



وزارة التعليم العالي والبحث
العلمي
جامعة ديالى
كلية التربية للعلوم الصرفة
قسم علوم الحاسوب

استخدام المصفوفات المثلثية السفلى والعليا LU Cholesk في

تطوير انظمة التشخيص

بحث مقدم

الى كلية التربية للعلوم الصرفة قسم علوم الحاسوب

وهو جزء من متطلبات نيل شهادة البكالوريوس

في تربية علوم الحاسوب

اعدادا الطالبة

زهراء محمدان محمود اسراء طحمة رشيد

بأشراف

م.م. باسم نجم الدين

٢٠١٨ م

١٤٣٩ هـ

الفصل الاول

١- المقدمة

استخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب، خوفاً من وقوع الرسائل الحساسة في أيدي العدو. حيث كان يوليوس قيصر (Julius Caesar) من أشهر القدامى الذين امتنوا الكتابة المعماة حيث قام بتطوير خوارزمية تعمية (مشفر Cipher) سميت باسمه شفرة قيصر (Caesar Cipher)؛ لتأمين اتصالاته ومراسلاته مع قادة جيوشه [5][2].

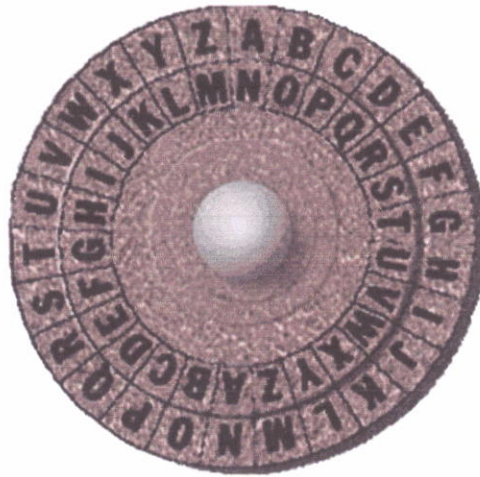
وظهرت فيما بعد العديد من الآلات التي تقوم بعمليات التشفير، ومنها Machine Enigma وشكل الكمبيوتر في بدايات ظهوره وسيلة جديدة للاتصالات الآمنة، وفك تشفير رسائل العدو. واحتكرت الحكومات في فترة الستينات حق التشفير وفك التشفير. وفي أواخر الستينات أسست شركة IBM مجموعة تختص بأبحاث التشفير، ونجحت هذه المجموعة في تطوير نظام تشفير أطلقت عليه اسم لوسيفر (Lucifer) [2]. وكان هذا النظام مثير للجدل، ورغم تحفظات الحكومة الأمريكية عليه لاعتقادها بعدم حاجة الشركات والمؤسسات الخاصة إلى أنظمة التشفير، إلا أنه قد حقق انتشاراً واسعاً في الأسواق. ومنذ ذلك الحين، أخذت العديد من الشركات تقوم بتطوير أنظمة تشفير جديدة، مما أبرز الحاجة إلى وجود معيار لعمليات التشفير.

ومن أبرز المؤسسات التي أسهمت في هذا المجال، المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standards and Technology- NIST) المعروف سابقاً باسم المكتب الوطني الأمريكي للمعايير (U.S. National Bureau of Standards)، إذ طور هذا المعهد عام ١٩٧٣ معياراً أطلق عليه معيار تشفير البيانات (Data Encryption Standard- DES). ويستند هذا المعيار إلى خوارزمية لوسيفر (Lucifer algorithm) التي تستخدم مفتاح تشفير بطول ٥٦ بت (bit)، وتشرط أن يكون لكل من المرسل والمستقبل المفتاح السري ذاته. وقد استخدمت الحكومة هذا المعيار الرسمي عام ١٩٧٦، واعتمدته البنوك لتشغيل آلات الصراف الآلي (ATM).

١-١- بعض طرق التشفير الكلاسيكية :-

١-١-١ خوارزمية قيصر (Caesar Cipher)

في التشفير ، شفرة قيصر هي واحدة من أبسط تقنيات التشفير و أكثرها انتشاراً . و هي نوع من أنواع خوارزميات التبدل التي يتم فيها تبديل كل حرف من النص الأصلي بحرف اخر حسب مفتاح التشفير المتفق عليه بين المرسل والمستقبل ، فمثلا لو كان مفتاح التشفير ٣ سيتم تدوير العجلة المبينة في الشكل [1] وتزحف الاحرف ثلاث مرات ، حيث سيتم استبدال كل حرف بالحرف الثالث بعده في الأبجدية فمثلاً نستبدل الحرف A بالحرف D و الحرف B بالحرف E (كما في الجدول ١) و هكذا بالنسبة لباقي الاحرف [5][2] .



الشكل (١) يوضح تقنية شفرة قيصر (Caesar Cipher)

Plain Text	A	B	C	D
Key	3	3	3	3
Cipher Text	D	E	F	G

الجدول رقم (١) يوضح استخدام خوارزمية قيصر (Caesar Cipher)

٢-١-١ خوارزمية الاستبدال (Substitution Cipher)

إن شفرة القيصر هي إحدى أنواع شفرات الاستبدال و لكنها من أبسط الأنواع حيث يمكن ابتكار شفرات أكثر تعقيداً باستخدام شفرة الاستبدال. فمثلاً يوضح الجدول (٢) خوارزمية استبدال بسيطة باستخدام المفتاح . ويمكن استخدام خوارزمية استبدال أكثر تعقيداً بمقابلة كل حرف من الأبجدية بحرف آخر لا على التعيين [5][2] .

Key	+1	+2	+3	+1	+2	+3	+1	+2
Plain	A	I	T	P	E	D	I	A
Cipher	B	K	W	Q	G	G	J	C

جدول (٢) يوضح استخدام خوارزمية الاستبدال (Substitution Cipher)

٣-١-١ الخوارزميات المتناظرة وغير المتناظرة (Asymmetrical and

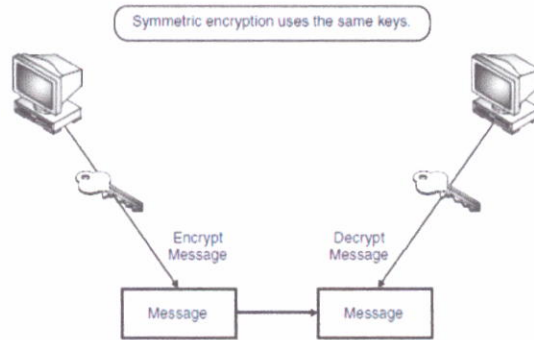
asymmetrical)

لا تعتمد الخوارزميات الحديثة للتشفير على الخوارزمية فقط؛ حيث أن معظم الخوارزميات معروفة ومنتشرة وإنما تعتمد على رقم يدعى المفتاح Key يتم استعماله في خوارزمية تشفير المعلومات وفي خوارزمية فك التشفير أيضاً حيث تعتبر عملية فك شفرة المعلومات في حال وجود المفتاح عملية سهلة وسريعة بينما هي عملية صعبة جداً إن لم تكن مستحيلة في معظم الحالات العملية .

تنقسم الخوارزميات التي تستخدم المفتاح إلى قسمين :

١-٣-١-١ خوارزمية التشفير المتناظرة : (encryption symmetric)

وفيها يكون مفتاح التشفير متماثلاً في كلا الطرفين وخوارزمية التشفير مشابهة لخوارزمية فك التشفير ($E = D$, $K_e = K_d$) [5].

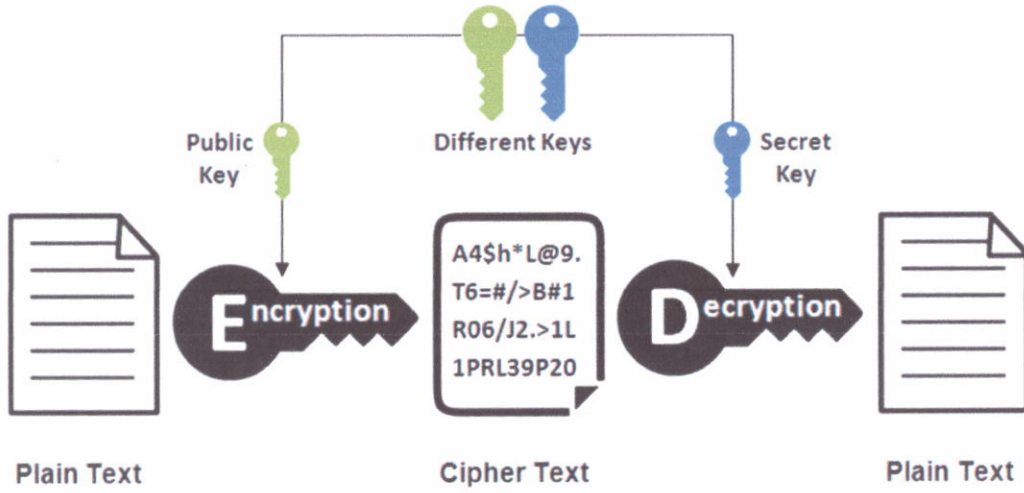


الشكل (٢) يوضح التشفير بالمفتاح المتناظر Encryption Symmetric

١-٣-٢-١ خوارزمية التشفير غير المتناظرة (encryption asymmetric)

وفيها يكون ($K_d \neq K_e$, $D \neq E$) وتسمى هذه الطريقة التشفير بالمفتاح العمومي .
(Algorithm key Public) حيث يسمى مفتاح التشفير K_e بالمفتاح العام key Public
والمفتاح K_d بالمفتاح الخاص (key Privet) [5].

Asymmetric Encryption



الشكل (٣) يوضح التشفير بالمفتاح غير المتناظر Asymmetric Encryption

٢-١- المصفوفات :

أخذ التحليل العددي منحى جديد كعلم منفصل وذلك في الأربعينات والخمسينات من القرن الماضي التطورات الحديثة زادت من مجال استخدام الطرائق العددية التي تسببت في الاستمرار بتطوير الحواسيب الرقمية بذواكر كبيرة وساهمت في حل المسائل الواقعية بخوارزميات رياضية [1]. هذا يعني انه يمكن اليوم معالجة أكثر المسائل تعقيدا من خلال كميات كبيرة من الحسابات العديدة ساهمت هذه التطورات في جعل الهوة بين الرياضيات والعلوم الاخرى والتكنولوجيا صغيرة خلال العقود الاخيرة. الطرائق الرياضية والنماذج الرياضية المتقدمة أصبحت تستخدم أكثر فأكثر في العديد من المجالات كما في الطب، والاقتصاد، والعلوم الاجتماعية.

١-٢-١ المصفوفات المثلثية :

١- يقال أن المصفوفة U من النوع $n \times n$ مصفوفة مثلثية عليا إذا كان $U_{ij} = 0$ لكل $i > j$. أي أن عناصر المصفوفة التي تقع تحت القطر تكون أصفاراً.

٢- تسمى المصفوفة L من النوع $n \times n$ مصفوفة مثلثية دنيا إذا كان $L_{ij} = 0$ عندما $i < j$. هذا يعني أن كل عناصر المصفوفة والتي تقع فوق القطر مساوية للصفر.

٣- المصفوفة القطرية $D=(d_{ij})$ من النوع $n \times n$ هي المصفوفة التي عناصرها تحقق $d_{ij}=0$ لكل $i \neq j$. إذا كانت $d_{ii}=1$ من أجل $i=1,2,\dots,n$ فإن المصفوفة في هذه الحالة تسمى مصفوفة أحادية ويرمز لها بالرمز I_n . لمصفوفة الأحادية الخاصية التالية:

$$I_n A = A I_n$$

حيث A مصفوفة مربعة من النوع $n \times n$.

١-٢-٢- التحليل المثلثي للمصفوفات

يتم تحليل المصفوفة A من النوع $n \times n$ إلى حاصل ضرب المصفوفتين $LU = A$ ، حيث L مصفوفة مثلثية دنيا و U مصفوفة مثلثية عليا من النوع $n \times n$.

لإنجاز هذا التحليل لا بد أن يكون لدينا قيم L_{ii} و U_{ii} من أجل $i = 1,2,\dots,n$. هناك في الواقع ثلاثة أساليب مشهورة وهي كالتالي [1]:

- ١- أسلوب دوليتيل (Doolittle) ويتضمن وضع $L_{ii}=1$ من أجل $i = 1,2,\dots,n$.
- ٢- أسلوب كروت (Crout) وهنا يتم وضع $U_{ii}=1$ من أجل $i = 1,2,\dots,n$.
- ٣- أسلوب شولسكي (Cholesk) وفي هذا الأسلوب نضع $L_{ii}=U_{ii}$ لجميع قيم i . يتم تطبيق هذا الأسلوب عندما تكون المصفوفة A مصفوفة موجبة بالتحديد [1].

استخدم الباحث التحليل المثلثي للمصفوفات لإيجاد نظام تشفير جديد حيث وجد الباحث طريقة لزيادة أمن المعلومات وتطوير طرق التشفير واستخدم طريقة LU Cholesk حيث قام الباحث بتطبيق الطريقة أعلاه في إنشاء نظام تشفير المكون من ثلاث أوجه بحيث يستطيع أي شخص إرسال البيانات بكل امنية وسرية عالية دون ان يتم اعتراضها من قبل اشخاص غير مخولين لذلك.

الفصل الثاني

٢- الدراسات السابقة

هناك العديد من الخوارزميات التي أجريت في مجال تطوير خوارزميات التشفير حيث :-

هناك نوعان من خوارزمية التشفير المتمثل الشفرات الكتلية والشفرات الحزمية؛ الشفرات الكتلية تشفر النص العادي فيقطع مثل DES و AES. ومن الأمثلة على ذلك شفرة قيصر وشفرة الوسادة الواحدة وغيرها أو بت واحد في الأدبيات هناك العديد من الأبحاث التي ركزت على التشفير الكلي والتشفير الحزمي .

قد ناقش الباحث Ragheb Toemeh ,Subbanagounder Arumugam (٢٠٠٨) التشفير التعويضي من خلال تطبيق الخوارزمية الجينية. ان امكانية تطبيق الخوارزمية الجينية للبحث في المساحة الرئيسية لنظام التشفير قد تم دراستها . في شفرة فيجنير تم تخمين حجم المفتاح من خلال تطبيق الخوارزمية الجينية. وان تحليل التردد تم استخدامه كعامل أساسي في الوظيفة الموضوعية [13] .

اما الباحث John Justin M, Manimurugan S (٢٠١٢) فقد ركز أساسا على أنواع مختلفة من تقنيات التشفير الموجودة، وتأطير جميع التقنيات معا كمسح للأدبيات .هدفت لدراسة تجريبية واسعة لتنفيذ مختلف تقنيات التشفير المتاحة. كما ركزت على تقنيات تشفير الصور، وتقنيات تشفير المعلومات، والتشفير المزدوج وتقنيات التشفير القائم على مبدأ التشويش. وتمد هذه الدراسة إلى بارامترات الأداء المستخدمة في التشفير [6] . وقام الباحث Prakash Kuppuswamy, Saeed Q Y Al-Khalidi (٢٠١٢) باقتراح خوارزمية مفتاح متمائل جديد باستخدام وحدات ٣٧ . وينبغي أن يتم توزيع المفتاح المتمائل بطريقة سرية مضمونة [9] .

وقام الباحث محمد مزيد دريباتي Mohamed Mezid Deribati (٢٠١٤) بوصف خوارزميتين متوازيتين لإيجاد حل جمل المعادلات الخطية خماسية الأقطار المتناظرة المربعة من المرتبة n .تتطلب الخوارزميتين $N = 2$ معالجا وكل معالج يمتلك n ذاكرة موضعية. تتضمن الخوارزمية الأولى كتابة المصفوفة خماسية الأقطار على شكل جداء مصفوفتين كل منهما مصفوفة ثلاثية الأقطار.

حيث اقترح الباحث محمد مزيد دريباتي حل جمل المعادلات الخطية ثلاثية الأقطار الناتجة خوارزمية متوازية. أما الخوارزمية الثانية فتتضمن تحليل المصفوفة خماسية الأقطار . أن الخوارزميتين فعاليتين وأن إحدهما أسرع من الأخرى بمرتبتين لحل نفس مسائل الاختبار (٢).

من مراجعة الدراسات أعلاه تمت ملاحظة ان جميع الابحاث ركزت على الية استخدام مفتاح متناظر دون الاعتماد على شكل المعادلة المستخدمة في عملية التشفير مما يعني ان هناك توجه واحد في عملية تحليل الشفرة ..الا وهو الاعتماد على مبدأ الاحتمالية في تخمين قيمة المفتاح المتناظر فقط دون الاخذ بنظر الاعتبار البارامترات الاخرى . بينما في الطريقة المقترحة فإنه من الصعوبة جدا ان يتم تخمين المفتاح كونه سيكون جزءا مدموجا ضمن خوارزمية التشفير نفسها ،

حيث سيتم دمج المفتاح مع قيم مصفوفة مثلثية سفلى التي نتجت عن تحويل المصفوفة A الى مصفوفتين مصفوفة مثلثية علوا ومصفوفة مثلثية سفلى وذلك بتطبيق طريقة التحليل Choliscy .
مما يجعل الامر معقدا على محلل الشفرة في تخمين اي من المفتاح او الدالة المستخدمة في عملية التشفير .

الفصل الثالث

٣- منهجية البحث :

٣-١- خوارزميات التشفير وفك التشفير :-

تتكون الطريقة من ثلاث خوارزميات وهي خوارزمية توليد المفتاح وخوارزمية التشفير وخوارزمية فك التشفير :

٣-١-١- توليد المفتاح :-

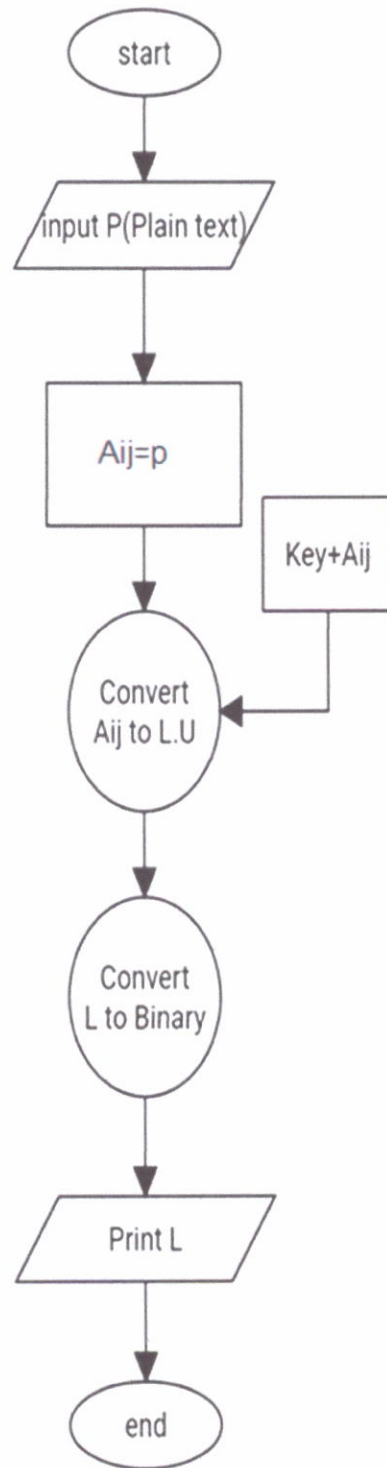
- 1 Input Key
- 2 $\text{Key} + A_{ik}$

٣-١-٢- خوارزمية التشفير :-

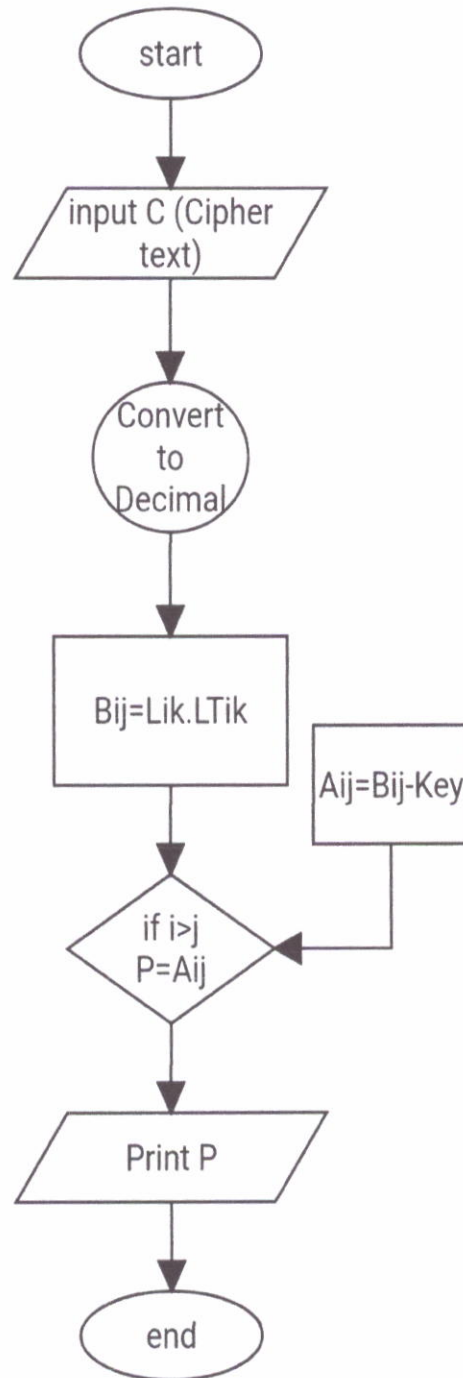
- 1- input p (plain text)
- 2- $B_{ij} = p$
- 3- $A_{ij} = B_{ij} + \text{key}$
- 4- $A_{ij} = L_{ik} \cdot U_{kj}$
- 5- Count L_{ik} to binary
- 6- Print L_{ik}

٣-١-٣- خوارزمية فك التشفير :-

- 1- Input c (cipher text)
- 2- Convert c to decimal
- 3- $a = L_{ik} \cdot L_{ik}^t$
- 4- If $i > j$ then $p = a_{ij}$
- 5- $P = p - \text{key}$
- 6- Print p

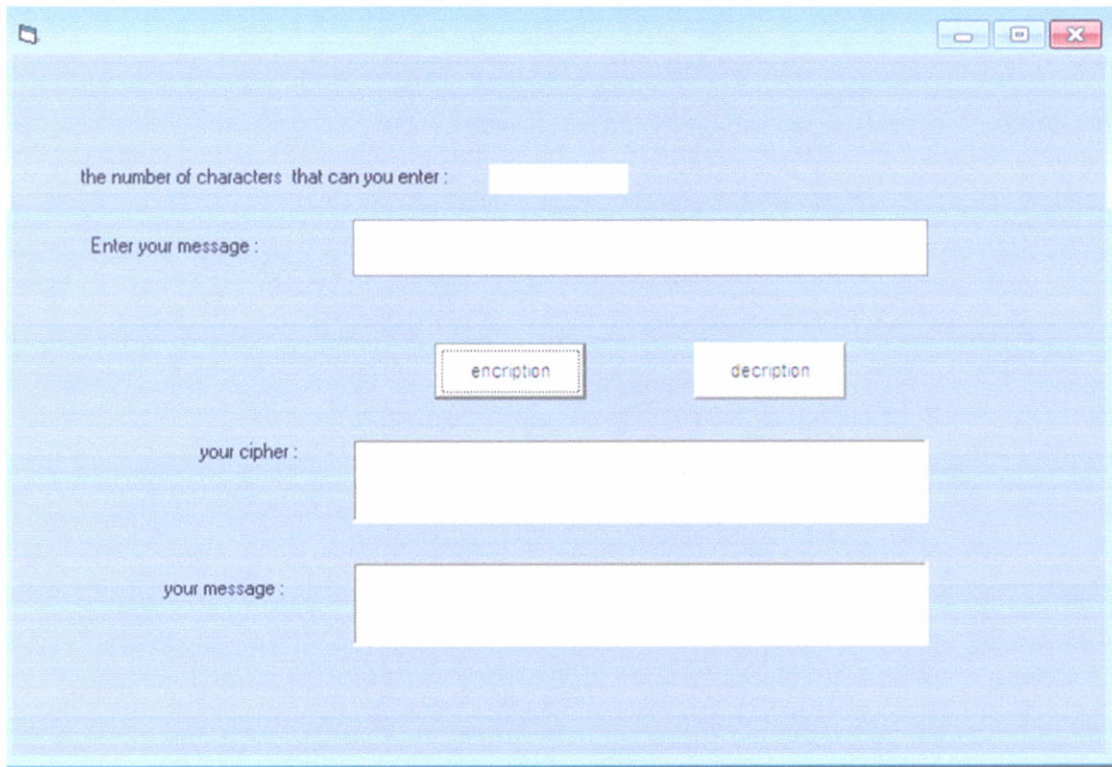


الشكل (٤) يوضح مخطط خوارزمية التشفير



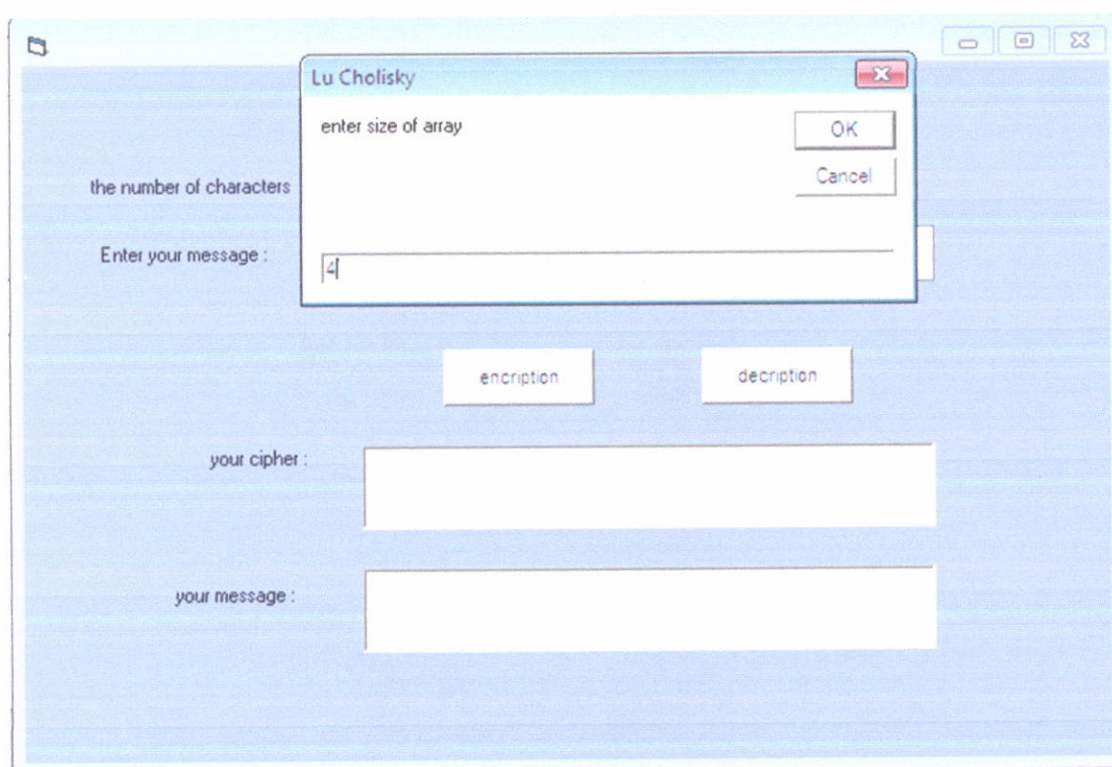
الشكل (٥) يوضح مخطط خوارزمية فك التشفير

٣-٢- عملية التشفير :



الشكل (٦) يوضح واجهة بداية برنامج التشفير وفك التشفير

٣-٢-١- الشكل (٧) يوضح واجهة البرنامج حيث يقوم المستخدم بإدخال عدد الصفوف او الاعمدة لمصفوفة مربعة ، سيمثل المثلث العلوي او السفلي للمصفوفة عدد احرف الرسالة التي يستطيع المستخدم ادخالها .



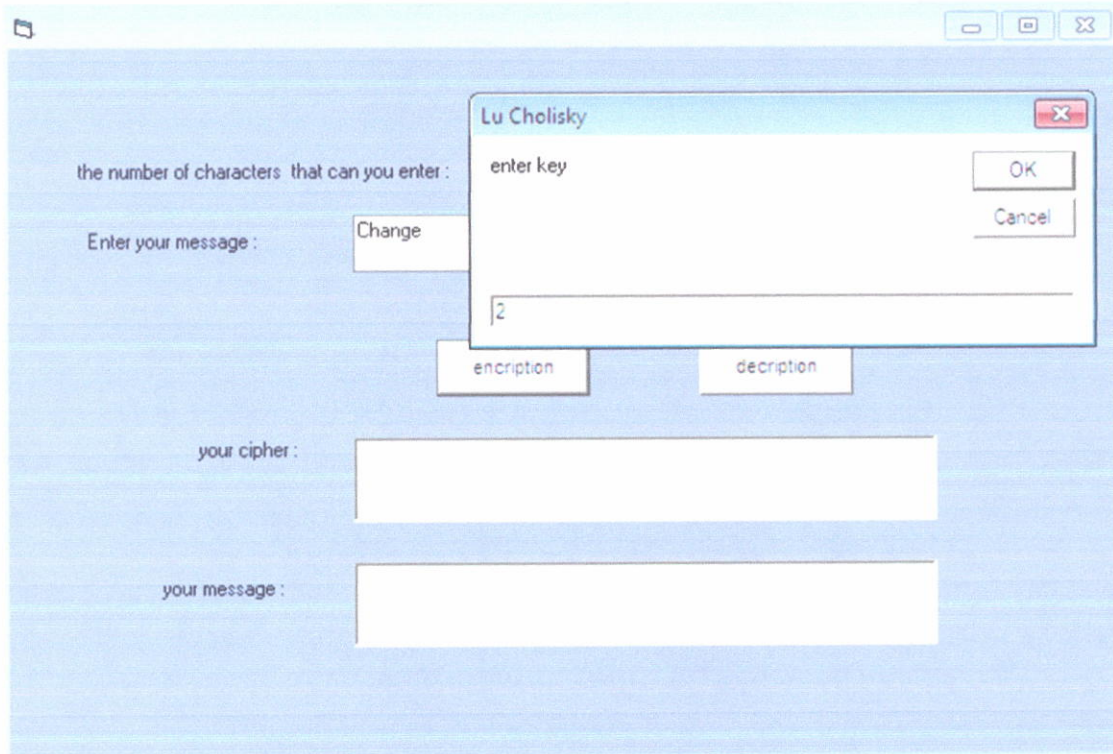
الشكل (٧) يوضح واجهة قراءة حجم المصفوفة

الشكل (٨) يوضح واجهة البرنامج حيث يقوم المستخدم بإدخال النص الصريح Plain Text في المربع الخاص بإدخال الرسالة ، والذي يتكون من ثلاث حروف حسب حجم المصفوفة التي يحتاج إليها المستخدم ، بينما يظهر في المربع اعلى مربع ادخال الرسالة مربع يوضح عدد الاحرف التي سيقوم المستخدم بإدخالها .

The screenshot shows a software window with a light blue background. At the top, there are standard window control buttons (minimize, maximize, close). Below these, the text "the number of characters that can you enter : 6" is displayed next to a small input field containing the number "6". Underneath, the label "Enter your message :" is followed by a text input field containing the word "Change". In the center, there are two buttons: "encryption" on the left and "decryption" on the right. Below the buttons, the label "your cipher :" is followed by a large empty text input field. At the bottom, the label "your message :" is followed by another large empty text input field.

الشكل (٨) يوضح واجهة ادخال الرسالة

الشكل (٩) يوضح واجهة ادخال مفتاح التشفير ، بعد ضغط المستخدم على زر التشفير
-٣-٢-٣ encryption يظهر المربع الخاص بإدخال مفتاح التشفير و الذي يكون عبارة عن n
من الارقام .



الشكل (٩) يوضح واجهة ادخال مفتاح التشفير

الشكل (١٠) يوضح انتهاء عملية التشفير وظهر الشفرة المكونة من ارقام ثنائية
-٤-٢-٣ . (1,0)

the number of characters that can you enter : 6

Enter your message : Change

encryption decryption

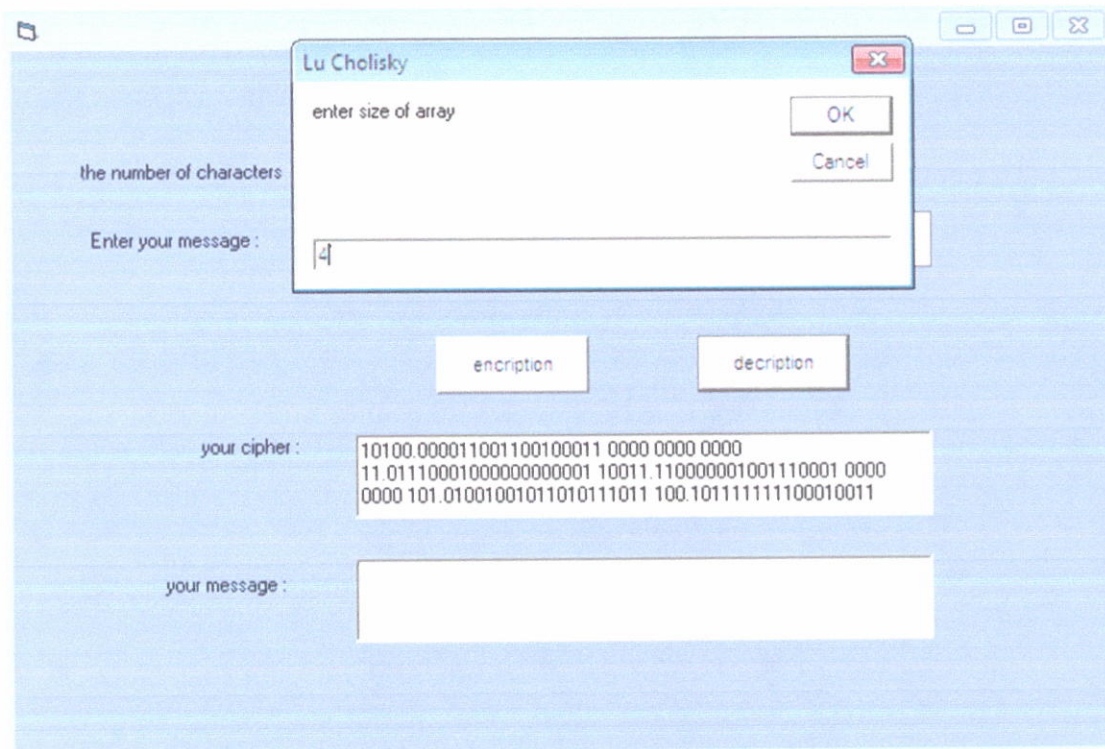
your cipher : 10100.000011001100100011 0000 0000 0000
11.01110001000000000001 10011.110000001001110001 0000
0000 101.01001001011010111011 100.101111111100010011

your message :

الشكل (١٠) يوضح انتهاء عملية التشفير

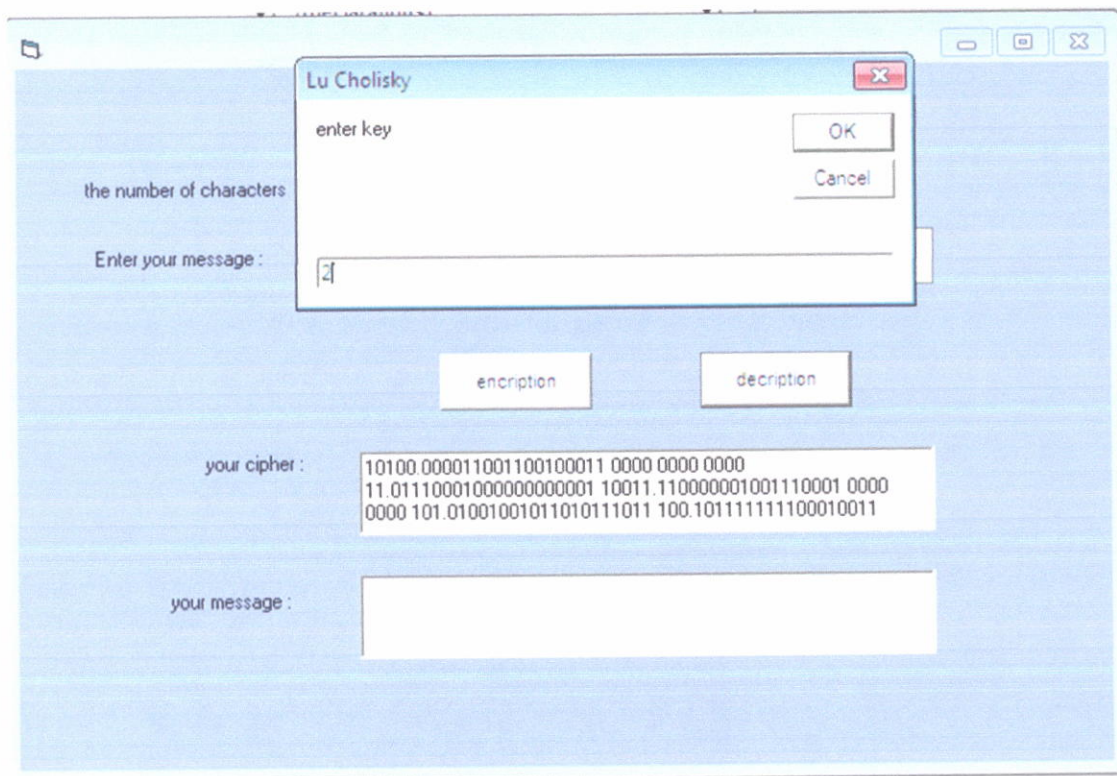
٣-٣- عملية فك التشفير :

١-٣-٣- الشكل (١١) يوضح واجهة بداية فك التشفير حيث عند ضغط المستخدم على زر decryption فك التشفير يظهر مربع ادخال عدد الصفوف او الاعمدة الخاص بالمصفوفة .



الشكل (١١) يوضح واجهة بداية فك التشفير

الشكل (١٢) يوضح الخطوة الثانية من عملية فك التشفير وهي عملية قراءة المفتاح
 ٢-٣-٣- الذي يكون متفق عليه بين المرسل والمستقبل .



الشكل (١٢) واجهة ادخال مفتاح فك التشفير

الشكل (١٣) يوضح انتهاء عملية فك التشفير وظهرت الرسالة او النص الصريح
-٣-٣-٣- Plain text

The screenshot shows a web application interface with a light blue background. At the top, there is a header bar with a small icon on the left and three window control buttons (minimize, maximize, close) on the right. The main content area contains the following elements:

- A label "the number of characters that can you enter :" followed by a text input field containing the number "6".
- A label "Enter your message :" followed by a large text input field containing the word "Change".
- Two buttons: "encryption" and "decryption", both with dashed borders.
- A label "your cipher :" followed by a text area containing three lines of binary code:

```
10100.000011001100100011 0000 0000 0000
11.011100010000000000001 10011.110000001001110001 0000
0000 101.01001001011010111011 100.101111111100010011
```
- A label "your message :" followed by a large text input field containing the word "Change".

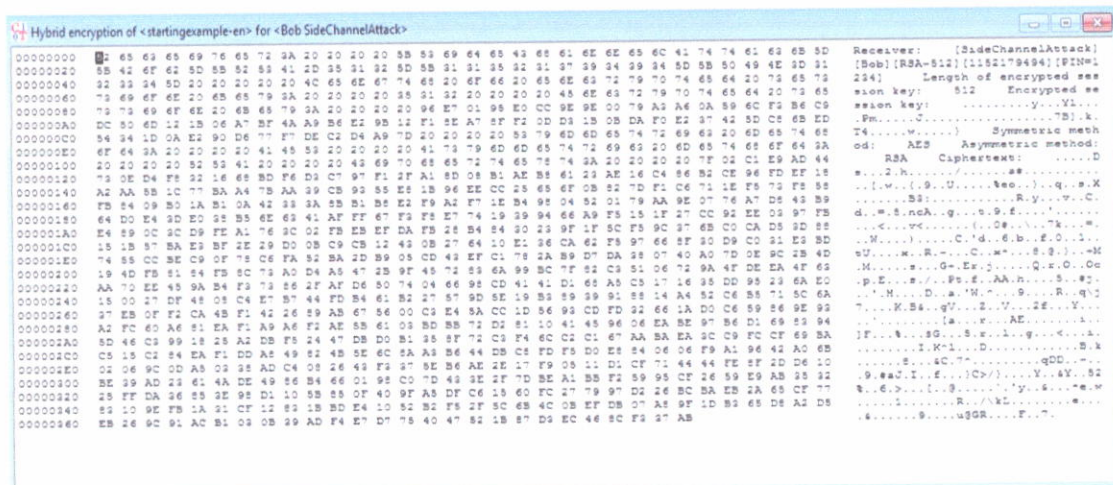
الشكل (١٣) يوضح واجهة انتهاء عملية فك التشفير

الفصل الرابع

٤- مناقشة النتائج :-

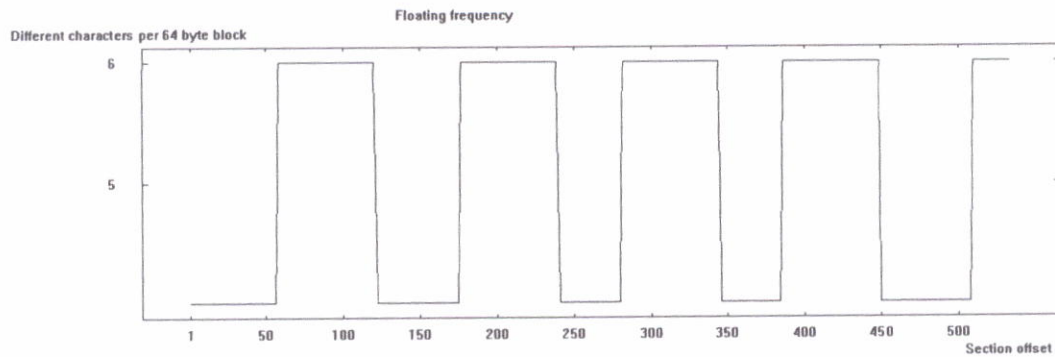
بعد اجراء الاختبارات الخاصة بعمليات التشفير على الشفرة الناتجة واستخدام برامج تحليل الشفرة 1. Cryp tool و 2. Cryp tool توصلنا الى النتائج الموضحة في الشكل (١٤) و (١٥) و (١٦) و (١٧) . والتي اثبتت عجز ادوات التحليل على كسر وتحليل الشفرة و بينت مدى قوة الخوارزمية المقترحة .

٤-١- الشكل (١٤) يوضح النتائج المحصلة من تحليل الشفرة باستخدام طريقة side channel attack1 . حيث اظهرت النتائج عدم قدرة الطريقة (التي تدعى من اقوى طرق تحليل الشفرة) على كسر وتحليل الشفرة وحسب ما موضح في الشكل (١٤) .



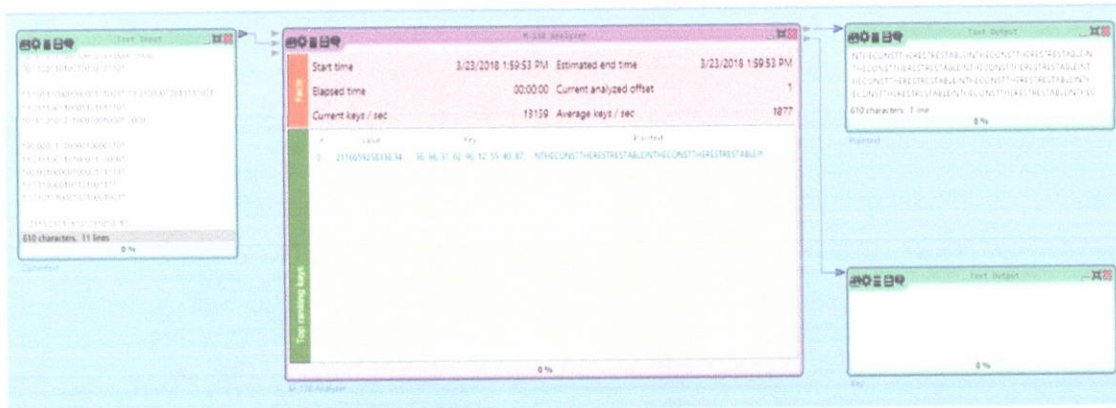
الشكل (١٤) side channel attack1

الشفرة . frequency . floating frequency الطريقة على كسر الشفرة . الشفرة



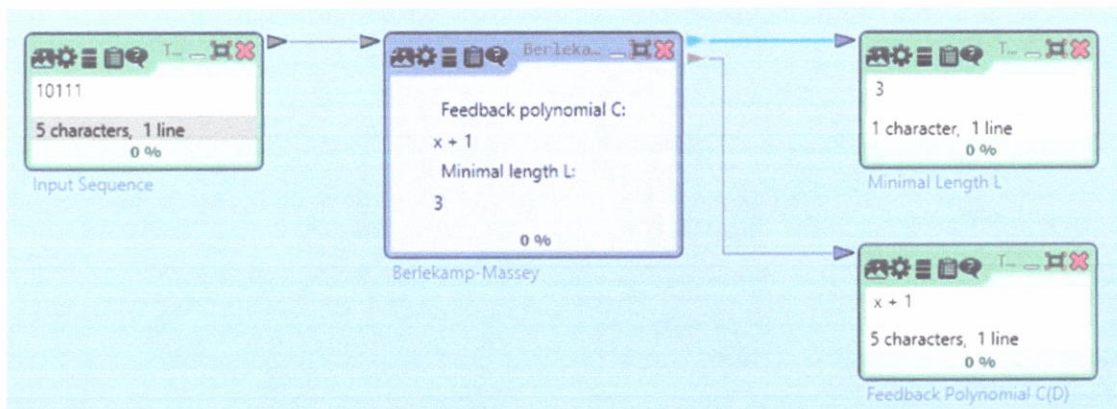
الشكل (١٥) floating frequency

الشكل (١٦) M-138 Analyzer . كما يظهر في الشكل (١٦) عدم استطاعة الطريقة على كسر الشفرة .



الشكل (١٦) M-138 Analyzer

٤-٤- الشكل (١٧) يوضح النتائج المحصلة من تحليل الشفرة باستخدام Burl-Kamp Massy Attack وتظهر النتائج عدم امكانية الطريقة على تحليل الشفرة .



الشكل (١٧) Burl-Kamp Massy Attack