الجمهورية اليمنية

جامعة العلوم والتكنولوجيا فرع إب

كليه الحاسبات وتكنولوجيا المعلومات

تخصص تقنية معلومات

بسم الله الرحمن الرحيم

عنوان البحث :

Hill Cipher

اعداد الطالبة

طلال حميد الشفق

صفاء عبد الكريم قمحان

سارة حسن رشاد

إشراف :

د / نشوان المُجمر

2014 م

الفهـــرس

١.١المقدمـــة :

منذ بداية اللغة المكتوبة ، البشر أرادو الاشتراك بالمعلومات سراً .وقد يمكن أن تكون المعلومات طلبات من الجنرال في أوقات الحروب ، رسالة بين المعجبين السريين ، أو معلومات بخصوص البعض من جرائم العالم الأكثر خسة . هذه هي الحاجة السرية وتطبيقاته العريضة الذي سبب الكتابة المشفرة وجعلت منطقة دراسة لآلآف السنين . غرض التشفير حماية الاتصالات السرية ويضمن سرية إبقاء المعلومات مخفيه من أي شخص الا للشخص المراد الارسال له والقادر على فك الشفرة . والتشفير هو عبارة عن تحويل البيانات الى بيانات غير صالحه للقراءة أو غير واضحة ،أما فك التشفير هو عكس التشفير يقوم بتحويل البيانات المشفرة الى بيانات واضحه ،وأنواع هذه الشفرات الشفرات الكلاسيكية التي تعتبر الاساس للكثير من الشفرات الحديثة ومن هذه الشفرات شفره هيل والتي هي موضوعنا .

٢.١شفـــره هيـــل :

كلما تقدم الوقت ، دراسة الكتابة المشفرة تستمر بشكل بالغ ، ومؤخراً أكثر ، بدء تضمين الرياضيات بمستوى عالي ، بهذه الرياضيات الأكثر تقدماَ جاءت شفرات متقدمة معتمده على فكرة مفاتيح الحل والتشفير . مفاتيح تشفير قيمه خاصه أو مجموعه قيم تستخدم في خوارزمية تشفير لتحويل النص الواضح Plaint text الى نص مشفر Cipher text . مفتاح التشفير هو نضير مفتاح فك التشفير تستخدم كجزء من خوارزمية حل لتحويل Cipher text الى Plaint text . شفره هيل سميت بهذا الاسم نسبه الى مخترعها Lester S Hill عام ١٩٢٩م ، عالم رياضيات امريكي أخذ الماجستير من جامعه كولمبيا ، والدكتوراه من جامعه يالي ، فلذلك كانت الشفرة متعلقة بالرياضيات وله مؤلفات بنطريه الأعداد ، وتعتبر شفره هيل أول شفره تتعامل مع ٣ حروف في نفس الوقت ، وهي تعتمد في عملها على الجبر الخطي مصفوفه n*n الى رسائل التشفير وفك التشفير ، ولكي نستطيع التشفير بها يجب أن يكون لديك أساسيات التعامل مع المصفوفات (ضرب المصفوفات بالذات)، وسنبدأ موضوعنا بشرح معكوس المصفوفة الل سنستخدمه لفك شفره الهيل .

1.3 Matrix

The matrix is a rectangular array of elements arranged in horizontal rows and vertical columns and usually enclosed in brackets. A general matrix form of A having n rows and m columns is :

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} = [a_{ij}]_{n\times m}$$

The order of a matrix A is :

Order (A) = no.of rows × no.of columns

= n × m

1.4 Transpose of a matrix (A^T)

A^T is obtained by converting the rows of A into columns in A^T . $A_{n\times m}$ then $A^T{}_{m\times n}$.

$A_{n\times m} = [a_{ij}]$ j=1,….,m and i=1,…,n

Then

$A^T{}_{m\times n} = [a_{ji}]$

Exp :

$$A=\begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix} \quad ' \quad A^T=\begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{bmatrix}$$

1.5 Matrix multiplication

For an n×p matrix $A=[a_{ij}]_{n\times p}$ and an p×m matrix $B=[b_{ij}]_{p\times m}$. Then the matrix product AB = $C=[c_{ij}]_{n\times m}$ is an n×m matrix where

$$c_{ij} = a_{i1}\, b_{1j} + a_{i2}\, b_{2j} + \dots\dots\dots + a_{ip}\, b_{pj}$$

$$c_{ij} = \sum_{k=1}^{p} a_{ik}\, b_{kj}$$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{np} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pm} \end{bmatrix} = [c_{ij}]_{n\times m}$$

We can multiply two matrices only when the number of columns in the first matrix equals the number of rows in the second matrix.

Exp :

Find AB if

$$B = \begin{bmatrix} 1 & 6 \\ 3 & -5 \\ -2 & 4 \end{bmatrix} \quad A = \begin{bmatrix} 1 & 1 & -1 \\ 2 & 0 & 3 \end{bmatrix} \quad ;$$

Sol :

$$AB = \begin{bmatrix} 3+3+2 & 3+3+2 \\ 2+0-6 & 12+0+12 \end{bmatrix}$$

$$AB = \begin{bmatrix} 8 & 9 \\ -4 & 24 \end{bmatrix}$$

1.6 Determinant

It is a number associated with a given square matrix. The determinant of A is denoted by

$|A|$ = Det (A) = D_A

1.6.1 Determinant of 2×2 matrix

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \Rightarrow |A| = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11}a_{22} - a_{12}\, a_{12}$$

Exp :

$$A = \begin{bmatrix} 2 & 5 \\ 3 & 4 \end{bmatrix}$$

$|A| = \begin{bmatrix} 2 & 5 \\ 3 & 4 \end{bmatrix}$ = (2 ×4) – (5 × 3) = 8 – 15 = -7

1.6.2 Determinant of 3×3 matrix

1.6.2.1 Minor

The Minor $|M_{ij}|$ of an element a_{ij} is the determinant of the matrix M_{ij} left when row i and column j have been deleted from the matrix A.

Exp :

Find M_{11} $|M_{11}|$, M_{13} $|M_{13}|$, M_{23} , $|M_{23}|$

$$A = \begin{bmatrix} -8 & 0 & 6 \\ 4 & -6 & 7 \\ -1 & -3 & 5 \end{bmatrix}$$

Sol :

$M_{11} = \begin{bmatrix} -6 & 7 \\ -3 & 5 \end{bmatrix}$ ‘ $|M_{11}| = \begin{vmatrix} -6 & 7 \\ -3 & 5 \end{vmatrix}$ = (-6×5) - (7×-3) = -30 + 21 = -9

$M_{23} = \begin{bmatrix} -8 & 0 \\ -1 & -3 \end{bmatrix}$ ‘ $|M_{23}| = \begin{vmatrix} -8 & 0 \\ -1 & -3 \end{vmatrix}$ = (-8 × -3) - (0 × -1) = 24

$M_{13} = \begin{bmatrix} 4 & -6 \\ -1 & -3 \end{bmatrix}$ ‘ $|M_{23}| = \begin{vmatrix} 4 & -6 \\ -1 & -3 \end{vmatrix}$ = (4 × -3) - (-6 × -1) = - 18

1.6.2.2 Cofactor

The cofactor $|C_{ij}|$ of an element a_{ij} is given by :

$|C_{ij}| = (-1)^{i+j} |M_{ij}|$

Where $|M_{ij}|$ is the minor of a_{ij}.

Exp :

Find $|C_{11}|$, $|C_{23}|$ for

$$A = \begin{bmatrix} -8 & 0 & 6 \\ 4 & -6 & 7 \\ -1 & -3 & 5 \end{bmatrix}$$

Sol :

$|C_{11}|= (-1)^{1+1} |M_{11}|$ = -9

$|C_{23}|= (-1)^{2+3} |M_{23}|$ = -1 × 24 = -24

1.6.2.3 Cofactor matrix

It is a matrix A^C formed by replacing every element in A by its corresponding cofactor.

$$A^C = \begin{bmatrix} |C_{11}| & |C_{12}| & |C_{13}| \\ |C_{21}| & |C_{22}| & |C_{23}| \\ |C_{31}| & |C_{32}| & |C_{33}| \end{bmatrix}$$

Exp :

Find the A^C of the following matrix

$$\text{A} = \begin{bmatrix} 2 & 3 & 4 \\ -5 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Sol :

$|C_{11}| = (1) \begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix}$ = 45 – 48 = -3

$|C_{12}| = (-1) \begin{vmatrix} -5 & 6 \\ 7 & 9 \end{vmatrix}$ = -(-45-42) = 87

$|C_{13}| = (1) \begin{vmatrix} -5 & 5 \\ 7 & 8 \end{vmatrix}$ = -40 – 35 = -75

$|C_{21}| = (-1) \begin{vmatrix} 3 & 4 \\ 8 & 9 \end{vmatrix}$ = -(27 - 32) = 5

$|C_{22}| = (1) \begin{vmatrix} 2 & 4 \\ 7 & 9 \end{vmatrix}$ = 18 – 28 = -10

$|C_{23}| = (-1) \begin{vmatrix} 2 & 3 \\ 7 & 8 \end{vmatrix}$ = -(16 - 21) = 5

$|C_{31}| = (1) \begin{vmatrix} 3 & 4 \\ 5 & 6 \end{vmatrix}$ = 18 – 20 = -2

$|C_{32}| = (-1) \begin{vmatrix} 2 & 4 \\ -5 & 6 \end{vmatrix}$ = -(12 + 20) = -32

$|C_{33}| = (1)\begin{vmatrix} 2 & 3 \\ -5 & -5 \end{vmatrix} = 10 + 15 = 25$

$$A^C = \begin{bmatrix} -3 & 87 & -75 \\ 5 & -10 & 5 \\ -2 & -32 & 25 \end{bmatrix}$$

Exp :

Find $|A|$ for

$$A = \begin{bmatrix} 2 & 3 & 4 \\ -5 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

To find the determinant of a matrix A we choose any row from the matrix as follows :

$|A| = 2\,|C_{11}| + 3\,|C_{12}| + 4\,|C_{13}|$

$|A| = (2 \times -3) + (3 \times 87) + (4 \times -75)$

$= -6 + 261 - 300$

$= -45$

1.7 Adjugate matrix

It is the transpose of the cofactor matrix.

$$\text{Adj (A)} = \begin{bmatrix} |c_{11}| & |c_{21}| & \cdots & |c_{n1}| \\ |c_{12}| & |c_{22}| & \cdots & |c_{n2}| \\ \vdots & \vdots & \vdots & \vdots \\ |c_{1n}| & |c_{2n}| & \cdots & |c_{nn}| \end{bmatrix} = (A^c)^T$$

Exp :

Find the Adj (A)

$$A = \begin{bmatrix} 2 & 3 & 4 \\ -5 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Sol :

$$\text{Adj}(A) = (A^c)^T = \left(\begin{bmatrix} -3 & 87 & -75 \\ 5 & -10 & 5 \\ -2 & -32 & 25 \end{bmatrix}\right)^T$$

$$= \begin{bmatrix} -3 & 5 & -2 \\ 87 & -10 & -32 \\ -75 & 5 & 25 \end{bmatrix}$$

1.8 Inverse of a matrix

1.8.1 Inverse of 2×2 matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Exp :

Find the A^{-1} for :

$$A = \begin{bmatrix} 3 & -1 \\ 5 & 4 \end{bmatrix}$$

Sol :

$$\det(A) = \begin{vmatrix} 3 & -1 \\ 5 & 4 \end{vmatrix} = (3 \times 4) - (-1 \times 5) = 12 + 5 = 17$$

$$A^{-1} = 17^{-1} \begin{vmatrix} 4 & 1 \\ -5 & 3 \end{vmatrix}$$

1.8.2 Inverse of 3×3 matrix

For an n×n matrix the inverse is :

$A^{-1} = \frac{1}{|A|} \text{Adj}(A)$

Exp :

Find the A^{-1} for :

$$A = \begin{bmatrix} 2 & 3 & 4 \\ -5 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

Sol :

$A^{-1} = \frac{1}{|A|} \text{Adj}(A)$

$$|A| = 2\begin{vmatrix} 5 & 6 \\ 8 & 9 \end{vmatrix} - 3\begin{vmatrix} -5 & 6 \\ 7 & 9 \end{vmatrix} + 4\begin{vmatrix} -5 & 5 \\ 7 & 8 \end{vmatrix}$$

= 2(45 – 48) -3(-45 – 42) +4(-40-35) = -45

$\text{Adj}(A) = (A^c)^T$

$$A^C = \begin{bmatrix} -3 & 87 & -75 \\ 5 & -10 & 5 \\ -2 & -32 & 25 \end{bmatrix}$$

$$(A^c)^T = \begin{bmatrix} -3 & 5 & -2 \\ 87 & -10 & -32 \\ -75 & 5 & 25 \end{bmatrix}$$

$$A^{-1} = \frac{1}{-45}\begin{bmatrix} -3 & 5 & -2 \\ 87 & -10 & -32 \\ -75 & 5 & 25 \end{bmatrix}$$

1.9 Determinant and Inverse of a matrix by using elementary row (column) operations

1.9.1 Elementary row (column) operations

Let B be a matrix obtained from $A_{n\times n}$ by one of the three elementary row(column) operations :

1. Interchange the i^{th} row(column) and j^{th} row(column) (H_{ij})

$$\Rightarrow |B| = |-A|$$

2. Multiply every element of the i^{th} row(column) by a scalar $\alpha \neq 0$ $(H_j(\alpha))$ Thus

$$|B| = \alpha|A|$$

3. Add α times the elements of j^{th} row(column) to the corresponding elements of the i^{th} row(column) $H_{ij}(\alpha)$ Thus

$$|B| = |A|$$

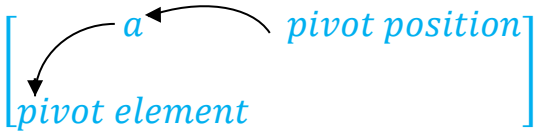
Exp :

$$\begin{bmatrix} 3 & 1 & 2 \\ 5 & 0 & 7 \\ 2 & 4 & 5 \end{bmatrix} \xrightarrow{H_{23}} \begin{bmatrix} 3 & 1 & 2 \\ 2 & 4 & 5 \\ 5 & 0 & 7 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 1 & 2 \\ 5 & 0 & 7 \\ 2 & 4 & 5 \end{bmatrix} \xrightarrow{H_{1(2)}} \begin{bmatrix} 6 & 2 & 4 \\ 5 & 0 & 7 \\ 2 & 4 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 1 & 2 \\ 5 & 0 & 7 \\ 2 & 4 & 5 \end{bmatrix} \xrightarrow{H_{12(3)}} \begin{bmatrix} 18 & 1 & 23 \\ 5 & 0 & 7 \\ 2 & 4 & 5 \end{bmatrix}$$

- By means of elementary row(column) operations, any square matrix can be reduced to upper triangular , lower triangular or diagonal matrix. For upper triangular at each step focus on one position (pivot position) and eliminates all elements below this position using the three elementary operations.



- All nonzero numbers are allowed to be pivots.
- If a pivot is ever 0 , then the pivotal row is interchange with a row below it to produce a nonzero pivot.
- Unless it is 0 , the first coefficient of the first row is taken as the first pivot.

$$\begin{bmatrix} a & b & c \\ 0 & e & f \\ 0 & 0 & i \end{bmatrix} \qquad \begin{bmatrix} a & 0 & 0 \\ d & e & 0 \\ g & h & i \end{bmatrix} \qquad \begin{bmatrix} a & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & i \end{bmatrix}$$

upper triangular lower triangular diagonal

1.9.2 Evaluating determinants by row (column) reduction

The involves substantially less computation than the cofactor expansion method. The idea is to reduce the given matrix to upper or lower triangular matrix by elementary row(column) operations. Then compute the determinant of the triangular matrix.

Exp :

Evaluate $|A|$ the by using row reduction method :

$$A = \begin{bmatrix} 0 & 1 & 5 \\ 3 & -6 & 9 \\ 2 & 6 & 1 \end{bmatrix}$$

Sol :

$$\begin{vmatrix} 0 & 1 & 5 \\ 3 & -6 & 9 \\ 2 & 6 & 1 \end{vmatrix} \xrightarrow{H_{12}} - \begin{vmatrix} 3 & -6 & 9 \\ 0 & 1 & 5 \\ 2 & 6 & 1 \end{vmatrix} \rightarrow -3 \begin{vmatrix} 1 & -2 & 3 \\ 0 & 1 & 5 \\ 2 & 6 & 1 \end{vmatrix}$$

$$\xrightarrow{H_{31(-2)}} -3 \begin{vmatrix} 1 & -2 & 3 \\ 0 & 1 & 5 \\ 0 & 10 & -5 \end{vmatrix} \xrightarrow{H_{32(-10)}} -3 \begin{vmatrix} 1 & -2 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & -55 \end{vmatrix}$$

$|A| =$ -3(1)(1)(-55) = 165

1.9.3 The inverse matrix using row operations

To find the inverse of an invertible matrix A , we must find a sequence of elementary row operations that reduces $A_{n\times n}$ to I_n then performing this same sequence of operations on I_n to produce A^{-1}

$[A|I] \xrightarrow{Row\ operations} [I|A^{-1}]$

Exp :

Find A^{-1} of

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{bmatrix}$$

Sol :

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & 5 & 3 & 0 & 1 & 0 \\ 1 & 0 & 8 & 0 & 0 & 1 \end{array}\right] \xrightarrow[H_{31(-1)}]{H_{21(-2)}} \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & -3 & -2 & 1 & 0 \\ 0 & -2 & 5 & -1 & 0 & 1 \end{array}\right]$$

$$\xrightarrow[H_{32(2)}]{H_{12(-2)}} \left[\begin{array}{ccc|ccc} 1 & 0 & 9 & 5 & -2 & 0 \\ 0 & 1 & -3 & -2 & 1 & 0 \\ 0 & 0 & -1 & -5 & 2 & 1 \end{array}\right] \xrightarrow{H_{3(-1)}} \left[\begin{array}{ccc|ccc} 1 & 0 & 9 & 5 & -2 & 0 \\ 0 & 1 & -3 & -2 & 1 & 0 \\ 0 & 0 & 1 & 5 & -2 & -1 \end{array}\right]$$

$$\xrightarrow[H_{13(-9)}]{H_{23(3)}} \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -40 & 16 & 9 \\ 0 & 1 & 0 & 13 & -5 & -3 \\ 0 & 0 & 1 & 5 & -2 & -1 \end{array}\right] = [I|A^{-1}]$$

$$A^{-1} = \begin{bmatrix} -40 & 16 & 9 \\ 13 & -5 & -3 \\ 5 & -2 & -1 \end{bmatrix}$$

2.1 Matrix Inversion in Hill Cipher

2.1.1 2 ×2 matrix

Exp :

$$A = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

$A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$\det(A) = \begin{vmatrix} 9 & 4 \\ 5 & 7 \end{vmatrix} = (9 \times 7) - (4 \times 5) = 43 \bmod 26 = 17$

Using Extended Euclidean Algorithm to find the inverse of the det(A) :

(26,17)

$26 = 17 \times 1 + 9$ ……(1)

$17 = 9 \times 1 + 8$ ……(2)

$9 = 8 \times 1 + 1$ ……(3)

$8 = 8 \times 1 + 0$ ……(4)

From eq(1) we have

$9 = 26 - 17 \times 1$ ……..(5)

From eq(2) we have

$8 = 17 - 9 \times 1$ …….(6)

From eq(3) we get

$1 = 9 - 8 \times 1$ ……(7)

Put eq(5) & eq(6) in eq(7) to get

$1 = 26 - 17 \times 1 - (17 - 9 \times 1)$

$= 26 - 17 \times 1 - 17 + 9 \times 1$

$= 26 - 17 \times 1 - 17 + (26 - 17) \times 1$

$= 26 - 17 - 17 + 26 - 17$

$= 2(26) - 3(7)$

Then the inverse of 17 = -3 = -3 + 26 = 23

$A^{-1} = \det(17)^{-1} \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}$

$A^{-1} = 23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} = \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix} \bmod 26$

Not :

R = remainder of $\frac{|a|}{m}$

$$r = \begin{cases} R & if\ a \geq 0 \\ m - R & if\ a < 0\ ;\ R \neq 0 \\ 0 & if\ a < 0\ ;\ R = 0 \end{cases}$$

161 mod 26 = 5

92 mod 26 = 14 ⇒ 26 – 14 = 12

115 mod 26 = 11 ⇒ 26 – 11 = 15

207 mod 26 = 25

$$A^{-1} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$$

2.1.2 3 ×3 matrix

Exp :

$$A = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

$A^{-1} = \frac{1}{|A|}$ Adj(A)

By choosing any row to find the determinant we get

$$|A| = (-1)^2 \times 6 \begin{vmatrix} 16 & 10 \\ 17 & 15 \end{vmatrix} + (-1)^3 \times 24 \begin{vmatrix} 13 & 10 \\ 20 & 15 \end{vmatrix} + (-1)^4 \times 1 \begin{vmatrix} 13 & 16 \\ 20 & 17 \end{vmatrix}$$

$$= 6\begin{vmatrix} 16 & 10 \\ 17 & 15 \end{vmatrix} - 24 \begin{vmatrix} 13 & 10 \\ 20 & 15 \end{vmatrix} + \begin{vmatrix} 13 & 16 \\ 20 & 17 \end{vmatrix}$$

= 6(16 × 15 – 17 × 10) – 24 (13 × 15 – 20 × 10) + (13 × 17 – 20 × 16)

= (6 × 70) – (24 × -5) + (-99)

= 420 +120 – 99 = 441 mod 26 = 25

$$\frac{1}{|A|} = \det(A^{-1}) = \det(25^{-1}) = 25$$

$$\text{Adj(A)} = (\text{A}^{\text{c}})^{T}$$

$$\text{A}^{\text{c}} = \begin{bmatrix} 70 & 5 & -99 \\ -343 & 70 & 378 \\ 224 & -47 & -216 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 & 5 & 5 \\ 21 & 18 & 14 \\ 16 & 5 & 18 \end{bmatrix}$$

$$(\text{A}^{\text{c}})^{T} = \begin{bmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{bmatrix}$$

$$A^{-1} = \frac{1}{|A|} \text{Adj(A)}$$

$$= 25 \begin{bmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 450 & 525 & 400 \\ 125 & 450 & 125 \\ 125 & 350 & 450 \end{bmatrix} \bmod 26$$

2-Hill Cipher - 2.2

مثـــال : تشفير وفك التشفير باستخدام مصفوفه 2 * 2

قبل أن تبدأ بالتشفير ، يجب أن يكون جدول الحرف قريب لديك .

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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

لدينا النص التالي : THE PROFESSOR IS EVIL

الأن نقوم في البداية بتقسيم النص الأصلي الى مجموعات Block كل واحد منها مكون من حرفين (لأننا أخترنا 2-Hill Cipher، في حاله أخترنا n سوف نقسم الحروف في النص الأصلي الى n حرف).

ولاحظ أننا سنتعمد هنا أن الحرف الأول A تكون قيمته 1 وليس 0 ، ويمكن إتباع الأسلوب القديم هو الحرف A تكون قيمته 0)

T H	E P	R O	F E	S S	O R	I S	E V	I L
20 8	5 16	18 15	6 5	19 19	15 18	9 19	5 22	9 12

ونقوم الآن بوضع هذه الارقام في مصفوفه النص الاصلي P .

$$P = \begin{bmatrix} 20 & 5 & 18 & 6 & 19 & 15 & 9 & 5 & 9 \\ 8 & 16 & 15 & 5 & 19 & 18 & 19 & 22 & 12 \end{bmatrix}$$

والآن نختار مصفوفه التشفير والتي يجب أن يكون لها معكوس حتى نستطيع فك التشفير ولتكن :

$$A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

نقوم بضرب المصفوفة A * P ، نضرب الصف الاول للمصفوفة A بالعمود الاول للمصفوفة P ، ثم نضرب الصف الثاني للمصفوفة A بالعمود الاول للمصفوفة P لينتج العمود الاول من المصفوفة الجديدة C

$$C=AP = \begin{bmatrix} 148 & 161 & 180 & 60 & 209 & 183 & 159 & 157 & 117 \\ 64 & 58 & 81 & 27 & 95 & 84 & 75 & 76 & 54 \end{bmatrix}$$ Mod 26

$$C= \begin{bmatrix} 18 & 17 & 24 & 8 & 1 & 1 & 3 & 1 & 13 \\ 12 & 6 & 3 & 1 & 17 & 6 & 23 & 24 & 2 \end{bmatrix}$$

الآن نقوم بتحويل المصفوفة الى أحرف

$$C=\begin{bmatrix} R & O & X & H & A & A & C & A & M \\ L & F & C & A & Q & F & W & X & B \end{bmatrix}$$

نقوم بترتيبها بعد ذلك ويخرج النص المشفر التالي :

RLQFXCHAAQAFCWAXMB

فك التشفير :

نقوم بفك التشفير ولفك التشفير نقوم بضرب المصفوفة (النص المشفر) في معكوس مصفوفة التشفير نبدأ بإيجاد معكوس مصفوفة التشفير

علينا أولاً اختيار المفتاح ، مثلاً كان :

$$A=\begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

-Det(A) =(5*3) – (2*6)=3

-Det(A^{-1}) = 9

$$A^{-1} = 9\begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} \mod 26 = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$$

(ارجع الى معكوس المصفوفة)

الآن نقوم بضرب المصفوفة E في معكوس المصفوفة A^{-1} لينتج المصفوفة D

$$D= A^{-1}E = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} * \begin{bmatrix} 18 & 17 & 24 & 8 & 1 & 1 & 3 & 1 & 13 \\ 12 & 6 & 3 & 1 & 17 & 6 & 23 & 24 & 2 \end{bmatrix}$$

$$D=A^{-1}E = \begin{bmatrix} 306 & 161 & 96 & 32 & 409 & 145 & 555 & 577 & 61 \\ 372 & 250 & 249 & 83 & 331 & 122 & 461 & 464 & 142 \end{bmatrix} MOD\ 26$$

$$D = \begin{bmatrix} 20 & 5 & 18 & 6 & 19 & 15 & 9 & 5 & 9 \\ 8 & 16 & 15 & 5 & 19 & 18 & 19 & 22 & 12 \end{bmatrix}$$

الآن نقوم بتحويل المصفوفة الى أحرف

$$D = \begin{bmatrix} T & E & R & F & S & O & I & E & I \\ H & P & O & E & S & R & S & V & L \end{bmatrix}$$

نقوم بترتيبها بعد ذلك ويخرج النص المشفر التالي :

THE PROFESSOR IS EVIL

مثـــال آخر:

قبل أن تبدأ بالتشفير ، يجب أن يكون جدول الحرف قريب لديك .

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

لدينا النص التالي : OUR UNIVERSITY

ولاحظ أننا سنتعمد هنا أن الحرف الأول A تكون قيمته0 وليس 1 ، ويمكن إتباع الأسلوب القديم هو الحرف A تكون قيمته 1)

O U	R U	N I	V E	R S	I T	Y X
14 20	17 20	13 8	21 4	17 18	8 19	24 23

ونقوم الآن بوضع هذه الارقام في مصفوفه النص الاصلي P .

$$P = \begin{bmatrix} 14 & 17 & 13 & 21 & 17 & 8 & 24 \\ 20 & 20 & 8 & 4 & 18 & 19 & 23 \end{bmatrix}$$

والآن نختار مصفوفه التشفير والتي يجب أن يكون لها معكوس حتى نستطيع فك التشفير ولتكن :

$$A = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

نقوم بضرب المصفوفة P * A ، نضرب الصف الاول للمصفوفة A بالعمود الاول للمصفوفة P ، ثم نضرب الصف الثاني للمصفوفة A بالعمود الاول للمصفوفة P لينتج العمود الاول من المصفوفة الجديدة C

$$C=AP = \begin{bmatrix} 206 & 233 & 149 & 205 & 225 & 148 & 308 \\ 210 & 225 & 121 & 133 & 211 & 173 & 281 \end{bmatrix}$$ Mod 26

$$C=\begin{bmatrix}24 & 25 & 19 & 23 & 17 & 18 & 22\\ 2 & 17 & 17 & 3 & 3 & 17 & 21\end{bmatrix}$$

الآن نقوم بتحويل المصفوفة الى أحرف

$$C=\begin{bmatrix}Y & Z & T & X & R & S & W\\ C & R & R & D & D & R & V\end{bmatrix}$$

نقوم بترتيبها بعد ذلك ويخرج النص المشفر التالي :

YCZRTRXDRDSRWV

فك التشفير :

نقوم بفك التشفير ولفك التشفير نقوم بضرب المصفوفة (النص المشفر) في معكوس مصفوفة التشفير نبدأ بإيجاد معكوس مصفوفة التشفير

علينا أولاً اختيار المفتاح ، مثلاً كان :

$$A=\begin{bmatrix}5 & 12\\ 15 & 25\end{bmatrix}$$

(ارجع الى معكوس المصفوفة)

الآن نقوم بضرب المصفوفة E في معكوس المصفوفة A^{-1} لينتج المصفوفة D

$$D=A^{-1}E=\begin{bmatrix}5 & 12\\ 15 & 25\end{bmatrix}*\begin{bmatrix}24 & 25 & 19 & 23 & 17 & 18 & 22\\ 2 & 17 & 17 & 3 & 3 & 17 & 21\end{bmatrix}$$

$$D=A^{-1}E=\begin{bmatrix}144 & 329 & 299 & 151 & 121 & 294 & 362\\ 410 & 800 & 710 & 420 & 330 & 694 & 855\end{bmatrix}\ MOD\ 26$$

$$D=\begin{bmatrix}14 & 17 & 13 & 21 & 17 & 8 & 24\\ 20 & 20 & 8 & 4 & 18 & 19 & 23\end{bmatrix}$$

الآن نقوم بتحويل المصفوفة الى أحرف

$$D = \begin{bmatrix} O & R & N & V & R & I & Y \\ U & U & I & E & S & T & X \end{bmatrix}$$

نقوم بترتيبها بعد ذلك ويخرج النص المشفر التالي :

OUR UNIVERSITYX

3-Hill Cipher - 2.3

مثـــال : تشفير وفك التشفير باستخدام مصفوفه 3 * 3

مثلاً لدينا جملة التشفير التالية : GYBNQKURP

بعد إعطاء كل حرف قيمته ، نقوم بوضعه داخل المصفوفة على شكل 3 * 3 ، (علماً بأن جدول الحرف يبدأ من 0 أي A=0) وتكون شكل المصفوفة كالتالي :

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

وليكن النص الأصلي هو : ACT ، وفي حال كان اكبر من ذلك يتم تقسيمة الى بلوكات ، كل واحد يتكون من ثلاثة حروف .

نقوم بوضع النص الاصلي داخل مصفوفة 1 * 3 :

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

الآن نقوم بعمليه ضرب المصفوفتين ، نضرب الصف الأول في المصفوفة الاولى بالعمود في المصفوفة الثانية نضع الناتج في المصفوفة الجديدة . وهكذا لباقي الصفوف نقوم بضربها بالعمود . ونأخذ الناتج بعمليه باقي القسة MOD 26

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \text{ MOD 26}$$

اذاً الناتج من هذا النص بعد تحويل هذه الارقام الى حروف (بمساعدة جدول الحروف) ، أي النص المشفر هو : POH

فك التشفير :

لفك التشفير ، كل ما علينا هو إيجاد معكوس المصفوفة (كما تعلمنا سابقاً) ، وتقوم بضربه في النص المشفر مع أخذ باقي القسمة على 26 ، كما هو موضح بالصورة :

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \text{ MOD 26}$$

اذاً الناتج من هذا النص بعد تحويل هذه الارقام الى حروف (بمساعدة جدول الحروف) ، أي النص الواضح هو ACT :

مثـــال آخر :

مثلاً لدينا جملة التشفير التالية : BCDCFDBAI

بعد إعطاء كل حرف قيمته ، نقوم بوضعه داخل المصفوفة على شكل 3 * 3 ، (علماً بأن جدول الحرف يبدأ من 0 أي A=0) وتكون شكل المصفوفة كالتالي :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{pmatrix}$$

وليكن النص الأصلي هو : COMPUTERS ، وفي حال كان اكبر من ذلك يتم تقسيمة الى بلوكات ، كل واحد يتكون من ثلاثة حروف .

نقوم بوضع النص الاصلي داخل مصفوفة 3 * 3 :

$$\begin{pmatrix} 2 & 15 & 4 \\ 14 & 20 & 17 \\ 12 & 19 & 18 \end{pmatrix}$$

الآن نقوم بعمليه ضرب المصفوفتين ، نضرب الصف الأول في المصفوفة الاولى بالعمود في المصفوفة الثانية نضع الناتج في المصفوفة الجديدة . وهكذا لباقي الصفوف نقوم بضربها بالعمود . ونأخذ الناتج بعمليه باقي القسة MOD 26

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{pmatrix} \begin{pmatrix} 2 & 15 & 4 \\ 14 & 20 & 17 \\ 12 & 19 & 18 \end{pmatrix} \equiv \begin{pmatrix} 66 & 112 & 92 \\ 110 & 187 & 147 \\ 98 & 167 & 148 \end{pmatrix} \text{ MOD 26}$$

$$\equiv \begin{pmatrix} 14 & 8 & 14 \\ 6 & 5 & 17 \\ 20 & 11 & 18 \end{pmatrix}$$

اذاً الناتج من هذا النص بعد تحويل هذه الارقام الى حروف (بمساعدة جدول الحروف) ، أي النص المشفر هو :

$$\begin{pmatrix} O & I & O \\ G & F & R \\ U & L & S \end{pmatrix}$$

والنص المشفر بعد الترتيب : OGUIFLORS

فك التشفير :

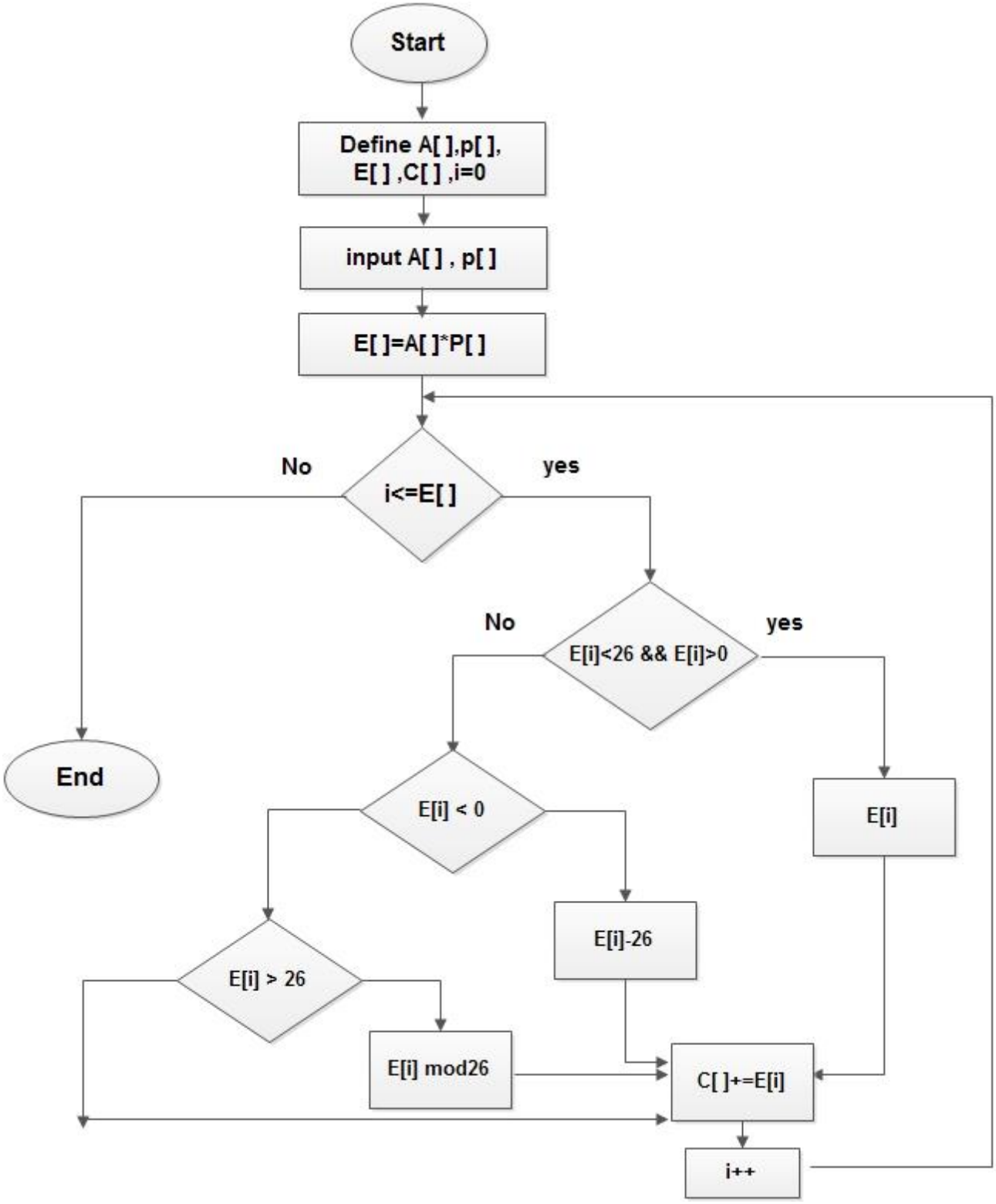
لفك التشفير ، كل ما علينا هو إيجاد معكوس المصفوفة (كما تعلمنا سابقاً) ، وتقوم بضربه في النص المشفر مع أخذ باقي القسمة على 26 ، كما هو موضح بالصورة :

$$\begin{pmatrix} 2 & 15 & 4 \\ 13 & 20 & 17 \\ 12 & 19 & 18 \end{pmatrix} \begin{pmatrix} 14 & 8 & 14 \\ 6 & 5 & 17 \\ 20 & 11 & 18 \end{pmatrix} \equiv \begin{pmatrix} 444 & 275 & 602 \\ 768 & 462 & 953 \\ 714 & 435 & 928 \end{pmatrix} \quad \text{MOD } 26$$

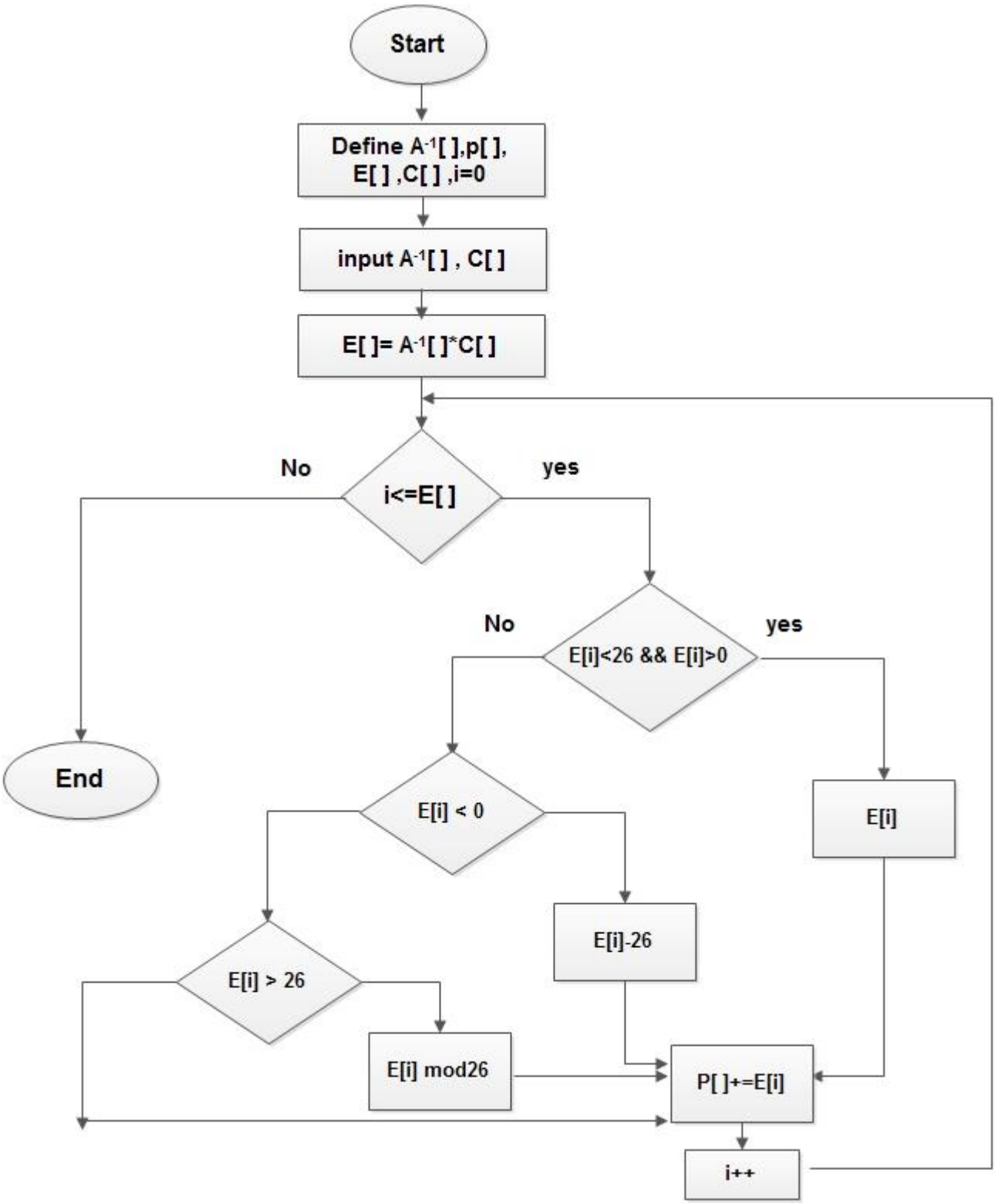
$$\equiv \begin{pmatrix} 2 & 15 & 4 \\ 14 & 20 & 17 \\ 12 & 19 & 18 \end{pmatrix}$$

اذاً الناتج من هذا النص بعد تحويل هذه الارقام الى حروف (بمساعدة جدول الحروف) ، أي النص الواضح هو : COMPUTERS

2.4 - Encryption Algorithm:



2.5 - Decryption Algorithm:



2.6- الجـــزء العمــلي :

استخدمنا لغة c# لتصميم وبرمجة خوارزمية hill وذلك لما تمتاز هذه ألغة من المرونة والبساطة في تنفيذ الأوامر البرمجية .

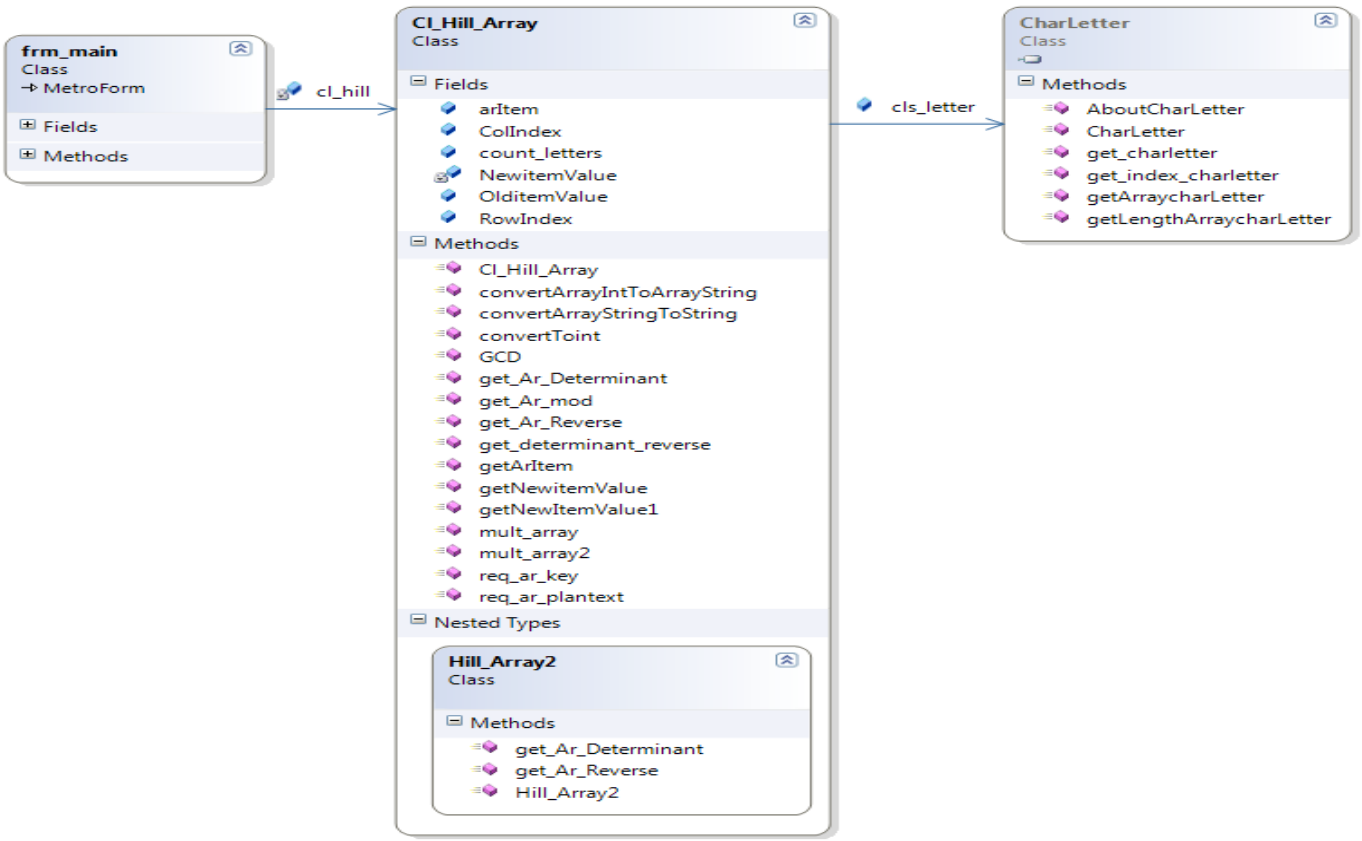
تم تنفيذ الخوارزمية باستخدام ثلاثة كلاسات وهي كما يلي :

١. **Cl_Hill_Array :** يحتوي على اغلب الدوال اللازمة لتنفيذ الخوارزمية ويحتوي على كلا س اخر والمسمى Hill_Array2 الذي بدورة يحتوي على الوظائف الخاصة التي تساعد في التعامل مع Hill2*2 .

٢. **En_CharLetter :** يحتو على كلاس CharLetter والذي بدورة يحتوي على الدوال اللازمة لعملية تحويل الأحرف الى أرقام أو العكس .

٣. **frm_main :** يقوم بتمثيل الواجهة الرسومية التي يتم من خلالها التفاعل و التعامل مع التطبيق و يستخدم الكلاسات السابقة لتنفيذ الخوارزمية .

مخطط ClassDiagram الذي يوضح الثلاثة الكلاسات السابقة والعلاقة فيما بينها في الشكل رقم (1.1)



الجدول رقم (1.2) التالي يوضح الدوال المستخدمة في الكلاس Cl_Hill_Array وشرحها :

الدالة أو الوظيـــفة	عمـــلها
Cl_Hill_Array	باني للكلاس بدون بارمترات .
req_ar_key	تقوم بتجهيز مصفوفة جملة التشفير حيث تستقبل متغير نص وتحوله الي مصفوفة من نوع نص حسب سياسات الخوارزمية .
req_ar_plantext	تقوم بتجهيز مصفوفة النص المراد تشفير حيث تستقبل متغير من نوع نص و متغير من نوع رقم وهو الذي يحدد إبعاد المصفوفة ،مخرجات هاذه الدالة هو مصفوفة النص المراد تشفيره
convertArrayStringToString	تقوم بتحويل مصفوفة نصية إلى نص تستقبل متغير من نوع مصفوفة نصية
convertToint	تستقبل مصفوفة نصية وترجع مصفوفة رقمية وذلك باستخدام وظائف الكلاس En_CharLetter
convertArrayIntToArrayString	عكس الدالة السابقة تستقبل مصفوفة من نوع رقم وترجع مصفوفة من نوع نص
mult_array2	تقوم بعملية ضرب مصفوفتين تستقبل مصفوفتين من نوع رقم وترجع مصفوفة تمثل ناتج الضرب
GCD	تقوم بإيجاد القاسم المشترك الأعظم بين قيمتين تستقبل قيمتين من نوع رقم وترجع قيمة من نوع رقم
get_Ar_Determinant	تقوم بإيجاد محدد المصفوفة تستقبل مصفوفة وترجع المحدد
get_Ar_Reverse	تقوم بعكس المصفوفة تستقل مصفوفة من نوع رقم وترجع مصفوفة من نوع رقم (معكوس المصفوفة)
get_determinant_reverse	تقوم بإيجاد معكوس رقم تستقبل رقمين n,m وترجع معكوس n .
getNewItemValue1	تستخدم ضمن الدالة get_Ar_Reverse تساعد في إيجاد معكوس المصفوفة
getNewitemValue	تستخدم ضمن الدالة getNewitemValue1 تساعد في إيجاد معكوس المصفوفة .
is_reverse	تقوم بفحص مصفوفة جملة التشفير هل تقبل العكس ام لا وترجع قيمة true او false

الجدول رقم (1.3) التالي يوضح الدوال المستخدمة في الكلاس En_CharLetter.CharLetter وشرحها :

الدالة أو الوظيفة	عملها
CharLetter()	باني الكلاس .
get_charletter(int charIndex)	تستقبل رقم الحرف ونعيد الحرف .
int get_index_charletter(string chaletter)	تستقبل متغير من نوع نص وهو الحرف المراد معرفة رقمة في جدول الأحرف شكل (1.1) ترجع رقم الحرف .
int getLengthArraycharLetter()	ترجع عدد الأحرف المستخدمة في شكل رقم (1.1)
void AboutCharLetter()	تعرض بعض المعلومات عن مبرمج الكلاس
string[] getArraycharLetter()	ترجع مصفوفة من نوع نص وهي المصفوفة الموضحة بالشكل رقم (1.1)

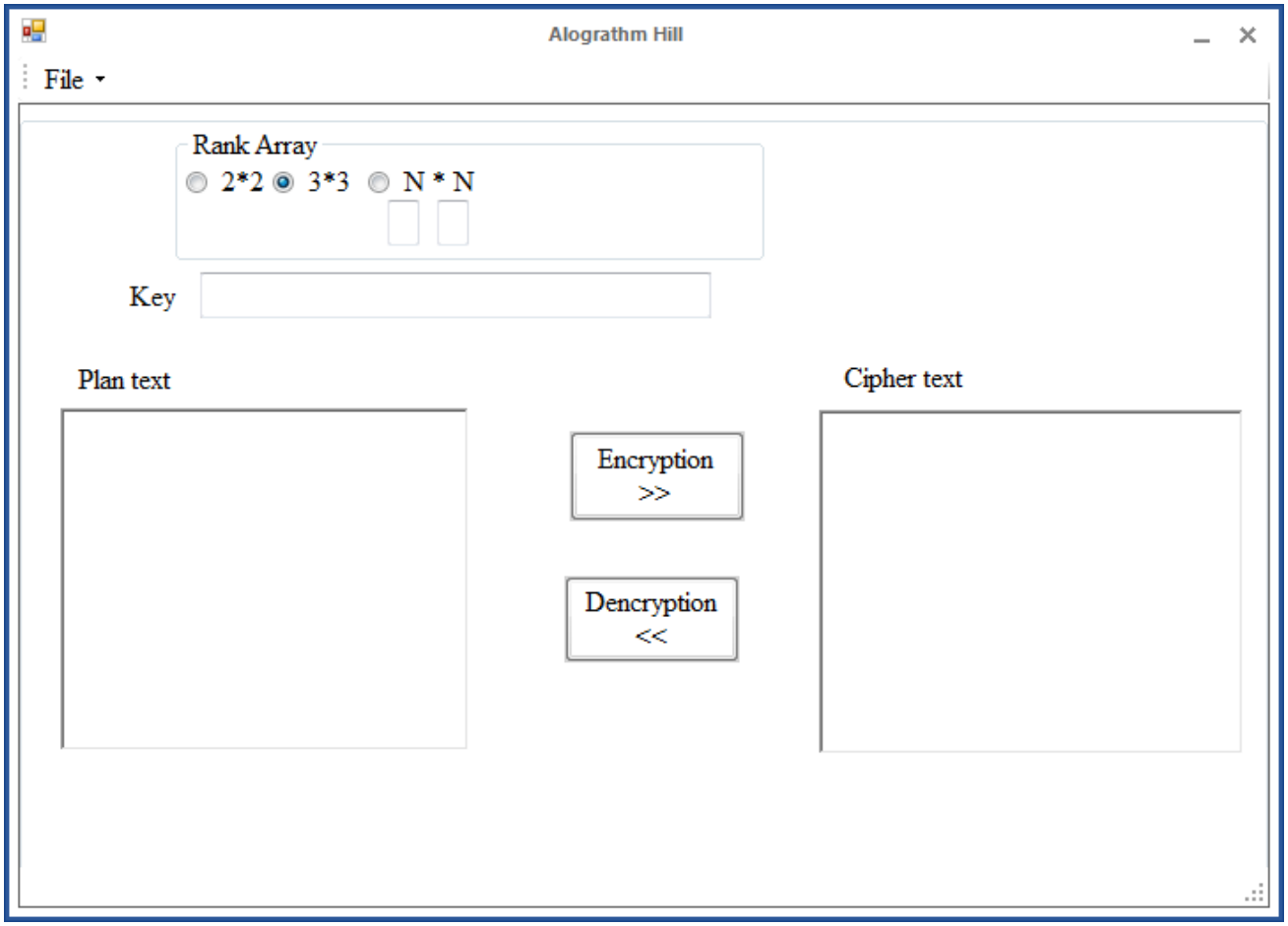
الجدول رقم (1.4) التالي يوضح الدوال المستخدمة في الكلاس frm_main وشرحها :

الدالة أو الوظيفة	عملها
frm_main	باني الكلاس .
Encryption	تقوم بعملية التشفير بمساعدة الكلاسات السابقة تستقبل مصفوفة التشفير ومصفوفة النص الواضح وترجع مصفوفة النص المشفر .
DEncryption	تقوم بعملية فك التشفير بمساعدة الكلاسات السابقة تستقبل مصفوفة التشفير ومصفوفة النص المشفر وترجع مصفوفة النص الواضح .
seting_key	أعداد مصفوفة التشفير(جملة التشفير) تستقبل متغير من نوع نص .

شرح واجهة التطبيق:

شاشة البرنامج:

شكل رقم (1.5) يوضح الواجهة الرئيسية للبرنامج :



كيفية عمل البرنامج :

- **عملية التشفير**

١. تحديد إبعاد المصفوفة .

٢. إدخال نص جملة التشفير التي سيتم تحويله إلى مصفوفة حسب الأبعاد المحددة .

٣. إدخال النص المراد تشفيره يجب ان يكون من مضاعفات بعد مصفوفة التشفير والذي سيتم تحويله إلى مصفوفة .

٤. الضغط عل زر Encryption .

٥. يتم عرض النص المشفر في مربع النص المشفر الموضح بالشكل رقم ٢

- **عملية فك التشفير**

١. تحديد إبعاد المصفوفة .

٢. إدخال نص جملة التشفير التي سيتم تحويله إلى مصفوفة حسب الأبعاد المحددة .

٣. إدخال النص المراد فك تشفيره يجب ان يكون من مضاعفات بعد مصفوفة التشفير والذي سيتم تحويله الى مصفوفة .

٤. الضغط عل زر Dencryption .

٥. يتم عرض النص الواضع في مربع النص الواضح الموضح بالشكل رقم (1.5) .

- **خيارات قائمة ملف:**

١. New يعمل على مسح جميع الحقول للبد بعملية تشفير او فك تشفير جديدة .

٢. Save .

A. Save Plant Text لحفظ النص الواضح .

B. Save Cipher Text لحفظ النص المشفر .

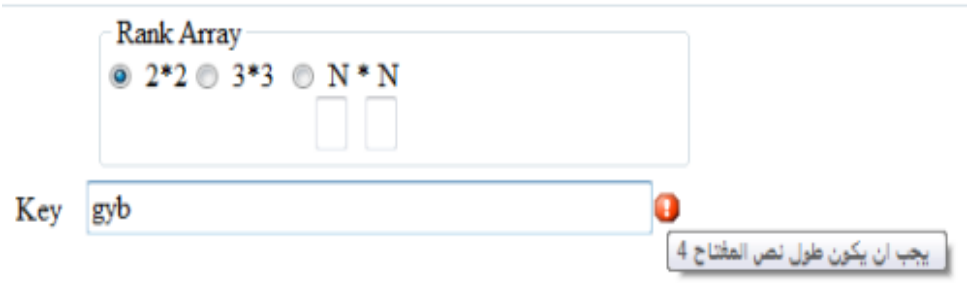
٣. Exit إغلاق البرنامج .

بعض رسائل الأخطاء والتنبيهات التي يصدرها البرنامج عن اجراء العمليات :

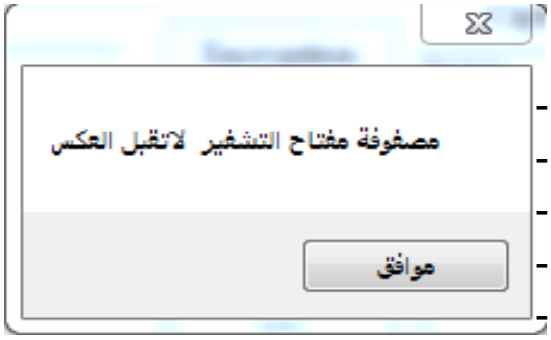
- **المتعلقة بجملة التشفير**

قبل عملية تشفير أو فك التشفير يجب إدخال جملة التشفير

- لا بد ان يكون طول جملة التشفير حسب البعد المحدد بمعنى اذ كان البعد 2*2 لابد ان يكون طول جملة التشفير ٤ وإذا كان البعد المحدد ٣*٣ يجب ان يكون طول جملة التشفير ٩

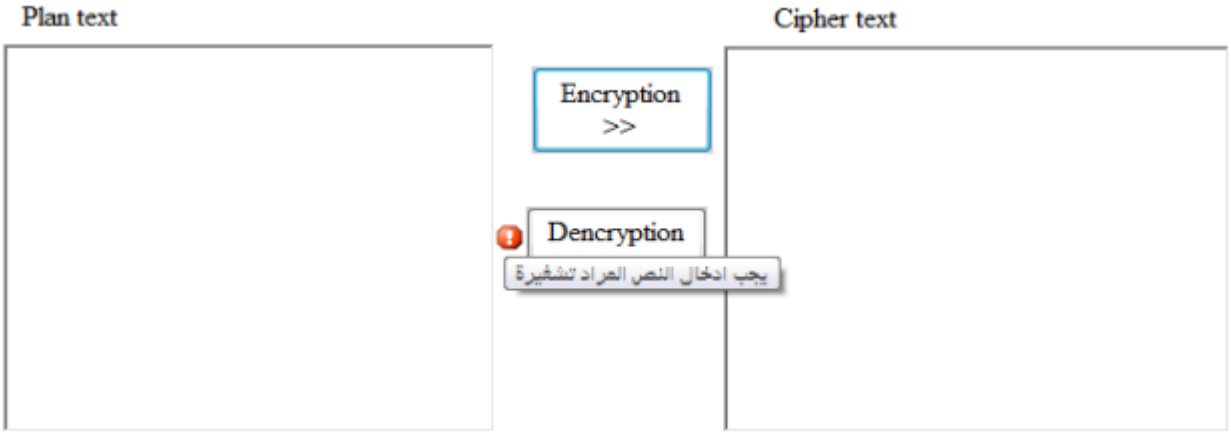


- يجب ان تكون مصفوفة جملة التشفير قابلة للعكس .



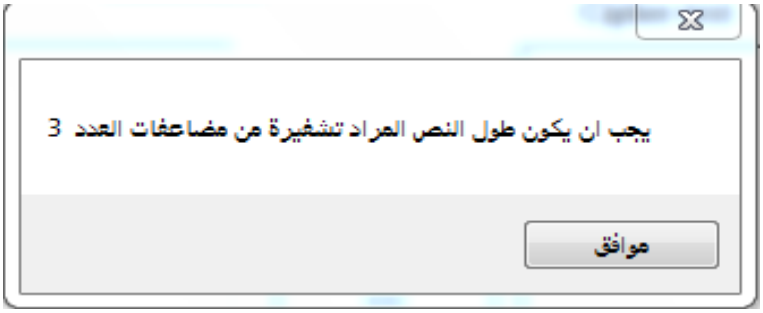
- **المتعلقة بنص الواضح عند عملية التشفير**

- يجب ان يكون طول النص الواضح(المراد تشفيره)من مضاعفات البعد المحدد بمعنى اذا كان البعد المحدد ٣*٣ يجب ان يكون طول النص المراد تشفيره من مضاعفات العدد ٣ (٣، ٩، ١٢ .....)

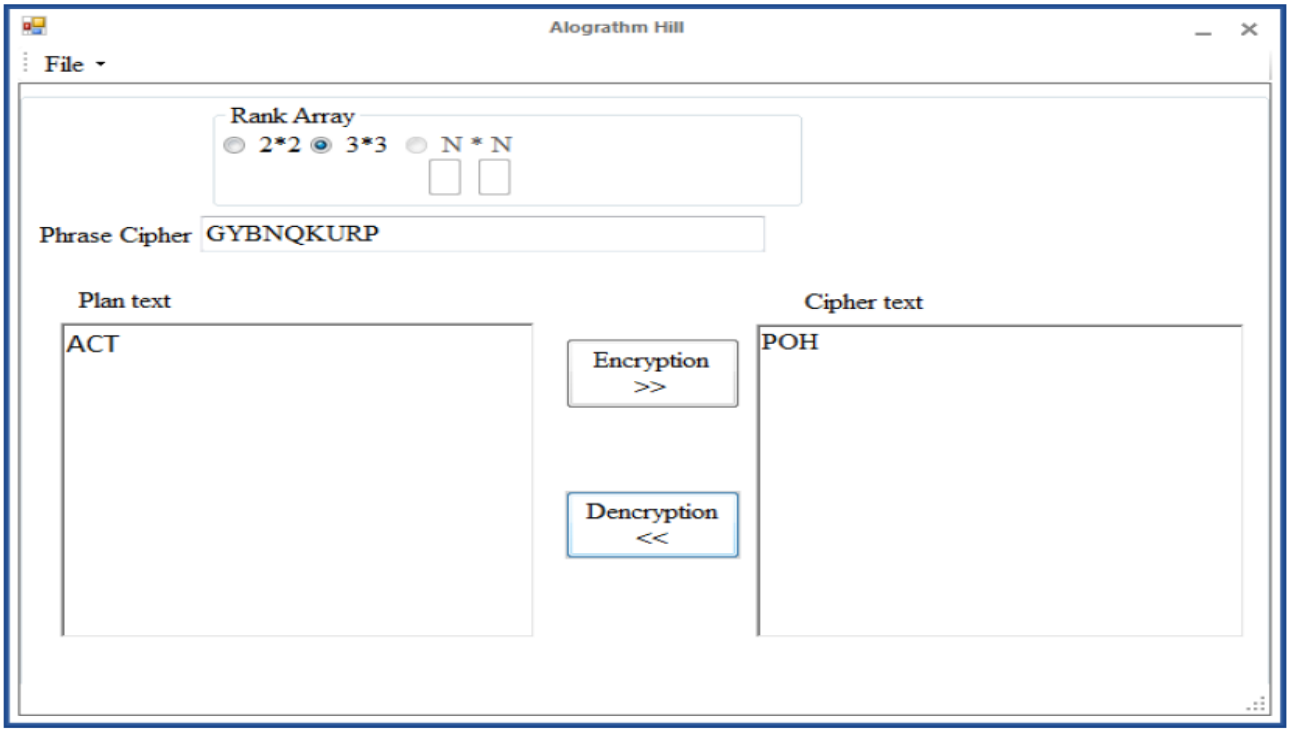


- **المتعلقة بنص المشفر عند عملية فك التشفير**

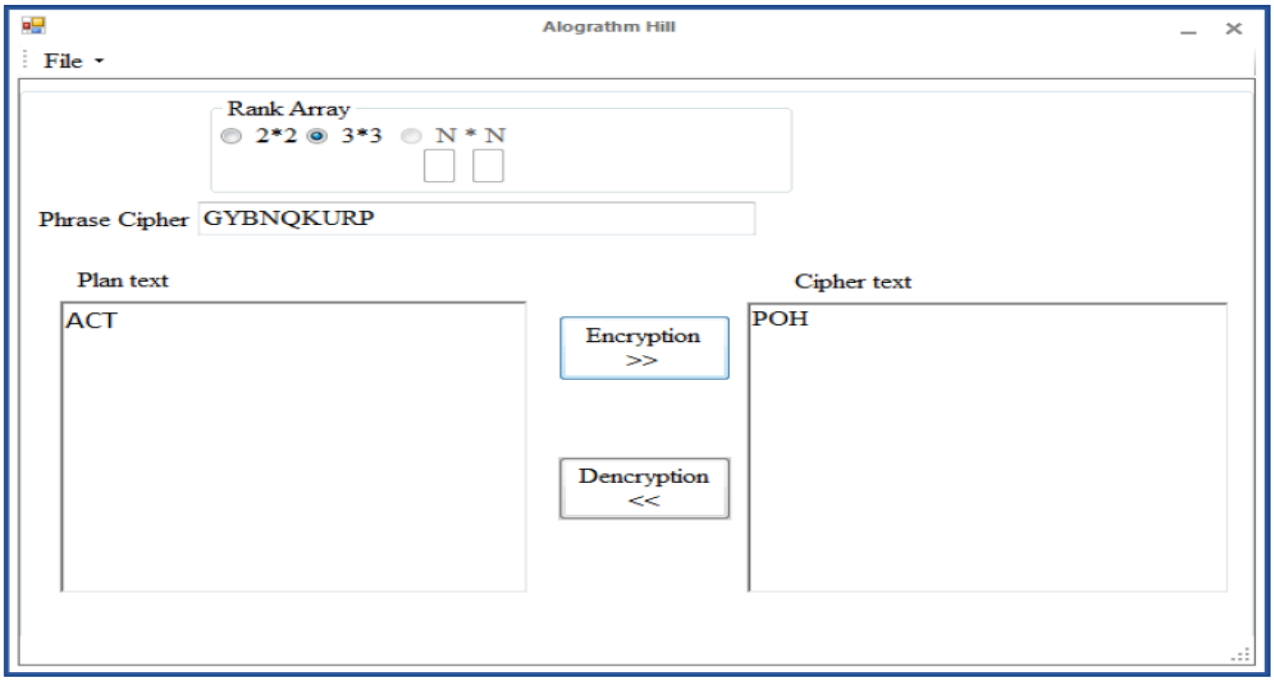
- يجب أن يكون طول النص المراد فك تشفيره من مضاعفات البعد المحدد بمعنى اذا كان البعد المحدد ٢*٢ يجب ان يكون طول النص المراد فك تشفيره من مضاعفات العدد ٢ (٢، ٤، ٨ .....) .



اختبار البرنامج : نقوم بتطبيق المثال المذكور سابقاً على المصفوفة الثلاثية 3*3 لدينا جمله التشفير GYBNQKURP ، والنص المراد تشفيره ACT نقوم بإجراء عملية التشفير فينتج النص POH كما هو موضح بالصورة التالية :



نقوم بعملية فك التشفير فينتج لدينا النص الواضح ACT كما في الصورة :



الاعمال المستقبلية للبحث :

كسر الشفرة هيل .

المراجع :

- **خوارزمية البعثرة العملية ذات الاتجاه الواحد باستخدام مصفوفة لا معكوس لها اعتماداً على تقنية هيل للتشفير - محمد ابو طه[1] ،رضوان طهبوب[2]**

- **Hill's Cipher: Linear Algebra in Cryptography – Ryan Doyle**

- **An Introduction to Hill Ciphers Using Linear Algebra- Brian Worthington**