مجلة القادسية للعلوم الصرفة المجلد 17 العدد 1 سنة 2012
ملحق بحوث المؤتمر العلمي سنة2008 ستار بدر سدخان / سلوى شاكر بعيوي ISSN-1997-2490

طريقة مقترحة حديثة لاستخدام تقنية النوافذ لتمييز مفتاح التشفير السري

ستار بدر سدخان المالكي / جامعة بابل/ كلية التربية/ قسم الرياضيات
سلوى شاكر بعيوي / جامعة القادسية/ كلية العلوم/ قسم علوم الحاسبات

الخلاصة:-

يعتبر تمييز مفاتيح التشفير السرية من الأمور المهمة للعاملين في كسر أنظمة التشفير او في تقويم هذه الأنظمة . حيث يمكن من خلال معرفة المفتاح تمييز خوارزمية التشفير سواء كانت خوارزمية تشفير تعويضية بسيطة او خوارزمية تشفير تعويضية معقدة (متعددة الهجائيات).

يعرض البحث مدخلاً حديثا الى تحليل الشفرات خلال تقديم تقنية حديثة لتمييز مفاتيح التشفير السرية وهذه التقنية هي تقنية النوافذ المطبقة على المدرج التكراري لإحصاء تكرار الحروف العربية. تعد هذه التقنية خطوة مرادفة لتقنية مسارات التعقيد الخطي المستخدمة مع أنظمة التشفير الانسيابي. وقومت نتيجة الطريقة المقترحة من خلال تنفيذها لعدد من النصوص المشفرة بمفاتيح مختلفة. أوضحت النتائج ان الطريقة المقترحة إمكانية تطبيقها على خوارزميات تشفير مختلفة .

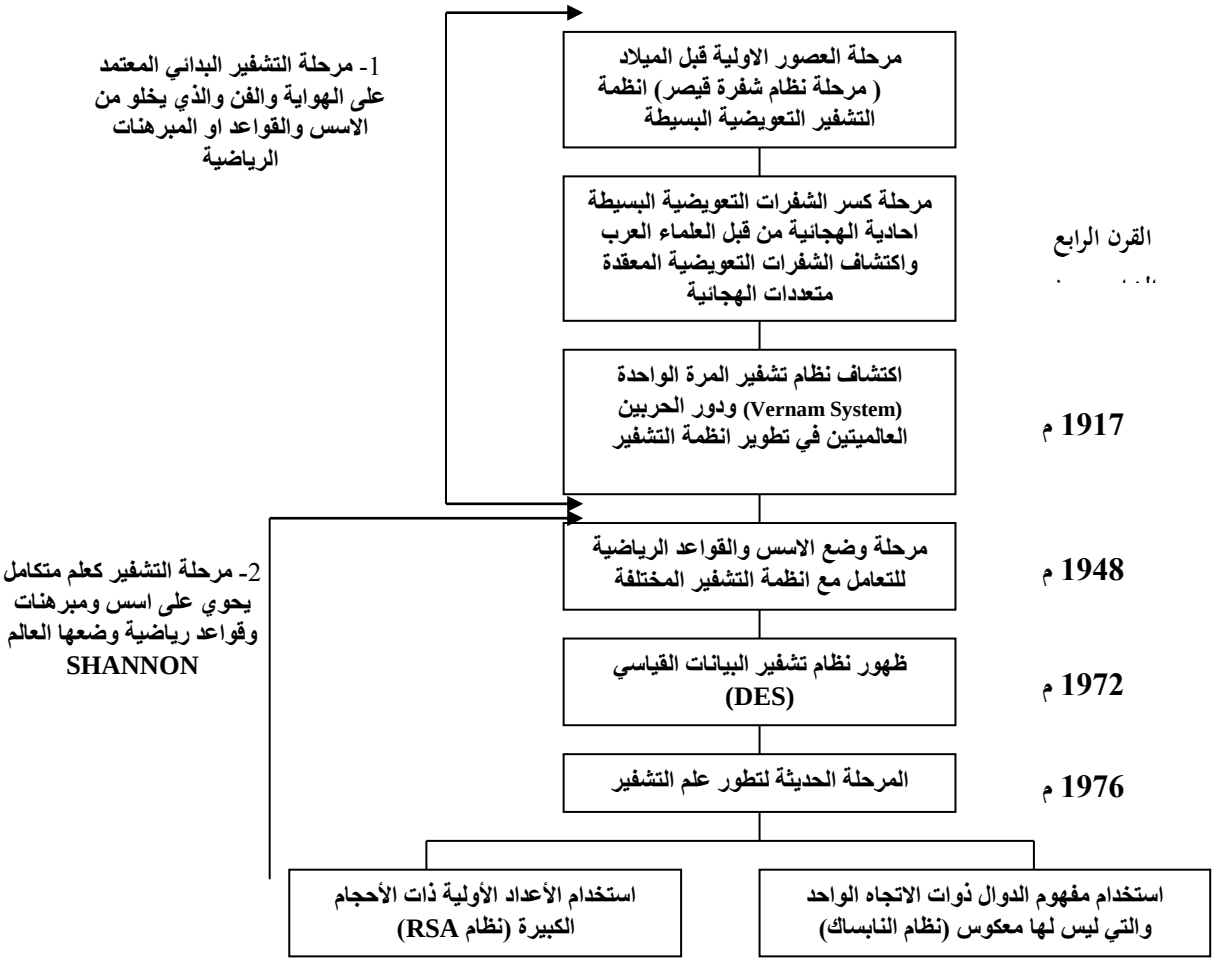
1-المقدمة

يعتبر علم التشفير وتحليل الشفرات من العلوم المتطورة باستمرار طالما كان هنالك تطورا ملموسا في الحاسبات الإلكترونية من خلال تصنيع المعالجات الدقيقة والسريعة جدا والدوائر الالكترونية الخاصة ذوات القابليات الواسعة ،وبعض التقنيات الحديثة لمعالجه الإشارة . وطالما كان هنالك تنافس بين المهتمين بصناعة (الأمن) وبين المتطفلين على خصوصيات الاخرين .

وقد نالت حماية المعلومات اهتمام كبيرا منذ آلاف السنين ، ولذلك وجد علم التشفير (*Cryptography*) لتوفير الحماية الكافية للمعلومات. يختص هذا العلم بتصميم الأنظمة الشفرية التي تحول النص الواضح الى نص مشفر وذلك لتمويه المعلومات بطريقة معينه تمنع الشخص غير المخول (المتصنت) من التعرف على محتواها.

سعى الإنسان منذ قديم الزمان لإيجاد الصور الملائمة للحفاظ على خصوصية رسائله وكتاباته وما تحتويه من كم هائل معلوماتي من تدخل الأطراف المتطفلة ، ولذلك ابتكر الإنسان عبر الزمن طرائق وأساليب عديدة مختلفة لتامين أمنية معلوماته ، فتراوحت هذه التقنيات بين البسيطة والمعقدة اعتماد على درجة أهمية تلك المعلومات وانتشار استخدامها . ولذلك وجد التشفير منذ قديم الزمان ويعتبر من أقدم الأساليب التقنية المستخدمة لضمان امن المعلومات. وتشير أدبيات هذه الموضوع الى الكثير من القصص والروايات عن الوسائل التي اتبعت من اجل حماية المعلومات المرسلة او المخزونة .

شهد هذا العلم تطورا كبيراً ومر بمراحل مختلفة منذ نشوئه ولغاية يومناً هذا ، حيث استخدم في بادي الأمر أنظمة تشفير بسيطة مثل الأنظمة التعويضية والأنظمة الابدالية تلتها مرحلة استخدام أجهزة ميكانيكية وكهربائية ثم إدخال دوال رياضية معقدة في تصميم وتنفيذ أجهزة التشفير المعقدة بعد التطور الكبير الذي شهده مجال الصناعات الالكترونية ، تلتها مرحلة ظهور أنظمة المفتاح العمومي والتي أنهت مشكلة توزيع المفاتيح السرية و تعتبر من المشاكل المعروفة ضمن المشاكل التي تواجهها الأنظمة الشفرية البسيطة. يوضح الشكل رقم (1) المراحل المتميزة لتطور هذا العلم واتجاهاته.



الشكل رقم (1) مراحل تطور علم التشفير

يقسم علم الشفرات(*Cryptology*) الى قسمين هما:-

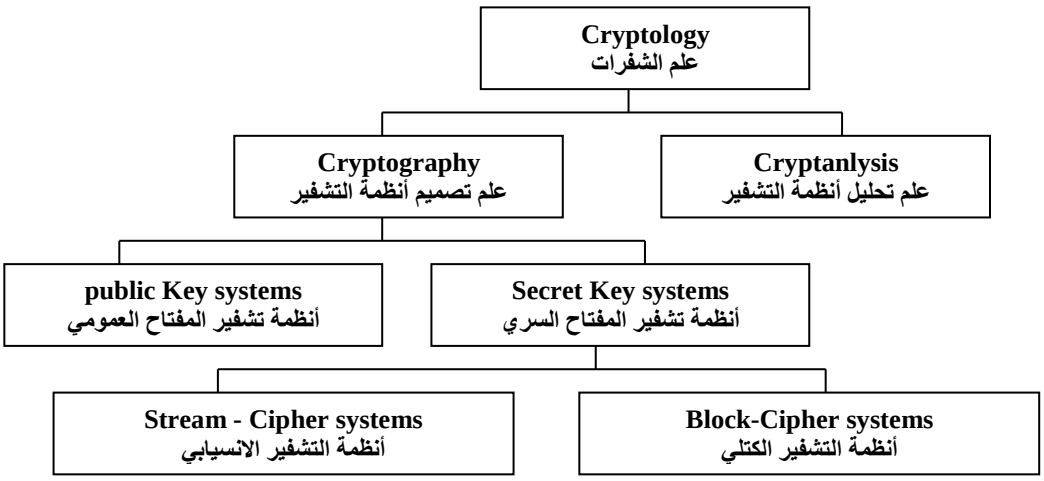
- علم التشفير(*Cryptography*) وهو علم تصميم وتنفيذ الأنظمة الشفرية (أي الطرائق التي يتم فيها تحويل النص الواضح الى نص مشفور وبتو فر المفتاح).
- علم تحليل أنظمة التشفير(*Cryptanalysis*) وهو العلم المختص بايجاد طرائق تحويل النص المشفر الى نص واضح دون توفر المفتاح او بتوفر جزء منه.

يحاول محلل الشفرة ان يكون دائما على معرفة تامة بخوارزمية نظام التشفير ، ويحصل على اكبر عدد ممكن من الرسائل المشفرة او أجزاء من النص الواضح وما يقابلها من النص المشفر، ان امتلاكه لتلك المعلومات التي يطلق عليها شروط الحالة الاسوء. عندما ياخذ المصمم هذه الافتراضات بنظر الاعتبار فان ذلك يزيد من أمنية النظام.

تقسم أنظمة التشفير الى قسمين هما

- أنظمة تشفير المفتاح العمومي(مثل نظام *RSA* ونظام النابساك)
- أنظمة تشفير المفتاح السري والتي بدورها تقسم الى قسمين هما
  - انظمه التشفير الانسيابية (*Stream cipher Systems*)
  - أنظمة التشفير الكتلية (*Block cipher Systems*)

وكما موضح في الشكل رقم (2) أدناه



شكل رقم (2) المخطط التوضيحي لأقسام علم الشفرات

تقوم أنظمة التشفير الكتلية بتقسيم الرسالة (النص الواضح) الى مقاطع(كتل) بأطوال ثابتة وتستخدم دالة تشفير واحدة لتنفيذ تشفير كل كتلة دخل أما أنظمة التشفير الانسيابية فهي الأنظمة التي يتم التشفير فيها بتاً بعد بت مع استخدام دالة تشفير متغيرة زمنياً.

تعتبر أنظمة التشفير التعويضية من الأنظمة الأولى التي وضعها الباحثون ومصمموا منظومات أمنية المعلومات. حيث تذكر أوليات هذا العلم بان نظام تشفير قيصر هو من أول الأمثلة حول هذه الأنظمة . ويشير المؤرخ الأمريكي كاهن [8] بأنه تم تحليل هذه الأنظمة في القرن الرابع عشر الميلادي من قبل العلماء العرب، باستخدام التقنية الأحصائية وهذا ما دعى العلماء الى البحث ووضع أنظمة تشفير اكثر تعقيداً من تلك والتي اطلق عليها تسمية أنظمة التشفير متعددة الهجائية حيث تمتلك خوارزميات هذه الأنظمة نوعا من المقاومة للهجوم الإحصائي.

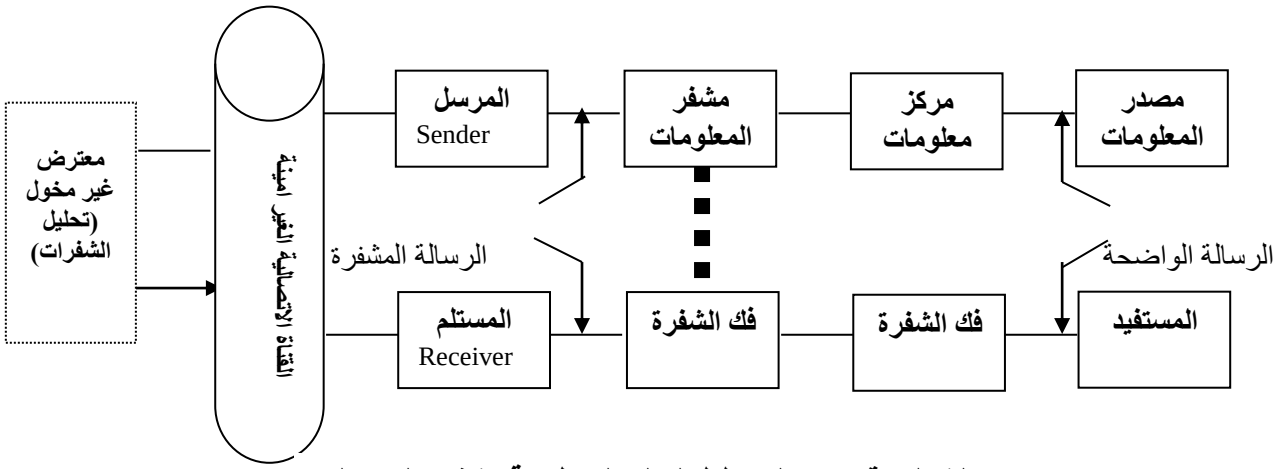
وتبعاً لموضوعة الفعل ورد الفعل فان هذا العلم يشهد على الدوام وضع خوارزميات هجوم مضادة لخوارزميات التشفير حيث تدرج خوارزميات مهاجمة التشفير تحت حقل الإجراءات التقنية المضادة (*ECM (Electronic Counter Measures*). أما خوارزميات التشفير فتدرج تحت حقل الإجراءات التقنية المضادة (*ECCM)(Electronic Counter Counter Measures*)، ولذلك فان الجهود تبذل في تعزيز قدرة الإجراءات المضادة من خلال إيجاد او وضع خوارزميات جديدة ذات تعقيد اقل من الخوارزميات المعروفة او يكون تعقيدها مقاربا لتعقيد الخوارزميات المعروفة[9].

يقدم البند الثاني فكرة مبسطة عن أنظمة التشفير التعويضية البسيطة والتركيز على النوع الضربي وذلك بذكر النموذج الرياضي لهذا النظام ودرج المعادلات الرياضية لعمليتي التشفير وفك الشفرة وكذلك التطرق الى ذكر مولد المفاتيح الخطية والمستخدم عموماً في أنظمة التشفير الحديثة والمسماة أنظمة التشفير الانسيابية والمستخدمة في السنوات الأخيرة بكثرة من قبل المستفيدين. أما البند الثالث فيعرض الطرائق التقليدية المستخدمة لتمييز المفتاح السري عموماً.

يعرض البند الرابع تفاصيل الطريقة المقترحة والمعتمدة على استخدام تقنية النوافذ المميزة للمفتاح الشفري في المدرج التكراري للحروف العربية ويعرض حالة دراسية. يعرض البند الخامس المناقشة والاستنتاجات والعمل المستقبلي.

2- أنظمة التشفير Cipher Systems

يعتبر الهدف الأساس لأنظمة التشفير هو تحويل النص الواضح الى نص غير واضح وذلك باستخدام مفتاح التشفير السري ، لضمان امنية النصوص الواضحة (الرسائل) وعدم الاطلاع على محتواها المعلوماتي عند سرقتها من أشخاص غير مخولين. ويوضح الشكل رقم (3) مخططا مبسطا لمنظومة تشفير الرسائل.



الشكل رقم (3) المخطط الكتلي لمنظومة تشفير الرسائل.

تتعرض المعلومات المرسلة عبر القناة الاتصالية غير الأمينة الى الاستراق بالوسائل المستخدمة من قبل الجهات المتطفلة، وكذلك تتعرض الى مؤثرات طبيعية ومصطنعة كثيرة تعتمد على نوعية وطبيعة نظام الاتصال [3].

ولذلك يركز مصممو الأنظمة الاتصالية المشفرة الى معالجة المعلومات بعد خروجها من المصدر وقبل دخولها الى القناة الاتصالية بصورة تؤمن الاحتياجات الآتية:-:

أ- الحصول على أعلى معدل لسرعة نقل البيانات والمعلومات.

ب-تحصين المعلومات والبيانات بإضافة قابلية كشف الخطأ وتصليحه من خلال مفاهيم إدخال الفائضية [1].

ج- إدخال مفهوم الحماية من خلال استخدام تقنيات التشفير والبعثرة (*Cipher and Scrambling*).

د- استخدام المفاهيم المقابلة في جهة الاستقبال لاسترجاع المعلومات المحورة الى أصلها المتولد من خرج المصدر.

ولذلك المخطط الكتلي بوضوح ما يمكن ان تتعرض له المعلومات من معالجات أساسية مطلوبة لأجل تحصينها خلال انتقالها عبر الساحة القتالية المفروضة عليها (وهي القناة الاتصالية) .

لذلك فان المشفر هو الجزء المسؤول عن طريقة او أسلوب تحويل المعلومات من صورتها الواضحة المفهومة الى الصورة غير الواضحة (السرية او المموهة) او غير المفهومة من قبل أي طرف غير مخول او غير مرغوب فيه، مثلا جهة غير صديقة.

تتكون عملية التشفير/ فك الشفرة من خمسة عناصر رئيسية هي:-

1) الرسالة الواضحة (*Plain Text or Message*)
2) الرسالة المشفور(*Ciper Text or Cryptogram*).
3) مفتاح التشفير السري (*Enciphering Secrect Key*).
4) مجموعة دوال التحويل الشفري

(*Enciphering Transformation functionor Enciphering Algorithm*).

5) مجموعة دوال التحويل لفك الشفرة

(*Enciphering Transformation function or Deciphering Algorithm*).

يحتاج أي نظام اتصال مشفر الى مفتاح لتأمين تنفيذ عمليتي التشفير وفك الشفرة، حيث يدخل هذا المفتاح الى خوارزمية (دوال التحويل الشفري) سويه مع الرسالة الواضحة. كما ان المستلم لابد ان يكون عارفاً للمفتاح السري وهذه المعرفة تساعده على استخلاص النص الواضح من النص المشفر. ولذلك فان المفتاح والنص المشفر يحددان النص الواضح بصورة وحيده.

غالباً ما تعتمد أمنية النظام الشفري على المفتاح المستخدم، ولذلك يجب توفر قناة أمينة لتوزيع المفتاح بين المرسل والمستلم وإلا فان سقوطه بيد الأشخاص غير المخولين يؤدي الى تحليل النظام الشفري.

يستطيع المتطفل الوصول الى النص المشفر،ولكنه لا يستطيع تحليل الشفرة دون معرفة المفتاح ومن هنا تبرز أهمية حماية المفتاح[2].

تعتبر أنظمة التشفير التعويضية (*substitution cipher systems*) من الأنظمة المهمة والواسعة الاستخدام،حيث تعرف على أنها الطريقة التي يتم بها تعويض او إحلال كل حرف من حروف الرسالة (النص الواضح) بحرف اخرمن خلال العلاقة المقامة بين حروف هجائية النص الواضح وحروف هجائية النص المشفر اعتماداً على مبدأ او

فكرة خوارزميات التعويض، حيث لا تتغير مواضع الحروف، وإنما الحروف نفسها هي التي تتغير فقط. يمكن القيام بالتعويض باستخدام حروف أخرى، او أرقام او رموز[7].

تقسم أنظمة التشفير التعويضية الى الأقسام الآتية:-

(أ) الأنظمة التعويضية وحيدة الهجائية .
(ب) الأنظمة التعويضية متعددة الهجائية.
(ج) الأنظمة التعويضية التخطيطية.

تعتبر الأنواع المصنفة ضمن القسم (أ) من الأنظمة ذات الأمنية المحدودة، وتحتوي على الأنظمة المعروفة الآتية:-

1. أنظمة التشفير الجمعية (*Additive Cipher System*).
2. أنظمة التشفير الضربية (*Multiplicative Cipher System*).
3. أنظمة التشفير المضاعفة او الهجينة [5](*Affine Cipher System*).
4. نظام التشفير المعكوس (*Reciprocal Cipher system*).

وعلى سبيل المثال ،فأن شفرة قيصر من الأمثلة على أنظمة التشفير الجمعية .

تعتبر خوارزمية نظام التشفير الضربي اعقد بالنسبة لمحلل الشفرة من خوارزمية نظام التشفير الجمعي وذلك عن التعامل مع المدرج التكراري لحروف النص المشفر.

يمكن التعبير رياضيا عن هذه الخوارزمية وكالاتي:

$$C = (P \times key) \bmod n \quad \dots \quad (1)$$

حيث ان : C هو Cipher(الحرف المشفر) ، P هو plain (الحرف الواضح)
key هو (المفتاح) ، n حجم الابجدية المستخدمة

هناك بعض خصائص المميزة لقيم المفتاح التي يمكن استخدامها مع هذه الخوارزمية حيث تحسب هذه القيم اعتماداً على تحقيق العلاقات التالية [4].

$$GCD(key, n) = 1 \qquad \dots \quad (2)$$

حيث ان (GCD) هو القاسم المشترك الاعظم للقيمتين key و n هو عدد حروف الابجدية للغة العربية والتي عددها 28 حرف. فان مجموعة عناصر المفاتيح هي، {3,5,9,11,13,15,17,19,23,25,27} أي ان عددها (11) مفتاحاً. والناتجة من تطبيق العلاقة (2) اعلاه.

مثال

شفر النص الواضح (جامعة بابل- كلية العلوم) باستخدام نظام التشفير التعويضي الضربي مع مفتاح تشفير سري قيمته 3 .

الحل:-

1- بما أن مبدأ عمل هذه الخوارزمية هو الضرب المعياري أي ان قيم حروف الرسالة تضرب مع قيمة المفتاح باعتماد على قيمة المعيار المقابل لعدد حروف هجائية النص الواضح وهو (28) حرف، لذلك يمكن تمثيل حساب قيم حروف النص المشفر حسب العلاقة المعيارية رقم (1)، لذلك تكون الرسالة المشفورة هي:- (ضتطهذ حتحش – رشيذ تشهشنط).
2- تعتمد قيم حروف النص الواضح على تسلسلها ضمن مواقعها في هجائية اللغة العربية (الابجدية المستخدمة) كما في الجدول رقم (1):-

جدول رقم (1) يبين حروف النص الواضح على تسلسلها ضمن مواقعها في الأبجدية المستخدمة

الحرف الواضح	تسلسله	نتائج عملية الضرب المعياري	الحرف المشفر

ا	1	3	ت
ب	2	6	ح
ت	3	9	ذ
ث	4	12	س
ج	5	15	ض
ح	6	18	ع
:	:	:	:
و	27	25	ن
ي	28	28	ي

3- ان الطرف المقابل (المخول) عند استلامه النص المشفر فانه يطبق المعادلة المعيارية التالية:-

$$P = (C \times key^{-1}) \bmod 28 \quad \ldots \quad (3)$$

أي يجب عليه حساب مقلوب المفتاح السري كالآتي:

$$(key \times key^{-1}) \bmod 28 = 1 \quad \ldots \quad (4)$$

4- ان محلل الشفرة (غير المخول)، والذي يفتقر الى معرفة قيمة المفتاح السري (key)، يكون الموقف بالنسبة له أكثر تعقيداً.

وبصورة عامة، تعاني أنظمة التشفير التعويضية من الضعف تجاه الهجوم الإحصائي والتخميني والمعتمد أساسا على خصائص اللغة ولا سيما التكرار للحروف الأحادية او الحروف الثنائية او الثلاثية او بداية ونهاية الكلمات.

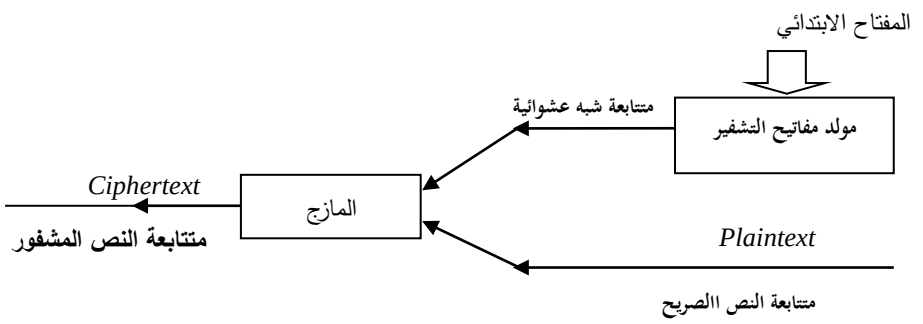
أنظمة التشفير الانسيابية Stream cipher system

تستخدم أنظمة التشفير الانسيابية مفتاحا منتهياً فقط، وتشبه بذلك نظام تشفير المرة الواحدة (*one time pad*)، وهو النظام الذي يستخدم متتابعة منتهية من المفاتيح تتولد باستقلال بعضها عن البعض) [6] . ويعتبر النظام الوحيد المبرهن على انه ذو أمنية مثالية ولا يحتاج شروط لبرهنة أمنيته (*unconditionally secure*). من السهولة التقدير بان أمنية هذا النظام ترتبط مباشرة بخواص مولدات المفاتيح شبه العشوائية.

يتكون نظام التشفير الانسيابي الموضح في الشكل (4) من جزأين أساسيين هما:

1- مولد سيل المفاتيح شبه العشوائي (*PSEUDO RANDOM KEY STREAM GENERATOR*)

2- المازج (*MIXER*).



الشكل (4) نظام التشفير الانسيابى

يقوم مولد المفاتيح بتوليد متتابعة شبه عشوائية اعتمادا على مفتاح ابتدائي، تدمج هذه المتتابعة مع متتابعة النص الواضح باستخدام المازج لتولد متتابعة النص المشفر . تكمن أمنية نظام التشفير الانسيابي في خوارزمية توليد سيل المفاتيح شبه العشوائية ولهذا السبب يتجه البحث دائماً عن المقاييس والمعايير الخاصة والتي يجب أخذها بالاعتبار عند التصميم .

تقاس عشوائية المتتابعة من خلال الاختبارات الأحصائية القياسية الآتية :-

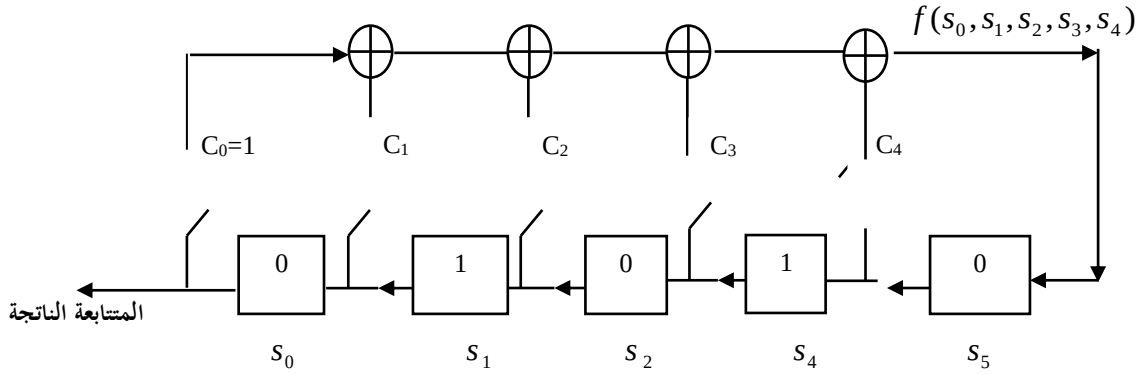
أ- اختبار التسلسل (Serial Test) ب-اختبار بوكر (Poker Test) ج-اختبار التنفيذ (Run Test)

د- اختبار الارتباط الذاتي (Auto Correlation Test) هـ- الاختبار الترددي [5] (Frequency Test) .

مسجلات الإزاحة المستخدمة في نظام التشفير الانسيابي

Linear Feed Back Shift Register (LFBSR)

تشترك معظم خوارزميات التشفير في استخدامها لمسجلات إزاحة ذوات تغذية مرتدة خطية ودوال ربط خطية او لاخطية لإنتاج متتابعات منتهية ذات دورات طويلة . يحتوي مسجل الإزاحة على n من المراحل (*Stages*) . أن محتوى كل مرحلة هو صفراً او واحداً ، ويسمى حالة المرحلة (*Stage*) وكما موضح في الشكل رقم (5) .



الشكل رقم (5) مولد مفاتيح ذو تغذية مرتدة خطية بخمسة مراحل وقيمة ابتدائية مقترحة

تسبب كل نبضة من نبضات السيطرة انتقال محتويات اية مرحلة الى المرحلة التي بعدها، مع الأخذ بنظر الاعتبار تأثير دالة التغذية المرتدة (*Feedback Function*).

يدعى مسجل الإزاحة بمسجل الإزاحة ذو تغذية مرتدة خطية اذا مثلت دالة التغذية المرتدة بالمعادلة الآتية:

$$f(s_0, s_1, ..., s_{n-1}) = c_0 s_0 \oplus c_1 s_1 \oplus ... \oplus c_{n-1} s_{n-1} \quad ... \quad (5)$$

حيث ان المعاملات c_i هي معاملات التغذية الخطية المرتدة وتأخذ القيمة صفر او واحد،

الطرائق التقليدية لتمييز المفتاح السري

يوجد العديد من الطرائق والتقنيات المعروفة والموضوعة منذ فترة زمنية قديمة، وهدفها الاساس هو مهاجمة أنظمة التشفير التعويضية البسيطة. والاعتماد الاساس لمعظم هذا الطرائق والتقنيات هو الحساب الاحصائي لمكونات هجائية النص الواضح والنص المشفور. وقد اشتهر العرب منذ مئات السنين بانهم كانوا اول من دخل هذة التقنيات . وسنطرق في هذة البند فكرتها الاساسية .

أ- الدراسة الأحصائية او التحليل الترددي (*Frequency Analysis*)

تعتبر التقنية الأحصائية البسيطة بانها الواسطة الاكثر اهمية في تحليل الشفرات ،وتعتمد على فكرة التردد النسبي لحدوث حرف منفرد في النص المشفر . فمثلا ، يوجد في النص الواضح الطويل اتباع الحروف ترددا نسبيا معين للحدوث ، والجدول رقم (2) يمثل التردد النسبي لحروف هجائية اللغة العربية ، حيث يمكن تقسيم هذه الحروف الى سبعة مجاميع اعتمادا على تكرارها النسبي .

الجدول رقم (2) يبين التردد النسبي لحروف هجائية اللغة العربية بحجم ملف 45770 حرف في حالة التشفير بالمفتاح الضربي رقم (3)

ت	الحرف	التردد النسبي	ت	الحرف	التردد النسبي
1	غ	0.50	15	ج	1.34
2	ر	4.94	16	م	5.97
3	أ	18.87	17	ض	0.69
4	ف	2.89	18	ح	1.93
5	ز	0.59	19	ن	5.46
6	ب	3.66	20	ط	1.07
7	ق	2.46	21	خ	0.78
8	س	2.40	22	ه	4.11
9	ت	4.77	23	ظ	0.22
10	ك	2.40	24	د	2.87
11	ش	0.96	25	و	5.61
12	ث	0.58	26	ع	3.77
13	ل	11.77	27	ذ	1.02
14	ص	0.90	28	ي	7.48

ولذلك فان محللي الشفرة يعتمدون أكثر على هذه الخصائص للغة والتي لاتتاثر كثيرا باستخدام أنظمة التشفير التعويضية . حيث تبقي خصوصية الحدوث مختصة بالحرف ولكنها تنتقل الى الحرف الشفري المقابل والذي تفترضه طريقة التشفير .وإذا علمنا ان الميزة المحددة لهذه الأنظمة هي أنها تجعل العلاقة بين حرف النص الواضح وحرف النص المشفر علاقة وحيدة .أذن يصبح الأمر سهلاً على محلل الشفرة ان يستثمر هذه المعرفة الأحصائية .

ب- طريقة التجربة والخطأ (*Trying And Error*)

يوفر الحاسوب أمكانية أعادة عملية ما آلاف من المرات في أجزاء من الثانية. وبسبب هذه القدرة يمكن اختزال معظم الجهد الشاق الخاص بطريقة التجربة والخطأ(لتحليل الشفرة يدوياً)، فمثلاً لتحليل شفرة نص مشفر بطريقة قيصر فطريقة التجربة والخطأ تستلزم أجراء عدد من المحاولات بقدر عدد المفاتيح الممكنة الاستخدام لتشفير النص الواضح في هذه الطريقة الشفرية وعددها 28 مفتاحاً. ولذلك تعتبر هذه العملية مستحيلة لو كانت عدد المفاتيح كبيرة جداً لخوارزمية تشفير ما.

4- الطريقة المقترحة *Proposed Method*

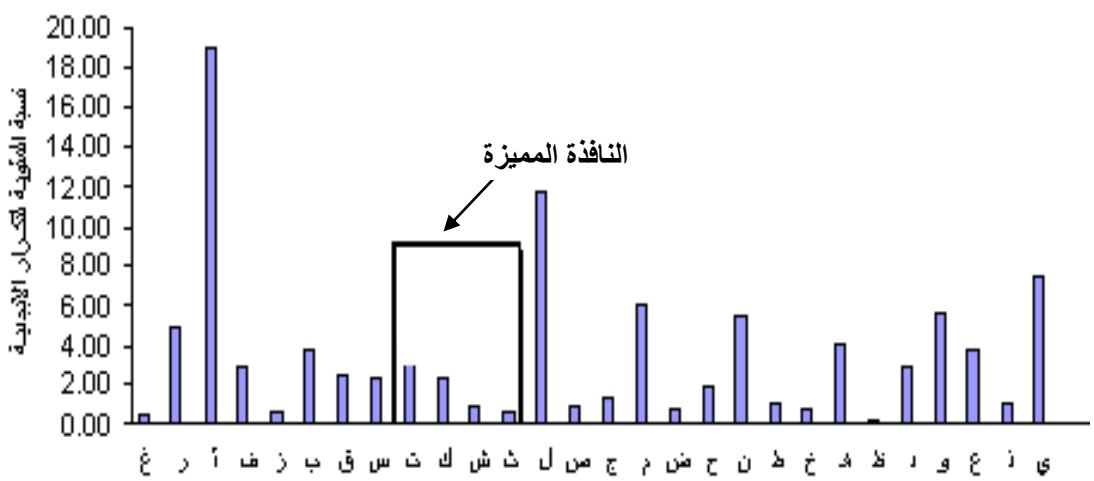
تعتمد هذه الطريقة على أنشاء قاعدة البيانات الخاصة بالنوافذ المميزة لكل حالة من حالات المفاتيح المختلفة حيث يتم تعين عرض النافذة على المدرج التكراري لإحصاء الحروف المنفردة وتخزن هذه النوافذ لأجل المقارنة مع النافذة المستخرجة من النص المشفر لأجل تمييز المفتاح وتتضمن هذه الطريقة بالخطوات التالية :-

أ- أنظمة التشفير التعويضية :

(1) حساب نسبة تكرار كل حرف من الأحرف الهجائية للنص المشفر.
(2) رسم المدرج التكراري (*Histogram*) لما سبق حسابه في (1) أعلاه.
(3) اختيار وتحديد النافذة الواضحة والمناسبة.
(4) مقارنة قيم نسب التكرار لهذه النافذة مع قاعدة المعلومات المخزونة وفي حالة تطابقها تكشف لنا وتمييز قيمة المفتاح السري لهذا النص.

بناء قاعدة البيانات

1. اختيار ملف طويل لهجائية لغة عربية بطول يقارب من 45770 حرفا. حيث تم اختيار نصوص مختلفة من حقول معرفية مختلفة، مثلا طبية وسياسية وعلمية وتجارية وعسكرية... الخ.
2. تشفير هذا النص باستخدام المعادلة رقم (1) والمفاتيح الممكنة وعددها(11)، وبذلك نحصل على (11) احد عشر ملفا مشفرا.
3. لجميع الملفات نحسب النسب المئوية لتكرار الحروف.
4. نرسم المدرج التكراري لكل ملف مشفر لكل مفتاح بواسطة الحاسوب، كما موضح في الشكل رقم (6) (لحالة واحدة للمفتاح 3).
5. تمييز عدد من الحروف المتتابعة في هذه الحالة (ت ، ك ، ش ، ث) والتي تعتبر متميزة في وجودها على المدرج التكراري ولا يمكن تكرارها في حالات المفاتيح الاخرى. وبهذا فهي تعتبر ميزة للمفتاح.
6. خزن هذه النوافذ ومفاتيحها على هيئة جدول او قاموس. علماً ان مواقع النوافذ وحروفها موضحة في الجدول رقم (3).



الشكل رقم (6) يبين المدرج التكراري للمتتابعة الأحرف الناتجة من الضربي بمفتاح (3)

الجدول رقم (3) : يبين النوافذ المميزة ومواقع النوافذ وحروفها

مفتاح التشفير	مواقع حروف النافذة المميزة	حروف النافذة
3	9 ، 10 ، 11 ، 12	ت ، ك ، ش ، ث
5	1 ، 2، 3 ، 4 ، 5، 6	ظ ، ح ، ل ، س ، أ ، ع
9	17 ، 18 ، 19 ، 20	ج ، ب ، و ، م
11	5 ، 6 ، 7 ، 8 ، 9	ت ، هـ ، ق ، ط ، ز
13	21 ، 22 ، 23	ق ، ح ، غ
15	5 ، 6 ، 7 ، 8 ، 9	غ ،ح ، ق ، د ، ل
17	1 ، 2، 3 ، 4 ، 5	ج ، د ، ض ، ف ، ن
19	8 ، 9 ، 10 ، 11	م ، و، ب ، ج
23	11 ، 12 ، 13 ، 14 ، 15 ، 16	ذ ، ف ، ت ، ص ، ن ، ر
25	9 ، 10 ، 11 ، 12 ، 13 ، 14	ن ، ح ، ض ، م ، ج ، ص
27	2 ، 3 ، 4 ، 5 ، 6 ،7	هـ ، ن ، م ، ل ، ك ، ق

ب- أنظمة التشفير الانسيابية

تم اختيار مولد مفاتيح خطي ذو خمسة مراحل كما موضح في الشكل رقم (5).

1. بافتراض قيمة ابتدائية معينة هي : {0 1 0 1 0}
2. ناخذ الحالات الممكنة لاعطاء متتابعة مفاتيح عشوائية ذات دورة بطول اعظم، وهي 6 حالات فقط لهذا المولد.
3. لكل حالة من الحالات نأخذ متتابعة بطول لايقل عن 40 بتا ثم نأخذ كل خمسة بتات ابتدأ من اول بت ونحولها الى ما يقابلها بالنظام العشري مثلا 11010=26 ، ثم نزحف بمقدار بت واحداة ونأخذ خمسة بتات جديدة(اربعة منها قديمة وواحدة جديدة) ونحسب المقابل العشري وهكذا نستمر الى ان نكمل المقابلات العشرية، ولتكن بحدود 32 رقما عشري.
4. نرسم المدرج التكراري وهو العلاقة بين تتابع الارقام العشرية ونبضات السيطرة على مولد المفاتيح .
5. نبحث على المدرج الناتج على جزء مميز له ولا يمكن ان يتكرر لحالات اخرى والشكل رقم (5) يوضح هذه الميزة.
6. نكرر نفس العملية للحالات الخمسة الاخرى.
7. نخزن النوافذ المميزة لكل حالة من الحالات الـ (6) وما يقابلها كدالة تغذية خلفية. كما موضح في الجدول رقم (4).

الجدول رقم (4) يوضح تتابع القسم المتزايد لدوال التغذية المرتدة المختلفة لمولد مفاتيح ذو خمس مراحل.

الحالة	دالة التغذية المرتدة	ارقام التتابع المتزايدة الخمسة
1	$S_0 + S_2$	31,30,28,24,19,6
2	$S_0 + S_3$	31,30,28,24,17,3
3	$S_0 + S_2 + S_3 + S_4$	31,30,28,25,18,4
4	$S_0 + S_1 + S_2 + S_3$	31,30,29,27,23,14
5	$S_0 + S_1 + S_2 + S_4$	31,30,29,27,22,12
6	$S_0 + S_1 + S_3 + S_4$	31,30,29,26,20,8

ان تطبيق هذه الطريقة على متتابعات المفتاح تتم بنفس السياق المذكور مع مقارنة المدرج التكراري للمتتابعة المفحوصة مع قاعدة البيانات.

حالة دراسية

(1) استخدام نصا عربيا واضحا بطول معين هو 4000 حرف.
(2) استخدام نظام تشفير التعويض وحيد الهجائية من النوع الضربي وتشفير النص العربي الواضح باستخدام قيمة مفتاح التشفير، ولكن مثلا هي القيمة (11). فينتج نصا مشفرا مقابلا للنص العربي الواضح.
(3) نحسب النسبة المئوية للتكرار حروف هجائية النص المشفر.
(4) رسم المدرج التكراري (*Histogram*) الذي يمثل العلاقة بين تسلسل حروف الهجائية وتكرار كل حرف.

(5) تحديد منطقة معينة على المدرج التكراري بعرض معين من الحروف ولا يتجاوز (5) ولتكن مواقع الحروف (5،6،7،8،9).
(6) سحب نافذة قياسية من قاعدة البيانات.
(7) مطابقة النافذة المسحوبة مع المدرج التكراري للرسالة المشفرة مع الأخذ بالاعتبار ان المطابقة تعتمد على مقارنة سلوك عناصر (مكونات النافذة) حيث يفترض ان يكون هذا السلوك مشابه في الاثنين وليس من الضرورة ان يكون متساويا في القيم.
(8) في حالة عدم تطابق النافذة المسحوب من قاعدة البيانات يتم تكرار الخطوة (7) اعلاه لسحب بقية النوافذ على التوالي لحين الحصول على النافذة المحدد لمفتاح التشفير السري.

5- المناقشة والاستنتاجات:-

1. عندما أخذنا حجوما متغيرة من النص المشفر باللغة العربية من الحجم 1000 حرف الى 45770 حرف ،ساعد هذا كثيراً على تحديد النوافذ ذات معالم واضحة والتي نستطيع من خلالها تحديد قيمة المفتاح الشفري السري المستخدم في عملية تشفير النص.
2. أمكانية التعامل مع المدرج التكراري حاسوبيا لمساعدة كاسر الشفرة لكسر شفرة النص .

ولتقويم النظام الشفري اعتمادا على سببين هما الوقت المطلوب والذاكرة المطلوبة لخزن النص كانا ضمن الإمكانات التي توفرها الحواسيب الموجودة في مختبرات قسم الحاسبات والتي أتاحت لنا أمكانية اختبار هذه الطريقة المقترحة وذلك لان تقنية النوافذ تختزل هذه المتطلبات.

3. تعتمد الطريقة المقترحة على الحسابات الأحصائية أولا، ولكنها تنحوا منحنى مختلفا عن الطرائق الأخرى والتي كانت تعتمد على مبدأ مقارنة تكرار الحروف حيث ان تلك الطرائق كانت تعاني من نقاط ضعف عديدة خصوصا عندما يكون النص المستلم قصيرا والذي كان يجعل تلك الطرائق غير مجدية ولكن ضمن هذه الطريقة أثبتت التجارب الطويلة انه يمكن تطبيق هذه الطريقة لنص بطول 1000 حرف.
4. ان طريقة بناء قواعد البيانات من الطرائق المعروفة ذات الاستخدام الكبير في تطبيقات الحاسوب خصوصا في التطبيقات ذات الصيغة المعقدة والتي تتطلب نوعا من الذكاء ولذلك يتوجه العلم حاليا لتوظيف الخبرة والذكاء في موضوع تحليل الشفرات وإمكانية محاكاة هذا الأمر ببناء أنظمة ذكية ولذلك تعتبر هذه الطريقة خطوة أولى في هذا الاتجاه.
5. ان تمييز النوافذ لحالة مولد المفاتيح أسهل مما هي عليه في حالة الأنظمة التعويضية حيث وجدنا ان الحالة المميزة لدالة الربط هي وجود خمسة حالات زيادة متتابعة تنتهي بالرقم 31، ولكن تختلف في الرقم الابتدائي، ولذلك يمثل الجدول رقم (4) العلاقة بين دالة الربط والحد الأدنى لحالات الزيادة المتتابعة.

References

[1] Berlkamp,A. "Algebraic coding Theory",1968.

[2] Charmox, j. " Data Security and Confidentiality in Europe", Computer and Security, No. 4, 1985.

[3] Denning .D. ,"Cryptography and Data Security", 1982.

[4] Jennifer. S and Piperzyk.J, "cryptography : An Introduction to Computer Security", 1989.

[5] Piper.J. and Beker . H.,"Cipher systems" , An Introduction to Communication Security", 1982.

[6] Rueppel , R.A. "Good Stream Cipher and hard to design", Proc.1989,int.conf.coranhan.

[7] بوروس بوزورت : الرموز الشفرات والحاسبات، مقدمة الى امن المعلومات ، ترجمة الدكتور المهندس ستار بدر سدخان وآخرون ، الكلية الهندسية العسكرية، 1989.

[8] دايفيد كاهن ، " تاريخ الكتابة السرية " ، 1967.

[9] ري. هـ. بيتبت : تقنيات الإجراءات الالكترونية المضادة والإجراءات المقابلة للإجراءات المضادة لأنظمة الاتصالات الرقمية ، د. المهندس جعفر وادي عبد السادة ود. المهندس ستار بدر سدخان و د. المهندس سعد عبد الرضا مكي ، الكلية الهندسية العسكرية ، 1989.

A New Proposed Method Using Windows Technique For Recognition Of Secure Keys

Sattar Bader Sadkan \college of Education \ Department Of Mathematics
Salwa shaker \ College of Science\ Department Of Computer

Abstract:-

Recognition of secret keys is considered as an important matter for the workers and specialists for analyzing of cryptographic algorithms, or for the evaluation of the security of these algorithms.

This paper presents a newly proposed method depending on the utilization of window's technique on the histogram of statistical occurrences of Arabic letters of the cipher messages.

This technique can be considered as an alternative tool for the linear complexity profile used with stream cipher system. The method tested through many examples, and it is founded to be promising to be applied for different cipher algorithms.