A modified version of Hill Cipher for Arabic letters using MATLAB

Fatma F. Omar*

Fatema M. Soleman

Faculty of Science, Gharyan University, Libya

*fatma.omar@gu.edu.ly

Received: 22.12.2023 Published: 07.02.2024

Abstract:

The Hill cipher is considered the first encryption technology that has some advantages in encrypting data. The aim of this research is to modify the Hill cipher to process letters of the Arabic alphabet. We have proven the success of the Hill encryption on letters of the Arabic alphabet and the research was supported by a number of different examples which were then processed using MATLAB.

Keywords: Hill cipher, Encryption, Decryption, Extended euclidean algorithm, Multiplicative inverse, Greatest common divisor.

نسخة معدلة من تشفير هيل لأحرف اللغة العربية باستخدام الماتلاب

د. فاطمة فرج سعيد عمر

فاطمة المبروك سليمان

كلية العلوم - جامعة غريان - ليبيا

الملخص:

يعتبر تشفير هيل أول تقنية تشفير لها بعض المزايا في تشفير البيانات. يهدف هذا البحث إلى تعديل شفرة هيل لمعالجة حروف الأبجدية العربية. لقد أثبتنا نجاح تشفير هيل على حروف الأبجدية العربية وتم دعم البحث بعدد من الأمثلة المختلفة والتي تمت معالجتها بعد ذلك باستخدام برنامج MATLAB.

الكلمات المفتاحية: تشفير هيل، التشفير، فك التشفير، خوارزمية إقليدية موسعة، المعكوس الضربي، القاسم المشترك الأكبر.

1. Introduction:

The Hill cipher was invented by (Hill, 1929, 1931). It is a block cipher that has several advantages such as disguising the letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for encryption and decryption, and its high speed and high throughput. but the Hill cipher is proved to be vulnerable to cryptanalysis attacks. Because of its linear nature, it suffers from the known-plaintext attack, i.e. attacker can obtain one or more plaintexts and their corresponding ciphertexts, (Stinson & Paterson, 2018). So several researches have been done to improve the security of the Hill cipher. See (Adinarayana et al., 2012; Chen et al., 2014; Ismail et al., 2006; Jayanthi & Srinivas, 2019; Kiele, 1990; Parmar & Bhatt, 2015; Sastry et al., 2010).

To obtain one or more ciphertexts, approaches based on smart combinations between linear algebra, arithmetical and statistical arguments have been developed under the strong assumption that "the text consists of meaningful English words" with an alphabet having 26 letters (Kanan & Abu Zayd, 2020 ; Lin & Lee, 2004; Rohim et al., 2021; Saeednia, 2000; Toorani & Falahati, 2011; Yeh et al., 1991). Roughly speaking, these methods consist mainly of recovering the key matrix row by row or column by column by exploiting statistical tools together with data on frequencies of occurrence of n-grams in the English language.

In this paper, we will apply Hill's code to the letters of the Arabic language, as we relied on the MATLAB program to create a table containing the letters of the Arabic language completely. Fortunately, we were able to obtain a modulus that is a relatively prime to all the numbers that follow it, and this opened more scope for us in choosing encryption keys.

This article is organized as follows. In the next section we give some basic definitions. In Section 3 we give a brief description Arabic alphabet. In Section 4 we demonstrate the performance of the Hill cipher on several test examples. Then we end with a conclusion.

2. Basic definitions:

Let us consider the following some basic definitions that will be used throughout the work. See, (Shoup, 2008).

Definition 2.1 We are given an integer $m > 1$, called the modulus. Then we say that two integers a and b congruent to one another modulo m (congruent ($\boldsymbol{mod}\ m$) for short), and we write $a \equiv b\ (\boldsymbol{mod}\ m)$, to mean that the difference $a - b$ is an integral multiple of m. In other words, $a \equiv b\ (\boldsymbol{mod}\ m)$ when $a = b + k \cdot m$ for some integer k (positive, negative, or zero).

Definition 2.2 For any positive integer $p > 1$ is said to be prime if there not exist positive integers a, b such that $p = ab$, where $1 < a, b < p$.

Definition 2.3 The *greatest common divisor* (gcd) of the integers a and b is the largest integer d which divides both integers, denoted $d = gcd(a, b)$. We stated that two integers a and b are relatively prime if and only if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if $gcd(a, b) = 1$.

Definition 2.4 (The multiplicative inverse). (Parthasarathy, 2012) Let a, m are given such that $a * b \equiv 1 * \boldsymbol{mod}(m)$, then b is said to be the *modular multiplicative inverse of* a.

Definition 2.5 (Extended Euclid's Algorithm). If a and b are positive integers, then there are always integers x and y so that the gcd of a and b equals $ma + nb$, i.e,

$$ma + nb = gcd(a, b) \qquad (1)$$

Definition 2.6 (The Hill cipher). Given a plaintext message $P = (P_1, P_2, \cdots)$ where P_i is a letter in some alphabet and invertible $m \times m$ matrix K, Hill cipher represents

P_i by numeric value $X_i \in Z_m (Z_m = \{0,1, \cdots, m-1\})$ and encrypts plaintext as

$Y = K \cdot X(\boldsymbol{mod}\, m)$, where X and Y are plaintext and ciphertext column vectors.

Similarly, Y is decrypted as $X = K^{-1} \cdot Y(\boldsymbol{mod}\, m)$, where $K^{-1}$is the inverse of K.

That is, $K \cdot K^{-1}(\boldsymbol{mod}\, m) = K^{-1} \cdot K(\boldsymbol{mod}\, m) = I$ holds, where is the identity matrix and $det(K)$ must be relatively prime to the modulus m, to satisfy this we require $gcd(\det(K)\ (\boldsymbol{mod}\, m),\ m) = 1$.

3. Proposition 3.1 (Our Arabic alphabet):

In this paper we applied Hill cipher to Arabic letters, as our alphabet consists of 37 letters where added the blank space □ to separate words, and tacked the number 26 in that order. (In your work on the computer, use the blank space itself, however, and not this special character!) When enciphering or deciphering, we shall represent the 37 characters in our Arabic alphabet in order by the nonnegative integers $0,1,\ldots,37$, as shown in Table (1), we shall denote the length of the alphabet by m. Note that, when working with Hill ciphers on the computer, you should make your functions as general as possible to handle various alphabets, you should be using an arbitrary integer $m > 1$ (and sometimes an arbitrary prime integer m) as the alphabet length. There is nothing magical about numbering the letters in our alphabet in ascending order (starting with 0). In practice, one would undoubtedly scramble the numbers in some

arbitrary order (known to both the sender and the receiver of an enciphered message) so as to make cracking the cipher a little more difficult. For simplicity's sake, we shall stick with the numbering scheme shown.

Table (1): Numerical representation of 37- letters of the Arabic alphabet

ء	آ	أ	ؤ	إ	ئـ	ا	ب	ـة	ت	ث	ج	ح	خ
0	1	2	3	4	5	6	7	8	9	10	11	12	13
د	ذ	ر	ز	س	ش	ص	ض	ط	ظ	ع	غ	□	ف
14	15	16	17	18	19	20	21	22	23	24	25	26	27
ق	ك	ل	م	ن	هـ	و	ى	ي					
28	29	30	31	32	33	34	35	36					

The number system Z_{37} is a field because 37 is prime. For convenience, we list in Table (2) the reciprocals (multiplicative inverses) of the nonzero elements of Z_{37}, where used the extended Euclidean algorithm $gcd(a,b) = a * x + b * y$ is particularly useful when a and b are coprime, since x is the multiplicative inverse of a modulo b, and y is the multiplicative inverse of b modulo a.

Table (2): Multiplicative inverses modulo 37

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	19	25	28	15	31	16	14	33	26	27	34	20	8	5
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
7	24	35	2	13	30	32	29	17	3	10	11	4	23	21
31	32	33	43	35	36									
6	22	9	12	18	36									

4. Illustrative Examples:

In this section, various test examples are provided to illustrate the performance of the Hill cipher on letters of the Arabic alphabet. where was made codes of Hill cipher implemented using MATLAB, see (Mihailescu & Nita, 2021).

Example 4.1 Encrypt the plaintext (السلام عليكم) using hill cipher for the given key (أبجد).

The key is the matrix of (أبجد)

$$K = \begin{bmatrix} ا & ب \\ ج & د \end{bmatrix} \Longrightarrow \begin{bmatrix} 2 & 7 \\ 11 & 14 \end{bmatrix},$$

since the key is a 2×2 matrix, plaintext should be converted into matrix of length 2.

$$P = \begin{bmatrix} ا & س & ا & □ & ل & ك \\ ل & ل & م & ع & ي & م \end{bmatrix} \Longrightarrow X = \begin{bmatrix} 6 & 18 & 6 & 26 & 30 & 29 \\ 30 & 30 & 31 & 24 & 36 & 31 \end{bmatrix}$$

$$Y = KX \ (\boldsymbol{mod}\ 37)$$

$$Y = \begin{bmatrix} 2 & 7 \\ 11 & 14 \end{bmatrix} \begin{bmatrix} 6 & 18 & 6 & 26 & 30 & 29 \\ 30 & 30 & 31 & 24 & 36 & 31 \end{bmatrix} \ (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 0 & 24 & 7 & 35 & 16 & 16 \\ 5 & 26 & 19 & 30 & 20 & 13 \end{bmatrix}$$

$$\Longrightarrow C = \begin{bmatrix} ء & ع & ب & ي & ر & ر \\ ئ & □ & ش & ل & ص & خ \end{bmatrix}.$$

Ciphertext: (ءئع□بشيلرصرخ).

For decrypt the ciphertext using Inverse of Key matrix

$$K^{-1} = \frac{1}{|K|} adj(K)$$

$$|K| = \begin{vmatrix} 2 & 7 \\ 11 & 14 \end{vmatrix} = -49 \ (\boldsymbol{mod}\ 37) = 25$$

From the Table (2) we find the multiplicative inverses of 25 is 3,

$$K^{-1} = 3\begin{bmatrix} 14 & -7 \\ -11 & 2 \end{bmatrix}(\boldsymbol{mod}\ 37) = \begin{bmatrix} 5 & 16 \\ 4 & 6 \end{bmatrix},$$

$$X = K^{-1}Y(\boldsymbol{mod}\ 37)$$

$$X = \begin{bmatrix} 5 & 16 \\ 4 & 6 \end{bmatrix}\begin{bmatrix} 0 & 24 & 7 & 35 & 16 & 16 \\ 5 & 26 & 19 & 30 & 20 & 13 \end{bmatrix}(\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 6 & 18 & 6 & 26 & 30 & 29 \\ 30 & 30 & 31 & 24 & 36 & 31 \end{bmatrix}$$

$$\Longrightarrow P = \begin{bmatrix} ا & س & ا & □ & ل & ك \\ ل & ل & م & ع & ي & م \end{bmatrix}$$

Plaintext: (السلام عليكم)

Example 4.2 Encrypt the plaintext (أحب بلادي) using hill cipher for the given key (حروف).

The key is the matrix of (حروف)

$$K = \begin{bmatrix} ح & ر \\ و & ف \end{bmatrix} \Longrightarrow \begin{bmatrix} 12 & 16 \\ 34 & 27 \end{bmatrix},$$

since the key is a 2×2 matrix, plaintext should be converted into matrix of length 2.

$$P = \begin{bmatrix} أ & ب & ب & ا & ي \\ ح & □ & ل & د & □ \end{bmatrix} \Longrightarrow X = \begin{bmatrix} 2 & 7 & 7 & 6 & 36 \\ 12 & 26 & 30 & 14 & 26 \end{bmatrix}$$

$$Y = KX\ (\boldsymbol{mod}\ 37)$$

$$Y = \begin{bmatrix} 12 & 16 \\ 34 & 27 \end{bmatrix}\begin{bmatrix} 2 & 7 & 7 & 6 & 36 \\ 12 & 26 & 30 & 14 & 26 \end{bmatrix}\ (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 31 & 19 & 9 & 0 & 34 \\ 22 & 15 & 12 & 27 & 2 \end{bmatrix}$$

$$\Longrightarrow C = \begin{bmatrix} م & ش & ت & ء & و \\ ط & ذ & ح & ف & أ \end{bmatrix}$$

Ciphertext: (مطشذنتحءفوأ).

For decrypt the ciphertext using Inverse of Key matrix

$$K^{-1} = \frac{1}{|K|} adj(K),$$

$$|K| = \begin{vmatrix} 12 & 16 \\ 34 & 27 \end{vmatrix} = -220 \ (\boldsymbol{mod}\ 37) = 2.$$

From the Table (2) we find the multiplicative inverses of 2 is 19,

$$K^{-1} = 2\begin{bmatrix} 27 & -16 \\ -34 & 12 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 32 & 29 \\ 20 & 6 \end{bmatrix}$$

$$X = K^{-1}Y \ (\boldsymbol{mod}\ 37)$$

$$X = \begin{bmatrix} 32 & 29 \\ 20 & 6 \end{bmatrix}\begin{bmatrix} 31 & 19 & 9 & 0 & 34 \\ 22 & 15 & 12 & 27 & 2 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 2 & 7 & 7 & 6 & 36 \\ 12 & 26 & 30 & 14 & 26 \end{bmatrix}$$

$$\Longrightarrow P = \begin{bmatrix} أ & ب & ب & ا & ي \\ ح & □ & ل & د & □ \end{bmatrix}$$

Plaintext: (أحب بلادي).

Example 4.3 Encrypt the plaintext (العلم نور) using hill cipher for the given key (حروف هجاء).

The key is the matrix of (حروف هجاء)

$$K = \begin{bmatrix} ح & ر & و \\ ف & □ & ه \\ ج & ا & ء \end{bmatrix} \Longrightarrow \begin{bmatrix} 12 & 16 & 34 \\ 27 & 26 & 33 \\ 11 & 6 & 0 \end{bmatrix},$$

since the key is a 3×3 matrix, plaintext should be converted into matrix of length 3

$$P = \begin{bmatrix} ا & ل & ن \\ ل & م & و \\ ع & □ & ر \end{bmatrix} \Longrightarrow \mathrm{X} = \begin{bmatrix} 6 & 30 & 32 \\ 30 & 31 & 34 \\ 24 & 26 & 16 \end{bmatrix}$$

$$Y = KX \ (\boldsymbol{mod}\ 37)$$

$$Y = \begin{bmatrix} 12 & 16 & 34 \\ 27 & 26 & 33 \\ 11 & 6 & 0 \end{bmatrix} \begin{bmatrix} 6 & 30 & 32 \\ 30 & 31 & 34 \\ 24 & 26 & 16 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 36 & 1 & 29 \\ 32 & 32 & 19 \\ 24 & 35 & 1 \end{bmatrix}$$

$$\Longrightarrow C = \begin{bmatrix} ي & آ & ك \\ ن & ن & ش \\ ع & ى & آ \end{bmatrix}$$

Ciphertext: (ينعآننكشآ)

For decrypt the ciphertext using Inverse of Key matrix

$$K^{-1} = \frac{1}{|K|} adj(K)$$

$$|K| = -784 \ (\boldsymbol{mod}\ 37) = 30$$

From the Table (2) we find the multiplicative inverses of 30 is 21

$$adj(K) = \begin{bmatrix} -198 & 363 & -124 \\ 204 & -374 & 104 \\ -356 & 522 & -120 \end{bmatrix}^t$$

$$K^{-1} = 21 \begin{bmatrix} -198 & 204 & -356 \\ 363 & -374 & 522 \\ -124 & 104 & -120 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 23 & 29 & 35 \\ 1 & 27 & 10 \\ 23 & 1 & 33 \end{bmatrix}$$

$$X = K^{-1}Y \ (\boldsymbol{mod}\ 37)$$

$$X = \begin{bmatrix} 23 & 29 & 35 \\ 1 & 27 & 10 \\ 23 & 1 & 33 \end{bmatrix} \begin{bmatrix} 36 & 1 & 29 \\ 32 & 32 & 19 \\ 24 & 35 & 1 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 6 & 30 & 32 \\ 30 & 31 & 34 \\ 24 & 26 & 16 \end{bmatrix}$$

$$\Longrightarrow P = \begin{bmatrix} ا & ل & ن \\ ل & م & و \\ ع & □ & ر \end{bmatrix}$$

Plaintext 'العلم نور'.

Example 4.4 Encrypt the plaintext (ديننا الإسلام) using hill cipher for the given key (لغة عربية).

The key is the matrix of (لغة عربية)

$$K = \begin{bmatrix} ل & غ & ة \\ □ & ع & ر \\ ب & ي & ة \end{bmatrix} \Longrightarrow \begin{bmatrix} 30 & 25 & 8 \\ 26 & 24 & 16 \\ 7 & 36 & 8 \end{bmatrix},$$

since the key is a 3×3 matrix, plaintext should be converted into matrix of length 3

$$P = \begin{bmatrix} د & ن & ا & س & م \\ ي & ا & ل & ل & □ \\ ن & □ & إ & ا & □ \end{bmatrix} \Longrightarrow X = \begin{bmatrix} 14 & 32 & 6 & 18 & 31 \\ 36 & 6 & 30 & 30 & 26 \\ 32 & 26 & 4 & 6 & 26 \end{bmatrix}$$

$$Y = KX\ (\boldsymbol{mod}\ 37)$$

$$Y = \begin{bmatrix} 30 & 25 & 8 \\ 26 & 24 & 16 \\ 7 & 36 & 8 \end{bmatrix} \begin{bmatrix} 14 & 32 & 6 & 18 & 31 \\ 36 & 6 & 30 & 30 & 26 \\ 32 & 26 & 4 & 6 & 26 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 22 & 23 & 0 & 6 & 12 \\ 1 & 23 & 15 & 26 & 33 \\ 22 & 19 & 7 & 33 & 29 \end{bmatrix}$$

$$\Longrightarrow C = \begin{bmatrix} ط & ظ & ء & ا & ح \\ آ & ظ & ذ & □ & ه \\ ط & ش & ب & ه & ك \end{bmatrix}$$

Ciphertext: 'طآطظظشءذبا□هحهك'.

For decrypt the ciphertext using Inverse of Key matrix

$$K^{-1} = \frac{1}{|K|} adj(K)$$

$$|K| = -7776 \ (\boldsymbol{mod}\ 37) = 31$$

From the Table (2) we find the multiplicative inverses of 31 is 6

$$adj(K) = \begin{bmatrix} -384 & -96 & 768 \\ 88 & 184 & -905 \\ 208 & -272 & 70 \end{bmatrix}^t$$

$$K^{-1} = 6 \begin{bmatrix} -384 & 88 & 208 \\ -96 & 184 & -272 \\ 768 & -905 & 70 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$= \begin{bmatrix} 27 & 10 & 27 \\ 16 & 31 & 33 \\ 20 & 9 & 13 \end{bmatrix}$$

$$X = K^{-1} Y (\boldsymbol{mod}\ 37)$$

$$X = \begin{bmatrix} 27 & 10 & 27 \\ 16 & 31 & 33 \\ 20 & 9 & 13 \end{bmatrix} \begin{bmatrix} 22 & 23 & 0 & 6 & 12 \\ 1 & 23 & 15 & 26 & 33 \\ 22 & 19 & 7 & 33 & 29 \end{bmatrix} (\boldsymbol{mod}\ 37)$$

$$\begin{bmatrix} 14 & 32 & 6 & 18 & 31 \\ 36 & 6 & 30 & 30 & 26 \\ 32 & 26 & 4 & 6 & 26 \end{bmatrix}$$

$$\Longrightarrow P = \begin{bmatrix} د & ن & ا & س & م \\ ي & ا & ل & ل & □ \\ ن & □ & إ & ا & □ \end{bmatrix}$$

Plaintext 'ديننا الإسلام'.

These programs are designed to perform encryption and decryption of letters using the Hill cipher method. The user can utilize the programs by clicking on the "run" button and then providing the plaintext to be encrypted, entering a key size. Similarly, decryption can be performed by providing the ciphertext to be decrypted.

Encryption and decryption Hill when size key matrix is 2 × 2

```
% Hill cipher code in matlab
% encryption Hill 2*2
clear all;clc;
Plaintext=input('Enter text::','s');
Keymatrix=input('Enter Key::','s');
Pl=double(Plaintext);
Ke=double(Keymatrix);
L=length(Pl);
n=mod(L,2);
if n~=0
    Ci=[Pl,1595];
else
    Ci=Pl;
end
L2=length(Ci);
for i=1:L2
if (Ci(i)>1595)
    Ci(i)=Ci(i)-5;
end
if (Ci(i)==32)
    ii=i;
    Ci(ii)=1595;
end
C=Ci;
end
for i=1:4
    if Ke(i)>1595
    Ke(i)=Ke(i)-5;
    end
    if (Ke(i)==32)
    ii=i;
    Ke(ii)=1595;
    end
```

```
      H=Ke;
  end
  C=reshape(C,2,L2/2)-1569;
  H=reshape(H,2,2)-1569;
  masg=mod((H'*C),37);
  masg1=reshape(masg,1,L2)+1569;
  for i=1:L2
  if (masg1(i)>1595)
      masg1(i)=masg1(i)+5;
  end
  if (masg1(i)==32)
      ii=i;
      masg1(ii)=1595;
  end
  D=masg1;
  end
  cich=char(D)
  %% Hill cipher code in matlab
  % Dncryption Hill 2*2
  d=round(det(H'));
  di=round(mod(d,37));
  ki=inv(H);
  adj=round(mod((d*ki),37));
  a=[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36];
  b=[1 19 25 28 15 31 16 14 33 26 27 34 20 8 5 7 24
35 2 13 30 32 29 17 3 10 11 4 23 21 6 22 9 12 18 36];
  s=a(1,1);
  for j=1:36
      if a(j)==di
      r(s)=b(j);
      end
  end
  mod_inv=mod((adj*r),37)';
  ciphertext=input('Enter text::','s');
  Ci=double(ciphertext);
  l=length(Ci);
  n=mod(l,2);
  if n~=0
      Ci=[Ci,1595];
```

```
else
    C=Ci;
end
l2=length(C);
for i=1:l2
    if (C(i)>1595)
    C(i)=C(i)-5;
    end
    if C(i)==32
    ii=i;
    C(ii)=1595;
    end
    P=C;
end
Pl=reshape(P,2,l2/2)-1569;
masg=mod((mod_inv*Pl),37);
masg1=round(reshape(masg,1,l2))+1569;
for i=1:l2
    if (masg1(i)>1595)
    masg1(i)=masg1(i)+5;
    end
    if masg1(i)==1595
    ii=i;
    masg1(ii)=32;
    end
    PL=masg1;
end
plain=char(PL)
```

Outputs

Example 4.1

```
Enter text::السلام عليكم
Enter Key::أبجد

cich =

ءئعبشىلرصرخ

Enter text::ءئعبشىلرصرخ
```

```
plain =
السلام عليكم
```

Example 4.2

```
Enter text::أحب بلادي
Enter Key::حروف

cich =

مطشنتحءفوأ

Enter text::مطشنتحءفوأ

plain =

أحب بلادي

>>
```

Encryption and decryption Hill when size key matrix is 3 × 3

```
% 2023/09/10
% Hill cipher code in matlab
% encryption Hill 3*3
clear all;clc;
Plaintext=input('Enter text::','s');
Keymatrix=input('Enter Key::','s');
Pl=double(Plaintext);
Ke=double(Keymatrix);
L=length(Pl);
n=mod(L,3);
if n~=0 && n==1
    Ci=[Pl,1595,1595];
elseif n~=0 && n==2
     Ci=[Pl,1595];
else
    Ci=Pl;
end
L2=length(Ci);
```

```
for i=1:L2
    if (Ci(i)>1595)
    Ci(i)=Ci(i)-5;
    end
    if (Ci(i)==32)
    ii=i;
    Ci(ii)=1595;
    end
    C=Ci;
end
for i=1:9
    if Ke(i)>1595
    Ke(i)=Ke(i)-5;
    end
    if (Ke(i)==32)
    ii=i;
    Ke(ii)=1595;
    end
    H=Ke;
end
C=reshape(C,3,L2/3)-1569;
H=reshape(H,3,3)-1569;
masg=mod((H'*C),37);
masg1=reshape(masg,1,L2)+1569;
for i=1:L2
if (masg1(i)>1595)
    masg1(i)=masg1(i)+5;
end
if (masg1(i)==32)
    ii=i;
    masg1(ii)=1595;
end
D=masg1;
end
cich=char(D)
%% Hill cipher code in matlab
% Dncryption Hill 3*3
d=round(det(H'));
di=round(mod(d,37));
ki=inv(H);
```

```
  adj=round(mod((d*ki),37));
  a=[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36];
  b=[1 19 25 28 15 31 16 14 33 26 27 34 20 8 5 7 24
35 2 13 30 32 29 17 3 10 11 4 23 21 6 22 9 12 18 36];
  s=a(1,1);
  for j=1:36
      if a(j)==di
      r(s)=b(j);
      end
  end
  mod_inv=mod((adj*r),37)';
  ciphertext=input('Enter text::','s');
  Ci=double(ciphertext);
  l=length(Ci);
  n=mod(l,3);
  if n~=0 && n==2
      Ci=[Ci,1595,1595];
  elseif n~=0 && n==1
      Ci=[Ci,1595];
  else
      C=Ci;
  end
  l2=length(C);
  for i=1:l2
      if (C(i)>1595)
      C(i)=C(i)-5;
      end
      if C(i)==32
      ii=i;
      C(ii)=1595;
      end
      P=C;
  end
  Pl=reshape(P,3,l2/3)-1569;
  masg=mod((mod_inv*Pl),37);
  masg1=round(reshape(masg,1,l2))+1569;
  for i=1:l2
      if (masg1(i)>1595)
      masg1(i)=masg1(i)+5;
```

```
    end
    if masg1(i)==1595
    ii=i;
    masg1(ii)=32;
    end
    PL=masg1;
end
plain=char(PL)
```

Outputs

Example 4.3

```
Enter text::العلم نور
Enter Key::حروف هجاء

cich =

ينعآنىكشآ

Enter text::ينعآنىكشآ

plain =

العلم نور
>>
```

Example 4.4

```
Enter text::ديننا الإسلام
Enter Key::لغة عربية

cich =

طآطظظشء ذبا□هجهك

Enter text::طآطظظشء ذبا□هجهك

plain =

ديننا الإسلام

>>
```

Example 4.5 Use MATLAB to Encrypt and decrypt the plaintext (كل الشكر و التقدير لمجلة الساتل العلمية على نشر ورقتنا) using hill cipher for the given key (عزيز أنت يا وطني).

The key is matrix of (عزيز أنت يا وطني)

$$K = \begin{bmatrix} ع & ز & ي & ز \\ □ & أ & ن & ت \\ □ & ي & ا & □ \\ و & ط & ن & ي \end{bmatrix} \Rightarrow \begin{bmatrix} 24 & 17 & 36 & 17 \\ 26 & 2 & 32 & 9 \\ 26 & 36 & 6 & 26 \\ 34 & 22 & 32 & 36 \end{bmatrix},$$

since the key is a 4×4 matrix, plaintext should be converted into matrix of length 4

$$P = \begin{bmatrix} ك & ل & □ & ل & ي & م & □ & ا & ا & م & ع & ن & و & ن \\ ل & ش & و & ت & ر & ج & ا & ت & ل & ي & ل & ش & ر & ا \\ □ & ك & □ & ق & □ & ل & ل & ل & ع & ة & ى & ر & ق & □ \\ ا & ر & ا & د & ل & ة & س & □ & ل & □ & □ & □ & ت & □ \end{bmatrix}$$

$$\Rightarrow X = \begin{bmatrix} 29 & 30 & 26 & 30 & 36 & 31 & 26 & 6 & 6 & 31 & 24 & 32 & 34 & 32 \\ 30 & 19 & 34 & 9 & 16 & 11 & 30 & 9 & 30 & 36 & 30 & 19 & 16 & 6 \\ 26 & 29 & 26 & 28 & 26 & 30 & 18 & 30 & 24 & 8 & 35 & 16 & 28 & 26 \\ 6 & 16 & 6 & 14 & 30 & 8 & 6 & 26 & 30 & 26 & 26 & 26 & 9 & 26 \end{bmatrix}$$

```
Enter text:: كل الشكر و التقدير لمجلة الساتل العلمية
على نشر ورقتنا
Enter Key::عزيز أنت يا وطني

cich =

عىءلقؤششصأكرثبةقكىاثآثيقؤوظوايإ إلهدجديد إخؤء زء غممكاح
فقظلق

Enter
text::
عىءلقؤششصأكرثبةقكىاثآثيقؤوظوايإ إلهدجديد إخؤء زء غممكاحفق
ظلق
```

```
plain =

كل الشكر والتقدير لمجلة الساتل العلمية على نشر
ورقتنا

>>
```

5. Conclusion

In this work we discussed Encryption and decryption for the alphabet Arabic by Hill cipher where we supported our new ideas through examples and then processed them using MATLAB. Our future work is focused on a symmetric substitution cipher that is actually a secure variant of the Hill cipher, we can also apply most of the previous studies to Arabic letters.

References

Adinarayana, R.K., Vishnuvardhan, B., Madhuviswanatham., & Krishna A.V.N. (2012). A Modified Hill Cipher Based on Circulant Matrices. *Procedia Technology*, (4), 114-118.

Chen, L., Guo, G., & Peng, Z. (2014). A Hill Cipher-Based Remote Data Possession Checking in Cloud Storage. *Security and Communication Networks*, *7*(3), 511-518.

Jayanthi, C.H Z., & Srinivas, V. (2019). Mathematical Modelling for Cryptography using Laplace Transform. *International Journal of Mathematics Trends and Technology*, *65*(2), 10-15.

Hill, L.S. (1929). Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, *36*(6), 306-312.

Hill, L.S. (1931). Concerning Certain Linear Transformation Apparatus of cryptography. *American Mathematical Monthly*, *38*, 135-154.

Ismail, I.A., Amin, M., & Diab, H. (2006). How to Repair the Hill Cipher. *Journal of Zhejiang University Science A*, *7*, 2022-2030.

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

Kiele, W.A. (1990). A Tensor-Theoretic Enhancement to the Hill Cipher System. *Cryptologia*, *14*(3), 225-233.

Lin, C.H., & Lee, C.Y. (2004). Comments on Saeednia's improved scheme for the Hill cipher. *Journal of the Chinese institute of engineers*, *27*(5), 743-746.

Mihailescu, M.I., & Nita, S.L. (2021). *Cryptography and Cryptanalysis in MATLAB Creating and Programming Advanced Algorithms*, New York, https://doi.org/10.1007/978-1-4842-7334-0

Parthasarathy. S. (2012). Multiplicative inverse in mod(m), *Algologic Technical*, 1-3.

Parmar, N.B., & Bhatt, K. (2015). Hill Cipher Modifications: A Detailed Review. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(3), 1467-1474.

Rohim, M.A, Santoso, K.A., & Hadi, A.F. (2021). Primary Key Encryption Using Hill Cipher Chain (Case Study: STIE Mandala PMB Site). *Advances in Computer Science Research*, *96*, 222-227.

Saeednia, S. (2000). How to Make the Hill Cipher Secure. *Cryptologia Journal*, *24*(4), 353-360.

Sastry, V., Shankar, N., & Bhavani, S. (2010). A Modified Hill Cipher Involving Interweaving and Iteration. *International Journal of Network Security*, *11*(1), 11-16.

Shoup, V. (2008). *A Computational Introduction to Number Theory and Algebra*, Second Edition, Cambridge University Press.

Stinson, D., & Paterson, M. (2018). *Cryptography: Theory and Practice*. 4th Edition, New York.

Toorani, M., & Falahati A. (2011). A Secure Cryptosystem Based on Affine Transformation. *Security and Communication Networks*, *4*(2), 207-215.

Yeh, Y.S, Wu, T.C, Chang, C.C., & Yang, W.C., (1991). A New Cryptosystem Using Matrix Transformation. *Proceedings of the 25th IEEE International Carnahan Conference on Security Technology*, 131-138.