ where $m = 4$, and if $r = 1,\ s = 3$ , then $A_1 = (3 \quad 2 \quad 5)$, $A_2 = (2 \quad 14 \quad 10)^T$. If we work with *mod* 26, then

$$A_2 * A_1 = \begin{pmatrix} 2 \\ 14 \\ 10 \end{pmatrix} (3 \quad 2 \quad 5)\ (mod\ 26) = \begin{pmatrix} 6 & 10 & 4 \\ 16 & 18 & 2 \\ 4 & 24 & 20 \end{pmatrix},$$

$$A_1 * A_2 = (3 \quad 2 \quad 5) \begin{pmatrix} 2 \\ 14 \\ 10 \end{pmatrix} (mod\ 26) = (18),\ A_1 * A_2 * A_1 = (2 \quad 12 \quad 10),$$

$$(2A_1 - (A_1 * A_2 * A_1))(mod\ 26) = (4 \quad 24 \quad 20).$$

Hence

$$K = \begin{pmatrix} 5 & 10 & 4 & 2 \\ 16 & 17 & 2 & 14 \\ 4 & 24 & 19 & 10 \\ 4 & 24 & 20 & 9 \end{pmatrix}.$$

We can verified that $K^2 = I\ (mod\ 26)$ easily.

Now, we give algorithm for using $\mathrm{K}^{-1}$ as Involutory key.

 

**Algorithm 3.1.1**
**Encryption:**

**Step E1:** Replace the letters of the plain text by the corresponded numerical values from table (1).

**Step E2:** Construct the matrix $P$ from the numerical valus that you get in step E1.

**Step E3:** Create the key matrix $K$ (the key of encryption) that satisfics $K = K^{-1}$.

**Step E4:** Calculate

$$KP\ (mod\ n\ ) = C.$$

**Step E5:** Replace the entries of the matrix $C$ by the corresponded letters from table (1) to get the cipher taxt.

**Decryption:**

**Step D1:** Replace the letters of the cipher text by the corresponded numerical values from table (1).

**Step D2:** Construct the matrix $C$ from the numerical valus that you get in step D1.

**Step D3:** Create the key matrix $K^{-1}$ (=$K$).

**Step D4:** Calculate

$$K^{-1}C(mod\ n) = P.$$

**Step D5:** Replace the entries of the matrix $P$ by the corresponded letters from table (1) to get the plain taxt.

We will explain all that by example (4.1).

### *3.2 Using $K^{-1}$ as Private Key*

Using $K^{-1}$ as a private key ($K^{-1} \neq K$ ) cosiders an asymmetric cryptograph, because the invertible square matrix $K$ uses as a key matrix in encryption, and its inverse $K^{-1}$ uses as a key matrix in decryption. In the case of using $K^{-1}$ as private key, then the plain text always can be described, because $K^{-1}K = I$. Also, the size of the plain text and cipher text is equal, so there is a one-to-one corresponding between the plain text and the cipher text.

In the fact, not all matrices have multiplicative inverse mod $n$. If $K$ is not invertible mod $n$, then we can not get the plain text from the cipher text, and the decryption fails to do.

Note that, an algorithm for using $\mathrm{K}^{-1}$ as Private Key is similar to that one used for an involutory key, just here we choose the key matrix $K$ that has multiplicative inverse $K^{-1}$ to use it for encryption (in step E3), and $K^{-1}$ to use it for decryption. We will explain that by example (4.2).

### *3.3 Using $K^{-1}$ in Cryptography Depending on ASCII*

This subsection is similar to the last subsections (3.1) and (3.2), but here we will use ASCII table [13]. By example (4.3) we can explain how to use the multiplicative inverse $K^{-1}$ of the invertible matrix $K$ as a private key in cryptography applied on message encoded by ASCII code. We will use the ASCII table in [13] to convert the letters into numbers, and the numbers into letters. Also, we can use $K^{-1}$ as an involutoty key by the same away.

## 4. Numerical Examples

### Example 4.1

Marwa wants to send a message to Asmaa. She will send

" CALL ME TO NIGHT "..

**Encryption:**

**Step E1:** Marwa replaces the message or the plain text into numbers using table (1) as in the following table (2):

**Table 2. Converting the plain text into numbers**

| Letter | Number | Letter | Number | Letter | Number | Letter | Number |
|---|---|---|---|---|---|---|---|
| **C** | **2** | **M** | **12** | **N** | **13** | **T** | **19** |
| **A** | **0** | **E** | **4** | **I** | **8** | **A** | **0** |
| **L** | **11** | **T** | **19** | **G** | **6** | **A** | **0** |
| **L** | **11** | **O** | **14** | **H** | **7** | **A** | **0** |

Note that, Marwa wrote the letters horizontally in four rows and vertically in four columns to get $P$ of size 4×4, and hence she can multiply $KP$.

**Step E2:** Marwa constructs the matrix $P$ from the numerical valus in table (2),

$$P = \begin{pmatrix} 2 & 12 & 13 & 19 \\ 0 & 4 & 8 & 0 \\ 11 & 19 & 6 & 0 \\ 11 & 14 & 7 & 0 \end{pmatrix}.$$

**Step E3:** Marwa chooses the involutory key $K$ (the key of encryption) that satisfics $K = K^{-1}$.

$$K = \begin{pmatrix} 17 & 24 & 2 & 18 \\ 20 & 17 & 21 & 7 \\ 8 & 2 & 10 & 21 \\ 20 & 18 & 21 & 6 \end{pmatrix}.$$

**Step E4:** Marwa calculates

$$KP\ (mod\ 26\ ) = \begin{pmatrix} 254 & 590 & 551 & 323 \\ 348 & 805 & 571 & 380 \\ 357 & 588 & 327 & 152 \\ 337 & 795 & 572 & 380 \end{pmatrix} (mod 26)$$

$$= \begin{pmatrix} 20 & 18 & 5 & 11 \\ 10 & 25 & 25 & 16 \\ 19 & 16 & 15 & 22 \\ 25 & 15 & 0 & 16 \end{pmatrix} = C.$$

**Step E5:** Marwa replaces the entries of the matrix $C$ by the corresponded letters from table (1) to get the cipher taxt as in the following table (3):

**Table 3. Converting the numbers into letters**

| Number | Letter | Number | Letter | Number | Letter | Number | Letter |
|---|---|---|---|---|---|---|---|
| 20 | U | 18 | S | 5 | F | 11 | L |
| 10 | K | 25 | Z | 25 | Z | 16 | Q |
| 19 | T | 16 | Q | 15 | P | 22 | W |
| 25 | Z | 15 | P | 0 | A | 16 | Q |

and hence, Marwa sends the following ciphered message:

" UKTZSZQPFZPALQWQ ".

**Decryption:**

Asmaa receives the ciphered message

" UKTZSZQPFZPALQWQ ".

**Step D1:** Asmaa replaces the letters of the cipher message by the corresponded numerical values from table (1) as following.

**Table 4. Converting the plain text into numbers**

| Letter | Number | Letter | Number | Letter | Number | Letter | Number |
|---|---|---|---|---|---|---|---|
| U | 20 | W | 22 | F | 5 | L | 11 |
| K | 10 | P | 15 | Z | 25 | Q | 16 |
| T | 19 | M | 12 | P | 15 | W | 22 |
| Z | 25 | Z | 25 | A | 0 | Q | 16 |

**Step D2:** Asmaa constructs the matrix $C$ from the numerical valus in table (4).

$$C = \begin{pmatrix} 20 & 18 & 5 & 11 \\ 10 & 25 & 25 & 16 \\ 19 & 16 & 15 & 22 \\ 25 & 15 & 0 & 16 \end{pmatrix}.$$

**Step D3:** Asmaa creates the key matrix $K^{-1}$ (=$K$).

**Step D4:** Asmaa calculates

$$K^{-1}C(mod\ 26) = \begin{pmatrix} 1068 & 1208 & 715 & 903 \\ 1144 & 1226 & 840 & 1066 \\ 895 & 669 & 240 & 676 \\ 1129 & 1236 & 865 & 1066 \end{pmatrix}(mod 26)$$

$$= \begin{pmatrix} 2 & 12 & 13 & 19 \\ 0 & 4 & 8 & 0 \\ 11 & 19 & 6 & 0 \\ 11 & 14 & 7 & 0 \end{pmatrix} = P.$$

**Step D5:** Asmaa converts the entries (numbers) of $P$ into letters as in the following table (5)

**Table 5. Converting the numbers into letters**

| Number | Letter | Number | Letter | Number | Letter | Number | Letter |
|---|---|---|---|---|---|---|---|
| 2 | C | 12 | M | 13 | N | 19 | T |
| 0 | A | 4 | E | 8 | I | 0 | A |
| 11 | L | 19 | T | 6 | G | 0 | A |
| 11 | L | 14 | O | 7 | H | 0 | A |

hence, Asmaa gets the original message :

" CALL ME TO NIGHT ".

**Example 4.2**

Nahla wants to send a message to Asmaa, it is

" MEET YOU TOMORROW ".

**Encryption:**

**Step E1:** Nahla replaces the message into numbers using table (1) as in the following table (6):

**Table 6. Converting the plain text into numbers**

| Letter | Number | Letter | Number | Letter | Number | Letter | Number | Letter | Number |
|---|---|---|---|---|---|---|---|---|---|
| M | 12 | T | 19 | U | 20 | M | 12 | R | 17 |
| E | 4 | Y | 24 | T | 19 | O | 14 | O | 14 |
| E | 4 | O | 14 | O | 14 | R | 17 | W | 22 |

Note that, Nahla wrote the letters horizontally in three rows and vertically in five columns to get $P$ of size $3 \times 5$ and hence she can multiply $KP(mod\ 26)$.

**Step E2:** Nahla constructs the matrix $P$ from the numerical valus in table (6),

$$P = \begin{pmatrix} 12 & 19 & 20 & 12 & 17 \\ 4 & 24 & 19 & 14 & 14 \\ 4 & 14 & 14 & 17 & 22 \end{pmatrix}.$$

**Step E3:** Nahla chooses the privat key $K$ (the key of encryption),

$$K = \begin{pmatrix} 2 & 3 & 4 \\ 5 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

**Stap E4:** Nahla enciphers the plain text as,

$$KP(mod\ 26) = \begin{pmatrix} 0 & 10 & 23 & 4 & 8 \\ 0 & 13 & 19 & 24 & 1 \\ 22 & 9 & 2 & 11 & 13 \end{pmatrix} = C.$$

**Step E5:** Nahla converts the numbers of the matrix $C$ into letters as the following table:

**Table 7. Converting the numbers into letters**

| Nnmber | Letter | Number | Letter | Number | Letter | Number | Letter | Number | Letter |
|---|---|---|---|---|---|---|---|---|---|
| **0** | **A** | **10** | **K** | **23** | **X** | **4** | **E** | **8** | **I** |
| **0** | **A** | **13** | **N** | **19** | **T** | **24** | **Y** | **1** | **B** |
| **22** | **W** | **9** | **J** | **2** | **C** | **11** | **L** | **13** | **N** |

Hence, Nahla send

" AAWKNJXTCEYLIBN ".

**Decryption:**

Asmaa receives the cipher message:

"AAWKNJXTCEYLIBN".

She has the decryption key already.

**Step D1:** Asmaa converts the letters of the cipher message into numbers using the table (1) as following.

**Table 8. Converting the plain text into numbers**

| Letter | Number | Letter | Number | Letter | Number | Letter | Number | Letter | Number |
|---|---|---|---|---|---|---|---|---|---|
| A | 0 | K | 10 | X | 23 | E | 4 | I | 8 |
| A | 0 | N | 13 | T | 19 | Y | 24 | B | 1 |
| W | 22 | J | 9 | C | 2 | L | 11 | N | 13 |

**Step D2:** Asmaa gets

$$C = \begin{pmatrix} 0 & 10 & 23 & 4 & 8 \\ 0 & 13 & 19 & 24 & 1 \\ 22 & 9 & 2 & 11 & 13 \end{pmatrix}.$$

**Step D3:** Asmaa creates the decryption key $K^{-1}$

$$K^{-1} = \begin{pmatrix} 15 & 1 & 10 \\ 15 & 24 & 12 \\ 1 & 1 & 25 \end{pmatrix}.$$

**Step D4:** Asmaa calculates

$$K^{-1}C(mod\ 26) = \begin{pmatrix} 220 & 253 & 384 & 194 & 25 \\ 264 & 570 & 825 & 768 & 300 \\ 550 & 248 & 92 & 303 & 334 \end{pmatrix}(mod 26)$$

$$= \begin{pmatrix} 12 & 19 & 20 & 12 & 17 \\ 4 & 24 & 19 & 14 & 14 \\ 4 & 14 & 14 & 17 & 22 \end{pmatrix} = P.$$

**Step D5:** Asmaa replaces the entries of the matrix $P$ by the corresponded letters from table (1) to get the plain taxt as,

**Table 9. Converting the numbers into letters**

| Number | Letter | Number | Letter | Number | Letter | Number | Letter | Number | Letter |
|---|---|---|---|---|---|---|---|---|---|
| 12 | M | 19 | T | 20 | U | 12 | M | 17 | R |
| 4 | E | 24 | Y | 19 | T | 14 | O | 14 | O |
| 4 | E | 14 | O | 14 | O | 17 | R | 22 | W |

Hence Asmaa gets

"MEET YOU TOMORROW".

**Example 4.3**

In this example, we explain how to use the multiplicative inverse of the invertible matrix in cryptography applied on message encoded by ASCII code. If we have the following Arabic message:

**"يوضح هذا البحث أهمية استخدام المعكوس الضربي للمصفوفات في التشفير, حيث قدمنا هذا المعكوس كمصفوفة مفتاحية في التشفير المتماثل و غير المتماثل".**

We want to encrypt and decrypt this message using $K^{-1}$ as a private key according to ASCII code. We will work on $\mathbb{Z}_{255}$ and use the table in [13].

**Encryption :**

**Step E1**: We order the characters of message in a matrix $X$ as following.

$X =$

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| ي | ه | ع | ف | ، | ل | ف | ر | ا |
| و | م | ك | و | ح | م | ت | — | ل |
| ض | ي | و | ف | ي | ع | ا | ا | م |
| ح | ة | س | ا | ث | ك | ح | ل | ت |
| — | — | — | ت | — | و | ي | م | م |
| ه | ا | ا | — | ق | س | ة | ت | ا |
| ذ | س | ل | ف | د | — | — | م | ث |
| ا | ت | ض | ي | م | ك | ف | ا | ل |
| — | خ | ر | — | ن | م | ي | ث | $X$ |
| ا | د | ب | ا | ا | ص | — | ل | $X$ |
| ل | ا | ي | ل | — | ف | ا | — | $X$ |
| ب | م | — | ت | ه | و | ل | و | $X$ |
| ح | — | ل | ش | ذ | ف | ت | غ | $X$ |
| ث | ا | ل | ف | ا | ة | ش | ي | $X$ |
| — | ل | م | ي | — | — | ف | ر | $X$ |
| أ | م | ص | ر | ا | م | ي | — | $X$ |

Note that, we completed the final column of the matrix $X$ by the character "$X$ ".

**Step E2**: We replace the characters of $X$ by numbers using the table in [13] to get the matrix $P$:

$$P = \begin{pmatrix} 234 & 231 & 236 & 225 & 172 & 228 & 225 & 209 & 199 \\ 232 & 229 & 227 & 232 & 205 & 229 & 202 & 32 & 228 \\ 214 & 234 & 232 & 225 & 234 & 236 & 168 & 199 & 229 \\ 174 & 201 & 188 & 168 & 171 & 227 & 205 & 228 & 202 \\ 32 & 32 & 32 & 170 & 32 & 232 & 234 & 229 & 229 \\ 231 & 199 & 199 & 32 & 226 & 188 & 201 & 202 & 168 \\ 208 & 211 & 228 & 225 & 207 & 32 & 32 & 229 & 203 \\ 199 & 202 & 214 & 246 & 229 & 227 & 225 & 168 & 251 \\ 32 & 206 & 209 & 32 & 230 & 229 & 246 & 203 & 88 \\ 199 & 207 & 200 & 199 & 168 & 213 & 32 & 251 & 88 \\ 228 & 199 & 246 & 228 & 32 & 225 & 199 & 32 & 88 \\ 200 & 239 & 32 & 202 & 231 & 232 & 228 & 232 & 88 \\ 205 & 32 & 228 & 212 & 208 & 225 & 202 & 218 & 88 \\ 171 & 199 & 228 & 225 & 199 & 201 & 212 & 234 & 88 \\ 32 & 228 & 229 & 234 & 32 & 32 & 225 & 209 & 88 \\ 195 & 229 & 213 & 209 & 199 & 229 & 234 & 32 & 88 \end{pmatrix}.$$

**Step E3:** We choose the privat key $K$ (the key of encryption),

$$K = \begin{pmatrix} 17 & 24 & 2 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 20 & 17 & 21 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 8 & 2 & 10 & 21 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 20 & 18 & 21 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 4 & 17 & 24 & 2 & 18 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 3 & 0 & 1 & 20 & 17 & 21 & 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 2 & 1 & 2 & 8 & 2 & 10 & 21 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 2 & 1 & 20 & 18 & 21 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 3 & 0 & 4 & 3 & 3 & 3 & 17 & 24 & 2 & 18 & 0 & 0 & 0 & 0 \\ 4 & 4 & 2 & 1 & 2 & 2 & 2 & 1 & 20 & 17 & 21 & 7 & 0 & 0 & 0 & 0 \\ 3 & 1 & 3 & 1 & 1 & 1 & 1 & 0 & 8 & 2 & 10 & 21 & 0 & 0 & 0 & 0 \\ 2 & 4 & 2 & 4 & 0 & 4 & 0 & 3 & 20 & 18 & 21 & 6 & 0 & 0 & 0 & 0 \\ 2 & 3 & 2 & 3 & 4 & 1 & 3 & 1 & 1 & 2 & 3 & 4 & 17 & 24 & 2 & 18 \\ 3 & 4 & 3 & 4 & 2 & 1 & 2 & 1 & 5 & 3 & 0 & 1 & 20 & 17 & 21 & 7 \\ 1 & 4 & 1 & 4 & 1 & 1 & 1 & 1 & 3 & 2 & 1 & 2 & 8 & 2 & 10 & 21 \\ 0 & 1 & 2 & 3 & 1 & 3 & 2 & 1 & 4 & 3 & 2 & 1 & 20 & 18 & 21 & 6 \end{pmatrix}$$

**Step E4:** $KP\ (mod\ 255) = C$,

$$KP(mod\ 255) = C = \begin{pmatrix} 101 & 249 & 48 & 117 & 170 & 160 & 204 & 153 & 199 \\ 56 & 44 & 232 & 65 & 31 & 208 & 147 & 44 & 54 \\ 225 & 197 & 195 & 137 & 67 & 229 & 29 & 99 & 165 \\ 114 & 72 & 16 & 129 & 65 & 210 & 144 & 103 & 80 \\ 137 & 98 & 36 & 117 & 232 & 118 & 79 & 235 & 209 \\ 128 & 181 & 118 & 140 & 93 & 166 & 40 & 68 & 37 \\ 35 & 123 & 18 & 85 & 164 & 226 & 51 & 220 & 190 \\ 99 & 160 & 76 & 151 & 131 & 116 & 127 & 36 & 213 \\ 10 & 207 & 117 & 208 & 229 & 208 & 168 & 135 & 28 \\ 48 & 1 & 31 & 1 & 46 & 103 & 112 & 186 & 104 \\ 175 & 118 & 87 & 173 & 226 & 205 & 153 & 27 & 57 \\ 226 & 171 & 87 & 73 & 74 & 101 & 146 & 40 & 31 \\ 53 & 153 & 161 & 19 & 113 & 213 & 108 & 59 & 138 \\ 109 & 241 & 10 & 39 & 103 & 47 & 201 & 141 & 89 \\ 61 & 41 & 176 & 229 & 230 & 115 & 114 & 187 & 171 \\ 173 & 229 & 140 & 139 & 96 & 80 & 120 & 249 & 102 \end{pmatrix}$$

**Step E5**: We convert the entries (numbers) of $C$ into characters to get the matrix $Y$:

$Y =$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| *E* | لآ | 0 | U | ت | | جـ | لأ | ا |
| 8 | ، | و | *A* | | ذ | ± | ، | 6 |
| فـ | عـ | أ | ┬ | C | مـ | | C | أـ |
| R | *H* | | · | A | ز | *B* | G | P |
| ┬ | *B* | $ | U | و | V | *O* | ض | ر |
| ° | ه | V | ┐ | ] | | ( | *D* | % |
| # | { | | *U* | ¤ | قـ | 3 | ┐ | ص |
| C | | L | « | √ | T | | $ | صـ |
| | د | *U* | ذ | مـ | U | L | ┼ | |
| 0 | V | W | | · | G | *P* | ف | *H* |
| خ | ث | *W* | ج | قـ | حـ | لأ | | 9 |
| قـ | لأ | | *I* | *J* | *E* | Φ | ( | |
| 5 | | | | *Q* | صـ | L | ; | ├ |
| *M* | ◌ّ | | \′ | G | / | ة | ┌ | *Y* |
| = | ) | · | مـ | نـ | *S* | *R* | ؛ | ث |
| ج | مـ | ┐ | ⊥ | V | *P* | X | لآ | *F* |

**Step E6**: We arrange the characters of the matrix $Y$ in the form of text to get the cipher text

" E8فـR┬... $F$ ".

Note that, we can not order all characters of $Y$ to get the cipher text in step E5 because we work by hand.

**Decryption:**

**Step D1:** The receiver orders the characters of message in a matrix.

**Step D2:** The receiver replaces the characters of the matrix that get in step D1 into numbers using the table in [13] and put them in the matrix $C$ (the same $C$ in step E4 of encryption).

**Step D3:** The receiver calculates $K^{-1}(mod\ 255)$.

$$K^{-1} = \begin{pmatrix}
0 & 2 & 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -9 & 1 & 8 & 0 & 2 & 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 5 & 0 & -5 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 3 & 0 & -3 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 38 & -3 & -38 & 0 & -12 & 1 & 11 & 0 & 2 & 0 & -2 & 0 & 0 & 0 & 0 \\
-1 & -22 & 2 & 22 & 0 & 7 & -1 & -7 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\
-1 & -17 & 1 & 17 & 0 & 5 & 0 & -5 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & -4 & 0 & 4 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-5 & -114 & 9 & 114 & 0 & 38 & -3 & -35 & 0 & -9 & 1 & 8 & 0 & 2 & 0 & -2 \\
3 & 70 & -6 & -70 & 0 & -23 & 2 & 22 & 0 & 5 & 0 & -5 & 0 & -1 & 0 & 1 \\
2 & 42 & -3 & -42 & 0 & -14 & 1 & 13 & 0 & 3 & 0 & -3 & 0 & -1 & 0 & 1 \\
1 & 15 & -1 & -15 & 0 & -5 & 0 & 5 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0
\end{pmatrix}$$

**Step D4:** The receiver calculates $K^{-1}C\ (\,mod\ 255)$ to get the matrix $P$ (the same $P$ that in step E2).

**Step D5:** The receiver converts the entries of $P$ into characters to get the matrix $X$ (the same $X$ that in step E1).

**Step D6:** The receiver arranges the characters of the matrix $X$ in the form of text to get the original message, as follows:

**" يوضح هذا البحث أهمية استخدام المعكوس الضربي للمصفوفات في التشفير, حيث قدمنا هذا المعكوس كمصفوفة مفتاحية في التشفير المتماثل و غير المتماثل ".**

## Conclusion

The observed results from our work clearly mention that using cryptography plays a vital and critical role in achieving the primary aims of security, such as authentication, integrity, and confidentiality. Also Mathematics plays important role in the different algorithms of encryption and decryption, where in this paper, we applied Hill Cipher algorithm, which depends on the multiplicative inverse of the matrix. We used the multiplicative inverse of the matrix as involutory key and as a private key, in these two cases we worked on $\mathbb{Z}_{26}$. Also we used ASCII code in our work, in this case we worked on $\mathbb{Z}_{255}$. We also presented various examples of the use of the multiplicative inverse of the matrix in encryption and decryption messages.

**References**

**[1]** A. M. Kanan, Z. Abu Zayd, Using The Moore-Penrose Generalized Inverse In Cryptography, International Scientific Journal, 148 (2020) pp. 1-14.

**[2]** CH. Jayanthi, V. Srinivas, Mathematical Modelling for Cryptography using Laplace Transform, International Journal of Mathematics Trends and Technology, February (2019), pp. 10-15.

**[3]** D. H. Griffel, Linear Algebra and Its Applications, Volume 1, a first course, New York: Linear Algebra and Its Applications, 1989.

**[4]** G. P. Lakshmi, Fingerprint Identification System combined with "Cryptography" for Authentication, International Journal of Engineering Science and Technology, 2 (2010) pp. 3054-3077.

**[5]** J. Levine, J. V. Brawley, Jr., Involutory Commutants With Some Applications to Algebraic Cryptography. I, Journal für die reine und angewandte Mathematik, 224 (1966) pp. 20-43.

**[6]** J. Levine, Hartwig, Applications of The Drazin Inverse to The Hill Cryptographic System. Part I., Cryptologia 4, (1980) pp. 71-85.

**[7]** J. Levine, Hartwig, Applications of The Drazin Inverse to The Hill Cryptographic System. Part II., Cryptologia 4, (1980) pp. 150-168.

**[8]** J. Levine, Varible Matrix Substitytion in Algebraic Cryptography, American Mathematics Monthly, 65 (1958) pp. 170-179.

**[9]** L. S. Hill, Cryptography in an algebraic alphabet, American Mathematics Monthly, 36 (1929) pp. 306-312.

**[10]** Maxrizal, B. D. Prayanti, A New Method Of Hill Cipher: The Rectangular Matrix As The Private Key, $2^{nd}$ International Conference on Science and Technology for Sustainability, 2 (2016) pp. 81-83.

**[11]** P. Christof, P. Jan, Understanding Cryptography, Springer-Verlag Berlin Heidelberg, 2010.

**[12]** S. Lipschutz, M. L. lipson, SCHAUM'S outlines: Linear Algebra, $4^{th}$ Edition, New York: The McGraw-Hill Companies, 2009.

**[13]** http://www.ascii.ca/cp864.htm.