دالة صلاحية جديدة لاستخدام الخوارزمية الجينية في كسر شفرات النصوص العربية و الإنكليزية المشفرة بطريقة نابساك- ميركل هيلمن

نور كاظم ايوب

جامعة بابل / كلية العلوم للبنات

Noor.kadhum@gmail.com

الخلاصة

لا يخفى ما لأمن المعلومات في حياتنا من دور مهم لاسيما بعد الثورة المعلوماتية الكبيرة التي شهدتها السنوات الماضية وقد بذلت مساع حثيثة في حماية المعلومات وتحصين الاتصالات، ولكن قابل هذا التطور الكبير في مجال الحماية تنامي لتيار معاكس يعمل على الاختراق ومحاولة كسر الشفرات واستخلاص المعلومات السرية بأي طريقة كانت. يقدِّم هذا العمل بحثاً جديداً ينظم إلى ركب البحوث السابقة التي تضطلع بمهمة كسر شفرة نابساك باستخدام الخوارزمية الجينية بأسلوب يخرج عن كلاسيكيات البحوث التي نشرت في هذا المجال. برهن النظام المقترح عن جدارة في كسر الشفرات المتولدة بطريقة نابساك والفضل في ذلك يعود الى استخدام دالة صلاحية جديدة إضافة إلى رؤية جديدة في استخدام الخوارزمية الجينية ككل.

الكلمات المفتاحية: نابساك، تشفير، الخوارزمية الجينية، كسر الشفرة

Abstract

It is no secret that for the important role of security of information in the life, especially after the massive information revolution of the past years. There are unremitting efforts to protect the information and communication channels. The great development in the field of protection is negotiable by growing of opposite stream that works on penetration, breaking codes and getting confidential information in any way. This paper discusses one of public encryption modes (Knapsack) then provides a way to break it through the use of a genetic algorithm manner deviate from the classics researches published in this field. The proposed system proved well-deserved break the cipher generated by Knapsack method because of using a new fitness function in addition to a new vision in the using of genetic algorithm in this problem as a whole.

Keywords: Knapsack, cipher, genetic Algorithm, cryptanalysis.

١. المقدمة

أدرك العالم منذ القدم أهمية المعلومات وضرورة حمايتها من الوقوع في أيد غير أمينة ولعل يوليوس قيصر من أوائل الذين انتبهوا إلى تلك النقطة فلا يكاد يخلو كتاب يتحدث عن التشفير من قصة القيصر الذي ابتكر أسلوبا فريدا في عصره لإخفاء المعلومات و تشفيرها بطريقة سميت باسمه فيما بعد ولازال هذا العلم في تطور حتى الآن .

رافق التشفير اتجاه أخر معاكس يحاول استخلاص المعلومات السرية المشفرة بطرائق غير قانونية وهو ما يعرف ب(كسر) أو (تحليل) الشفرة الذي تطور هو الآخر ليصبح علماً في حد ذاته والحرب بين الاتجاهين على أشدها لاسيما مع ظهور أنظمة ذكية استطاعت إنجاز نجاحات كبيرة ومتوالية في حل مسائل معقدة وفي مجالات شتى وهذا ما أدى لزيادة شعبية هذه الأنظمة نظراً لتأثرها جميعاً بالأنظمة البيولوجية وقدرتها على حل مسائل غير خطية .

تُعد الخوارزميات الجينية من أهم أعمدة الذكاء الاصطناعي وتعرف بأنها خوارزميات البحث العامة التي تسعى دائماً للحصول على المثالية في الحلول التي تقدمها وتمتاز بأنها تقترح عدد من الحلول تنظمها بشكل مجتمع حيث تسود روح التنافس بين أفراده في محاولة ليكون كل منهم حلاً مثالياً .

2. نظرة إلى البحوث السابقة

في الوقت الذي تحرص مختلف الجهات على الحفاظ على سرية ما تملكه من المعلومات كانت الجبهات المعادية حريصة أيضا على الوصول إلى تلك المعلومات مهما كلف الأمر وتسخر جميع الوسائل المتاحة في سبيل خدمة هذا الهدف ولاشك بان طرائق الذكاء الاصطناعي كانت سلاحا مزدوجا أسهمَ في خدمة الطرفين المتنازعين ولاسيما الخوارزميات الجينية التي تمتاز بقدرتها على عرض حلول متعددة للمشكلة ولا تزال أرضاً خصبةً للأبحاث حتى يومنا هذا .

في العام 2007 قام صبحي حمادي وآخرون بتوظيف الخوارزمية الجينية لحل مسألة نابساك المستخدمة كإحدى شفرات المفاتيح العامة وقد خلص الباحثون إلى أنَّ الخوارزمية الجينية تعدٌّ طريقة قوية وناجحة جداً في إيجاد التمثيل الثنائي الصحيح لِما يسمى نابساك الصعبة (hard knapsack) [صبحي، ٢٠٠٧] وفي العام نفسه أشاد بونام جارج (Poonam Garg) وآخرون بأداء الخوارزمية الجينية في كسر شفرات نابساك [Poonam Garg, 2007].

في العام ٢٠٠٩ استخدمت رواء الدباغ الخوارزمية الجينية المدمجة (Compact genetic algorithm) في كسر شفرات نابساك من نوع ميركل هيلمان حيث تعتمد فكرة هذا النوع من الخوارزميات الجينية على مبدأ التوزيع الاحتمالي حيث يتم إنشاء متجه الاحتمالات الذي يمثل تكرار لكل فرد بقيم ابتدائية تساوي 0.5 لكل موقع في المتجه ثم تحدث قيم المواقع بواقع $1/n \pm$ (حيث n يمثل حجم المجتمع). الغاية من هذا المتجه هو استخدامه كمقياس للتوقف حيث تتوقف الخوارزمية الجينية عندما تكون قيم جميع المواقع في المتجه أما 1 أو 0. أوضحت نتائج البحث كفاءة الخوارزمية الجينية بنوعيها البسيطة والمدمجة في كسر شفرات ميركل هيلمان [Rawa'a, 2009].

في العام ٢٠١٤ شارك فريق بحثي مكون من ثلاثة باحثين في كسر احد أنواع أنظمة نابساك التي تعتمد على مصفوفة مثلث باسكال و الذي يعرف باسم (supper Pascal knapsack cryptosystem) حيث يعتمد هذا النظام على تكوين مثلث باسكال بإنشاء مصفوفة يكون فيها قيم العناصر الواقعة في الصف الأول و العمود الأخير واحد، أما بقية القيم فتشتق من المعادلة ($a_{ij}=a_{i,j-1} + a_{i-1,j}$)، وقد طبق الباحثون الخوارزمية الجينية بلغة ماتلاب الإصدار ٢٠٠٩ لمهاجمة هذه الشفرات وخلص البحث إلى أن الخوارزمية الجينية استطاعت كسر الشفرات في وقت قصير باستخدام مجتمع مكون من ٦٠ فرداً بواقع ٢٠ دورة جينية [Safaa , 2014].

٣. تشفير نابساك– ميركل هيلمان

بعد أن كانت طرائق التشفير معتمدة على استخدام مفتاح واحد للتشفير، حدثت في سبعينيات القرن الماضي طفرة في طرائق وأساليب التشفير على يد رالف ميركل، مارتن هيلمان و وايتفيلد ديفي [Nrich,2011] وذلك بانطلاق فكرة الإعلان عن مفتاح التشفير وتركه مباحا لعامة الناس مع الاحتفاظ بآخر يظل سرا مخفيا إلا عن الأشخاص المخولين بفك الشفرة وقراءة الرسالة الأصلية. اقترح العالمان ميركل وهيلمان شفرة تطبق مبادئ التشفير المعلن وتستثمر فكرة حقيبة الظهر (نابساك) لتوليد هذه الشفرة التي سميت باسميهما [صبحي، ٢٠٠٧]، و كأي خوارزمية تشفير معلن فان هذه الطريقة تمر بالمراحل الآتية :

<u>المرحلة الأولى : توليد مفتاح سري</u> : وهو عبارة عن متجه يمتاز كل عنصر فيه بأنه اكبر من مجموع العناصر السابقة له. بالطبع فان استخدام مثل هذا المفتاح لغرض التشفير سيجعل الشفرة سهلة الكسر، لذا يتبع

هذه المرحلة خطوة تعزز من قوة الطريقة وتعمد إلى إيقاع الطرف المعادي في الفخ. يترك هذا المفتاح لأغراض فك الشفرة.

المرحلة الثانية : نابساك.. المصيدة (trapdoor Knapsack): في هذه الخطوة يستخدم المفتاح السري لتوليد المفتاح المعلن الذي يستخدم في عملية تشفير النصوص ولا مانع من تسريبه للعامة لأنه لا يمكن أن يكون مزدوج الاستخدام أي لا يمكن أن يستخدم في فك الشفرة وهنا يكمن الفخ إذ انه من السهل اشتقاق المفتاح المعلن من المفتاح السري لكن العكس غير ممكن. إن توليد المفتاح المعلن يتبع الخطوات الآتية [Poonam, 2007]:

Algorithm 1 : Public Key Generator

Input: SECRET KEY (S)
Output: PUPLIC KEY (T)
Begin
Step 1: Select an integer value *U* greater than sum of all elements of super increasing sequence.
Step 2: Select another integer W that the gcd(U,W)=1, that is number U and W are reciprocally prime.
Step 3: Produce the public key (T) by applying T=(W *S) mod U
End

المرحلة الثالثة: التشفير : بعد أن أصبح مفتاح التشفير في متناول اليد، يمكن استخدام الخوارزمية الآتية لتشفير الرسالة (message) باستخدام المفتاح المعلن (T):

Algorithm 2: Knap Encryption

Input: PUPLIC KEY (T), Message (M)
Output: Cipher stream
Begin
Step1: Let M1 be the message after trimming blanks.
Step 2: For each letter in M1 do
a- Get ASCII code ,name it X.
b- Convert x into binary of 8 bits, call it Y.
c- Calculate C by performing sum of the product of Y and X.
d- Append C with the cipher stream.
End
End

من الجدير بالذكر أن عملية تحويل شفرة الاسكي إلى الترميز الثنائي (الخطوة b) ينتج عنها الترميز الثنائي معكوسا فعلى سبيل المثال أن التمثيل الثنائي شفرة الحرف (E) هي :

[0 0 0 0 1 0 0 0 1 0 1]

لكن المستخدم في هذه الخوارزمية سيكون :

[1 0 1 0 0 0 1 0 0 0 0]

لو نظرنا إلى التمثيل الثنائي الأصلي على انه متجه فان قيمة البت الأول في هذا التمثيل تتواجد في الموقع الأخير من هذا المتجه ولو ظل الحال على ما هو عليه فان البت (الموقع) الأول من الترميز الثنائي سيقابله الموقع الأخير من متجه المفتاح المعلن في حين أن المنطق يفرض أن يكون البت الأول في الترميز الثنائي مقابلا للموقع الأول من المتجه الذي يمثل مفتاح التشفير وعليه فان استخدام التمثيل الثنائي الأصلي سيتسبب في إنتاج شفرات خاطئة و لذلك يتم عكسه.

الترميز الثنائي المعكوس لرمز ما يتم مقابلته مع المفتاح العلني وتحسب الشفرات بجمع قيم المفتاح الموجودة في المواقع التي يقابلها القيمة (1) في الترميز الثنائي المعكوس أما المواقع التي يقابلها (0) فإنها تهمل وناتج هذه العملية سيكون شفرة ذلك الرمز. تتكرر هذه العملية لكل حرف من حروف الرسالة المراد تشفيرها. المثال الآتي يوضح فكرة التشفير، لنفرض أن :

الرسالة الأصلية : help me، W= 13 ،U=14141

المفتاح السري (S):

[10 12 28 56 109 219 443 882 1768 3532 7066]

المفتاح المعلن (T):

[130 156 364 728 1417 2847 5759 11466 8843 3493 7012]

الجدول الآتي يوضح تشفير حروف الرسالة:

جدول (١) : مثال لتوضيح التشفير بطريقة ميركل هيلمان

الحرف	شفرة الاسكي	التمثيل الثنائي المعكوس	شفرة نابساك
H	72	0 0 0 1 0 0 1 0 0 0 0	٧٢٨+ ٥٧٥٩ = 6487
E	69	1 0 1 0 0 0 1 0 0 0 0	١٣٠+٣٦٤ + ٥٧٥٩ = ٦٢٥٣
L	76	0 0 1 1 0 0 1 0 0 0 0	٣٦٤+ ٧٢٨ +٥٧٥٩ = ٦٨٥١
P	80	0 0 0 0 1 0 1 0 0 0 0	١٤١٧+٥٧٥٩ = ٧١٧٦
M	77	1 0 1 1 0 0 1 0 0 0 0	130+364 + 728+5759= ٦٩٨١

وعليه فان (help me) بعد التشفير بهذه الطريقة سوف تصبح:

[6487 6253 6851 7176 6981 6253]

أما عملية فك الشفرة فتتم بتطبيق خطوات الخوارزمية الآتية [Nrich, 2011] :

Algorithm3: Knap Decryption

Input: SECRET KEY (S), Cipher stream (C), W,U
Output: Message(M)
Begin
Step1: get W^{-1}.
Step 2: For each code in C do
a- $M= (W^{-1} *C) \bmod U$
b- Solve M with S as 0-1 knapsack, call the resulted 8-bit vector, X.
c- Convert X to the ASCII code, call it Y.
d- Convert Y into equivalent character and append it to Message .
End
End

٤. الخوارزميات الجينية

تندرج الخوارزمية الجينية ضمن إطار الذكاء الاصطناعي وتنتمي تحديدا إلى مجموعة الخوارزميات التطورية. أسست مبادئها على يد البروفيسور جون هولاند[Naveen , 2011] في سبعينيات القرن الماضي حيث ظهرت فكره الخوارزمية الجينية البسيطة على يديه آنذاك.

تعد الخوارزمية الجينية احد الأدوات المستخدمة في تحسين ومحاولة الارتقاء بالنتائج إلى مستوى يقترب من الكمال والمثالية ولهذا استخدمت مدمجه مع طرائق الذكاء الأخرى لتعويض نقص ما تعاني منه تلك الطرائق لأجل إعطاء نتائج أفضل ومن الأمثلة على ذلك :

١) تستخدم الخوارزمية الجينية في حقل التصنيف بكثرة ولاسيما في مجال تقليص الخصائص واستخلاص ما هو مهم منها ومن ثم تسليم هذه الخصائص إلى احد أدوات التصنيف وهذا يساهم بفعالية في رفع أداء هذه الأنظمة.

٢) يمكن ان تساهم في منح المنطق المضبب قابلية التعليم التي يفتقر إليها ويمكن تجنيد الخوارزمية الجينية في هذا المجال عن طريق توليد القواعد الضبابية التي يعتمد عليها النظام المضبب لكي يتمم عمله وهو أسلوب ناجح في حال كون عدد معاملات ومتغيرات النظام كبيرا او عندما يصعب الاستعانة بالخبراء لبناء مثل تلك القواعد.

٣) تعدُّ الخوارزمية الجينية مدرب فعال للشبكة العصبية التي تحتاج إلى هذه المرحلة حيث تعمل على ضبط أوزان الشبكة.

تتبع الخوارزمية الجينية أسلوبا مميزاً جعلتها تتفرد عن الأسلوب الكلاسيكي في إيجاد الحلول للمشاكل المعروضة، فالطرائق الأخرى التي يلجأ إليها الباحثون تعتمد على خطوات رياضية و تقدم حلا واحدا، بينما تستخدم الخوارزمية الجينية مبدأ العشوائية لتوليد العديد من الحلول المحتملة يطلق عليها اسم كروموسومات.

الكروموسوم هو عبارة عن متجه يحوي عددا ثابتا من المواقع التي يصطلح عليها مسمى (جينات) وقد يكون طول الكروموسوم متغيرا بحسب طبيعة المشكلة ومتطلباتها. تنظم الكروموسومات في مجاميع تولد تباعاً وتسمى (مجتمعات) [Dilbag, 2013] يولد المجتمع الأول عادة بصوره عشوائية ويتم تقييم طل كروموسوم فيه عن طريق دالة الصلاحية التي تعتمد في صياغتها على المشكلة التي بنيت لأجلها الخوارزمية وتستخدم هذه الدالة كمعيار لقياس جودة كل حل (كروموسوم) تقدمه الخوارزمية.

لا تكتفي الخوارزمية الجينية بتوليد مجتمع واحد ولكنها تشرع بتوليد العديد من المجتمعات بثلاث خطوات تتكرر حتى يتحقق شرط التوقف والذي غالبا ما يكون الوصول للعدد الأقصى من المجتمعات المسموح بتوليده وهو ما يحدده مصمم الخوارزمية. الخطوات الثلاثة المشار لها سابقا هي: انتقاء كروموسومات من المجتمع ليلعبوا دور الآباء الذين يحدث تزاوجاً بينهم من خلال خلط الجينات ليتم إنتاج أفراد [Yali Liu, 2015] وكروموسومات جديدة تختبر إمكانية حدوث تغيرات على جيناتها بفعل عامل الطفرة. في نهاية المطاف يتم اختيار الكروموسوم الأفضل ليكون حلا نهائيا للمسالة المعروضة.

٥. استخدام الخوارزمية الجينية لكسر شفرة نابساك–ميركل هيلمان

نظرا لامتلاك الخوارزمية الجينية القدرة على توليد حلول عشوائية، فمن الممكن استغلال هذه القابلية في كسر شفرة النابساك حيث ستقوم الخوارزمية الجينية بمحاكاة لعملية التشفير حيث ان مفتاح التشفير معلوم ولكن نص الرسالة الأصلية هي الهدف. يتم كسر شفرات نابساك بالاعتماد الخوارزمية الجينية على وفق الخطوات الآتية:

Algorithm4: Genetic Breaking

Input: PUPLIC KEY (T), Cipher stream (C)
Output: Message(M)
begin
Step1: Generate initial population ;
Step 2: Evaluate the chromosomes of population ;

Step 3 Let the generation counter (g) =0;
Step 4: While (there are unbreaked code) do
4-1 Select two chromosomes to be parents;
4-2 mate them using 1X to get offspring;
4-3 Mutate offspring using complement method;
4-4 Evaluate the new offspring and put into new population;
4-5 Increment g by 2;
End while
End.

وفيما يلي توضيح لمعاملات الخوارزمية الجينية المستخدمة لكسر شفرات نابساك:

- **التمثيل الكروموسومي:** تفترض الطريقة أن كل كروموسوم تقترحه الخوارزمية الجينية ما هو إلا التمثيل الثنائي لرمز موجود في النص الأصلي متجاوزة ً بذلك الخطوة (a–2) من الخوارزمية رقم (٢) وتكمل بقية الخوارزمية بصورة اعتيادية ولان هذا الرمز قد ينتمي إلى احد الأبجديتين – العربية أو الانكليزية– فان عدد الجينات في الكروموسوم يساوي ١١، وللتخلص من مشكلة اختلاف شفرات الحروف الكبيرة والصغيرة في اللغة الانكليزية يتم توحيد حالة هذه الحروف في الرسائل بتحويلها إلى حروف كبيرة ويتم التخلص من الفراغات. وبتطبيق الخطوات (c–2) و(d–٢) من الخوارزمية رقم (٢) يتحول كل كرموموسوم في النهاية الى شفرة نابساك افتراضية.

- **تقييم كفاءة الكروموسوم و دالة الصلاحية:** لكسر هذه الشفرات فان الخوارزمية الجينية تعمل على محاكاة التشفير بتوليد ترميز ثنائي (بصيغته المعكوسة) وتعمل على توليد شفرات بجمع قيم المفتاح المعلن التي يقابلها 1 في الكروموسوم ومن ثم تقارن هذه الشفرات مع شفرات النص المشفر فان وجدت تطابق فان ذلك دليل على نجاح الكروموسوم وبالتالي فان النظام سوف يسعى إلى إيجاد الحرف الأصلي وإلا فان الكروموسوم اخفق في كسر شفرة اي رمز من رموز النص المشفر وبالتالي فان النظام يستخدم دالة صلاحية تعتمد على فكرة بسيطة و في الوقت نفسه كفوءة :

للدلالة على فشل الكروموسوم في كسر اي شفرة، تكون قيمة الصلاحية لمثل هذا الكروموسوم (0) أما في حالة وجود تطابق بين الشفرة التي أنتجها الكروموسوم وشفرة ما في النص المشفر، فان صلاحية الكروموسوم ستكون (١) للإشارة الى التطابق بين الشفرتين، ويترتب على ذلك الأمور الآتية :

١) استخلاص الحرف الأصلي وذلك بتحويل الكروموسوم من الترميز الثنائي إلى شفرة الاسكي ومن ثم تحويل الأخير إلى الرمز المقابل لتلك الشفرة حيث يضاف هذا الرمز إلى رموز السلسلة المسترجعة.
٢) عدم البحث عن هذه الشفرة مجدداً وذلك بحذفها من النص المشفر.

وبصياغة الدالة بهذه الطريقة فان البحث يقدم رؤية جديدة لمعاملات الخوارزمية الجينية المستخدمة لكسر هذا النوع من الشفرات إذ إنّ جميع الأبحاث التي تناولت هذا الموضوع اعتمدت دالة صلاحية ثابتة تبدو للقارئ وكأنها القاسم المشترك الذي تتداوله هذه البحوث حيث تحتسب بالطريقة الآتية :

- إذا كان sum اقل أو يساوي target فان الصلاحية هي:

$$F(x)= 1- (|sum – target | / Target)^{1/2}$$

- إذا كان sum اكبر من target فان :

$$F(x)= 1- (|sum – target | / maxdif)^{1/6}$$

حيث :

sum :هي الشفرة التي أنتجها الكروموسوم

target :هي شفرة الحرف المراد كسرها

maxdif: تحتسب من خلال المعادلة (maxdif = max (Target, Full sum – Target
حيثFull sum تمثل مجموع كل المكونات في نابساك.

- **<u>مقياس توقف الخوارزمية الجينية:</u>** لن تتوقف الخوارزمية الجينية حتى يتم كسر الشفرات وكشف النص الأصلي بالكامل وبذلك فانه يعلن عن انتهاء عمل الخوارزمية الجينية ونجاحها في استرجاع النص الأصلي، أما الوقت المستغرق لذلك فيتباين من تنفيذ لآخر بسبب اعتماد الخوارزمية الجينية على مبدأ العشوائية وهذا يعني إن الحلول المتولدة تختلف في كل تنفيذ ولكن بالإجمال فان الأمر لن يتعدى عدة مجتمعات حتى يتحقق المطلوب و يظهر النص الأصلي الذي تم تشفيره.
- **<u>مقياس كفاءة النظام المقترح:</u>** لقياس كفاءة النظام وبيان مدى فاعليته في كسر شفرات نابساك تم اعتماد المعادلة الآتية :

دقة النظام =(عدد الشفرات التي تم كسرها÷ عدد الشفرات الكلية في النص المشفر)× ١٠٠%

الجدول التالي يوضح مثالا تطبيقياً للخطوات السابقة :

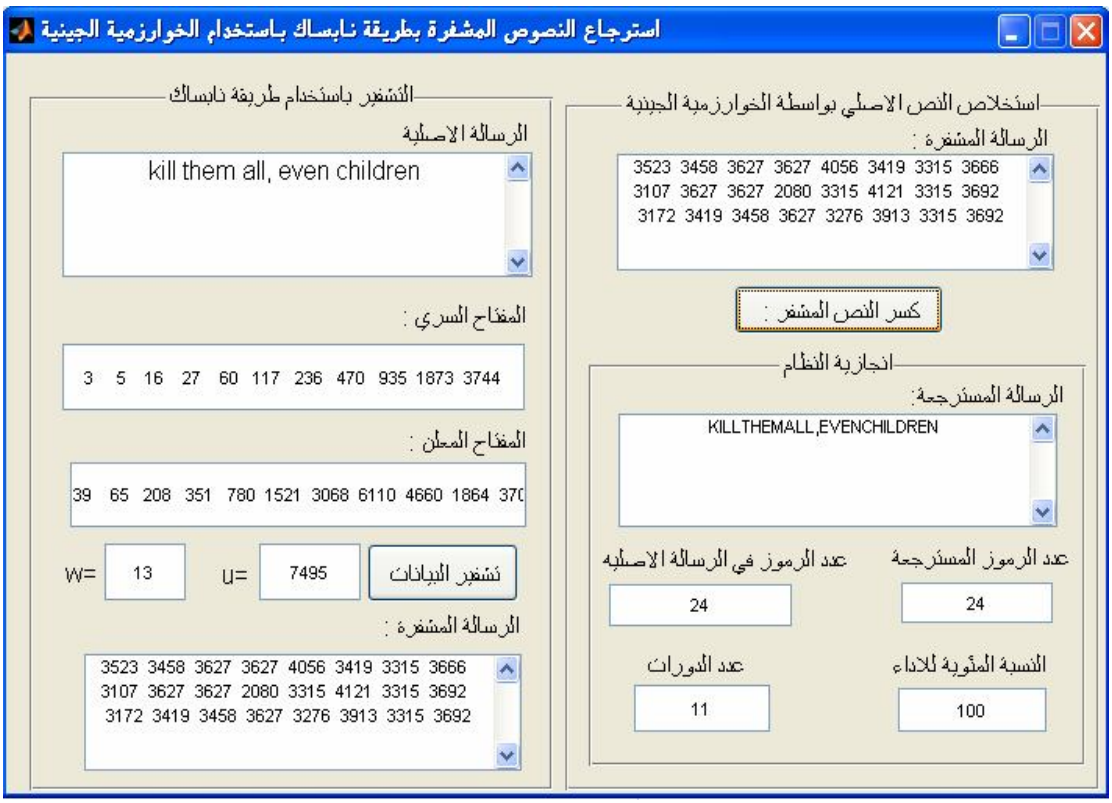
جدول (٢): كسر شفرة الرسالة باستخدام الخوارزمية الجينية

رقم الدورة	الكروموسوم (الترميز الثنائي المعكوس)	الترميز الثنائي الأصلي	الحرف المكتشف
١	1 0 1 1 0 0 1 0 0 0 0	0 0 0 0 1 0 0 1 1 0 1	M
1	0 0 0 1 0 0 1 0 0 0 0	0 0 0 0 1 0 0 1 0 0 0	H
٥	0 0 1 1 0 0 1 0 0 0 0	0 0 1 1 0 0 1 0 0 0 0	L
٣	1 0 1 0 0 0 0 1 0 0 0	0 0 1 0 0 0 0 1 0 1 0	E
٨	0 0 0 0 1 0 1 0 0 0 0	0 0 0 0 1 0 1 0 0 0 0	P

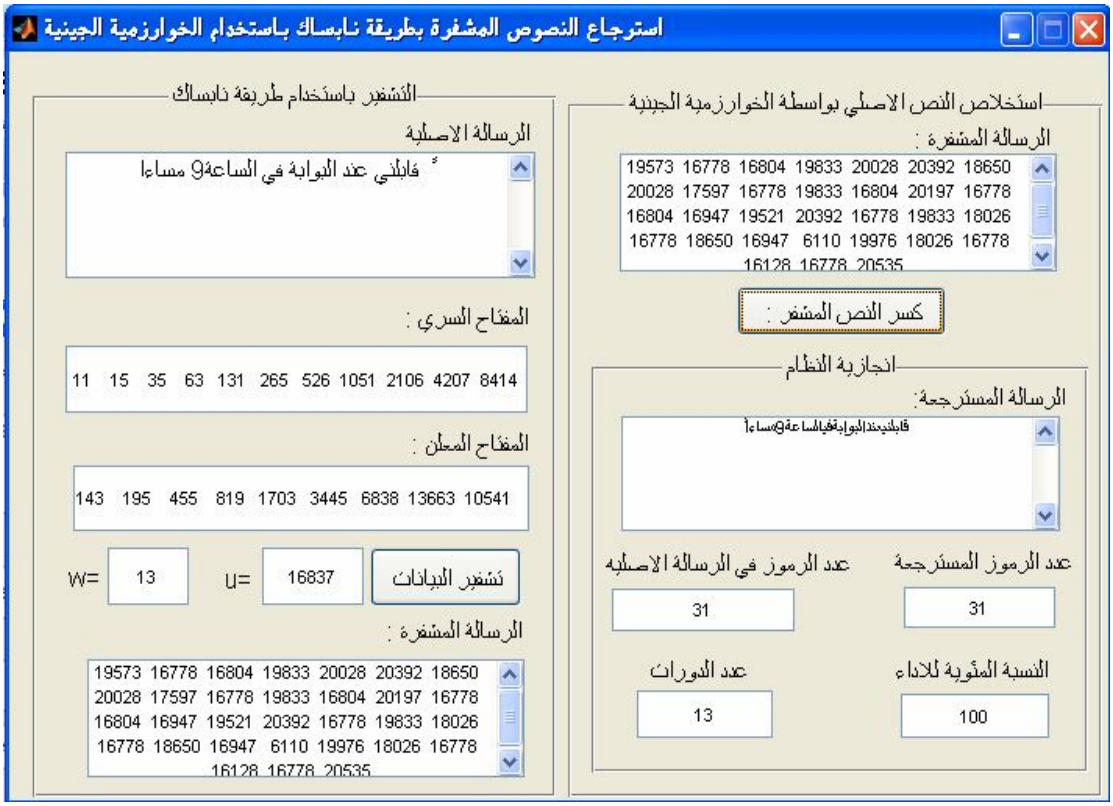
٦. نتائج تطبيق الطريقة المقترحة

تم استخدام ماتلاب الإصدار R2011a في برمجة النظام المقترح. لفحص مدى قدرة الخوارزمية الجينية على كسر شفرات نابساك كان لابد من توفير هذه الشفرات عن طريق تشفير الرسائل باستخدام الخوارزمية رقم (٢) كمرحلة ممهدة وضرورية لاختبار قدرة النظام المقترح على تحقيق الأهداف التي بُني من اجلها .

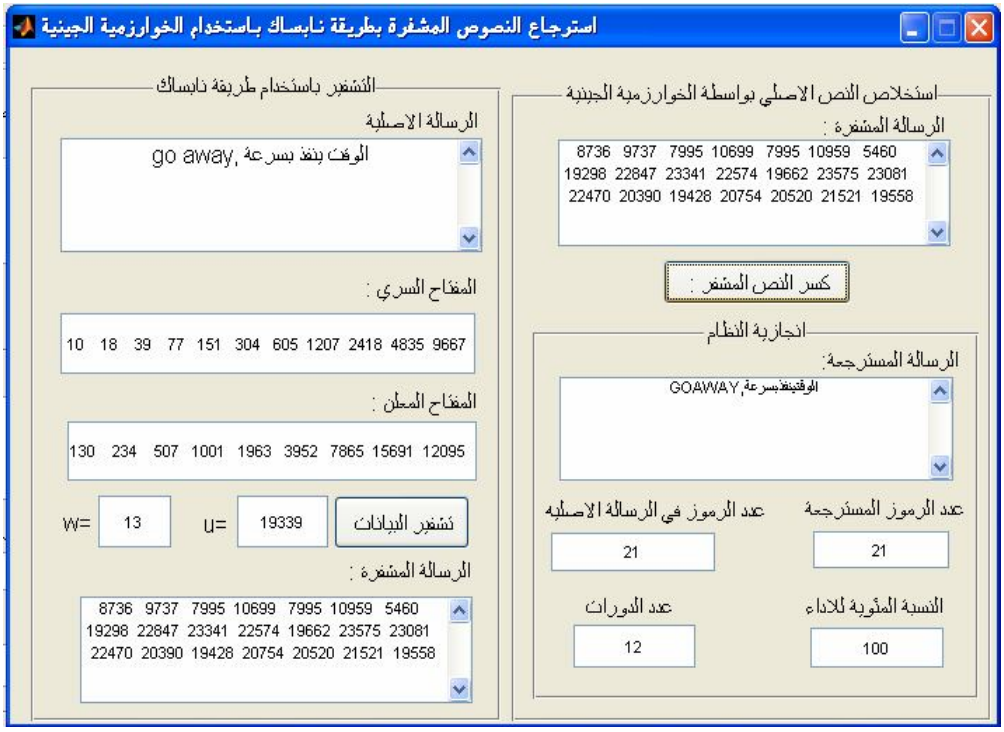
لقد تم إخضاع البرنامج لعدد من التجارب التي تضمنت نصوصا ًتحوي أرقاماً وحروفاً وحتى علامات التنقيط وكان بعض هذه النصوص هجينا بين الأبجديتين العربية والانكليزية واتضح أن البرنامج يتمكن من كسر شفرات نابساك بدقة 100 % ولا يحتاج إلا لبضع مجتمعات لإتمام الأمر والأشكال ١، ٢ و٣ ما هي إلا أمثلة تبرهن على صحة ذلك.



شكل (١) : مثال لاسترجاع رسالة مكتوبة بالانكليزية



شكل (٢) : مثال لاسترجاع رسالة مكتوبة بالعربية



شكل (٣) : مثال لاسترجاع رسالة مكتوبة بخليط من العربية و الانكليزية

٧. تحليل أداء النظام و مقارنته مع أداء البحوث ذات العلاقة

يتمكن النظام من كسر جميع الشفرات في النص المشفر بغض النظر عن لغة الرسالة المشفرة (عربية، انكليزية، خليط بين اللغتين) ولذلك فان النسبة المئوية للنظام في أي تنفيذ يساوي ١٠٠% .

يتميز النظام عن بقية البحوث التي استخدمت الخوارزمية الجينية في كسر شفرات نابساك ميركل–هيلمان بتبسيط استخدام الخوارزمية الجينية لهذا الغرض مما يؤدي إلى تقليل الوقت مع تحقق اداء مثالي في كسر جميع الشفرات ويعود الفضل في ذلك إلى النقاط الاتية:

أ- الطريقة المقترحة تستغل كل مجتمع تولّده الخوارزمية الجينية في كسر أكثر من شفرة بدلاً من استخدام الخوارزمية الجينية لكسر شفرة واحدة فقط من النص المشفر.

ب- اقتراح دالة صلاحية تعمد إلى تخصيص ١ لكل كروموسوم قادر على كسر شفرة ما فيما تخصص ٠ لكل كروموسوم لا يتمكن من التعرف على أي شفرة وعلى الرغم من بساطة هذه الدالة إلا أن النتائج أثبتت كفاءتها و قوتها.

٨. الاستنتاجات والأعمال المستقبلية

بعد تطبيق النظام المقترح لكسر شفرات نابساك أظهرت النتائج أن النظام يتمكن من استخلاص النص الأصلي من النص المشفر بطريقة نابساك بالاعتماد على التوظيف الذكي لإمكانيات الحاسوب كما أثبتت التجارب أن استخدام الخوارزميات الجينية طريقة ناجعة جداً في كسر الشفرات حيث استطاعت الطريقة تقديم حل نموذجي بعد البحث ضمن عدة حلول مقترحة في عدد من الأجيال وبذلك وفرت وقتاً وعناء الحصول على الشفرة يدويا أو بطرائق أخرى وفيما يلي جملة من الاقتراحات التي يمكن العمل بها مستقبلاً في محاولة الارتقاء بالنظام الحالي :

– تعديل النظام بحيث يصبح قادراً على كسر أنواع أخرى من شفرات نابساك كالتي تم توضيحها في الأبحاث السابقة (الفقرة ٢) وتسجيل أداء النظام ومقارنته مع الأداء المتحقق في كسر شفرات ميركل هيلمان.

- استخدام طرائق أخرى لكسر شفرات نابساك ومقارنة أدائها مع أداء الخوارزمية الجينية.
- استخدام طرائق أخرى لتنفيذ عمليات التزاوج والانتقاء والطفرة وقياس وقت البرنامج قبل التعديل وبعده لدراسة مدى تأثير هذه الطرائق على النظام لغرض اعتماد الخيارات الأفضل.

المصادر

اولاً : المصادر الأجنبية

Dilbag Singh and Etal., 2013. "To Design a Genetic Algorithm for Cryptography to Enhance the Security ", International Journal of Innovations in Engineering and Technology, Vol. 2, No. 2.

Naveen Singh and Etal., 2011." Computational Intelligence In Circuit Synthesis Through Evolutionary Algorithms And Particle Swarm Optimization", International Journal of Advances in Engineering and Technology, Vol. 1,No. 2,pp.198-205.

Nrich Team,2011." The Knapsack And Public Key Cryptogrphy", university of Cambridge.

Noor K.Al-Mahdy,2013."Using Genetic Fuzzy Algorithms As a Tool For Diagnosing Breast Cancer, MSC thesis ,Babylon University .

Pankaj Mehta and Etal., 2015." Genetic Algorithm and Operators", International Journal Of Engineering Sciences and Research Technology, Vol.4,No.2.

Poonam Garg, and Etal., 2007." An Enhanced Cryptanalytic Attack on Knapsack Cipher using Genetic Algorithm" , International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol.1, No.12.

Rakesh Kumar1, Mahesh Kumar,2010." Exploring Genetic Algorithm for Shortest Path Optimization in Data Networks", Global Journal of Computer Science and Technology, Vol. 10 No. 11.

Rawa'a D. Al-Dabbagh,2009." Compact Genetic Algorithm For Cryptanalysis Trapdoor 0-1 Knapsack Cipher", Journal of Al-Nahrain University,Vol.12, No.2, June, pp.137-145.

Ranjith, 2014." Analog Circuit Optimization With Genetic Algorithm", International Journal For Technological Research In Engineering Vol. 1, No. 11.

Safaa S. Omran and Etal, 2014."Using Genetic Algorithm To Break Supper Pascal Knapsack Cipher", Cihan University, First International Conference.

Swati Mishra, Siddharth Bali,2013." Public Key Cryptography Using Genetic Algorithm",International Journal of Recent Technology and Engineering (IJRTE),Vol.2, No.2.

Yali Liu,2015." Image Denoising Method based on Threshold, Wavelet Transform and Genetic Algorithm", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8, No. 2 , pp. 29-40.

ثانياً: المصادر العربية

خلود موسى عمران، ٢٠١١." استخدام الخوارزمية الجينية في تقييم كفاءة الخدمات التعليمية لأحد الأقسام العلمية لإحدى الكليات في محافظة البصرة"، مجلة الكوفة للرياضيات والحاسبات، المجلد/١،العدد/ ٤.

صبحي حمادي حمدون، ٢٠٠٧." تحليل شفرة نابساك باستخدام الخوارزمية الجينية"، مجلةالرافدين لعلوم الحاسبات والرياضيات .المجلد / ٤، العدد /٢.