Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

# تصميم خوارزمية تشفير باستخدام الارقام السومرية

الهام حسن عزيز/ مدرس مساعد وفاء محمود جاسم / أستاذ مساعد
قسم أنظمة الحاسوب قسم صحة المجتمع
elhamhassan72@yahoo.com wafamahmod396@yahoo.com
هيئة التعليم التقني/الجامعة التقنية الشمالية /المعهد التقني كركوك

**المستخلص :-**

يعد الاستخدام الواسع لتقنية الحاسوب والاتصالات في ارسال واستلام الرسائل والمعلومات يحتاج الى طرق وخوارزميات جديدة لحماية هذه المعلومات عن طريق التشفير (Encryption).

ان هدف البحث هو تصميم خوارزمية جدبدة تقوم بتشفير المعلومات باستخدام الارقام السومرية والنظام العددي السومري حيث ابتكر السومريين الكتابة التصويرية (البكتوكرافات) وتمكنوا من ابتكار الارقام التي يرجع تأريخها الى ٣٣٠٠ ق.م ,تم خلال البحث تصميم خوارزمية تشفير تعويضية باستخدام لغة فيجول بيسك ( Visual Basic) لتحويل الرسائل المدخلة (النص الصريح ) سواءا كان حروف او رموز او اعداد الى اشكال صورية(رمزية) والتي هي عبارة عن سلسلة من الارقام المسمارية (النص المشفر ) غير مفهومة للمستلم مما يؤدي الى عدم معرفة المتطفل لمحتويات الرسالة وبالتالي يزيد من درجة امنية وصلادة المعلومات المرسلة وذلك لكون النظام الاعداد السومرية غير معروفة لدى العديد من الناس وامكانية استخدامها في تشفير الرسائل والتقارير الطبية .استنتجت من خلال الدراسة بسهولة استخدام الخوارزمية وعدم تكلفتها او احتياجها الى اجهزة اضافية وبالمرونة العالية. كما اوصت الدراسة بتطوير الخوارزمية باستخدام طرق تشفير مزدوجة اكثر قوة التي تعمل على اكثر من مفتاح مع امكانية تطويرها باستخدام طرق تشفير ولغات برمجية كـ(Matlab,vb.Net)اخرى بهدف زيادة قوة التشفير .

**الكلمات المفتاحية : التشفير ، الخوارزمية التعويضية ، النظم العددية السومرية ,تصميم.**

٢٠١٦ ٢٠١٧

*Kirkuk University Journal /Scientific Studies (KUJSS)*
**Volume 12, Issue 3, June 2017**
**ISSN 1992 – 0849**

# Design Adaptive Encryption Algorithm by using Sumerian numbers

**Elham hassan Aziz**
**Assistant Lecturer**
**Computer System Dept.**
**wafamahmod396@yahoo.com**

**Wafa Mahmood Jasim**
**Assistant professor**
**Community Health Dept.**
**elhamhassan72@yahoo.com**

**Foundation of Technical Institute/Northern Technical University**
**Kirkuk Technical Institute**

## Abstract

The widely uses of computer and communication technology in sending and receiving the message and information need a new processes and algorithms for protection them and this was done by Encryption .

The study aimed to design a new algorithm encryption by using the Sumerian number and numerical system which was innovated through the induction of a new pictographic picture and they prepared the recent number since 3000 B.C.

During the research design compensatory encryption algorithm using Visual Basic to convert the input messages (explicit text), whether it was letters or symbols or prepare
to form a(symbol) token, which is a series of cuneiform symbols (cipher text)Incomprehensible to the recipient, leading to lack of knowledge of the spam message contents and thus increases the degree of security and hardness information sent And to the fact that the Sumerian numbers are not known to many people with the possibility of use in the letters and medical reports encryption .During the conclusion of the study easily use the algorithm and

the lack of cost or their need additional hardware and high flexibility. The study also recommended the development of the algorithm using double encryption more powerful ways which operates the keys and with the possibility of developed using encryption methods of programming languages such as (matlab, vb.net) and the other, in order to increase the strength of encryption .

**Keyword: Encryption , substitution algorithm, Sumerian system number, design**

٢٠١٧ ٢٠١٦

**١-المقدمة :**

تعتبر سرية المعلومات من المواضيع المهمة التي تأخذ حيز مهم من الجانب الاكاديمي والتطبيقي من خلال توفير طرق وخوارزميات جديدة لحماية المعلومات التي يتم تبادلها خلال وسائل التي يتم فيها استخدام الحاسوب وخصوصا نحن نعيش

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

في عصر ولادة الحكومات الالكترونية. ورغم تزايد الاهتمام بسرية المعلومات حديثا الا ان "أمن المعلومات " استخدم قبل ولادة وسائل تكنولوجيا المعلومات ،حيث يعود الى ٤٠٠٠ سنة حيث كان الانسان يفضل اخفاء كتابته .

نتيجة الى الاستخدام الهائل للمعلومات والبيانات من خلال الانترنيت ولاهمية المعلومات فانه يتطلب تأمين الحماية والمصداقية والموثوقية لهذه المعلومات والمحافظة عليها لذلك ظهرت وسائل حماية متنوعة مثل وضع كلمة السر ، و استخدام التشفير (Cryptography) وايضا تقنيات الاخفاء (Hiding) او تغطية المعلومات . **[ ١]**

ان عملية التتشفير للبيانات يتم من خلاله تحويل البيانات الى شفرات غير مفهومة وذلك يؤدي الى الحفاظ على سرية المعلومات وايضا يعتبر احدى طرق المحافظة على سرية المعلومات ضد اي اختراق مقصود **.[ ٢]**

يوجد هنالك عدة اهداف للتشفير منها الخصوصية او السرية ( Confidentiality ) حيث المعلومات يطلع عليها عدد محدد من الاشخاص المخولون للاطلاع على البيانات، واثبات الهوية ( Integrity) ، وكذلك تكامل البيانات ( Integrity) ويقصد بها حفظ المعلومات من اي تغيير من قبل اشخاص ليس مسموح لهم بذلك ،اضافة الى عدم الجحود ( Non-repudiation ) ويعني ذلك عدم انكار الشخص للعمل الذي قام به ،اضافة الى الجاهزية (Availability) اي توفر المعلومات عند الطلب .**[ ٢]**

كما انه استخدام خوارزميات التشفير لاي نظام معلوماتي او شبكة حاسوب تؤدي الى تحمّل الحواسيب جهد اضافي لغرض معالجة النصوص الواضحة وتحويلها من نصوص واضحة الى نصوص مشفرة وبالعكس ، ويختلف هذا الجهد حسب تعقيد الخوارزمية ولذلك هنالك عدة مباديء اساسية يجب ان تؤخذ بنظر الاعتبار عند تصميم خوارزمية جديدة من حيث الدقة والامنية والسرعة والاقتصاد والمرونة **.[ ٣]**

تعتمد جميع الخوارزميات في عملية التشفير على مبدئين عامين وهما التعويض ( substitution) والذي فيه يتم اعادة ربط كل عنصر من عناصر النص الواضح (بت، حرف ، مجموعة بتات ، او حروف ) مع عنصر اخر ، وكذلك النقل ( transposition) والذي يتم خلاله اعادة ترتيب جميع عناصر النص الواضح .**[ ٣]**

**٢ـ هدف البحث :**

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

يهدف البحث الى تصميم خوارزمية تشفير تعويضية(Substitution cipher) وهي تقنية ابدال النص الواضح بحرف او اعداد او رموز وذلك باستخدام (ASCII) "American standard code for information interchange " حيث يتم ابدال كل حرف او رقم بما يقابله في جدول الاسكي المخزون داخل الحاسبة وهو جدول ثابت (Standard)[ ٤] [٥]. ومن ثم تمثيلها بالارقام السومرية، من خلال تصميم جدول لكافة الارقام والحروف الموجودة في لوحة المفاتيح وما يقابلها من (ASCII) اضافة الى الارقام السومرية وكما موضح في ملحق (١) اضافة الى جدول (٦) ,استنادا للنظام العددي الذي استخدمه السومريين ، لغرض عملية التشفير وفك التشفير في هّذه الخوارزمية .

**٣-اهمية البحث**:

تم استخدام الاعداد السومرية في بحثنا لغرض التشفير ، حيث استخدم السومريين النظام العشري منطلقين من عدد اصابع اليد ثم تطور الابداع الفكري عندهم في الالف الثالث قبل الميلاد في فترة فجر السلالات حيث تطور النظام العشري الى النظام الستيني وايضا اكتشفوا مبدأ "المرتبة العددية " .[ ٦]

ان عملية تحليل او فك الشفرة من خلال دراسة الرسالة المشفرة بهذه الطريقة تعتبر صعبة لكون الخط المسماري غير معروف لدى الكثيرين وكذلك النظام العددي للسومريين غير مفهوم ولا يمكن معرفته الا من قبل المختصين بهذا المجال اضافة الى المرونة الكبيرة لهذه الطريقة في امكانية تطويرها .

**٤-البحوث السابقة:**

توجد الكثير من الدراسات عن الخطوط والارقام السومرية منها دراسة وصفية للباحث ابراهيم هاندرك والمقدمة سنة ٢٠١٠ بعنوان "دراسة وصفية عن الخطوط السومرية " والتي تحدث فيها عن الخط السومري وطريقة استخدام هذه الرمو[ ٧ ]،كما توجد دراسات حول استحداث طرق تشفير جديدة من قبل الباحثين حيث قدمت الباحثة نجاة حميد قاسم في سنة ٢٠١١ بنشر بحثها بعنوان "خوارزمية مقترحة لكشف

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

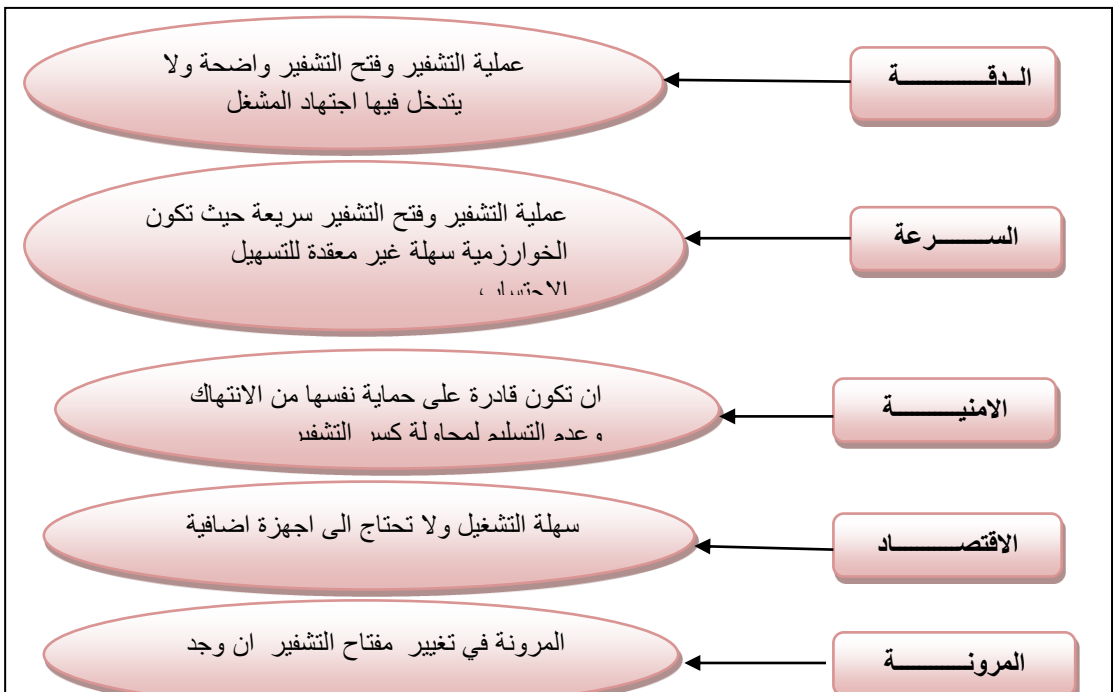
التلاعب او التزوير في الرسائل والوثائق المرسلة عبر الشبكة "[ ٨]، وكذلك الباحثة غادة محمد طاهر الدباغ في سنة ٢٠١٣ بحثها "استخدام طريقة البعثرة العشوائية في تشفير الوسائط المتعددة " [ ٩ ]،كما قام الباحثان معن عبد الخالق يحيى و عمر تحسين سهيل سنة ٢٠١٠ بتقديم بحثهم المعنون "طريقة جديدة لاستخدام الصور الرقمية في اخفاء الملفات الصورية "[ ١٠ ].

**٥-الجانب النظري :-**

توجد مجموعة من التعاريف والمباديء الاساسية في عملية التشفير لابد من ذكرها في عملية التشفير التقليدية وهي:

**٥- ١-التشفير(Encryption)** : هي عملية ترميز الرسالة حتى يكون معناها غير مفهوم .بينما فتح الشفرة ( Decryption) هي العملية المعاكسة للتشفير وتعني عملية تحويل الرسالة الى شكلها الطبيعي .[ ٤]

**٥-٢ -خصائص التشفير الجيدة :**[ ٦ ] ان الشكل (١) يبين اهم خصائص التشفير الجيدة



Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

**شكل ( ١) خصائص التشفير الجيدة**

**٥-٣** - ان خوارزمية التشفير هي عبارة عن دالة رياضية تستخدم في عملية التشفير او فتح الشفرة.[٤]ويتكون التشفير التقليدي عادة من نص واضح (الرسالة الاصلية ) (plaint text) والتي تتعامل معها خوارزمية التشفير( Encryption Algorithm ) كمدخلات ،بينما تكون مخرجاته هي الرسالة المشفرة (Cipher text)،اضافة الى مفتاح ان كان موجود، ولابد من وجود خوارزمية لفتح التشفير والتي تعتبر عبارة عن معكوس خوارزمية التشفير. **[ ٣ ]**

يمكن تصنيف انظمة التشفير الى :-

اولا-نوع العمليات المستخدمة في تحويل النص الواضح الى النص المشفر وكافة الخوارزميات تعتمد على مبدأين وهما كما يلي:-

- التبديل ( Substitution) حيث يتم فيها تحول كل عنصر في النص الواضح (بت وحرف او مجموعة من البتات و الاحرف ) الى عنصر اخر .
- التعويضية ( Transposition) حيث يتم في هذا النوع اعادة ترتيب عناصر النص الواضح للحصول على النص المشفر .

ثانيا- عدد مفاتيح المستخدمة في الخوارزمية وهنالك منظومتان :

- المتناظرة ( Symmetric) في هذه الحالة يتم استخدام المرسل والمستقبل نفس المفتاح ويسمى التشفير التقليدي (تشفير بالمفتاح الواحد).
- غير المتناظرة (Asymmetric) في هذه الحالة استخدام المرسل مفتاح يختلف عن ما يمكن ان يستخدمه المستلم ويسمى هذا النوع التشفير ذات المفتاح العام (ذات المفتاحين).

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

ثالثا- طريقة معالجة النص الواضح ويوجد لها نوعان وهما :

•التشفير الكتلي (Block Cipher) حيث يتم فيها معالجة عناصر ادخال الكتلة الاولى وينتج عن ذلك كتلة واحـــــدة

كأخراج لكتلة واحدة .

•التشفير السيلي (Stream Cipher) و يتم فيها معالجة عناصر الادخال بصورة مستمرة ، ناتج عنصر واحـــد كل

مرة وهكذا تتم معالجة جميع العناصر .[ ٤ ]

**٤-٥ مقارنة طريقة التشفير المقترحة مع طريقة تشفير (تعويضية )-:**

يمكن مقارنة طريقة التشفير المقترحة مع طريقة شفرة قيصر وكما موضح ادنا :-

**جدول (١) مقارنة الشفرة التعويضية (شفرة قيصر)مع التشفير باستخدام الارقام السومرية**

| اوجه المقارنة | التشفير باستخدام شفرة قيصر | التشفير باستخدام الارقام السومرية |
|---|---|---|
| **التعريف** | - يعتمد على استبدال كل حرف بحرف اخر يكون تسلسله ثابت بعده في الحروف الابجدية | يعتمد على استبدال كافة الرموز كالارقام والحرف الى الارقام السومرية. |
| **قوة التشفير** | -تمتاز بالبساطة وامكانية التخلص من النص الصريح بعد تشفيره مباشرة. | -تمتاز كونها غير معروفة وامكانية تشفير كافة الرموز الموجودة في لوحة المفاتيح<br>-تحويل كل رمز الى مايقبله من صور الارقام المتكونة من اكثر من صورة يزيد من قوة التشفير |

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

| | | |
|---|---|---|
| **محاسنه** | -لغة النص الصريح يمكن معرفتها ويمكن قرائتها | -لا يمكن فك تشفير النص المشفر كون النظام العددي السومري غير معروف.<br>-تمتاز بالمرونة وامكانية زيادة قوة التشفير فيها |
| **مساوئها** | - تعتبر خوارزمية معروفة لذلك يمكن بسهولة فك التشفير. | - يحتاج مساحة خزن كبيرة لكون النص المشفر عبارة عن مصفوفة صورية |
| **اوجه المقارنة** | التشفير باستخدام شفرة قيصر | التشفير باستخدام الارقام السومرية |
| **التعريف** | - يعتمد على استبدال كل حرف بحرف اخر يكون تسلسله ثابت بعده في الحروف الابجدية | يعتمد على استبدال كافة الرموز كالارقام والحرف الى الارقام السومرية. |
| **قوة التشفير** | -تمتاز بالبساطة وامكانية التخلص من النص الصريح بعد تشفيره مباشرة. | -تمتاز كونها غير معروفة وامكانية تشفير كافة الرموز الموجودة في لوحة المفاتيح<br>-تحويل كل رمز الى مايقبله من صور الارقام المتكونة من اكثر من صورة يزيد من قوة التشفير |
| **محاسنه** | -لغة النص الصريح يمكن معرفتها ويمكن قرائتها | -لا يمكن فك تشفير النص المشفر كون النظام العددي السومري غير معروف.<br>-تمتاز بالمرونة وامكانية زيادة قوة التشفير فيها |
| **مساوئها** | - تعتبر خوارزمية معروفة لذلك يمكن بسهولة فك التشفير. | - يحتاج مساحة خزن كبيرة لكون النص المشفر عبارة عن مصفوفة صورية |

### ٥-٥ الارقام والاعداد السومرية

تعتبر الحضارة السومرية من اقدم الحضارات في العالم حيث يرجع الى الالف الخامس قبل الميلاد واستخدموا الكتابة المسمارية على الالواح الطينية وكانت من سمات التطور للارقام كما يلي :

١- استخدموا نظامين للترقيم الاول بسيط ويعتمد على طريقة الترتيب البسيط للارقام . كما هو واضح في جدول رقم (٢)

**جدول رقم(٢) تمثيل مرتبة الاحاد السومرية**

| العدد بالنظام العشري | ١ | ٢ | ٣ | ٤ | ٥ | ٦ | ٧ | ٨ | ٩ | ١٠ |
|---|---|---|---|---|---|---|---|---|---|---|
| العدد بالنظام السومري |  | | | | | | | | | |

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

٢- ثم ابتكروا للاعداد التي تتجاوز الستين "المرتبة العددية " اي تحديد قيمة العدد بالنسبة الى مرتبته من الاعداد الاخرى وعن طريق العددين الواحد والعشرة كما هو واضح في الجدول رقم(٣).

**جدول رقم (٣)تمثيل مرتبة العشرات السومرية**

| عدد بالنظام العشري | ١٠ | ٢٠ | ٣٠ | ٤٠ | ٥٠ | ٦٠ | ٧٠ | ٨٠ | ٩٠ | ١٠٠ |
|---|---|---|---|---|---|---|---|---|---|---|
| العدد بالنظام السومري | | | | | |  | | | | |

٣- طور السومريين نظامهم الرقمي باتجاه النظام الستيني اي مضاعفات العدد ٦٠ (١-١٠-٦٠-٦٠٠-٣٦٠٠.....)واعتبره مقاس في التعاملات الحسابية ل جدول رقم (٤).

كان اختيارهم للنظام الستيني لاسباب عدة منها ان النظام يقبل القسمة على اعداد كثيرة دون الباقي وبذلك تجنبوا الحصول على الكسور اثناء العمليات الحسابية .

٤- ان الحجم والمكان له تأثير مهم في كتابة الاعداد السومرية في النظام الستيني .

**جدول رقم (٤) تمثيل المرتبة العددية في النظم العددية السومرية**

| العدد | الاحاد | مرتبة الستينات x60 | ×٣٦٠٠ |
|---|---|---|---|
| ١ | | | |
| ١٠ |  | | |
| ٦٠ | | | |
| ٦٠+١=٦١ | | | |
| ٦٠×٦٠=٣٦٠٠ | | | |

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

| | | | |
|---|---|---|---|
| ٣٦٠٠×٢=٧٢٠٠ | | | |

**٦- الجانب العملي** :

تم تنفيذ خوارزمية التشفير باستخدام ( visual basic) اضافة الى استخدام برنامج ( Photo Shop) في تشكيل الاعداد السومرية حيث تم العمل على مرحلتين :_

المرحلة الاولى : تشكيل الاعداد السومرية من خلال الحصول على صور لارقام مرتبة الاحاد (١ الى ١٠ ) اضافة الى صورة الرقم ( ٦٠) من الانترنيت **[١٥]**، وتطبيق كافة التأثيرات الخاصة بالصورة واستعارة اجزاء مختلفة من صور الارقام وتجميعها معا وتعديل ابعاد الصورة من خلال استخدام الادوات المختلفة لبرنامج Photo Shop وهي (copy , paste، select imagersize ,crop , cut).**[١١]** ودمجها من اجل الحصول على ارقام تحتوي على مرتبة العشرات والستينات (كما يتم تسميتها في النظام العددي السومري ).

المرحلة الثانية :- تم بعد ذلك خزن هذه الارقام في مصفوفة صورية احادية البعد تحتوي على رموز مختلفة بحيث كل خلية في المصفوفة تحتوي على صورة العدد ،و يمكن الاستدلال عليها فيما بعد من خلال فهرست المصفوفة ( index) .

المثال التالي يوضح لنا كيفية تشكيل الاعداد في النظام العددي لدى السومريين :-

مثال : لغرض الحصول على العدد ١١٥ يكون كالتالي:-

**جدول رقم(٥) تكوين الاعداد السومرية**

| العدد المطلوب | مكونات العدد | الشكل النهائي |
|---|---|---|
| ٦٠ + ٥٠ + ٥=١١٥ | + + | |

حيث نلاحظ من الجدول اعلاه ان العدد ١١٥ يتكون من ثلاث مراتب الاحاد الرقم ٥ وشكله ( ) والخمسين وشكله( ) ومن مرتبة الستينات وشكله ( ).

تم تصميم جدول والذي هو عبارة عن (ASCII) لكافة الرموز والارقام والحروف التي نحتاجها في تشفير الرسالة المدخلة مضافا اليها الارقام السومرية وحسب نظام الترقيم العددي لدى اجدانا السومريين وكما هو مبين في الجدول رقم(٦) وملحق (أ).

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

**جدول رقم (٦) تمثيل بعض الاحرف بـ(ASCII) والاعداد السومرية**

| Character | Ascii | Picture of Sumerian no | Numerical representation of Sumerian no | Character | Ascii | Picture of Sumerian no. | Numerical representation of Sumerian no. |
|---|---|---|---|---|---|---|---|
| back space | 8 | | | { | 123 | | |
| tab | 9 | | | \| | 124 | | |
| enter | 13 | | | } | 125 | | |
| z | 122 | | | ~ | 126 | | |

**٦-١-خوارزمية برنامج التشفير**

١- البداية

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

٢-قراءة الرسالة المراد تشفيرها (Plaint text)

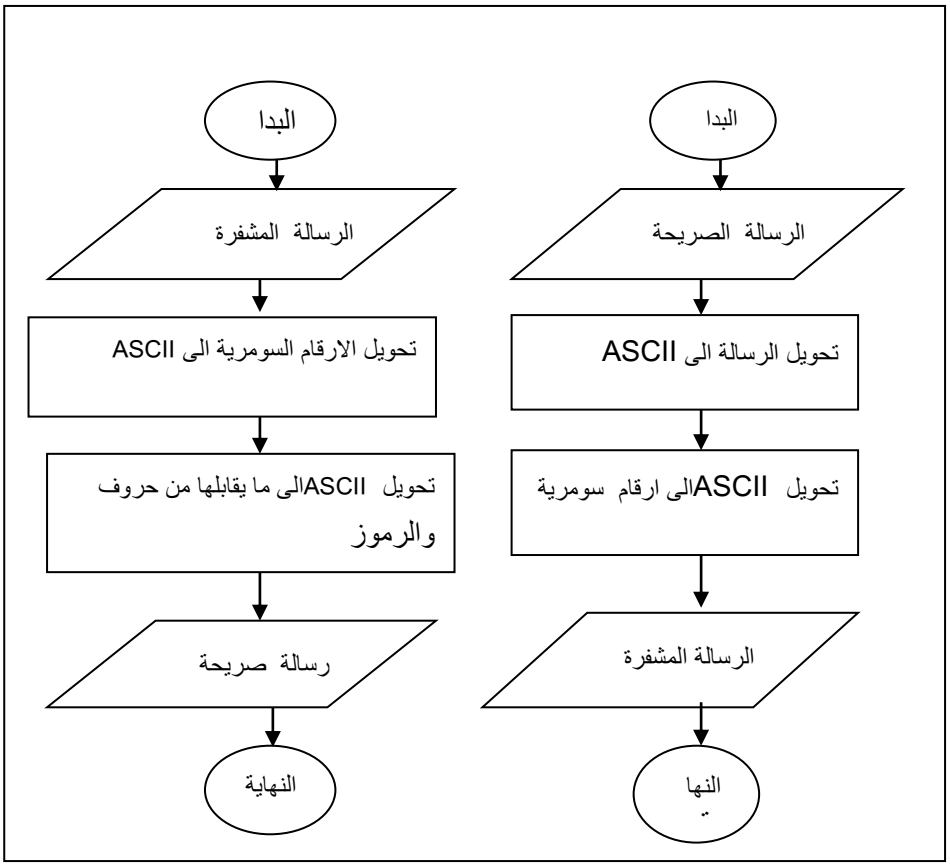
٣-تحويل كل رمز من الرسالة الى مايقابلها من ( ASCII) .

٤-تحويل رموز( ASCII) الى صور الارقام السومرية باستخدم الجدول المرفق في ملحق رقم (١) وخزنها في مصفوفة صورية.

٥- الحصول على الرسالة المشفرة ( Cipher text).

٦- النهاية

اما لفك التشفير فهي تشبه خطوات خوارزمية التشفير ولكن بالعكس.وكما موضح في الشكل (٢)




**الشكل رقم(٢) المخطط الانسيابي للخوارزمية البحث**

المثال التالي يوضيح كيفية عمل خوارزمية التشفير التي تتم خلال البرنامج

١- نفرض لدينا كلمة ( Computer)

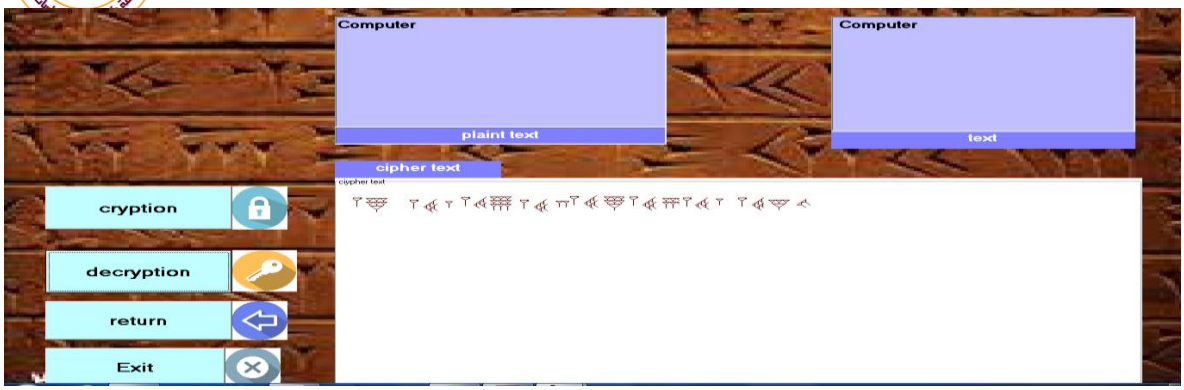
Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

٢- يقوم البرنامج بتحويل حروف النص المدخل الى الاسكي كود ومن ثم يقوم بإيجاد الرقم بالنظام العددي السومري معتمدا على الجدول ( ١) وكما موضح في الجدول رقم (٧) اما لفك التشفير فتكون بنفس الخطوات ولكن بالاتجاه المعاكس وهذا ما نلاحظه في الشكل ( ٣ )

**جدول رقم(٧) تحويل كلمة (computer)الى ارقام سومرية**

| plaint text | ascii code | picture of Sumerian number | | | numerical representation of Sumerian no. |
|---|---|---|---|---|---|
| C | 67 | | | | |
| o | 111 | | |  | |
| m | 109 | | | | |
| p | 112 | | | | |
| u | 117 | | | | |
| t | 116 | | | | |
| e | 101 | | | | |
| r | 114 | | | | |

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849




شكل (٣) يوضح تشفير كلمة كومبيوتر

**٦-٢- مراحل تشغيل النظام :-**

**الشكل (٤) الواجهة الرئيسية**

الواجهة الرئيسية الشكل (٤)تحتوي على عدة اختيارات وهي :

1-البداية

٢- ادخال النص المراد تشفيره

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

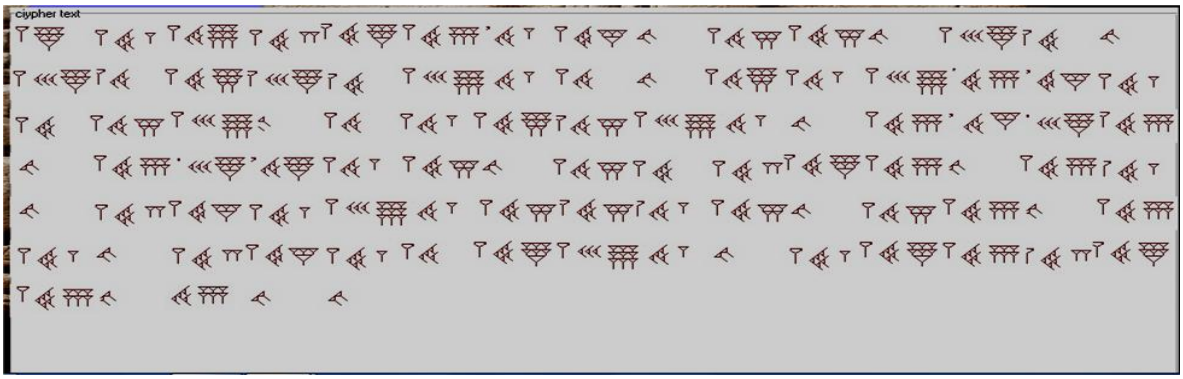
٣-اختيار خوارزمية التشفير .

٤- فك التشفير او الرجوع الى الواجهة الرئيسية

٥-الخروج

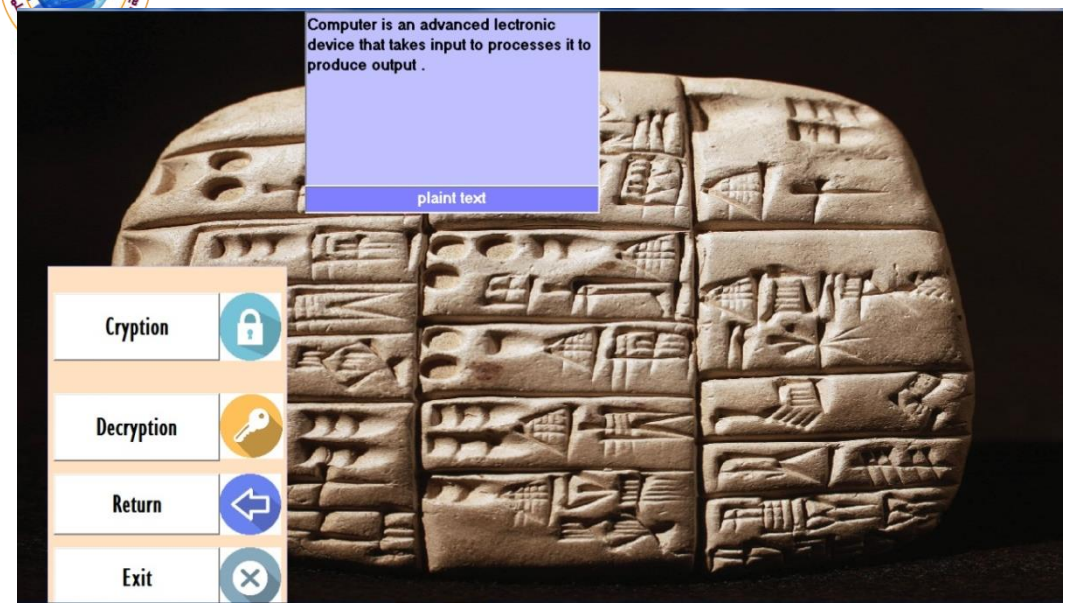
اما طريقة عمل النظام يتم عن طريق ادخال نص صريح (الرسالة المراد تشفيرها ) ومن خلال البرنامج يتم تحويل كل حرف او رمز الى (ASCII) ومن ثم يتم تحويل اسكي الى الرمز المقابل له في الارقام السومرية وحسب ما هو موجود في الملحق (١) الذي تم تصميمه خلال البحث حيث يحتوي الجدول على الاعداد السومرية (صور تشفير) الاحرف والارقام والرموز الشائعة والمستخدمه في لوحة المفاتيح والتي تم استخدامه خلال عملية التشفير لغرض الحصول على الرسالة المشفرة (Cipher text) .

لضغط على مفتاح التشفير ، كما موضح في الشكل رقم (٦) يتم الحصول على النص المشفر التالي :

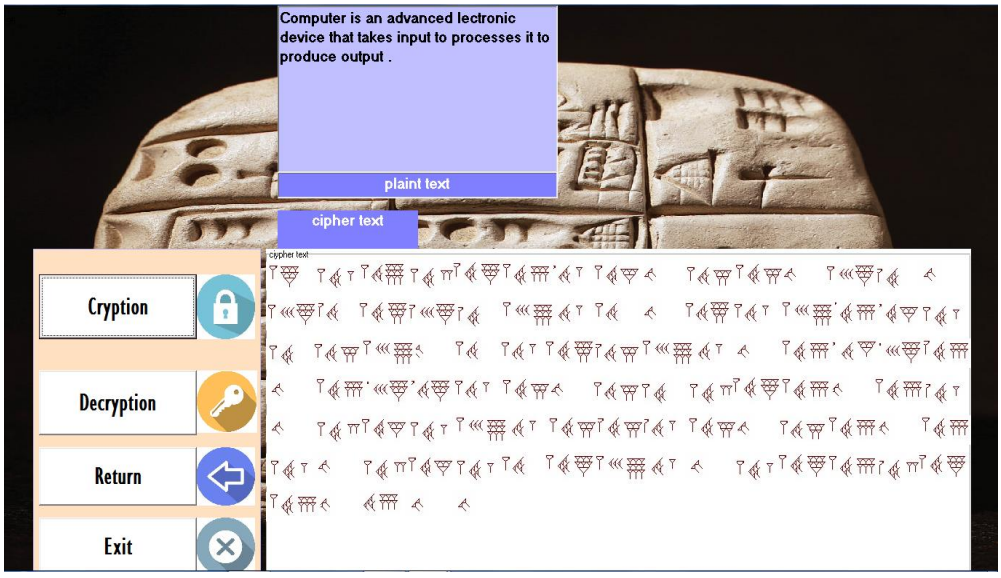



اما لغرض فك التشفير فتكون العملية عكسية حيث يتم قراءة النص المشفر ومن ثم تحويل الرسالة المشفرة (Cipher text)الاعداد السومرية الى (ASCII) ومن ثم الى الرسالة الاصلية ( Plaint text) وكما واضح في الشكل (٧) .

*Kirkuk University Journal /Scientific Studies (KUJSS)*
**Volume 12, Issue 3, June 2017**
**ISSN 1992 – 0849**

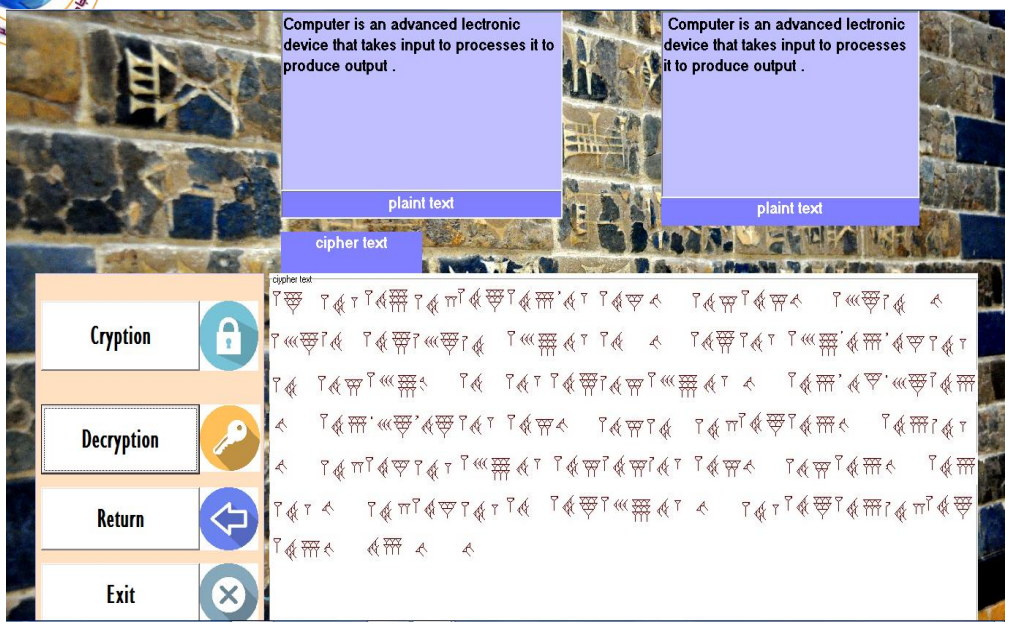



**الشكل (٥) واجهة ادخال الرسالة الصريحة**




الشكل (٦ ) عملية التشفير

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849




الشكل (٧ ) فك التشفير

## الاستنتاجات والتوصيات :

ان عملية كسر الشفرة تكاد ان تكون صعبة كون ان النص المشفر غامض وغير مفهوم حيث ان الارقام السومرية غير معروفة لدى الكثير من الناس في الوقت الحالي ، كما تمتاز هذه الخوارزمية بالمرونة ويمكن استخدامها في علمية تشفير الرسائل او التقارير الطبية ، اضافة الى ذلك تعتبر الخوارزمية سهلة وغير مكلفة ولاتحتاج الى اجهزة اضافية .

يمكن تطوير الخوارزمية من خلال استخدام طرق تشفير مزدوجة اكثر قوة كالخوارزميات التي تعمل على توليد اكثر من مفتاح مثل (RSA,DES) وغيرها من طرق التشفير بالاضافة الى استخدام الارقام السومرية ، مع امكانية بناء نظام الكتروني متكامل لترجمة الالواح الطينية المكتوبة بالخط المسماري لغرض التعليم والترجمة.

وبما ان الارقام السومرية عبارة عن اشكال صورية يمكن اعادة تنفيذ خوارزمية البحث باستخدام لغات البرمجة اخرى مثل ماتلاب (Matlab) مستفيدين من خصائص هذه اللغة في التعامل مع الصور في تشكيل الارقام واستخدام خوارزميات الاخفاء والتشفير في تطوير هذه الخوارزمية .

## المصادر

[١] الحمامي، علاء حسين والحمامي محمد علاء، (٢٠٠٨ )" إخفاء المعلومات الكتابة المخفية والعلامة المائية"، أثراء للنشر والتوزيع عمان ،الاردن ،ص(٢٨-٣٤) .

[٢] الارياني،اروى يحيى، (٢٠٠٨)،" اساسيات تحليل وتصميم نظم المعلومات "،ط١ ،شعاع للنشر والعلوم ، سوريا ، ص198

[٣]محمد "سجى ابراهيم و محمد ،فارس ادريس ،(٢٠١٣) ،"طريقة مقترحة للاخفاء داخل ملفات الصوت"،*مجلة الرافدين لعلوم الحاسوب والرياضيات* ،المجلد(١٠)،العدد(١)،ص(٢٨٥-٢٩٥).

[٤]الحمامي، د.علاء حسين واخرون، (٢٠٠٧)،"تكنولوجيا امنية المعلومات وانظمة الحماية"،طبعة الاولى،دار وائل للنشر والتوزيع،عمان, الاردن ،ص(١٠٠، ١٢٤).

[٥] صادق ،دلال ،واخرون،( ٢٠٠٨)،"امن المعلومات "،دار اليازوري العلمية للنشر والتوزيع ،عمان الاردن ،ص١٠٨.

[٦] شطب ،د.محمد ،"الارقام والاعداد في وادي الرافدين "متاح على الموقع :
http://al-nnas.com/ARTICLE/MShatab/nm2.pdf

[٧] هندرك،ابراهيم ،(٢٠١٠)،"دراسة وصفية للخطوط المسمارية "،كلية العلوم الانسانية ،جامعة ليدن ,هولندا، متاح على الموقع :
https://openaccess.leidenuniv.nl/handle/1887/16107

[٨] قاسم،نجاة حميد،(٢٠١١)،" خوارزمية مقترحة لكشف التلاعب والتزوير في الرسائل والوثائق المرسلة عبر الشبكة"،*مجلة علوم ذي قار*،المجلد(٣)،العدد(١)،ص( ١١١-١٢١).

[٩] الدباغ،غادة محمد طاهر،( ٢٠١٣)،"استخدام البعثرة العشوائية في تشفير الوسائط المتعددة "،*مجلة مجلة الرافدين لعلوم الحاسوب والرياضيات "*،المجلد(١٠)،العدد(١)،ص(١٠٩-١٢٢) .

[١٠] يحيى،معن عبد الخالق واخرون،( ٢٠١٠)"طريقة جديدة لاستخدام الصور الرقمية في اخفاء الملفات النصية السرية"،*مجلة التقني*،مجلد(٢٣)،العدد(٦)، ص( ٤٤-٥٤).

[١١] يوسف،مصطفى محسن، (٢٠١٣)،"تعلم photoshop 7ME "،جامعة الفيوم ،مصر،متاح على موقع: www.kutub.info_11818

[١٢] مطيع ،د.ياسر صادق،واخرون،(٢٠٠٩)،"مهارات البرمجة بلغة فيجول بيسك "،الطبعة الاولى، مكتبةالمجتمع العربي للنشر والتوزيع ،عمان ،الاردن .

[١٣] البهنسي ،سعد صديق ، واخرون،(٢٠٠٩)،"معالجة الصور بواسطة الكومبيوتر"،طبعة الاولى،مكتبة المجتمع العربي للنشر والتوزيع ،عمان ،الاردن ، ص١٥٠ .

[١٤] عيسى،رناجاسم،عيسى،رهام جسم،( ٢٠١٢)،"استخدام الخوارزميات الجينية في تشفير بيانات صورة رمادية واخفاءها في صورة"،*مجلة الرافدين لعلوم الحاسوب والرياضيات* "،المجلد(١٠)،العدد(١) ،ص(١٦٩-١٨٢).

[١٥] رشيد،د.فوزي رشيد ،(٢٠٠٩)،"قواعد اللغة السومرية "،دار صفحات للدراسات والنشر،سوريا ،ص٨١.

[16]-Loshin,Peter,"Simple Steps To Data Encryption ",(2013),Elsevier Inc.USA,internat:

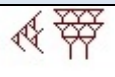
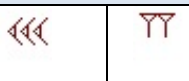
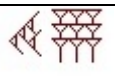
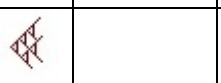
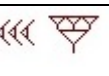
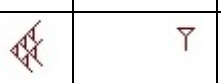
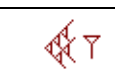
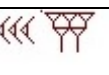
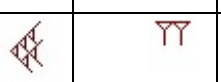
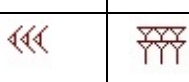
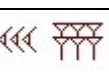
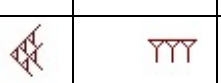
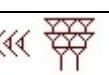
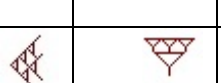
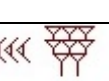
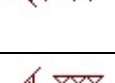
https://www.elsevier.com/books/simple-steps-to-data-encryption/loshin/978-0-12-411483-8

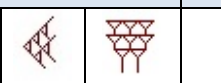
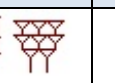
[17] Halvorson,Michael,"Microsoft visual basic step by step ",(2013), Orielly Media Inc.USA,internat:

https://jurisma1992.files.wordpress.com/2015/03/ms-microsoft-visual-basic-2013-step-by-step.pdf

**ملحق (١)Appendix بعض الاحرف الشائعة في نظام ASCII ( American standard code for information interchanging) مع مايمثلها بالنظام العدد السومري**

*Kirkuk University Journal /Scientific Studies (KUJSS)*
**Volume 12, Issue 3, June 2017**
**ISSN 1992 – 0849**

| Character | Ascii | Picture of Sumerian no | Numerical representation of Sumerian no | Character | Ascii | Picture of Sumerian no. | Numerical representation of Sumerian no. |
|---|---|---|---|---|---|---|---|
| 0 | 48 | |  | Space | 32 |  | |
| 1 | 49 | |  | ! | 33 | | |
| 2 | 50 |  | | “ | 34 | |  |
| 3 | 51 |  |  | # | 35 | |  |
| 4 | 52 |  | | $ | 36 |  |  |
| 5 | 53 |  | | % | 37 | |  |
| 6 | 54 |  | | & | 38 | |  |
| 7 | 55 | | | ‘ | 39 | | |
| 8 | 56 | |  | ( | 40 | | |
| 9 | 57 | | | ) | 41 | | |

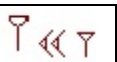
| Character | Ascii | Picture of Sumerian no | Numerical representation of Sumerian no | Character | Ascii | Picture of Sumerian no. | Numerical representation of Sumerian no. |
|---|---|---|---|---|---|---|---|
| : | 58 |  |  | * | 42 | | |
| > | 62 | | | + | 43 | | |

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 12, Issue 3, June 2017
ISSN 1992 – 0849

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ؟ | 63 | | | | | / | 47 | | | | |
| @ | 64 | | | | | T | 84 | | | | |
| A | 65 | | | | | U | 85 | | | | |
| B | 66 | | | | | V | 86 | | | | |
| C | 67 | | | | | W | 87 | | | | |
| , | 44 | | | | | X | 88 | | | | |
| - | 45 | | | | | Y | 89 | | | | |
| . | 46 | | | | | Z | 90 | | | | |
| w | 119 | | | | | X | 120 | | | | |
| | | | | | | Y | 121 | | | | |

| Character | Ascii | Picture of Sumerian no | | | Numerical representation of Sumerian no | Character | Ascii | Picture of Sumerian no. | | | Numerical representation of Sumerian no. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| M | 77 | | | | | J | 74 | | | | |
| N | 78 | | | | | K | 75 | | | | |
| O | 79 | | | | | L | 76 | | | | |
| P | 80 | | | | | k | 107 | | | | |

*Kirkuk University Journal /Scientific Studies (KUJSS)*
**Volume 12, Issue 3, June 2017**
**ISSN 1992 – 0849**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Q | 81 | | | |  | l | 108 | | | | |
| R | 82 |  |  | | | m | 109 |  | | | |
| S | 83 | |  | | | n | 110 |  | | | |
| s | 115 |  | | | | o | 111 |  | |  | |
| t | 116 |  | | | | p | 112 |  | |  | |
| u | 117 |  | | | | q | 113 |  | | | |
| v | 118 |  | | | | r | 114 |  | | | |