Hyper Secure Algorithm for Text

Melad jader saeed
meladjader@uomosul.edu.iq
College of Computer Science and Mathematics
University of Mosul, Iraq

Received on : 29/4/2010 **Accepted on :25/10/2010**

ABSTRACT

Classical encryption methods depend on two basic encryption method, namely MONO ALPHABET and POLY ALPHABET.

In this research, we developed a hybrid encryption algorithm to overcome the weaknesses in both methods and employed the basic methods of themselves. The output ciphertext is characterized with the high security when it does not give the expected results using the basics to break the code, namely, (adoptig the frequencies of the language used i.e. Frequency Analysis, besides Coincidence and Kasiski test).

The problem of distributing the secret key has been also overcome by adopting a new technique to hide the key inside the encrypted text in a nearly proposed way. Experimental result has been demonstrated that it is difficult to determine the used encryption method ,in this algorithm we used MATLAB.

Keyword: mono alphabet, poly alphabet, encryption, secret.

خوارزمية سرية هجينة للنصوص

ميلاد جادر سعيد

كلية علوم الحاسوب والرياضيات، جامعة الموصل

تاريخ الاستلام: 2010/4/29 **تاريخ القبول: 2010/10/25**

الملخص

اعتمدت طرق التشفير الكلاسيكية على طريقتين أساسيتين وهما طريقة التشفير أحادية الهجائية MONO ALPHABET وطريقة التشفير متعددة الهجائية POLY ALPHABET .

في هذا البحث تم تطوير خوارزمية تشفير مهجنة تجاوزت نقاط الضعف الموجودة في كلا الطريقتين واعتمدت الطرق الأساسية نفسها. امتاز النص المشفر الناتج بالأمنية العالية من حيث عدم إعطاء النتائج المتوقعة عند استخدام الأساسيات المعتمدة في كسر الشفرة وهي (اعتماد ترددات اللغة المستخدمة Frequency Analysis والصدفة Coincidence واختبار كاسيسكي Kasiski Test) .

كما تم تجاوز مشكلة توزيع المفتاح السري Secret key وذلك باعتماد أسلوب جديد وهو إخفاء المفتاح داخل النص المشفر بطريقة جديدة مقترحة، أوضحت التجارب العملية صعوبة تحديد نوع الطريقة المستخدمة في التشفير، وقد تم بناء هذه الخوارزمية باستخدام لغة MATLAB.

الكلمات المفتاحية: أحادية التهجئة، متعددة التهجئة، تشفير، سرية.

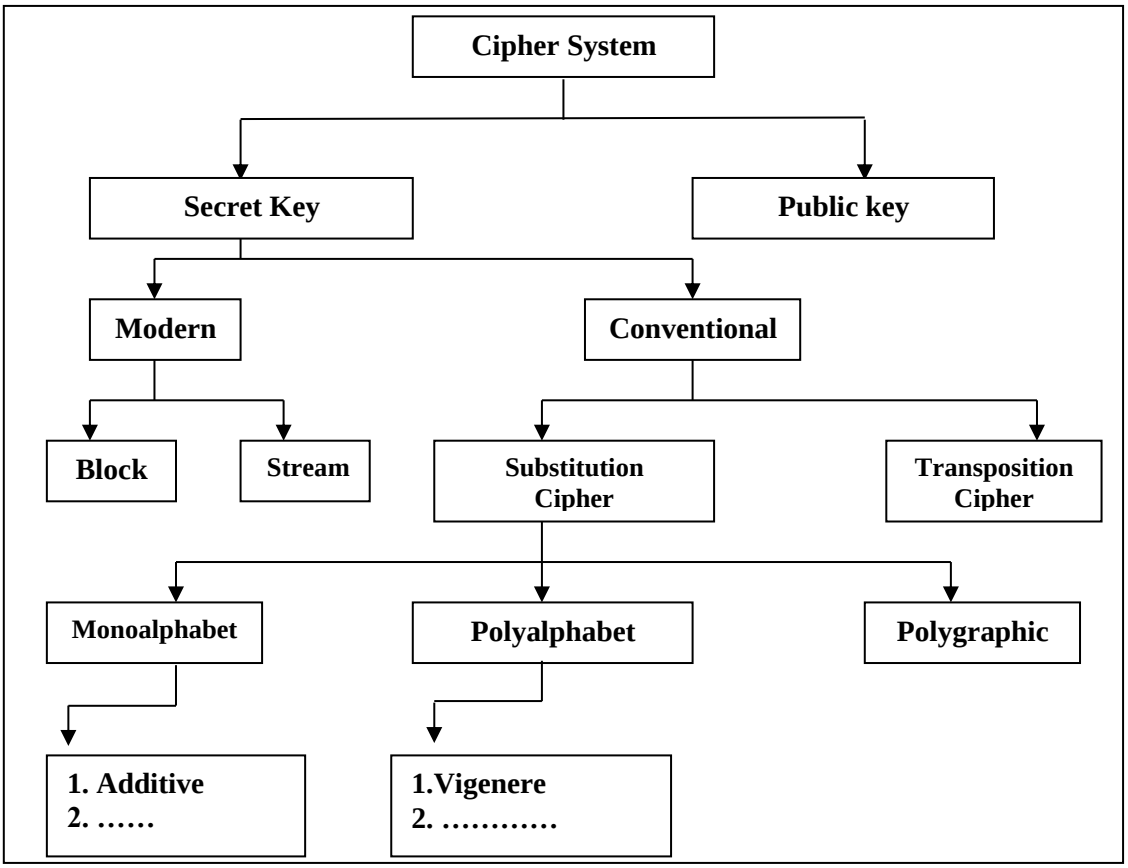
1. المقدمة Introduction

شهد العصر الحالي التقدم التقني وخاصة في مجال الحاسوب بتنفيذ أنظمة أكثر صعوبة من السابق لمعالجة مشاكل الأمنية الجديدة البالغة التعقيد، بسبب أن الأنظمة الحديثة قد قطعت أشواطا بعيدة في مجالات الاحتياجات الإنسانية مما يتطلب الحاجة إلى هندسة الأمنية Security Engineering للأخذ بنظر الاعتبار الصفات الرياضية والمادية للأنظمة الأمنية لتطويرها بطريقة أكثر فاعلية.وقد تفاقمت مشكلة الأمنية هذه الأيام وذلك لاعتماد جميع الأعمال الإنسانية على مفردات المكننة (Assets) وهي الحواسيب والمعلومات وخطوط الاتصال وكذلك أصبحت هذه المفردات تتعرض لأخطار متنوعة يصعب على النظام الأمني الواحد الوقوف تجاهها

لان لكل خطر هناك الخطوات والسياسة الأمنية المختلفة الواجب إتباعها لحماية هذه المفردات [1]. إن مفردة (Asset) تعني أي شي ضمن النظام المعلوماتي وله قيمة تتطلب درجة مختلفة من الحماية. إن أكثر هذه المفردات التي تتطلب حماية في بيئة أنظمة المعلومات هي المعلومات أو البيانات نفسها، وهذه البيانات دائما يمكن تصنيفها إلى عامة، أو حساسة أو سرية أو عالية السرية. إن بناء نظام يلبي متطلبات الأمنية يكون صعب جداً بسبب أن المشكلة المطلوب معالجتها هي ليست ساكنة لكنها متحركة. وأي نظام امني يصنف حسب ثلاث حقائق [3, 2] :

1. العملية الرياضية التي يعتمد عليها تحويل النص الأصلي إلى النص المشفر باستخدام مفتاح التشفير.
2. النص المشفر الناتج هل المطلوب تكوينه كمجاميع Block أو كسلسلةٍ Stream .
3. نوعية المفتاح المستخدم هل هو منفرد private أو مزدوج public - private.

ولتحديد أي نظام يلائم متطلبات النظام الأمني المراد استخدامه لحماية المعلومات يجب معرفة الأنواع الأساسية لأنظمة التشفير ومن ثم تحديد المناسب منها وهي موضحة بالشكل (1)[4]



شكل (1). أنظمة التشفير

التشفير الإبدالي Transposition Cipher:

1-1 التشفير الإبدالي Transposition Cipher:

يتم في هذا التشفير إعادة ترتيب حروف الرسالة الواضحة بحيث تبقى كما هي بينما يتغير موقعها [5,1] ولهذا فان النص المشفر يحتوي نفس أحرف النص الأصلي ولكن الترتيب مختلف ومن أمثلته طريقة Zig-Zag، طريقة المربع الكامل وغيرها.

2-1 التشفير التعويضي Substitution Cipher :

في تقنية التعويض يتم استبدال حروف النص الواضح بحروف أخرى أو أعداد أو رموز. إذا نظرنا إلى النص الواضح كسلسلة من البتات، فأن الشفرة التعويضية هي عبارة عن استبدال نماذج بتات الشفرة الواضحة بنموذج بتات النص المشفر.اي انه يكون موقع حرف النص الواضح ثابت لكن قيمته سوف تتغير.وهي تنقسم إلى قسمين[1 ,6]:

- شفرة التعويض الأحادية الهجائية Monoalphabet
  ومن أمثلتها (addative, **Caesar's cipher** ,affine)
- شفرة التعويض المتعددة الهجائية Polyalphabet
  ومن أمثلتها (Vigenere, Beaufort)

1-2-1 شفرة الجمع المعياري Additive Cipher:

تعتبر من الطرق التعويضية الأحادية الهجائية حيث يتم استبدال كل حرف في هذه الشفرة بحرف يكون تسلسله ثابت بعده في الحروف الأبجدية [1] أي يقع على بعد n إلى يمين الحرف المراد تشفيره ضمن الأبجدية. ويمكن استخدام المعادلة التالية

$$P + n = \mathbf{C} \mod 26, \qquad 0 \le C \le 25$$

حيث أن: P أحرف النص الأصلي و C أحرف النص المشفر و n مقدار الإزاحة.

تعتبر هذه الشفرة بسيطة لان القانون التابع لها هو سهل التذكر وان الضعف الرئيسي في هذه الشفرة انه يمكن توقع النموذج بكامله، كما انه في هذه الشفرة يمكن ملاحظة ما يلي:

1. خوارزمية التشفير وفك الشفرة معروفة.
2. يوجد 26 مفتاح فقط لتجربتها.
3. لغة النص الصريح معروفة ومن السهل قراءتها.

2-2-1 شفرة الفيجينير Vigenere Cipher:

إن ضعف شفرة الحروف المنفردة هو بالتوزيع المتكرر والذي يعكس توزيع الحروف الأبجدية المحددة.الشفرة التي يكون تشفيرها أكثر سرية هي التي تضع توزيع منتشر والذي لا يعطي أي معلومات لمحلل الشفرة[4,3].

واحدة من الطرق التي تنشر التوزيع هي شفرة الفجينير وهي تقوم بعملية التشفير عن طريق سلسلة من الشفرة القيصرية المختلفة تعتمد على حروف المفتاح المستخدم حيث انه كل حرف في المفتاح يحدد الشفرة القيصرية المستخدمة لتشفير ذلك الحرف.

كما انه يمكن استخدام الجدول الموضح بالشكل (2) لتسهيل عملية التشفير وفك الشفرة

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

شكل (2). Vigenere Table

ويمكن أيضا القيام بعملية التشفير وفك الشفرة رياضياً عن طريق المعادلتين الاتيتين

$C_i = P_i + K_i \quad \text{mod } 26$ للتشفير

$P_i = C_i - K_i \quad \text{mod } 26$ لفك الشفرة

حيث أن P أحرف النص الأصلي C أحرف النص المشفر

K تمثل أحرف المفتاح I تسلسل الحرف

من أهم مميزات طريقة الفجينير إخفاءها ترددات الحروف الأصلية حيث أن الحرف الواحد في اللغة يمكن أن يتحول إلى أكثر من حرف في النص المشفر، وذلك يرجع إلى سبب استخدام أحرف المفتاح متغيرة وبهذا تتغير ترددات الأحرف الأصلية ويصبح من الصعوبة كسر هذه الطريقة بالاعتماد على ترددات الحروف المستخدمة Character Frequency.

إن مساعدة صغيرة من توزيعات التكرار ونماذج الحروف، يمكن كسر شفرة التعويض باليد. لذلك، فان برامج الحاسوب ومع كمية مناسبة من النص المشفر يستطيع محلل الشفرة الجيد ان يكسر مثل هذه الشفرة في

ساعة واحدة . حتى بالنسبة للشخص غير المدرب فمن الممكن ان يحدد النص الواضح في يوم واحد أو أكثر. ولسوء الحظ فان الشفرة المتعددة الحروف هي ليست مقاومة للكسر. الطريقة المستخدمة لكسر مثل هذه الشفرة هي بتحديد عدد الحروف الأبجدية المستخدمة، ومن ثم تجزئة النص المشفر إلى الأجزاء التي تم تشفيرها بنفس الحروف الأبجدية، وحل كل جزء كتعويض أحادي الهجائية. وهنالك أدوات فعالة تستطيع فتح شفرة رسائل كتبت بعدد كبير من الحروف هما طريقة كاسيسكي لتحديد نموذج تكرار التشفير والصدفة لتوقع الحروف المستخدمة في التعويض إضافة إلى ترددات الأحرف نفسها[1 ,7]. كما انه تم إثبات أن الخوارزميات التي تستخدم التعويض والإبدال غير آمنة وذلك بسبب التحليلات الإحصائية للغة. إضافة إلى أن التعويض التي يتم إتباعه بالإبدال أكثر أمانا ومقاومة لكسر الشفرة. وهذا هو الجسر الواصل بين خوارزميات التشفير الكلاسيكية وخوارزميات التشفير الحديثة [8].

بعد ملاحظة نقاط الضعف في كلا النوعين ودراستها وتحليلها وكمحاولة لتلافي هذه النقاط، ارتأينا في بحثنا هذا التهجين بين النوعين وفق قواعد وأسس لإنتاج طريقة أكثر تعقيداً وسرية ولزيادة قوة الطريقة المقترحة فقد تم استخدام مفتاح متغير Variant يختلف نوعه وطوله حسب النص المراد تشفيره للابتعاد عن مشاكل المفتاح الثابت Static.

2. الخوارزمية المقترحة للتشفير

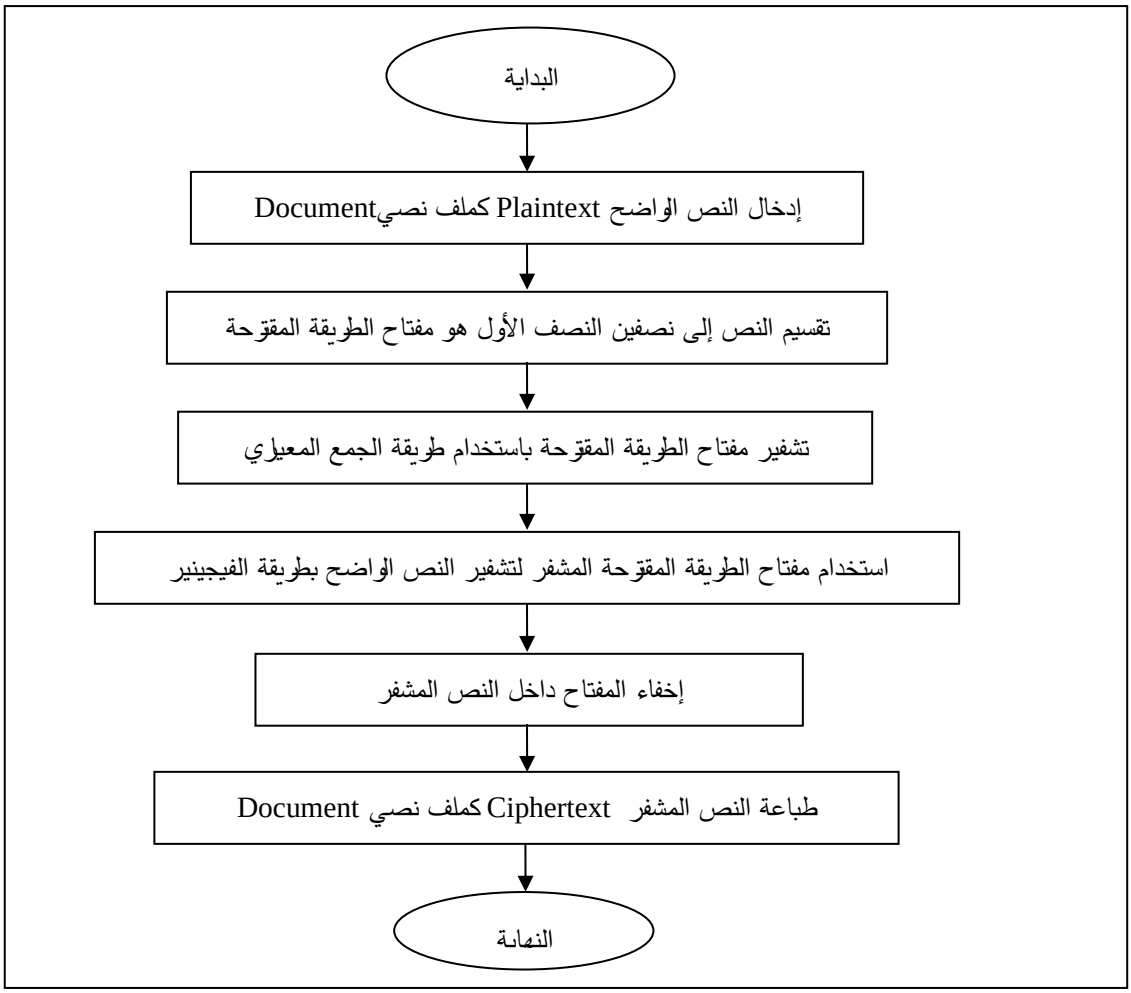
يمكن تلخيص الخوارزمية المقترحة للتشفير بالخطوات التالية:

المدخلات: النص الواضح المراد تشفيره Plaintext بصورة ملف نصي Document

1. قراءة النص الواضح (المدخلات)
2. تقسيم المدخلات إلى قسمين واستخدام النصف الأول بعد معالجته كمفتاح للتشفير بطريقة الفجينير.
3. استخدام طريقة الجمع المعياري لتشفير المفتاح المعتمد في هذه الطريقة المقترحة (النصف الأول من النص الواضح المدخل) مع اعتماد طوله كقيمة للمفتاح المستخدم في تلك الطريقة.
1. استخدام المفتاح الناتج في الخطوة السابقة لتشفير النص (المدخلات) بأكملها باعتماد طريقة الفيجينير
2. إخفاء مفتاح التشفير المستخدم بطريقة الفيجنير داخل النص المشفر الناتج من الخطوة السابقة باستخدام طريقة إخفاء جديدة مقترحة
3. طباعة النص المشفر

المخرجات: نص مشفر Ciphertext بصورة ملف نصي Document

والشكل (3) يوضح المخطط الانسيابي لخطوات عمل الطريقة المقترحة



الشكل (3). المخطط الانسيابي لخطوات عمل الطريقة المقترحة

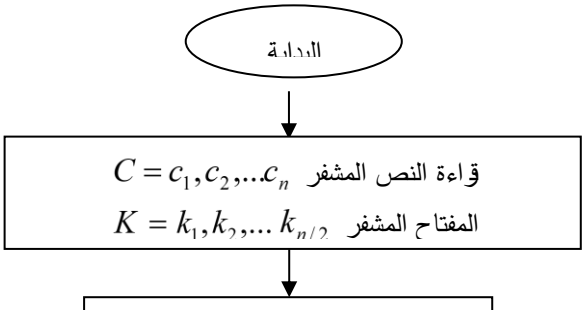
3. خوارزمية الطريقة المقترحة للإخفاء

المدخلات: النص المشفر بطريقة فيجينير والمفتاح المشفر بطريقة الجمع المعياري.

1. تقسيم النص المشفر إلى نصفين
2. إجراء عملية XOR بين العنصر الأول من النصف الثاني من النص المشفر والعنصر الأول من المفتاح.
3. خزن القيمة الناتجة بالخطوة السابقة بعد العنصر الأول في النصف الثاني من النص المشفر.
4. الانتقال إلى العنصر التالي من كل من الجزء الثاني من النص المشفر والمفتاح.
5. الاستمرار بهذه العملية لحين الوصول إلى نهاية النص وبهذه الحالة نكون قد وصلنا إلى نهاية المفتاح أيضا.
6. طبع النص الناتج من التشفير والإخفاء

المخرجات:النص المشفر وهو يمثل غطاء للمفتاح المخفي داخله

والشكل (4) يوضح المخطط الانسيابي لخوارزمية الإخفاء المقترحة



1. الخوارزمية المقترحة لفك الشفرة

يمكن تلخيص الخوارزمية المقترحة لفك الشفرة كما يلي:

المدخلات: النص المشفر Ciphertext $C = c_1, c_2, ...c_n$ كملف نصي Document File

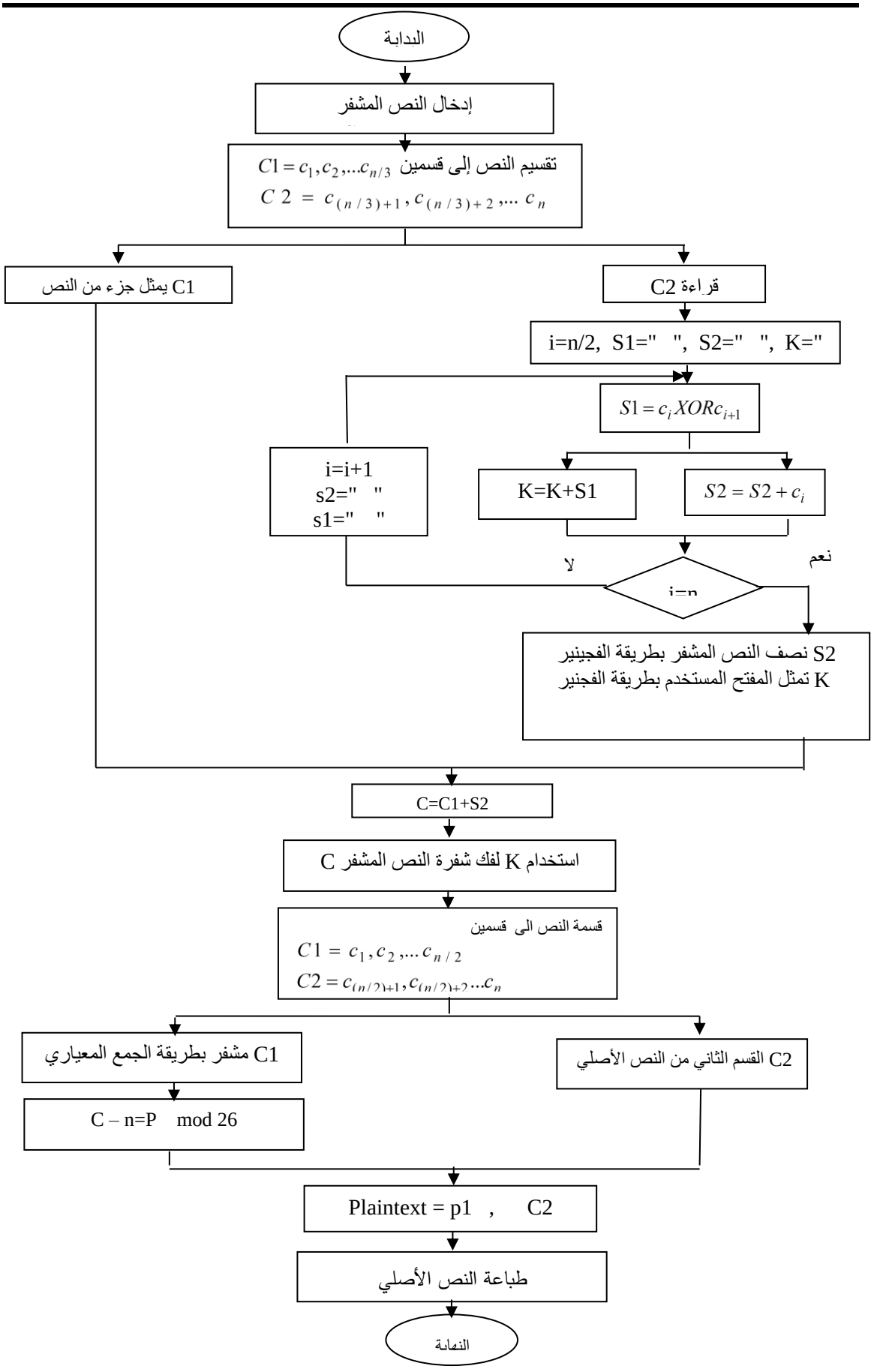
1. تقسيم النص المدخل إلى قسمين، لمعرفة طول المفتاح المستخدم لكون النص المشفر يتكون من نص مشفر ومفتاح مخفي بداخله، وطول ذلك المفتاح هو نص طول النص الأصلي،
   $C1 = c_1, c_2, ...c_{n/3}$ يمثل جزء النص المشفر بطريقة الفيجينير
   $C2 = c_{(n/3)+1}, c_{(n/3)+2}, ...c_n$ يمثل القسم الذي يحوي نصف النص المشفر إضافة إلى المفتاح المخفي ،ويكون طوله ضعف القسم الأول
2. قراءة C2 للكشف عن المفتاح المخفي بداخلها.
3. إجراء عملية XOR بين كل حرفين متتاليين في C2
4. خزن أول قيمة مستخدمة في XOR في متغير S2، وخزن ناتج عملية XOR داخل متغير Kيمثل المفتاح المستخدم في الفجينير
5. استخدام المفتاح الناتج K لفك شفرة النص المشفر بطريقة الفجينير.
6. قسمة النص الناتج إلى قسمين
   $C1 = c_1, c_2, ...c_{n/2}$ يكون مشفر بطريقة الجمع المعياري
   $C2 = c_{(n/2)+1}, c_{(n/2)+2}...c_n$ يمثل جزء من النص الأصلي
7. فك شفرة الجزء الأول باستخدام المعادلة التالية

   C - n=**P** mod 26 $0 > P > 25$
8. دمج الجزء الأول بعد فك شفرته والجزء الثاني ينتج النص الأصلي

   Plaintext = p1 , p2

المخرجات: النص الواضح Plaintext مخزون بملف نصي Document File

والشكل (5) يوضح المخطط الانسيابي لخوارزمية فك الشفرة للطريقة المقترحة



الشكل (5). المخطط الانسيابي لفك شفرة الطريقة المقترحة

5. التحـليل

5-1 التحليل بواسطة ترددات الأحرف Character Frequency Analysis

من المعلوم أن ترددات الأحرف الانكليزيـة تمتلك نسب معروفة لا تتغير باختلاف النص الانكليزي مـع الأخذ بنظر الاعتبار أن النص هو نص عام أي غير محدد بموضوع معين. والجدول (1) يوضح ترددات الأحرف للغة الانكليزية، بعد تطبيق الخوارزمية المقترحة فان ترددات الأحرف أصبحت عشوائية وتتباين من مثال إلى آخر [4].

جدول (1). ترددات الحروف للغة الانكليزية

Letter	Frequency
E	0.127
T	0.097
I	0.075
A	0.073
O	0.068
N	0.067
S	0.067
R	0.064
H	0.049
C	0.045
L	0.040
D	0.031
P	0.030
Y	0.027
U	0.024
M	0.024
F	0.021
B	0.017
G	0.016
W	0.013
V	0.008
K	0.008
X	0.005
Q	0.002
Z	0.001
J	0.001

5-2 الصدفة Coincidence

وهي طريقة لتقييم مدى مطابقة توزيع معين إلى توزيع الحروف في اللغة الانكليزية، إن طريقة الصدفة هي قياس للفروقات بين تكرارات التوزيع. يتم احتساب دليلا للتطابق اعتمادا على المعادلة التالية [1]

$$IC = \frac{\sum_{\lambda=A}^{Z} F_\lambda (F_\lambda - 1)}{n \times (n-1)}$$

حيث إن n عدد حروف النص المشفر.

IC قيمة عددية ثابتة تعتمد على نوع اللغة، ففي اللغة الانكليزية تكون قيمتها تقريباً 0.065

$F\lambda$ تردد حرف رقم λ في الرسالة المشفرة

نستخدم قيمة دليل التطابق IC للتأكد من نوع النظام المستخدم في تشفير الرسالة إذا كان تعويضي أو أحادي، وحسب الجدول (2) التالي

m	1	2	5	10	large
IC	0.065	0.052	0.043	0.041	0.038

الجدول (2). العلاقة بين IC وعدد حروف المفتاح

فإذا كان الشخص ليس لديه أي معلومات عن النص الواضح فانه يقوم بحساب قيمة IC، فإذا كانت القيمة الناتجة قريبة من 0.065 هذا يعني انه قد تم استخدام احد طرق التشفير الأحادية الهجائية وبخلافه فانه يكون قد تم استخدام احد الطرق المتعددة الهجائية [2].

إلا انه في هذا البحث بعد تطبيق الخوارزمية المقترحة على عدة أمثلة اتضح انه في بعض الأحيان تظهر قيمة IC اقل من القيمة المحددة والبعض الآخر أكثر من القيمة. وهذا يربك المتطفل في تحديد طريقة التشفير المستخدمة هل هي أحادية أو متعددة الهجائية لأنه تم التهجين بينهما.

3-5 اختبار كاسيسكي Kasiski Test

تعتمد هذه الطريقة على انتظام اللغة الانكليزية، ليس فقط الحروف ولكن أيضا مجاميع الحروف والكلمات المكررة.

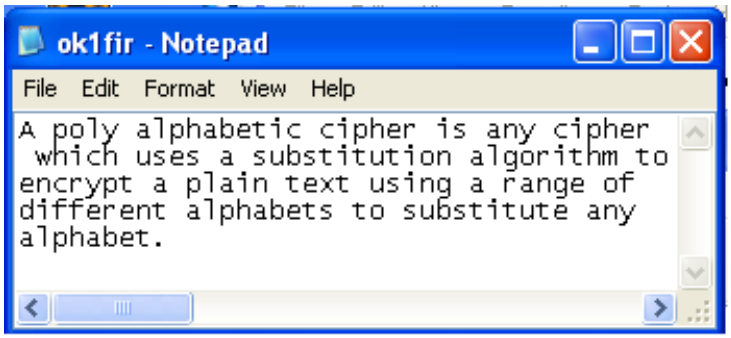
تتبع طريقة كاسيسكي هذه القاعدة: إذا تم ترميز رسالة باستخدام n من الحروف الأبجدية في دوران دائري، وإذا ظهرت كلمة محددة أو مجموعة حروف k من المرات في رسالة النص الواضح، فإنها يجب أن ترمز تقريبا k/n من نفس الحروف الأبجدية [1] .

بالنسبة إلى طريقة كاسيسكي فان الخطوات التي تتبعها هي:

1. تحديد النماذج المكررة لثلاثة حروف أو أكثر.
2. لكل نموذج اكتب الموقع الذي يبدأ فيه النموذج.
3. احسب الفرق بين نقاط البداية للبدايات الناجحة
4. حدد كل العوامل لكل حرف
5. إذا تم استخدام شفرة التعويض متعددة الحروف، فان طول المفتاح سيكون واحد من العوامل التي تظهر غالبا في خطوة رقم 4

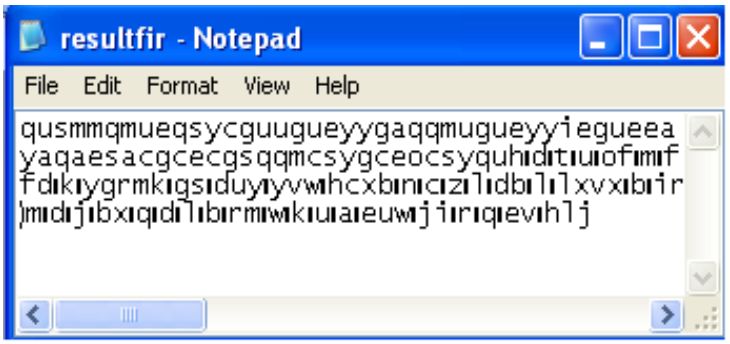
6. النتائج:

يوضح الشكل (6) النص الصريح الذي سيتم تشفيره بالطريقة المقترحة



شكل (6). النص الصريح

ويمثل الشكل (7) النص المشفر



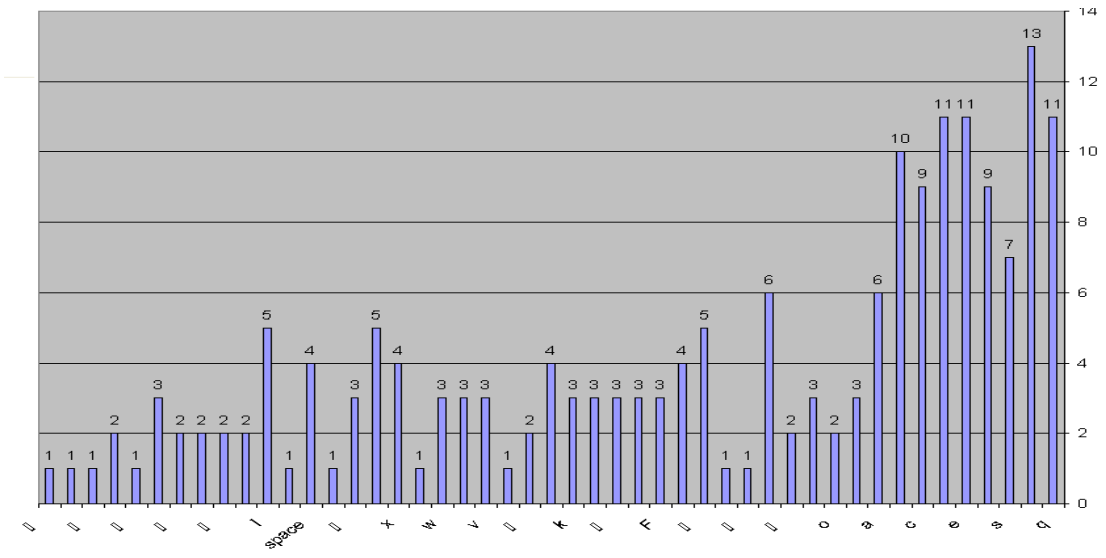
شكل (7). النص المشفر

وكانت ترددات الحروف للنص المشفر كما موضح في الجدول رقم (3) والشكل رقم (8)

جدول (3). ترددات الحروف للنص المشفر

Letter	frequency	Letter	frequency	Letter	frequency	Letter	frequency	Letter	frequency
q	11	o	2		3	x	4		2
u	13	h	3		3	b	5	j	3
s	7		2	k	3		3		1
m	9	d	6	r	4	n	1		2
e	11		1		2	space	4		1
y	11	t	1		1	z	1		1
c	9		5	v	3	l	5		1
g	10		4		3		2		
a	6	F	3	w	3		2		
i	3		3		1		2		

تمثل special Charchter أحرف خاصة



شكل(8). ترددات الحروف للنص المشفر

يلاحظ من الجدول رقم (3) والشكل رقم (8) أن الترددات تختلف اختلافا كبيراً عن الترددات الأصلية للغة الانكليزية.

كما انه تم تطبيق اختبار كاسيسكي على النص المشفر والجدول (4) يوضح نتائج الاختبار

جدول (4). نتائج اختبار كاسيسكي على النص المشفر

sequence	Distance	Factorization
gue	8	2^3
eyy	12	$2^3 * 3$
gce	13	1*13
qqm	31	1*31

نلاحظ من الجدول السابق انه لا توجد علاقة محددة بين السلاسل لتحديد الطريقة المستخدمة.

أما بالنسبة قيمة IC فقد تم حسابه وكانت النتيجة IC= 2.19387

وهي قيمة لا تنطبق على الشروط المتعارف عليها لتحديد الطريقة

وكذلك الوقت كان قليل جداً Time=1.2856 mc

7. الاستنتاجات:

بما أن خوارزميات التشفير ممكن أن تكسر قبل وصول الرسالة إلى الطرف المعني وذلك عند توافر الوقت والمعلومات الكافية للمتطفل سواءاً كانت تحديد الخوارزمية المستخدمة في عملية التشفير أو إيجاد الضعف العام في الخوارزمية. لذا سعينا في هذا البحث لإيجاد طريقة تحتاج وقت طويل لمهاجمة الرسالة من قبل المتطفل عن طريق استخدام هجين لأكثر من نوع من أنواع التشفير متداخلة فيما بينها إضافة إلى استخدام طريقة جديدة لإخفاء المفتاح المشفر بطريقة تختلف عن الطريقة التقليدية.

وقد تم قياس نتائجها بعدة مقاييس معتمدة للتأكد من فعاليتها وقوتها كما أن وقت التشفير قليل جدا وكذلك فك الشفرة وهذا هو احد المعايير المعتمدة في قياس كفاءة الخوارزمية. ولتصميم نظام صحيح للتشفير هنالك معايير لقياس كفاءة النظام وهي معايير شانون [9]

1. درجة السرية المقدمة من قبل الطريقة
2. حجم المفتاح
3. بساطة عملية التشفير وفك الشفرة
4. امتداد الخطا
5. تمديد الرسالة المشفرة

فالخوارزمية المقترحة قد تقدم سرية عالية، أما المفتاح فهو بسيط ولكن لا يستطيع المتطفل استنتاجه بسهولة لأننا نستطيع التحكم بحجمه ومن ثم تشفيره بطريقة تختلف عن الطريقة المستخدمة لتشفير النص الأصلي.

اما بالنسبة إلى بساطة عملية التشفير وفك الشفرة فتعتبر بسيطة لأننا نعتمد على جهاز الحاسوب والذي يعتبر متوفر وسهل الاستخدام للكثير. أما عن نسبة الخطأ فلا مجال للخطأ لأنه تم إعادة النص الأصلي بعد تشفيره وكان مطابق للنص قبل التشفير بنسبة 100%.وفي حالة وقوعه فانه ينحصر في موقعه ولا يتجاوز أكثر بسبب اختلاف المفتاح بين حرف وآخر.

أما بالنسبة لتمديد الرسالة فقد ازداد حجم الرسالة بما يعادل نصف الطول الأصلي وهذه ضريبة صغيرة مقابل السرية الكبيرة التي توفرها الطريقة.

أما حين مناقشة الطريقة طبقاً لفرضية أسوأ الاحتمالات [10, 9]

1. حصول المتطفل على معلومات كاملة عن نظام التشفير
2. حصول المتطفل على كمية كبيرة من النص المشفر
3. حصول المتطفل على كمية مساوية من النص الأصلي والمشفر

فإذا حصل المتطفل على خوارزمية التشفير المستخدمة فسيكون اعتماد سرية الطريقة على المفتاح (والذي يعتمد على حجم الملف الأصلي المراد تشفيره) والذي يكون مخفي بداخل النص المشفر والذي قد يوهم المهاجم بأن الطريقة التي حصل عليها هي طريقة لتشفير النص مباشرة ولكن النص المشفر يحوي على مفتاح مخفي.

وإذا افترضنا أن يكون لدى المتطفل جزء من النص المشفر أو أن يكون لديه جزء من النص الصريح وما يقابله من النص المشفر فلن يُمكنه اكتشاف بقية الرسالة ولا يستطيع تخمين الخوارزمية ولا معرفة المفتاح لان أي رمز أو كلمة في الرسالة لا تتكرر بياناته المشفرة ولو تكرر الرمز نفس الرمز أو الكلمة بموقع آخر.

8. التوصيات:

1. استخدام طريقة كبس مناسبة لكبس النص المشفر حيث انه تم تطبيق اغلبها ولكن لم تؤدي المطلوب بدقة ، لأنها تزيد من حجم الملف المشفر كما تم أيضا استخدام الشبكات العصبية للكبس Neural Network ولم يتم الحصول على نتائج مرضية.
2. تطبيق هذه الخوارزمية على الصور والصوت.

المصادر

[1] الحمامي،علاء حسين،العاني، سعد عبدالعزيز ، (2007)، تكنولوجيا امنية المعلومات وأنظمة الحماية

[2] F.Tipton Harold , CISSP. Micki Krause, CISSP,(2007), "information security management handbook" sixth edition

[3] Vigenere Cipher, Wikipedia the free encyclopedia http://en.wikipedia.org/wiki/vigen%c3%a8re-cipher

[4] Wilson Phillip I and Garcia Mario, March(2006)," A modified Version of the Vigenere Alogrithm" ,IJCSNS international Jornal of computer science and Network security, vol. 6 No. 3B

[5] Stallings, William,(2005),"Cryptography and Network Security", principles and practice

[6] Eskicioglu Ahmet and Litwin Louis, "Cryptography: the science and Art of Secure communications"

[7] Henk C.A. Van Tiborg.ed,(2005),"Encyclopedia of cryptography and security (first ed).springer.pp.115.ISBN 038723473x.

[8] Menezes A., Oorschot p.van and Vanstone s. (2001),"Handbook of applied cryptography" http://www.cacr.math.uwater100.ca/hac

[9] Beker, Henry and Piper, fred (1982),"cipher system the protection of communications .pp. 162-166

[10] Cecil Larry,(1998),"An Examination of Encryption Technology in Every day use",PW-10 submission, matters of science, Dr. Morry Fiddler