# Stream Cipher Using Genetic Algorithm

**Melad jader saeed**
*meladjader@uomosul.edu.iq*
*University of Mosul/ College of Computer Science and Mathematics*
**Received on : 21/4/2009** **Accepted on :4/10/2009**

**ABSTRACT**

The research tackles newly suggested method in generating the random key used in stream cipher, by generating the key randomly using rand function and then applying randomness conditions if the produced key satisfy the conditions then its accepted key other wise,Genetic Algorithm (GA) are used to produce the key stream.

The proposed method used new structure style to hide the encrypted key withen the text. In addition simple hash function is used to check the integrity of the empeded encrypted key.

**Keyword**: stream, genetic, encryption, random

# التشفير الانسيابي باستخدام الخوارزمية الجينية

**ميلاد جادر سعيد**

*كلية علوم الحاسبات والرياضيات، جامعة الموصل*

**تاريخ الاستلام: 2009/4/21** **تاريخ القبول: 2009/10/4**

**الملخص**

تناول البحث طريقة مقترحة جديدة في توليد المفتاح المستخدم في التشفير الانسيابي Stream Cipher, من خلال استخدام الخوارزمية الجينية Genetic Algorithm عن طريق توليده عشوائياً باستخدام دالة Rand, ومن ثم اخضاعه لشروط العشوائية المعتمدة فاذا كان مطابق يستخدم للتشفير والا سوف يتم استخدام الخوارزمية الجينية Genetic Algorithm لتكوين المفتاح الجيني العشوائي والذي يكون بطول النص المراد تشفيره.

استخدمت الطريقة المقترحة هيكلية جديدة لاخفاء المفتاح المشفر ضمن النص المنقول, بالاضافة الى انه تم التاكد من سلامة المفتاح المنقول(Integrity) باستخدام دالة تمويه بسيطة.

## 1. المقدمة Introduction:

من اهم التحديات التي يواجهها الاقتصاد الرقمي بالخصوص وكذلك مختلف التعاملات الالكترونية عبر شبكة الانترنيت هي مسالة امن المعلومات وعدم الثقة المتزايدة في هذا الاقتصاد وعدم توفر ضمانات كافية تحمي المنخرطين في هذا النظام الجديد والتعامل معه بكل ثقة واطمئنان, على هذا الاساس تبرز اهمية تشفير البيانات او تعميتها لضمان سريتها عند تنقلها عبر الشبكة

والامضاء الالكتروني للتاكد من هوية مرسل المعلومات ووصولها كاملة دون تغيير الى الجهة التي يفترض ان تصلها [2].

ويعتبر التشفير الانسيابي واحدا من اهم انظمة التشفير الحديثة نسبياً والمستخدم في انظمة الاتصالات والخزن كوسيلة امنة للحفاظ على المعلومات.

تصنف انظمة التشفير الانسيابي من انظمة المفتاح السري المهمة ( secret key system) التي تستخدم مفتاح سري واحد في عمليتي التشفير وفك الشفرة. تمتاز هذه الانظمة بانها الاكثر شيوعاً واستخداماً في مجال التشفير لما لها من خصائص مهمة منها:-

- عدم تزايد الاخطاء في حالة وقوعها.
- سهولة استخدامها في التطبيقات العملية.
- سرعة تنفيذها.

ومن جهة اخرى فان الخوارزمية الجينية Genetic Algorithm ايضا تعتبر من الاساليب الحديثة, اذ برزت اهمية استخدامه في حل المسائل المعقدة اضافة الى حل المسائل الصعبة في بحوث العمليات وكذلك حل مسائل التشفير وكسر الشفرة.ويعتمد اسلوب الخوارزمية الجينية في حل المسائل المختلفة على افكار مستنبطة من علم الوراثة وهي تهتم بشكل عام بكيفية انتاج افراد جدد تمتلك صفات معينة (مرغوبة او غير مرغوبة) وذلك من خلال التعديل او التداخل او التبديل الذي يحصل على المجموعات المورثة بهدف تكوين افراد جدد[9,6].

ومع ملاحظة هذه المميزات فقد تم الاستفادة من GA في هذا البحث لتوليد مفتاح التشفير الانسيابي,بعد الاطلاع على بعض البحوث السابقة التي تناولت استخدامات GA مع التشفير وفك الشفرة ومن امثلتها:حيث قام الباحث [8] باستخدام الخوارزمية الجينية بإيجاد افضل مفتاح لاستخدامه لتشفير النصوص باسلوب التشفير التعويضي substitution cipher, اما الباحث [1] فقد استخدم GA في ايجاد طول المفتاح السري الذي سوف يستخدم في تحليل شفرة permutation cipher, اضافة الى ذلك فقد استخدم الباحث [7] GA لكسر النص المشفر بطريقة التشفير الابدالي Transposition cipher, واخيرا قام الباحثون [4] بتقديم ثلاثة طرق للحدس التخميني للوصول للامثلية optimization heuristic ( Simulated (annealing genetic algorithm, tabu search, التي استخدمت في كسر النص المشفر باستخدام Transposition cipher.

اما في هذا البحث فقد تم الاستفادة من الخوارزمية الجينية باقتراح طريقة جديدة لتوليد المفتاح العشوائي المستخدم في التشفير الانسيابي.

**2. التشفير الانسيابي Stream Cipher:**

ان انظمة التشفير الانسيابي تقسم النص الصريح M الى مراتب ثنائية ....$m_1,m_2,m_3$او رموز متتابعة, وتقوم بتشفير كل $m_i$ باستخدام $k_i$ من متتابعة المفتاح .....$k_1,k_2,k_3$ أي أن [3]

$$E_k(M)=E_{k1}(m_1)E_{k2}(m_2)E_{k3}(m_3).....$$

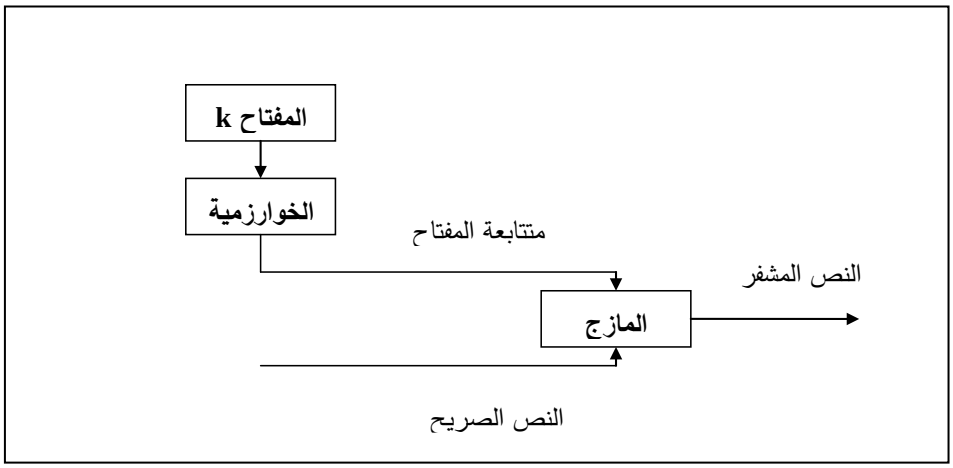
تكون هذه الانظمة دورية عندما تكون متتابعة المفتاح دورية ذات دورة بطول d , أي تكرر نفسها بعد d رمز.

يتكون نظام التشفير الانسيابي من جزئيين اساسيين هما:

1. خوارزمية توليد متتابعة المفتاح
2. المازج Mixer

تقوم الخوارزمية بتوليد متتابعة المفتاح اعتماداً على مفتاح يغذيها ثم تمزج المتتابعة المتولدة مع النص الصريح بواسطة المازج لتوليد النص المشفر.

في حالة استخدام النظام الثنائي في تمثيل النص الصريح والنص المشفر يكون المازج هو عملية الجمع بمعيار(2) أي XOR.




الشكل (1) يوضح نظام التشفير الانسيابي

عملية التشفير تتم كما يلي:

$$C_i=E_{ki}(m_i) =m_i \oplus k_i$$

حيث $c_i,m_i,k_i$ تمثل رتب ثنائية من مفتاح, والنص الأصلي والمشفر على التوالي و $\oplus$ تمثل المازج اما عملية فك الشفرة فتتم كالآتي

$D_{ki}(c_i) = c_i \oplus k_i$

- يمكن تقسيم انظمة التشفيرالانسيابي الى قسمين هما
  1. انظمة التشفيرالانسيابي الخطية
  2. انظمة التشفيرالانسيابي اللاخطية

اعتمدت الطرق السابقة في توليد المفتاح على مسجلات الازاحة (shift register) الخطية واللاخطية:

1. ان استخدام مسجلات الازاحة يحتاج الى كلفة في تصنيعه.
2. قد يؤدي استخدام مسجلات الازاحة الى ظهور مفتاحين متشابهين.
3. عملية توليد المفتاح باستخدام مسجلات الازاحة يحتاج الى الوقت وهذا يؤثر على عملية سرعة التشفير.
4. تكرار المفتاح اكثر من مرة على طول النص قد يؤدي الى زيادة احتمال اكتشافه.

وقد تم الاعتماد على خصائص عشوائية المفتاح الناتج بتطبيق شروط العشوائية المعتمدة [5]

### 3. دالة التمويه Hash Function:

ان دالة التمويه هي دالة رياضية إدخالها عبارة عن سلسلة من البيانات ذات طول متغير والتي تمثل بيانات الرسالة نفسها وقد تطبق على المفتاح ايضاً حيث تقوم دالة التمويه بتحويل الطول المتغير (العشوائي) للبيانات المدخلة الى سلسلة من البيانات ذات طول ثابت Fixed Length والتي عادة يكون طولها اصغر من طول البيانات المدخلة. ونستطيع من خلالها تمييز الرسالة الاصلية والتعرف عليها بدقة, حتى ان أي تغير في مفتاح الرسالة ولو كان في بت واحد سيقضي الى بصمة مختلفة تماماً ومن غير الممكن استقاق دالتين متساويتين لرسالتيين مختلفتين, كما انها تستخدم للتاكد من ان الرسالة قد جاءت من مصدرها دون تعرضها لاي تغير اثناء عملية النقل.وقد تم استخدام دالة التمويه البسيطة Simple hash function حيث تقوم هذه الدالة باجراء عملية XOR حسب المعادلة التالية [10]:

$$B_{i2} \ldots B_{im} \oplus C_i = B_{i1}$$

$C_i$ = تسلسل الترميز الثنائي في دالة التمويه

M = عدد الترميز الثنائي في الإدخال

$B_{ij}$= تسلسل الترميز الثنائي في byte المحدد(j)

$\oplus$ = عملية XOR

والإجراء يكون حسب مايلي:

1. فرض قيمة ابتدائية ل byte بالقيم صغفر
2. نقوم بالخطوات التالية
   - اجراء عملية XOR للـ byte التالي مع السابق
   - تدوير القيمة الناتجة باتجاه اليسار مرتبة واحدة فقط

**4. الخطوات العامة للخوارزمية الجينية:**

1. انشاء الجيل الابتدائي
2. ايجاد دالة الهدف ومدى اللياقة واحتمالية المساهمة لمقاطع الجيل الابتدائي
3. اختبار الاباء selection
4. التداخل الابدالي Crossover
5. التغير ضمن المقطع الواحد Mutation
6. معيار توقف الخوارزمية الوراثية

**5. هدف البحث:**

للحصول على تشفير اكثر سرية واسرع في التنفيذ واقل كلفة تم اقتراح خوارزمية هجينة بالاستفادة من الخواص الجينية لتكوين مفتاح والتاكد من عشوائيته باستخدام طرق معتمدة. وبدلاً من اعادة توليد المفتاح عند الجهة المستقبلة, فقد استخدمت طريقة جديدة لاخفاء المفتاح داخل النص المشفر قبل ارساله, وقد تم التاكد من سلامة المفتاح المستلم باستخدام دالة التمويه.

**6. الطريقة المقترحة لتكوين المفتاح:**

تم الاعتماد على الخوارزمية الجينية لتفادي المساوئ التي تسببها الطريقة التقليدية. في بادئ الامر تم تكوين جيل عشوائي للمفتاح باستخدام دالة rand في لغة Matlab مع ملاحظة ان طول المفتاح يجب ان يكون بطول النص المراد تشفيره, ثم تقاس العشوائية لكل فرد من الجيل حسب الشروط المعتمدة [5]

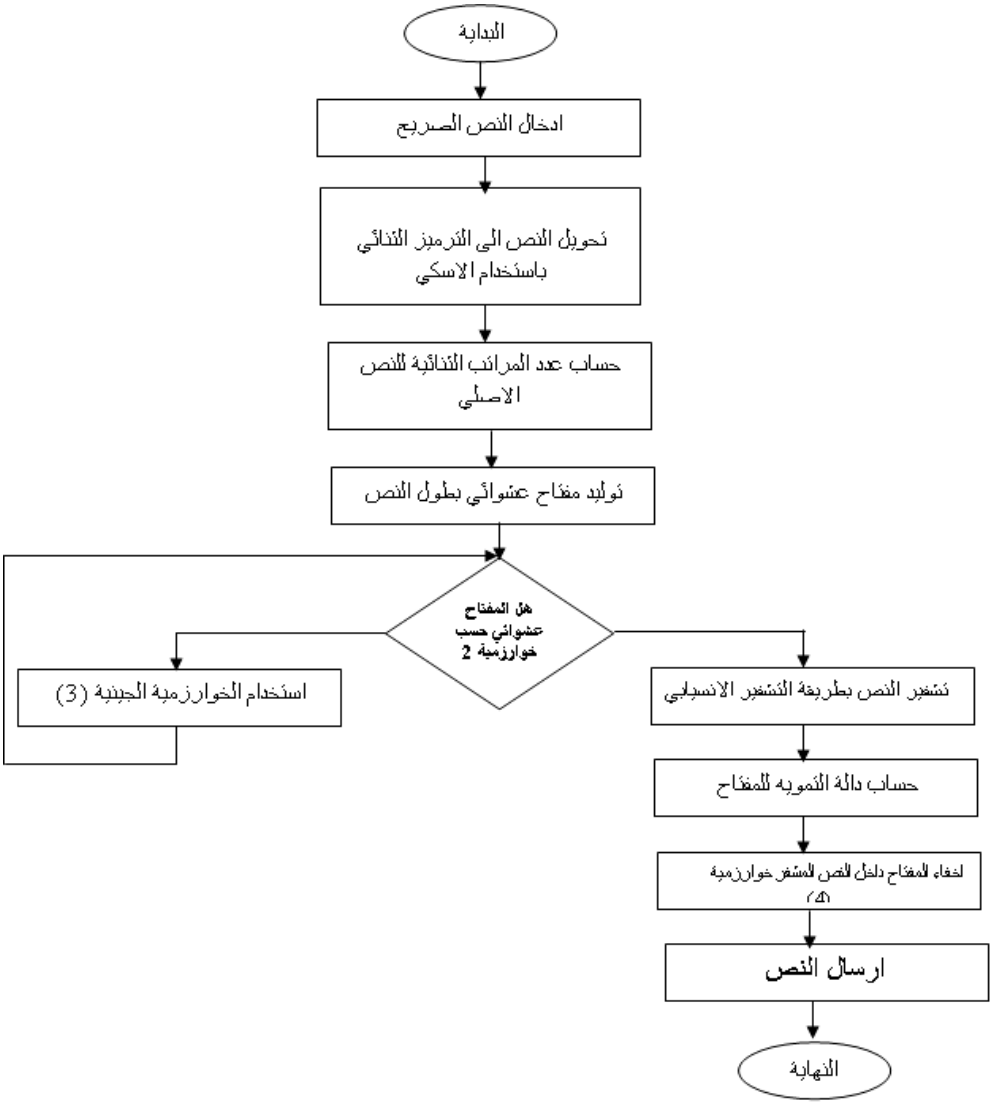
في حالة تحقق الشروط فان الفرد هو عشوائي وسوف يستخدم للتشفير.وفي حالة كون الجيل الابتدائي كله لايحقق الشروط يتم استخدام الخوارزمية الجينية.

### 6.1 هيكل عمل الطريقة المقترحة:

ان اهم مقومات التشفير الناجح هو الخوارزمية المعتمدة وسرية المفتاح, وقد تم اعتماد الخوارزمية التالية:

**خوارزمية (1)**

1. البداية
2. ادخال النص الصريح المراد تشفيره
3. تحويل النص الصريح الى الترميز الثنائي باستخدام الاسكي (Ascii Code) .
4. حساب عدد المراتب الثنائية bits المتكون منها النص بعد تحويله للنظام الثنائي
5. توليد المفتاح بصورة عشوائية بشرط ان يكون طوله بطول النص المراد تشفيره
6. اختبار عشوائية المفتاح حسب الخوارزمية (2)
7. في حالة عدم تحقيقه لشروط الخوارزمية (2) يتم استخدام الخوارزمية الجينية (3)
8. في حالة تحقيقه للشروط يستخدم المفتاح لتشفير النص الصريح باستخدام طريقة التشفير الانسيابي باجراء عملية XOR
9. حساب دالة التمويه Hash Function للمفتاح ووضع النتيجة في نهاية النص بعد تشفيره
10. اخفاء المفتاح داخل النص المشفر حسب الخوارزمية (4)
11. حساب عدد احرف النص الاصلي ووضعه في اخر النص
13. ارسال الرسالة
14. النهاية




الشكل (2) يوضح هذه الخوارزمية

**خوارزمية (2) اختبار العشوائية**

تم استخدام شروط المعتمدة لاختبار العشوائية[5] وكما يلي :

1. البداية
2. F=0
3. اذا كان المراتب الثنائية المساوية لـ"1" = المراتب الثنائية المساوية لـ "0" فان F1=1 والا F1=0
4. اذا كان هناك كتلة من المراتب الثنائية بقياس n ولا يوجد فجوة من المراتب الثنائية بقياس n فان F2=1 والا F2=0
5. اذا كان هناك فجوة من المراتب الثنائية بقياس n-1 ولا يوجد كتلة من المراتب الثنائية بقياس n-1 فان F3=1 والا F3=0
6. حساب دالة F=F1+F2+F3
7. اذا كان F=3 فان الفرد عشوائي وبخلافه فان الفرد غير عشوائي وسوف يتم ستخدام الخوارزمية الجينية
8. النهاية

**الخوارزمية (3) الخوارزمية الجينية**

1. البداية
2. توليد جيل عشوائي يسمى الجيل الابتدائي
3. حساب دالة F=Fitness وترتيبها
4. ايجاد الاحتمالية بقسمة قيمة (مجموع Fitness\Fitnesses)
5. اجراء عملية Selection باستخدام عجلة روليت وذلك بتوليد افراد جدد عشوائياً ايضا
6. ثم اجراء عملية Crossover بين الجيل الجديد والقديم
7. اجراء طفرة Mutation عشوائيا على الجيل الجديد
8. يتم اختيار نسبة من الجيل القديم والجديد حسب 40 قديم الى 60 جديد
9. اعادة عملية اختبار العشوائية مرة اخرى على الجيل الجديد
10. النهاية

**خوارزمية (4) مقترحة للاخفاء**

تم اقتراح خوارزمية جديدة للاخفاء وكما يلي:

1. البداية
2. المفتاح يحول الى ترميز الاسكي
3. يحشر ضمن النص المشفر بتسلسل عشوائي
4. يكتب هذا التسلسل في نهاية النص المشفر
5. النهاية

**الخوارزمية المقترحة لفك الشفرة**

1. البداية
2. استلام الرسالة المشفرة
3. اعتماد الرقم الاخير لمعرفة عدد احرف النص الاصلي وهو يساوي عدد احرف المفتاح
4. اعتمادا على الارقام التالية للرقم الاول يتم معرفة تسلسل احرف المفتاح وبعدد الرقم الاول.
5. تحويل ارقام المفتاح الى الترميز الثنائي
6. الحصول على دالة التمويه متمثلة بالرقم الذي يلي ارقام تسلسل المفتاح
7. الحصول على ارقام النص المشفر وهي الارقام المتبقة جميعها.
8. تحويل ارقام النص المشفر الى الترميز الثنائي
9. اجراء عملية XOR بين ترميز المفتاح والنص المشفر
10. الحصول على النص الأصلي الصريح
11. النهاية

**6.2 التطبيق العملي:**

**1. ادخال النص المراد تشفيره**

تم في البدء ادخال النص المراد تشفيره وكان

| **النص الأصلي** |
| --- |
| **help me** |

ثم تم تحويله الى الاسكي ثم الى النظام الثنائي وأصبح بالشكل

| 0100 0100 0100 0001 0100 1000 0100 1100 0100 1001 0100 0001 |
| --- |

بعد ذلك تم حساب عدد bits المتكون منها النص وهو no. of bits=48

**2. توليد المفتاح**

تم استخدام دالة rand لتوليد ؤقم عشوائي طوله بطول النص المراد تشفيره بعد تحويله للنظام الثنائي وليكن:

| 0010 1111 0100 0000 1110 1101 1111 1111 0101 0101 1101 1110 |
|---|

**3. اختبار عشوائية المفتاح**

تم بناء دالتين لاختبار عشوائية المفتاح

الدالة الاولى:

تقوم بحساب عدد الواحدات والاصفارفي المفتاح وترجع قيمة F1

اما صفر في حالة الغير مساواة

او واحد في حالة المساواة

وفي هذا المثال F1=0

الدالة الثانية:

نقوم بادخال قيمة n وهي تمثل عدد الواحدات المتكتلة المطلوبة وكان n=10 والبحث عن هذه n ضمن سلسلة المفتاح وترجع قيم

اما صفر في حالة عدم وجود كتلة بقياس n

او واحد في حالة وجود كتلة قياسها n

وفي المثال F2=0 وكذلك ترجع

اما صفر في حالة عدم وجود فجوة بقياس n-1

او واحد في حالة وجود فجوة بقياس n-1

وفي المثال F3=0

وبالنتيجة فان دالة الهدف F تكون نتيجتها

Fitness=F=F1+F2+F3

Fitness=0

وبما ان قيمة دالة الـ fitness لاتساوي 3 وهي دالة تعظيم سوف نستخدم الخوارزمية الجينية.

**4. استخدام الخوازمية الجينية**

❖ يتم في البداية توليد مجتمع ابتدائي من الافراد, ان انشاء الجيل الابتدائي يعد نقطة الانطلاق في حل المسألة, ومعظم الباحثين في هذا المجال بينوا ان عملية بناء الجيل الابتدائي تتم بصورة عشوائية, وتتم برمجياً عن طريق استخدام دالة (rand) التي تاتي بقيم عشوائية تتراوح بين صفر والواحد وعدد الافراد يختلف من مسالة الى اخرى اعتماداً على نوعية المسالة وليكن:

0100 1111 0100 0000 0100 1111 0111 0000 0001 1110 0101 1010
0010 1111 0100 0000 1110 1101 1111 1111 1101 0101 1101 1110
0111 1111 1110 1111 0000 0000 0110 1101 0010 1100 11111111
0110 1110 1110 1111 0101 1000 0001 1001 1111 1111 1010 1110

❖ **بناء دالة Fitness**

حساب الدوال

| F1 | F2 | F3 | No. of cromosom | F |
|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 2 | 1 |
| 0 | 1 | 1 | 3 | 2 |
| 0 | 1 | 0 | 4 | 1 |

❖ **بناء دالة الاحتمالية**

تم بناء هذه الدالة لايجاد احتمالية مساهمة كل مقطع من المقاطع بالطريقة التاليه

Pro=Fitness/total Fitness

Pro1=2/4=1/2
Pro2=1/4
Pro3=1/4
Pro4=0

❖ **الاختيار Selection**

في هذا البحث تم اختيار طريقة عجلة الروليت لاختيار افراد من الجيل الحالي لانتاج جيل جديد وتم ذلك عن طريق بناء الدالة sel.

الدالة sel:

تم بناء الدالة sel التي تعتمد في اختيار العناصر على طريقة عجلة الروليت يكون الادخال الى هذه الدالة قيم المصفوفة pro التي تمثل الاحتمالية بعد ذلك يتم توليد مصفوفة ارقام

عشوائية باستخدام الدالة الجاهزة rand ومن ثم مقارنة كل قيمة من القيم العشوائية مع قيم المصفوفة pro ومن ثم تكوين مصفوفة جديدة newpro

Newpro

| No. of cro. | Fitness |
|---|---|
| 3 | 2 |
| 3 | 2 |
| 3 | 2 |
| 2 | 1 |

هذه هي الكروموسومات التي سوف تشترك بعملية التزاوج.

### ❖ التزاوج Crossover

تم بناء دالة تقوم بعملية التزاوج بعد ان تم اختيار الافراد من الجيل الابتدائي ليكون لها دور في توليد الجيل الاتي, تبدا عملية التزاوج اذ يقوم كل فردين جديدين ضمن المجتمع الجديد,وتم في هذا البحث الاعتماد على التزاوج من النوع البسيط Simple Crossover حيث تم توليد رقم عشوائي واعتماده كازاحة ضمن الكروموسوم يتم عندها اجراء عملية التدخل الابدالي (التزاوج).

0111 1111 1110 1111 0000 0000|0110 1101 0010 1100 1111 1111
0111 1111 1110 1111 0000 0000|0110 1101 0010 1100 1111 1111

0111 1111 1110 1111 0000 0000 0110 1101 0010 1100 1111 1111
0111 1111 1110 1111 0000 0000 0110 1101 0010 1100 1111 1111

0111 1111 1110 1111 0000 0000|0110 1101 0010 1100 1111 1111
0010 1111 0100 0000 1110 1101|1111 1111 1101 0101 1101 1110

0111 1111 1110 1111 0000 0000 1111 1111 1101 0101 1101 1110
0010 1111 0100 0000 1110 1101 0110 1101 0010 1100 1111 1111

### ❖ الطفرة Mutation

بعد اجراء عملية التزاوج ياتي دور الطفرة في تغير النتائج التي نتجت من عملية التزاوج, تم اخذ نسبة الطفرة مساوي الى 0.01 وتم تمثيل الطفرة عن طريق تكوين دالة mut

**1**111 1111 1110 1111 0000 0000 0110 1101 0010 1100 1111 1111
0111 1111 **0**110 1111 0000 0000 0110 1101 0010 1100 1111 1111
0111 1111 1110 1111 **1**000 0000 1111 1111 1101 0101 1101 1110
0010 1111 0100 0000 1110 **0**101 0110 1101 0010 1100 1111 1111

❖ **تقييم افراد الجيل الجديد**

بعد توليد الجيل الجديد يتم تقييم افراده بنفس الطريقة التي تمت في الجيل الابتدائي.

❖ **الاحلال**

في هذا البحث تم الاعتماد على طريقة تاخذ بنظر الاعبار كل افراد الجيل من كلا النوعين الجيد والرديء فتم اخذ نسبة 60 % من الافراد الجيدين ونسبة 40% من الافراد السيئين.

وعلى فرض انه تم الحصول على كروموسوم يطابق الحالة N=10 ويحقق الدوال F1=1, F2=1, F3=1 وكما يلي:

0000 0000 0110 0110 1111 1111 1101 0101 0001 1001 1111 0000

F=F1+F2+F3 =3

**4. عملية التشفير :**

ان التشفير المستخدم هو التشفير الانسيابي Stream Cipher وكما يلي

النص المراد تشفيره

0100 0100 0100 0001 0100 1000 0100 1100 0100 1001 0100 0001

المفتاح المستخدم في عملية التشفير

0000 0000 0110 0110 1111 1111 1101 0101 0001 1001 1111 0000

ناتج عملية التشفير أي بعد اتمام عملية XOR

0100 0100 0010 0111 1011 0111 1001 1001 0101 0000 1011 0001

**5. حساب دالة التمويه Hash Function للمفتاح**

بعد تطبيق القانون الخاص بهذه الدالة ينتج لدينا دالة التمويه التالية

0101 0101 وبعد تحويلها وجد انها تساوي 133

وبعد تحويل النص المشفر كان بالشكل 68 39 183 153 80 177

وكذلك المفتاح بعد تحويله كان بالشكل 00 102 256 213 25 240

- ولكي تتم عملية تشفير النص وفكه بالصورة الصحيحة كان لابد من توفر النص المشفر والمفتاح لدى الجهة المستلمة للرسالة المشفرة ايضا ليتسنى لها فتح التشفير وقد تم اخفاء المفتاح المشفر في داخل الرسالة المشفرة .

وكنتيجة للتشفير والاخفاء ودالة التمويه اصبح النص الجاهز للارسال بالشكل التالي مع اخذ بنظر الاعتبار تغير الفراغات بين الارقام الى اصفار لزيادة التمويه:

**0001020680256021303901830153025080024001770133000001003004008001000 6**

**فك الشفرة:**

بعد استلام النص المشفر وحسب خوارزمية فك الشفرة يكون اخر رقم يمثل عدد احرف النص المشفر وكذلك المفتاح وهو 6

وكذلك مواقع المفتاح هي 10, 8, 4, 3, 1, 0

وهي 00 102 356 213 25 240

ودالة التمويه هي 133 نعيد حسابها للتاكد من وثوقية الملف المرسل, وكان النص الاصلي هو 68 177 80 153 183 39

وبعد التحويل النظام الثنائي واجراء عملية الـ XOR

كان الناتج

0100 0100 0100 0001 0100 1000 0100 1100 0100 1001 0100 0001

وبعدها ينتج 68 65 72 76 73 75

وبعد تحويلها الى الاحرف فان الناتج كان help me

وهو النص الاصلي.

**7. زمن التشفير وفك الشفرة:**

تم قياس سرعة تنفيذ خوارزمية التشفير وفك الشفرة للتأكد من سرعتها وكانت النتائج كما موضحة بالجدول التالي علما بان البرنامج طبق على حاسبة ذات مواصفات عالية وهي

Labtop acer

- Intel Celeron M processor 430 (1.73 GHz,533 MHz FSB, 1 MB L2 cacha)
- Intel Graphics Media Accelerator 950

| طول النص المشفر | زمن التشفير | زمن فك الشفرة |
|---|---|---|
| 20 حرف | 0.2656 s | 0.1563 s |
| 40 حرف | 0.2813 s | 0.1371 s |
| 80 حرف | 0.4814 s | 0.3111 s |
| 100 حرف | 0.5110 s | 0.4078 s |

نلاحظ من الجدول اعلاه ان زمن التشفير للنصوص وفكها جيدة ولا تخضع لاي قاعدة لانها تعتمد في تشفير النصوص على عملية تكوين المفتاح باستخدام الخوارزمية الجينية. كما نلاحظ انه وقت فك الشفرة يكون اقل من وقت التشفير لانه في عملية فك الشفرة لايتم استخدام الخوارزمية الجينية.

**8. الاستنتاجات والتوصيات:**

ان الطريقة المقترحة لتحسين عملية التشفير باستخدام التشفير الانسيابي تمتاز بامكانية تنفيذها على اية حاسبة يتوفر بها النظام المعمول به Matlab, اضافة الى صعوبة الحصول على مفتاح التشفير ضمن النص المشفر.

كما تمتاز الطريقة المقترحة بالسرية لما يمتاز به المفتاح من عشوائية مما يؤدي الى اخفاء الخواص الاحصائية للغة النص الصريح ومعرفة جزء من متتابعة المفتاح لايفيد في معرفة المتتابعة كلها كون المفتاح غير متكرر كما في مسجلات الازاحة الخطية واللاخطية المعروفة. لهذا تتميز الطريقة بثباتها امام هجوم النص الواضح المعلوم (know plantext attack) .

كما يمكن الاعتماد على تقنيات ذكائية اخرى لتوليد المفتاح كاستخدام الشبكات العصبية, اضافة الى امكانية دمج اكثر من خوارزمية للتشفير والاستفادة من الخوارزمية الجينية بتوليد المفتاح لها, واستخدام دالة التمويه المعروفة والتي تحقق المواصفات المطلوبة لدالة التمويه كـ SHA-1, MD5.

***المصادر***

[1] Aleksey G.,Vladimir M.,2008,"Genetic Algorithm for finding the key's length and cryptanalysis of the permutation cipher", International Journal information theories &Application,vol.15.

[2] AL-Etewi, Raya Jasim Esaa,2001, "Design Hybird Crytography System and Attacking Stream Cipher Using Neural Network", M.Sc. Research, College of computer Sciences and Mathematics, University of Mosul,Iraq.

[3] A.menezes, P.va Oorschot nd S.Vanstone,1996,'Hand book of applied Cryptography".

[4] Dimovski A., GligoroSKI D.,2003,"Attacks on the Transposition ciphers using optimization Huristics", in proceedings of the second International conference on Tools for Al,Faculty of Natural Sciences and Mathematics, Ss. Cyril and Methodist University Archimedean b.b., PO Box 162 ,1000 skopje, Macedonia.

[5] Fred piper,1982,"Cipher system the protection of communication".

[6] Mitchell, M., 1996,"An Introduction to Genetic Algorithms", MIT Press, London

[7] R.Toemeh, S.,2007,"Breaking Transposition Cipher with GA",electronics & Electric Al Engineering, No.7 (79).

[8] Salim B. Ghusoon, 2008, "Application of polyalphabetic Substitution cipher using genetic Algorithm", Raf.J. of comp. & math's.,vol.5, No.1.

[9] Schmidt, M. Stiden, T.,1997,"Genetic Algorithms, Neural Networks and Fuzzy Logic",Laboratory of computer and information Science, Helsinki University of Technology , Espoo, Finland.

[10] William Stallings, 2005,"Cryptography and Network security principles and practic