مجلة جامعة بخت الرضا العلمية العدد العاشر مارس 2014م [ISSN 1858-6139]
University of Bakht Alruda Scientific Journal Issue No. 10 March 2014

دور خوارزمية التشفير المتحركة الجديدة في معالجة عيوب التشفير المتناظر بالإحلال

إعداد

خالد عبد الله عبيد — **اشرف قسم السيد**

طالب الدكتوراه / جامعة الرباط الوطني — **استاذ مشارك /جامعة المستقبل**

ABSTRACT

The dynamic algorithm encryption is a new algorithm encryption that has a strong ability to encrypt text files as an implementation symmetric encryption substitution. This study aims to treat the drawbacks of symmetric encryption substitution mainly represented in handling the plain text through: encryption analysis brute force. This can be carried out through the new dynamic encryption algorithm, which provides authentication and efficiency as one of the most important encryption requirements. This paper includes standardization algorithm depending on the fundamental principles such as Kirchhoff's and Kais ski's and Ebin Alkindy way. The study results in presenting the role of dynamic encryption algorithm in the treatment of the symmetric encryption drawbacks by preventing relative frequency of letters. Moreover, it uses humorous keys to prevent the encryption analysis.

المستخلص

خوارزمية التشفير المتحركة هي خوارزمية تشفير جديدة ذات إمكانيات كبيرة في تشفير الملفات النصية كأحد تطبيقات التشفير المتناظر بالإحلال.تهدف هذه الدراسة إلى معالجة عيوب التشفير المتناظر بالاحلال والمتمثلة بصورة رئيسية في الوصول إلى النص الواضح من خلال: أ/تحليل التشفير ب/البحث الشامل. وذلك عن طريق خوارزمية التشفير المتحركة الجديدة والتي وفرت الفعالية وإثبات الهوية كأحد أهم متطلبات التشفير بصورة عامة. تضمنت هذه الورقة معايرة هذه الخوارزمية على المبادئ الأساسية لقياس مدى فعالية الخوارزمية كمبدأ كيريكوف (Kerckhoffs) ومبدأ كيسسكي (Kaisiski) وإسلوب بن الكندي (Ebin alkindy) . وخلصت نتائج الدراسة إلى إبراز دور خوارزمية التشفير المتحركة في علاج عيوب التشفير المتناظر بالاحلال من خلال عدم امكانية التطبيق المعياري للحروف ، كما تميزت الخوارزمية بالعدد الكبير للمفاتيح الذى يحد من تحليل الشفرة . الكلمات الاساسية : التشفير المتناظر بالاحلال ، النص الواضح ، هجوم الكسر الأعمى .

1. المقدمة Introduction

عملية التشفير هي عملية تجمع بين علم الرياضيات وعلم الحاسوب، هي العلم والمقدرة على حماية البيانات من الاختراق حيث تستخدم في معظم المجالات والتطبيقات التقنية والعملية ،الطلب على عملية التشفير في تزايد لحماية البيانات لكن ما يتم حفظه وتأمينه اليوم من الممكن ان يتعرض للاختراق في الغد [1].

2.1 تعريف المشكلة:

من أهمية بقاء المعلومات والبيانات في سرية تامة يصعب إختراقها صمم الباحثان خوارزمية جديدة في تشفير ملفات البيانات كأحد تطبيقات التشفير المتناظر بالإحلال .

3.1 الأهداف:

الحصول على تشفير أكثر سرية وأسرع في التنفيذ وأقل تكلفة وبأقل المكونات المادية للحاسوب ، كما لايمكن تحليل النص المشفر بطرق التحليل المختلفة للوصول للنص الواضح ، أما هجوم الكسر الاعمى أو مايعرف بالبحث الشامل يصعب معه الوصول للنص الواضح ، لما تتمتع به خوارزمية التشفير المتحركة من خواص ، كما تهدف الخوارزمية الجديدة الى تحقيق درجة عالية من السرية لملفات البيانات وتوفير مفتاح خارجي يجعل البيانات في مأمن ويحافظ على سريتها ، توفير مستوى عال من الأمنية وذلك من خلال القاعدة التى بنيت عليها ، إمكانية الاستخدام على الحروف الكبيرة أو الصغيرة (CAPITAL & small letter) ، توفيرالإستخدام الإقتصادى في الأجهزة الإلكترونية دون الحاجة إلى مساحات تخزينية جديدة (126,976 bytes 124 KB) ، تتمكن الخوارزمية من تشفير البيانات مهما كان حجمها ، تحتوى الخوارزمية على خاصية التحقق من صحتها .

2. التعريف بالتشفير:

يُعرَّف التشفير بأنه عملية تحويل المعلومات إلى شفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها .

1.2 أهداف التشفير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي :

- ✓ **السرية أو الخصوصية (Confidentiality)**:

هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

- ✓ **تكامل البيانات (Integrity)**:

وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

- ✓ **إثبات الهوية (Authentication)**:

وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).

- ✓ **عدم الجحود (Non-repudiation)**:

وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن المعلومات [2].

ومن ناحية أخرى تستخدم المفاتيح keys (وهى معلومات سرية) في تشفير Encryption النصوص المرسلة و فك تشفيرها Decryption من قبل صاحبها المسموح له بتسلمها ، و ترتكز قوة و فعالية التشفير على نوعية الخوارزميات المستخدمة ، كانت عملية التشفير و لا زالت في بعض

الحالات تتم بواسطة مفتاح سري يستخدم لتشفير النصوص و في نفس الوقت لفك تشفيرها وترجمتها إلى وضعها الأصلي ، وهو ما يعبر عنه بالتشفير المتناظر Symmetric Encryption ، كما يسمى أيضا بالتشفير الأساسي أو التشفير باستخدام المفتاح الواحد ، إسلوب التشفير هذا مفيد من حيث قدرته على تحويل محتوى الرسالة الأصلية إلى معلومات غير مفهومة .

2.2 عيوب التشفير المتناظر بالاحلال :

يعتبر تحليل التشفير وهجوم الكسر الأعمى من أكبر عيوب التشفير المتناظر بالاحلال فما هما :

أولاً : تحليل التشفير: ويعتمد هذا الأسلوب على تحليل التشفير بناء خوارزمية معينة والاعتماد على بعض معطيات النص المشفر المعروفة للمحلل (المهاجم) لاستنتاج النص الصريح أو استنتاج المفتاح المستخدم ، يتطلب هذا الأسلوب أن تكون خوارزمية التشفير معروفة بالنسبة للمحلل ، وقد يستخدم المحلل بعض الطرق الإحصائية للحصول على النص الصريح أو المفتاح الشكل رقم (1) يوضح التكرار النسبي النموذجي لاستخدام الحروف الانجليزية [3] .

ثانياً : هجوم الكسر الأعمى أو البحث الشامل : في هذا الأسلوب يحاول المهاجم تجريب كل المفاتيح المحتملة على مقطع من النص المشفر ويستمر في هذه المحاولات حتى يتحصل على نص صريح مفهوم وواضح ، في هذا الأسلوب كلما زاد طول المفتاح أصبح كسر الشفرة أكثر صعوبة ، إن الزمن المطلوب لتحليل الشفرة بهذا الأسلوب يعتمد بدرجة كبيرة على مقدرات الحاسوب المستخدم .

3. الطرق :

سيتناول الباحثان في الفقرة الاولى الدراسات السابقة بينما في الفقرة التالية كيفية عمل خوارزمية التشفير المتحركة وطريقة فك خوارزمية التشفير المتحركة .

1.3 الدراسات السابقة

يود الباحثان أن يشيرا إلى قلة الدراسات السابقة والمتخصصة في ذات الموضوع إلا أنه قد إضطلع على القليل الصادر منها وإن لم يجد دراسة أقرب إلى ماذهب إليه إلا إنه يرى ضرورة عرض ما إضطلع عليه من دراسات تناولت بعض الجوانب المتعلقة بالموضوع وذلك بغرض الاستفادة من منهجها وبعض ماخلصت إليه من نتائج .

1.1.3 درس هاشم أبوبكر[4] خوارزميات أمن البيانات والتي تقوم على إستبدال كل حرف بالحرف الذي يليه بعدد متغير غير ثابت من المواقع ، يعتمد على الحرف المقابل له في الكلمة المفتاحية المستخدمة ، وكمثال توضيحي إذا كان لدينا DAGGER الكلمة المفتاحية المستخدمة في تشفير النص ' IDESOFMARCH '.

النص الأصلـــي: I D E S O F M A R C H

الكلمة المفتاحية مكررة: D A G G E R D A G G E

النص المشفـــر : L D K Y S W P A X I L

باستخدام جدول مواقع الأحرف التالي:

الحرف	A	B	C	D	E	F	G	H	I	J	K	L	M
الموقع	00	01	02	03	04	05	06	07	08	09	10	11	12

الحرف	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
الموقع	13	14	15	16	17	18	19	20	21	22	23	24	25

فكل حرف في النص الأصلي يستبدل به الحرف الذي يليه بعدد المواقع التي يمثلها الحرف المناظر له في الكلمة المفتاحية، مثلا: I الذي له رقم الموقع 8، يناظره في الكلمة المفتاحية الحرف D، موقعه 3، إذن الحرف الجديد هو 8 + 3 = 11 (الحرف L) وهكذا.... في حالة حرفين مثل Z +Y (49 = 24 + 25) يؤخذ باقي القسمة على 26 كموقع للحرف الجديد .

49 mod 26 = 23

.X = 23

المستقبل في هذه الخوارزمية يجب أن يعرف الكلمة المفتاحية لفك تشفير الرسائل.

أهم النتائج التي توصلت إليها الدراسة :

1- لم تجعل المفتاح ثابتاً كما في حالة يوليوس قيصر بل جعلته متغيراً.

2- إستبدال كل حرف بالحرف الذي يليه بعدد متغير غير ثابت من المواقع .

3- الإعتماد على الحرف المقابل في الكلمة المفتاحية المستخدمة .

ملاحظات الباحث حول الدراسة :

تقوم هذه الدراسة على فكرة خوارزمية أقرب من خوارزمية التشفير المتحركة ، فهى أشبه في طريقة عملها وعمل الخوارزمية الجديدة التى نحن بصددها ، غير أنها تفقد الكثير من أساسيات السرية ، فمن السهل الوصول الى النص الاصلي وبأقل مجهود ممكن .

ومرة أخرى المستقبل في هذه الخوارزمية يحتاج إلى معرفة المفتاح، أي جدول التبديل المستخدم في التشفير، وبما أن هناك 26! (مضروب 26) جدول تبديل ممكن (تقريبا 2810) فهذه الطريقة يمكن لغيرمحترفي التشفير فكها ببساطة وذلك بالقيام ببعض عمليات التحليل.

2.1.3 درست نورة عبدالمحسن الصميخي[5] سياسة الخصوصية التشفير بالطرق الكلاسيكية ،ونجد في هذه الدراسة شفرتين الاولى شفرة الضرب وهذا ماسنتناوله في الفقرة الاولى بينما سنتناول في الفقرة الثانية الشفرة المختلطة .

أولاً : شفرة الضرب :

يمكن تمثيل هذه الشفرة بالمعادلة التالية :

النص المشفر = النص الأصلي * مفتاح التشفير (باقي القسمة) على عدد الحروف الكلي.

عند استخدام هذه الطريقة في التشفير يجب أولاً التأكد من أن(مفتاح التشفير) و(عدد الحروف لكلي– أي مجال أو نطاق المفتاح) أوليان في ما بينهما أي أن القاسم المشترك الأكبر لهما يساوي 1، في ما عدا ذلك لن تكون الشفرة قابله للكسر.

ولتوضيح هذه الطريقة أكثر سنطبقها عملياً في المثال التالي:

والمفتاح = 7 ومن المعلوم أن العدد الكلي للحروف الانجليزية هو 26 حرف بفرض أن النص الأصلي هو :Islam بداية نقوم بإيجاد القيمة العددية لكل حرف انظر شكل(2) .

i	=	08
s	=	18
l	=	11
a	=	00
m	=	12

شكل رقم (2) إيجاد القيمة العددية لكل حرف

ثم نقوم بإيجاد البديل لكل حرف حسب قاعدة شفرة الضرب:

i	=	08	* 7	Mode 26	=	4	E
s	=	18	* 7	Mode 26	=	22	W

l	=	11	* 7	Mode 26	=	25	Z
a	=	00	* 7	Mode 26	=	00	A
m	=	12	* 7	Mode 26	=	6	G

إذن النص بعد التشفير هو : EWZAG

ويمكن تمثيل معادلة الكسر لهذه الشفرة كالتالي :

النص الأصلي = النص المشفر * النظير الضربي باقي القسمة على عدد الحروف الكلي .

ولكسر هذه الشفرة نقوم أولاً بإيجاد النظير الضربي للمفتاح ويحسب من خلال المعادلة التالية:

(المفتاح * النظير الضربي) باقي القسمة على العدد الكلي = 1

أي أنه في مثالنا السابق سيحسب كما يلي :

inverse =15 --> inverse mod 26 = 1*7

ثم نقوم بتطبيق معادلة الكسر على كل حرف من حروف النص المشفر :

E	=	4	* 15	Mode 26	=	08	I
W	=	22	* 15	Mode 26	=	18	S
Z	=	25	* 15	Mode 26	=	11	L
A	=	00	* 15	Mode 26	=	00	A
G	=	6	* 15	Mode 26	=	12	M

شكل رقم (3) معادلة كسر الحرف من حروف النص المشفر

ثانياً : الشفرة المختلطة:

سُميت بذلك لأنها تخلط بين الطريقتين السابقتين، حيث يتم الضرب أولاً ثم الجمع خلال عملية التشفير.

ويمكن تمثيل معادلة التشفير لها بأن :

النص المشفر = (النص الأصلي* مفتاح1 + مفتاح 2) باقي القسمة على العدد الكلي .

المفتاح 1: هو المفتاح لشفرة الضرب.

المفتاح 2: هو المفتاح لشفرة الجمع .

ولكسر هذه الشفرة نقوم بطرح النظير الجمعي للمفتاح 1 أولا – لكسر شفرة الجمع- ثم نضرب بالنظير الضربي للمفتاح 2 ، كما في المعادلة التالية :

النص الأصلي =((النص المشفر – المفتاح2)*النظير الضربي للمفتاح 1) باقي القسمة على العددالكلي .

وتتم بنفس الطريقة التي شرحناها لكلشفرة على حدا سابقاً ..

أهم النتائج التي توصلت إليها الدراسة :

1- الخلط بين الطريقتين السابقتين، حيث يتم الضرب أولاً ثم الجمع خلال عملية التشفير، صعب من كسر الخوارزمية بسهولة .
2- تعتبر الدراسة تطوير لطريقة سايبر قيصر التي إعتمدت الجمع فقط .
3- كل من يريد كسر الخوارزمية عليه تجربة كل المفاتيح المحتملة والبالغ عددها 26 مفتاحا على مستوى النص المشفر .

ملاحظة الباحث حول الدراسة:

- تواجه هذه الخوارزمية الكثير من الصعوبات والمتمثلة في سهولة كسر الخوارزمية والوصول الى النص الواضح .

- تحتاج الخوارزمية إلى الكثير من التطوير حتى تصبح تعمل على شكل خوارزمية متوازية.
- تعتبر من الخوارزميات التقليدية حيث أنها لم تقدم أي حلول لمشكلة تكرار الحروف داخل النص المشفر .
- كما يمكن استخدام إسلوب الكسر الأعمى لتحليل الشفرة الناتجة من استخدام خوارزمية التشفير وذلك بتجريب كل المفاتيح المحتملة والبالغ عددها 26 مفتاحا على مستوى الكلمة في النص المشفر .

خلاصة الدراسات السابقة :

لاشك أن الباحثان قد إستفادا من االدراسات السابقة التي تم إستعراضها وذلك من خلال منهجية البحث وإرتباطها بإهتمامات الباحثان :

1- حيث شكلت أرضية جيدة ومؤثرة .
2- الاستفادة من منهجية الدراسات السابقة ونتائجها وتوصياتها كمؤشرات هادية لدراسة الدراسات السابقة .

2.3 خوارزمية التشفير المتحركة :

1 : يتم إدخال كلمة السر وهي عبارة عن أي كلمة (والكلمة يتم تحويلها إلى قيمة عددية عبارة عن مجموع مواقع كلمة السر في جدول ASCII (الآسكى كود)).
2 : يتم جمع مواقع حروف أي كلمة في النص الأصلي.
3 : نحسب رقم ترتيب أي كلمة في النص الأصلي .
4 : ومن ثم يتم جمع مواقع حروف الكلمة مع رقم الترتيب زائداً الرقم السرى فيصبح لدينا قيمة الشفرة .
5 : إذا كانت قيمة الشفرة (مجموع مواقع قيمة الحروف زائداً رقم الترتيب زائداً الرقم السرى) أكبر من 26 نستخدم الدالة mod للحصول على باقي القسمة فقط .
6 : يتم ترتيب الحروف إبتداءً من الحرف الذي يقابل قيمة الشفرة مع الحروف الهجائية .
7 : يتم تشفير هذه الكلمة إبتداءً من حرف الشفرة وذلك بتعويض حروفها بمقابلاتها من الحروف الهجائية لكل كلمة .
8 : يتم تكرار هذه الخطوات حتى آخر كلمة في الملف الأصلي .

ويمكن التعبير عن خوارزمية التشفير المتحركة رياضيا على النحو التالي :

$$E_i = [(w + s + n_i) \bmod 26] \ldots\ldots\ldots\ldots\ldots (1)$$

حيث

w = password
s = sum of position word
n_i = indexing of word

$$P_i = [(w + s + n_i) \bmod 26] \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

مثال :

إذا كانت كلمة السر هي : exceptional إثتثنائي / ممتاز

والنص المطلوب تشفيره هو :

This message is not too hand to break

الخطوة الأولى :

يتم حساب حروف كلمة السر من جدول الآسكي كود

e	x	c	e	p	t	i	o	n	a	L	= 1180
101	120	99	101	112	116	105	111	110	97	108	

الخطوة الثانية :

يتم جمع عدد حروف أي كلمة في النص الأصلي :

t	h	i	S	= 10
1	2	3	4	

m	e	s	s	a	g	e	= 29
1	2	3	4	5	6	7	

i	s	= 3
1	2	

n	o	T	= 6
1	2	3	

t	o	O	= 6
1	2	3	

h	a	n	D	= 10
1	2	3	4	

t	o	=3
1	2	

b	r	e	A	k	= 15
1	2	3	4	5	

الخطوة الثالثة :

يتم حساب رقم ترتيب أي كلمة في النص الأصلي :

النص / كلمة / كلمة	رقم ترتيب الكلمة في النص
this	1
message	2
is	3
not	4

too	5
hand	6
to	7
break	8

الخطوة الرابعة :

يتم جمع عدد الحروف مع رقم الترتيب زائداً الرقم السري فيصبح لدينا قيمة الشفرة :

Plain text	Position +	Indexing +	Secure No.	=	Total Value
this	10	1	1180	=	1191
message	28	2	1180	=	1210
is	3	3	1180	=	1186
not	6	4	1180	=	1190
too	6	5	1180	=	1191
hand	10	6	1180	=	1196
to	3	7	1180	=	1190
break	15	8	1180	=	1203

الخطوة الخامسة :

نبحث عن الحرف الذي يقابل قيمة الشفرة في الحروف الهجائية بعد إستخدام الدالة mod للحصول على رقم ينحصر بين 0 و25 :

Plain text	Total value	Mod 26	Value code	Character code
this	1191	/ 26 =	21	V
message	1210	/ 26 =	14	O
is	1186	/ 26 =	16	Q
not	1190	/ 26 =	20	U
too	1191	/ 26 =	21	V
hand	1196	/ 26 =	0	A
to	1190	/ 26 =	20	U
break	1203	/ 26 =	7	H

الخطوة السادسة :

يتم ترتيب الحروف إبتداءً من الحرف الذي يقابل قيمة الشفرة مع الحروف الهجائية

this						1191		/ 26		= 21		V
a	b	c	d	e	f	g	h	i	J	k	l	M
V	W	X	Y	Z	A	B	C	D	E	F	G	H

n	o	p	q	r	s	t	u	v	W	x	y	Z
I	J	K	L	M	N	O	P	Q	R	S	T	U

الخطوة السابعة :

نبدأ بتشفير هذه الكلمة وذلك بتعويض حروفها بمقابلاتها من الحروف الهجائية .

Plain text			this			1191		/ 26		= 21		V
a	b	c	d	e	f	g	h	i	J	k	l	m
V	W	X	Y	Z	A	B	C	D	E	F	G	H
n	o	p	q	r	s	t	u	v	W	x	y	z
I	J	K	L	M	N	O	P	Q	R	S	T	U
Cipher text			OCDN									

وبناءً على ذلك نجد أن الكلمة this أصبحت OCDN وعليه يمكن إجراء التشفير على بقية الكلمات كالتالي :

Plain text			message			1210		/ 26		= 14		O
a	b	c	d	e	f	g	h	i	J	k	l	m
O	P	Q	R	S	T	U	V	W	X	Y	Z	A
n	o	p	q	r	s	t	u	v	W	x	y	z
B	C	D	E	F	G	H	I	J	K	L	M	N
Cipher text			ASGGOUS									

Plain text			is			1186		/ 26		= 16		Q
a	b	c	d	e	f	g	h	i	J	k	l	m
Q	R	S	T	U	V	W	X	Y	Z	A	B	C
n	o	p	q	r	s	t	u	v	W	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P
Cipher text			YI									

Plain text			not			1190		/ 26		= 20		U
a	b	c	d	e	f	g	h	i	J	k	l	m
U	V	W	X	Y	Z	A	B	C	D	E	F	G
n	o	p	q	r	s	t	u	v	W	x	y	z
H	I	J	K	L	M	N	O	P	Q	R	S	T
Cipher text			HIN									

Plain text			too			1191		/ 26		= 21		V
a	b	c	d	e	f	g	h	i	J	k	l	m
V	W	X	Y	Z	A	B	C	D	E	F	G	H

n	o	p	q	r	s	t	u	v	W	x	y	z
I	J	K	L	M	N	O	P	Q	R	S	T	U
Cipher text			OJJ									

Plain text			hand			1196		/ 26		= 0		A
a	b	c	d	e	f	g	h	i	J	k	l	m
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
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher text			HAND									

Plain text			to			1190		/ 26		= 20		U
a	b	c	d	e	f	g	h	i	J	k	l	m
U	V	W	X	Y	Z	A	B	C	D	E	F	G
n	o	p	q	r	s	t	u	v	W	x	y	z
H	I	J	K	L	M	N	O	P	Q	R	S	T
Cipher text			NI									

Plain text			break			1203		/ 26		= 7		H
a	b	c	d	e	f	g	h	i	J	k	l	m
H	I	J	K	L	M	N	O	P	Q	R	S	T
n	o	p	q	r	s	t	u	v	W	x	y	z
U	V	W	X	Y	Z	A	B	C	D	E	F	G
Cipher text			IYLHR									

وبالتالي يتم تحويل النص الواضح إلى نص مشفر فيكون الناتج النهائي كالتالي :

Plaintext : this message is not too hand to break
Ciphertext : OCDN ASGGOUS YI HIN OJJ HAND NI IYLHR

3.3 خوارزمية فك التشفير المتحركة :

في فك خوارزمية التشفير المتحركة الامر لايختلف كثيراً عن التشفير بطريقة الخوارزمية المتحركة ، بحيث نجد أن الخطوات التي تم بها التشفير هي ذات الخطوات التي سيتم بها فك التشفير ، وعليه ستكون كالآتي :

1 : يتم إدخال كلمة السر التي تم بها التشفير (يتم تحويلها إلى قيمة عددية عبارة عن مجموع مواقع كلمة السر فى جدول الآسكي كود).

2 : يتم جمع مواقع حروف أي كلمة في النص المشفر .

3 : نحسب رقم ترتيب أي كلمة في النص المشفر .

4 : ومن ثم يتم جمع مواقع حروف الكلمة مع رقم الترتيب زائداً الرقم السرى فيصبح لدينا قيمة الشفرة التي سيبدأ منها فك التشفير .

5 : إذا كانت قيمة الشفرة (عدد الحروف زائداً رقم الترتيب زائداً الرقم السرى) أكبر من 26 نستخدم الدالة mod للحصول على باقي القسمة فقط .
6 : يتم ترتيب الحروف إبتداءً من الحرف الذي يقابل قيمة الشفرة مع الحروف الهجائية .
7 : يتم فك هذه الكلمة إبتداءً من حرف الشفرة وذلك بتعويض حروفها بمقابلاتها من الحروف الهجائية لكل كلمة .
8 : يتم تكرار هذه الخطوات حتى آخر كلمة في الملف المشفر .

مثال : إذا كانت كلمة السر هي : exceptional إثتثنائي / ممتاز
والنص المطلوب فك تشفيره هو :

OCDN ASGGOUS YI HIN OJJ HAND NI IYLHR

الخطوة الأولى :

يتم حساب حروف كلمة السر من جدول الآسكي كود(مرفق)

e	x	c	E	p	t	i	o	n	A	L
101	120	99	101	112	116	105	111	110	97	108

= 1180

الخطوة الثانية :

يتم جمع مواقع حروف أي كلمة في النص المشفر :

O	C	D	N	= 10
1	2	3	4	

A	S	G	G	O	U	S	= 29
1	2	3	4	5	6	7	

Y	I	= 3
1	2	

H	I	N	= 7
1	2	3	

O	J	J	= 6
1	2	3	

H	A	N	D	= 10
1	2	3	4	

N	I	= 3
1	2	

I	Y	L	H	R	= 15
1	2	3	4	5	

الخطوة الثالثة :

يتم حساب رقم ترتيب أي كلمة في النص المشفر :

الشفرة	رقم الترتيب في النص
OCDN	1
ASGGOUS	2
YI	3
HIN	4
OJJ	5
HAND	6
NI	7
IYLHR	8

الخطوة الرابعة :

يتم جمع الرقم السري زائداً مجموع الحروف مع رقم ترتيب الحرف فيصبح لدينا قيمة الشفرة :

Plain text	Position +	Indexing +	Secure No.	=	Total Value
OCDN	10	1	1180	=	1191
ASGGOUS	28	2	1180	=	1210
YI	3	3	1180	=	1186
HIN	6	4	1180	=	1190
OJJ	6	5	1180	=	1191
HAND	10	6	1180	=	1196
NI	3	7	1180	=	1190
IYLHR	15	8	1180	=	1203

الخطوة الخامسة :

نبحث عن الحرف الذي يقابل قيمة الشفرة في الحروف الهجائية بعد إستخدام الدالة mod للحصول على رقم ينحصر بين 0 و25 :

Plain text	Total Value	Mod 26	Value code	Character code
OCDN	1191	/ 26 =	21	V
ASGGOUS	1210	/ 26 =	14	O
YI	1186	/ 26 =	16	Q
HIN	1190	/ 26 =	20	U
OJJ	1191	/ 26 =	21	V
HAND	1196	/ 26 =	0	A
NI	1190	/ 26 =	20	U
IYLHR	1203	/ 26 =	7	H

الخطوة السادسة :

يتم ترتيب الحروف إبتداءً من الحرف الذي يقابل قيمة الشفرة (v) مع الحروف الهجائية

OCDN	1191	/ 26	= 21	V

الخطوة السابعة :

نبدأ بفك تشفير هذه الكلمة وذلك بإحلال حروفها بمقابلاتها من الحروف الهجائية .

V	W	X	Y	Z	A	B	C	D	E	F	G	H
a	b	c	d	e	f	g	h	i	J	k	l	M
I	J	K	L	M	N	O	P	Q	R	S	T	U
n	o	p	q	r	s	t	u	v	W	x	y	Z

وبناءً على ذلك نجد أن الكلمة OCDN أصبحت this وعليه يمكن إجراء التشفير على بقية الكلمات كالتالي :

Cipher text			OCDN			1191		/ 26		= 21		V
V	W	X	Y	Z	A	B	C	D	E	F	G	H
a	b	c	d	e	f	g	h	i	J	k	l	m
I	J	K	L	M	N	O	P	Q	R	S	T	U
n	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			this									

Cipher text			ASGGOUS			1210		/ 26		= 14		O
O	P	Q	R	S	T	U	V	W	X	Y	Z	A
a	b	c	d	e	f	g	h	i	J	k	l	m
B	C	D	E	F	G	H	I	J	K	L	M	N
n	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			message									

Cipher text			YI			1186		/ 26		= 16		Q
Q	R	S	T	U	V	W	X	Y	Z	A	B	C
a	b	c	d	e	f	g	h	i	J	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P
n	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			is									

Cipher text			HIN			1190		/ 26		= 20		U
U	V	W	X	Y	Z	A	B	C	D	E	F	G
a	b	c	d	e	f	g	h	i	J	k	l	m
H	I	J	K	L	M	N	O	P	Q	R	S	T
n	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			not									

Cipher text			OJJ			1191		/ 26		= 21		V
V	W	X	Y	Z	A	B	C	D	E	F	G	H

A	b	c	d	e	f	g	h	i	J	k	l	m
I	J	K	L	M	N	O	P	Q	R	S	T	U
N	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			too									

Cipher text			HAND			1196		/ 26		= 0		A
A	B	C	D	E	F	G	H	I	J	K	L	M
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
n	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			hand									

Cipher text			NI			1190		/ 26		= 20		U
U	V	W	X	Y	Z	A	B	C	D	E	F	G
a	b	c	d	e	f	g	h	i	J	k	l	m
H	I	J	K	L	M	N	O	P	Q	R	S	T
n	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			to									

Cipher text			IYLHR			1203		/ 26		= 7		H
H	I	J	K	L	M	N	O	P	Q	R	S	T
a	b	c	d	e	f	g	h	i	J	k	l	m
U	V	W	X	Y	Z	A	B	C	D	E	F	G
n	o	p	q	r	s	t	u	v	W	x	y	z
Plain text			break									

وبناءً على ذلك يتم تحويل النص المشفر إلى النص الواضح فيكون الناتج النهائى كالتالى :

OCDN ASGGOUS YI HIN OJJ HAND NI IYLHR

this message is not too hand to break

4. تحليل خوارزمية التشفير المتحركة :

نستعرض في هذا الجزء بعض أدوات قياس الخوارزمية متمثلة في استخدام تحليل التشفير وإسلوب الكسر الأعمى .

1.4 أدوات معايرة خوارزمية التشفير المتحركة

هناك أسلوبان يمكن استخدامهما لمعرفة النص الصريح ولفك تشفير الرسالة المشفرة دون معرفة تفاصيل نظام التشفير المستخدم أو المفتاح مسبقاً وهما:

1.1.4 تحليل التشفير:

ويعتمد هذا الأسلوب على تحليل التشفير بناء خوارزمية معينة والاعتماد على بعض معطيات النص الصريح المعروفة للمحلل (المهاجم) لاستنتاج النص الصريح أو استنتاج المفتاح

المستخدم، يتطلب هذا الأسلوب أن تكون خوارزمية التشفير معروفة بالنسبة للمحلل ، قد يستخدم المحلل بعض الطرق الإحصائية للحصول على النص الصريح أو المفتاح ومن طرق التحليل .

1.1.1.4 إسلوب بن الكندي :

يعتمد إسلوب ابن الكندي لتحليل الشفرة على الحقيقة أن التشفير لا يغير التكرار النسبي لاستخدام الحروف في النص الصريح، وأيضا كلما كان حجم النص المشفر كبيرا زاد احتمال استنتاج النص الصريح أو المفتاح المستخدم في التشفير[6].

إن تطبيق إسلوب بن الكندي على خوارزمية التشفير المتحركة نجده لايحقق أي نجاح ، بل يعتبر إسوب بن الكندي لا مجال لتطبيقه في خوارزمية التشفير المتحركة وذلك لغياب خاصية التكرار النسبى للحروف في النص المشفر، وبالتالي لايمكن تطبيق التكرارالمعياري للحروف .

2.1.1.4 طريقة كيسسكي KAISISKI

هذه الطريقة بسيطة حيث يجب ملاحظة حرفين أو ثلاثة حروف تتكرر كثيرا ولكن بشرط أن لايفصل بينها حرف آخر ، مثلا لو تكررت الحروف XYZ كثيرا ، وكل مره تتكرر فيها هذه الحروف تأتي مجتمعة مع بعضها بهذا الشكل ، يمكن التعرف على عدد المفاتيح وذلك بحساب عدد الحروف التي تأتي بين الـ XYZ الأولى والثانية ، ومن ثم يتم حساب عدد الحروف بين الـ XYZ الثانية والثالثة ، وهكذا الى النهاية ، بعدها يمكن بقليل من المحاولة معرفة عدد المفاتيح **[7]** .

نجد أن تطبيق طريقة كيسسكي على خوارزمية التشفير المتحركة لكشف النص المشفر والوصول إلى النص الواضح لن تجد لها مكاناً ، حيث أنالتشفير على مستوى الكلمة يحدث تغييراً جزرياً في نوع الحروف فكل كلمة ولو تكررت أكثر من مرة في النص يكون لها حروف تشفير تختلف عن سابقتها من الكلمات المراد تشفيرها.

2.1.4 هجوم الكسر الأعمى أو البحث الشامل :

في هذا الأسلوب يحاول المهاجم تجريب كل المفاتيح المحتملة على مقطع من النص المشفر ويستمر في هذه المحاولات حتى يتحصل على نص صريح مفهوم وواضح ، في هذا الأسلوب كلما زاد طول المفتاح أصبح كسر الشفرة أكثر صعوبة ، إن الزمن المطلوب لتحليل الشفرة بهذا الأسلوب يعتمد بدرجة كبيرة على مقدرات الحاسوب المستخدم.

يعتبر إسلوب التشفير "آمنا بشكل مطلق" unconditionally secure " إن لم يحتو النص المشفر على معلومات كافية لاستنتاج النص الصريح المقابل له مهما بلغ عدد النصوص المشفرة والمتوفرة لدى المحلل ومن المفروض في هذه الحالة أن لا يتمكن المحلل فك تشفير الرسالة مهما توفر له من الوقت والقدرة الحاسوبية، حيث لا تتوفر المعلومات اللازمة لذلك .

لا توجد خوارزمية تشفير آمنة بشكل مطلق ، إلا في حالة أساليب التشفير المعروفة باسم "الطبعة التي تستخدم مرة واحدة" (one-time pad) ، لذلك تصمم خوارزميات التشفير بناءَ على الآتي:

- أن تكون تكلفة تحليل الشفرة تفوق قيمة المعلومات المشفرة .
- أن يكون الزمن اللازم لتحليل الشفرة يفوق الفترة الزمنية المفيدة للمعلومات المشفرة [8] .

إذن عن طريق إسلوب البحث الشامل لن تنجو أي خوارزمية مهما عظم شأنها من الوصول الى النص الصريح ، ولكن يبقى زمن الوصول إلى النص الصريح هو الفيصل في مدى صمود هذه الخوارزمية وملائمتها لطبيعة البيانات التى تم تشفيرها .

ففي خوارزمية التشفير المتحركة العدد المحتمل للمفاتيح يساوى 26! *xمفتاحاً محتملاً ، حيث x تساوي عدد الكلمات في النص المشفر ، أن هذا العدد الكبير للمفاتيح يزيد من صعوبة تحليل الشفرة ويحد من إمكانية الكسر الأعمى كإسلوب لتحليل شفرة خوارزمية التشفير المتحركة .

جدول رقم (1) يوضح إسلوب البحث الشامل[9]

26 characters (permutation)	**$26! = 4 \times 10^{26}$**	**$2 \times 6.4 \times 10^{12}$ years = 10^{26} µs**	**6.4×10^{6} years**

3.1.4 مبدأ كيركوف [10]

أن أحد مبادئ علم التشفير الحديث يعرف بمبدأ كيركوف (Principle Kerckhoffs) ، و هو أستاذ جامعي هولندي ، ويعتبر من الشخصيات المهمة في علم التشفير في القرن التاسع عشر، وقد قام بنشر مقالتين بعنوان "التشفير العسكري" وصّف من خلالهما المبادئ الأساسية لبناء نظام تشفير، وأحد هذه المبادئ - ويدعى مبدأ كيركوف- ينص على أن أمان النظام يجب ألا يعتمد على بقاء خوارزمية التشفير سرية ، بمعنى أن اكتشاف الخوارزمية المستخدمة يجب ألا يؤثر إطلاقاً على أمان النظام ، والواقع أن التشفير في العصر الحديث قائم على مبدأ نشر خوارزمية التشفير!.

ولهذا المبدأ عدة مبررات منطقية وعملية ، أولها أن نشر الخوارزمية سيؤدي إلى محاولة اختراقها من قبل عدد كبير من الخبراء ، وبالتالي إذا نجت من هذه المحاولات فإنها ستكون محلاً للثقة، كما أنه من الممكن اكتشاف الخوارزمية المستخدمة في التشفير باستخدام تقنيات الهندسة العكسية (Reverse Engineering) ، وهذا ما حصل فعلاً في خوارزمية التشفير المستخدمة في الأجهزة الخلوية (GSM) ، فقد قامت الشركة المصنعة بتجاهل مبدأ كيركوف وأبقت خوارزمية التشفير سرية ، ولم يستغرق الأمر وقتاً طويلاً حتى تمت عملية اكتشاف الخوارزمية وكسرها! وبالتالي وبالرغم من تشفير البيانات المرسلة عبر الأجهزة الخلوية العادية إلا أنها لا تعتبر آمنة لهذا السبب.

هذا المبدأ يوضح سبب أمان الأنظمة مفتوحة المصدر، فهذه الأنظمة لا تعتمد لتحقيق الأمان على سرية الخوارزمية ، وهي بهذا الشكل تكون أكثر أماناً من الأنظمة مغلقة المصدر[11].

وقد تميزت خوارزمية التشفير المتحركة بمبدأ كيركوف حيث لم تبقى على سرية الخوارزمية وإنما إعتمدت نشر الخوارزمية بل والحصول عليها لايغير من فعاليتها ،وهو ماجرى عليه التشفير في العصر الحديث .

5. النتائج :

سيتناول الباحثان في هذا الفصل ماتوصلوا إليه من نتائج عملية جراء تنفيذ خوارزمية التشفير المتحركة وماخضعت إليه من قياسات ، وذلك من خلال المزايا التى وفرتها الخوارزمية الجديدة والتى عالجت بها معظم نقاط الضعف في التشفير خاصة التي إتسمت بها طرق التشفيرالمتناظر بالإحلال التقليدية وذلك من خلال الآتي :

1.5 إختلاف المفتاح في كل كلمة يجعل من الحروف المتشابهة في أكثر من كلمة في النص الأصلي مختلفة في النص المشفر .

2.5 خوارزمية التشفير المتحركة تقف صلبة أمام تحليل الشفرة باستخدام تحليل اللغة ، الذى يعتمد على تحديد التكرار النسبي لاستخدام الحروف في الرسالة المشفرة ومقارنته بالتكرار النسبي النموذجي لاستخدام الحروف الانجليزية ، حيث أوضح ابن الكندي طريقة لتحليل الشفرة في كتابة المنشور في القرن التاسع ، والذي تم اكتشافه في العام 1987 في اسطنبول .

3.5 مهما كانت القيمة الناتجة من جمع عدد حروف الكلمة مضافاً إليها رقم الترتيب كبيراً فانه بواسطة الدالة mod يتم الحصول على رقم في المدى 0 إلى 25 وهذا يعني إستبعاد حدوث أي خطأ في تحديد قيمة الشفرة .

4.5 يشكل التشفير على مستوى الكلمة تغييراً جزرياً في نوع الحروف فكل كلمة ولو تكررت أكثر من مرة في النص يكون لها حروف تشفير تختلف عن سابقتها من الكلمات المراد تشفيرها .

5.5 يستحيل التكهن وإكتشاف الكلمات الصغيرة مثل is , on , to , in , the , too , you .

6.5 وجود مفتاح خارجي للتشفير ولفك الشفرة يزيد من عملية أمنية التشفير.

7.5 تبادل المفاتيح يعتبر ميزة أساسية لهذه الخوارزمية بحيث يقلل من إمكانية الوصول للنص الاصلي.

8.5 إمكانية تشفير النص الواضح أكثر من مرة وذلك بإستخدام أكثر من مفتاح ، بمعنى أن النص الواضح يمكن إعادة تشفيره بعدد غير محدود من كلمات السر، وبالتالي يصعب التكهن للحصول على النص الأصلي .

9.5 في حالة ماإذا كان باقي القسمة يساوي صفراً فإن النص الواضح سيساوي النص المشفر ، وذلك كما رأيناه في المثال السابق عند تشفير كلمة hand ، يمكن تجاوز ذلك بتغيير كلمة السر بكلمة أخري حتى لايكون باقي القسمة صفراً .

6. الخلاصة :

وعليه فمن أهمية بقاء المعلومات والبيانات في سرية تامة يصعب إختراقها قدمت هذه الورقة خوارزمية جديدة في تشفير ملفات البيانات النصية كأحد تطبيقات التشفير المتناظر بالإحلال ، معالجة بذلك العيوب التى لحقت بالتشفير المتناظر بالاحلال لاسيما بعد أن تم هجره ، وبذلك تفتح الباب واسعاً لمزيد من الدراسات في هذا المجال الهام لاسيما وأن خوارزمية التشفير المتحركة الجديدة التي تعتمد طريقة التشفير المتناظر قدمت نص مشفر يصعب اختراقه ، كما حققت درجة عالية من السرية لملفات البيانات وذلك بتوفير مفتاح خارجي جعل البيانات في مأمن ومحافظة على سريتها .

7. المراجع

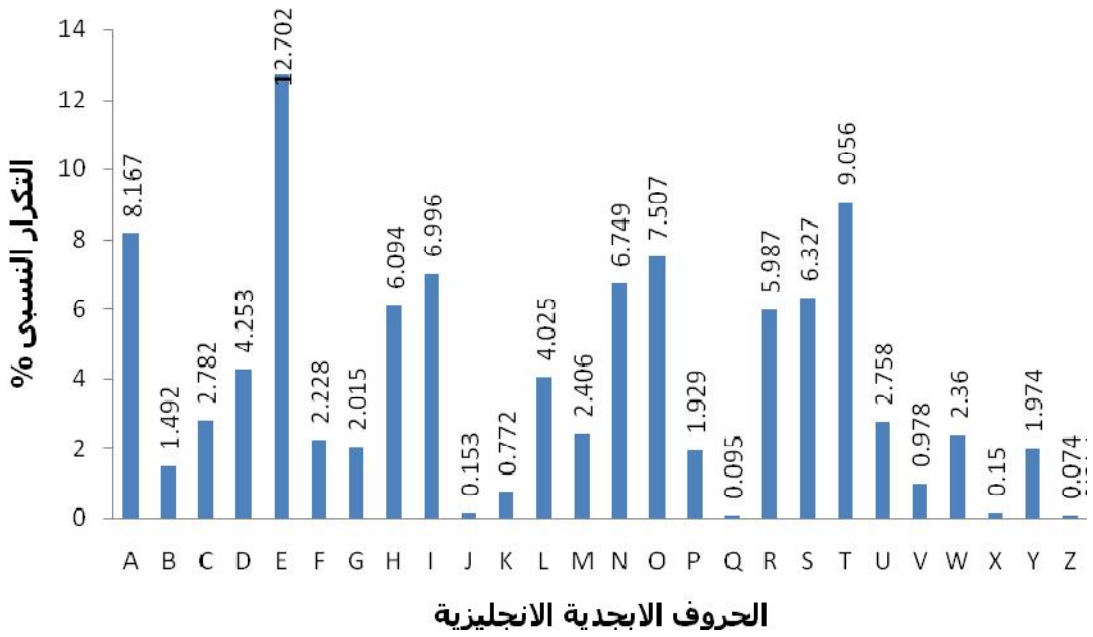
[1]محمد ابو طه ورضوان طهبوب ، خوارزمية البعثرة العملية ذات الاتجاه الواحد باستخدام مصفوفة لا معكوس لها اعتماداً على تقنية هيل للتشفير ، © *Communications of the Arab Computer Society, Vol. 4 No.1, August, 2011* ، جامعة بوليتكنيك فلسطين، كلية المهن التطبيقية، ص.ب.198، الخليل، فلسطينm_abutaha@ppu.edu، جامعة بوليتكنيك فلسطين، كلية الهندسة، ص.ب.198، الخليل، فلسطين radwant@ppu.edu ، صفحة 2 .

[2] سامي محمد شريف عبد **الله - 2008 - أمن** الحواسيب – منشورات جامعة السودان المفتوحة - برنامج الحاسوب - رمز المقرر ورقمه حسب 5043 ، صفحة 60 .

[3] William Stallings Cryptography and Network Security Principles and Practices, Fourth Edition و Publisher: Prentice Hall و Pub Date: November 16, 2005, page 39 .

[4] دراسة : هاشم أبوبكر ، خوارزميات أمن البيانات، نشر 2005/22/08 .

[5] نورة عبد المحسن الصميخي ، جامعة الملك سعود ،مركز التميز لأمن المعلومات © 2012 - سياسة الخصوصية التشفير بالطرق الكلاسيكية تصنيفات ، أمن المعلومات في التعاملات الإلكترونية .
[6] سامي محمد شريف ، مرجع سابق ذكره ، ص 108 .
[7] عالم البرمجة والمبرمجين، منتديات العاصفة ،منتدى لغة+ + c / c
Available at http://www.3asfh.net/vb Accessed March 2013 .
[8] سامي محمد شريف مرجع سابق ذكره ، ص 53 .
[9] Available at www.up.edu.ps/upinar/moodledata/299/ch2-part1.ppt Accessed April 2013
[10] Available at http://www.alahham.wordpress.com Accessed June 2013
.
[11] المرجع السابق ذكره .



الشكل رقم (1) التكرار النسبي النموذجي لاستخدام الحروف الانجليزية [3]