توليد مفاتيح أنظمة التشفير اللامتماثل باستخدام الخوارزمية الجينية لتشفيروفك الشفرة أسئلة الامتحانات الوزارية والكتب الرسمية

فارس حسن رضا

المديرية العامة للتربية في محافظة نينوى

الملخص:

شفرة RSA المستخدمة في عمليات إرسال المعلومات بين المناطق البعيدة والتي تستخدم المفتاح العام في التشفير.

تناول البحث دراسة مفهوم كل من الشفرة بشكل عام وشفرة RSA والخوارزمية الجينية ، وقد ركز البحث على كيفية بناء الدليل من مفاتيح الشفرة (RSA) باستخدام الخوارزمية الجينية.

تم عرض الجانب العملي والتطبيقي للبحث من خلال توضيح الإدخالات المستخدمة في المسالة مثل عدد الأجيال وحجم المجتمع وطول الكروموسومات وكذلك q , p التي تم توليدهم بشكل عشوائي وحساب قيمة n , **ø(n)** وإمرارها على الخوارزمية الجينية لإيجاد كل قيم المفتاح العام (e) لنفس (n) وحساب قيمة المفتاح الخاص(d) لكل (e) من خلال معادلة المفتاح الخاص بعد ذلك خزن هذه المفاتيح في دليل المستخدم , بعد تكوين الدليل تصبح المفاتيح جاهزة التوزيع لغرض التشفيروفك التشفير بطريقة(RSA) .

الفصـــــل الأول

المقـــــــدمة

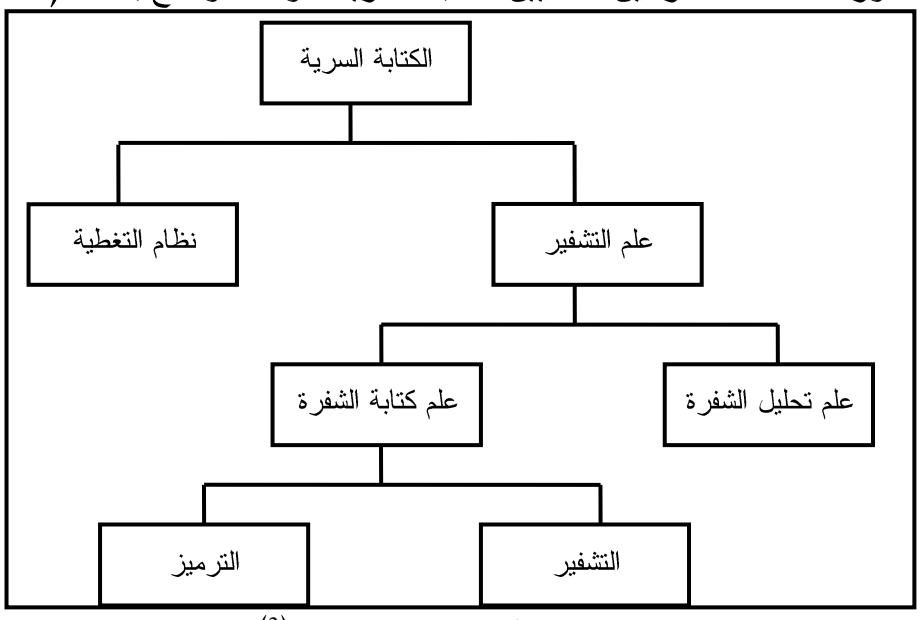
1.1 تمهيد:

عرف علم التشفير أو التعمية منذ القدم , حيث استخدم في المجال الحربي والعسكري. فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة. وذكر أن للعرب محاولات قديمة في مجال التشفير. واستخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل اثناء الحروب . فقد كان قصدهم من استخدام التشفير هو اخفاء الشكل الحقيقي للرسائل فيما لو سقطت في يد العدوفإنه منالصعب عليه فهمها وأفضل طريقة استخدمت في القدم هي طريقة القيصر يوليوس وهو أحد قياصرة الروم أما في عصرنا الحالي فقد بتت الحاجة

ملحةلاستخدامهذا العلم" التشفير" وذلكلارتباط العالم بعضه ببعض عبر شبكات مفتوحة . إذ يتم استخدام هذه الشبكات في نقل المعلومات الكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة ,عسكرية كانت أم مدنية . فلا بد من طرق تحفظ سرية المعلومات . وقد بذلت الجهود الكبيرة من جميع انحاء العالم من خلالها تبادل البيانات مع عدم إمكانية كشف محتواها[1]. وعليه فالكل يدرك أهمية التشفير وازدياد الحاجة إليه ولاسيما في هذه الأيام مع الانتشار الواسع للإنترنت وكثرة سرقة المعلومات والبيانات الشخصية فتكمن أهميته بالحفاظ على سرية المعلومات الهامة والحساسة وعدم وصولها إلى الأشخاص غير المرغوب فيهم، ومن الممكن أيضاً بواسطة التشفير التقليل من حجم المعلومات أثناء انتقالها خلال ضغط البيانات، وضمان هوية المصدر المرسل للرسالة[2] ولتسريع وصول المعلومات السرية والمهمة فسوف يتناول هذا البحث بناء دليل من مفاتيح شفرة RSA باستخدام الخوارزمية الجينية.

1. 2 الكتابة السرية :

من السهل أن نعلل أهمية الكتابة السرية للمعلومات أو الجهات العسكرية بصورة خاصة ، حيث أن حصيلة المعارك والحروب تعتمد على مدى سرية الاتصالات ومدى قابلية العدوعلى اختراقها . وبصورة عامة هناك فرعين أساسيين للكتابة السرية ، وكما موضح بالشكل(1-1).



الشكل (1-1)أنواع الكتابة السرية[3]

1. 2. 1 نظام التغطية :

فن أخفاء المعلومات داخل أشياء أخرى جاءت كلمة Steganography (نظام التغطية) من الإغريق ، وتتألف من مقطعين (Steganos) وتعني مغطاة أو سرية ، و (Graphy) وتعني الكتابة أو الرسم فهماً معيناً يعنيان مصطلح الكتابة المغطاة[3][4].

1. 2. 2 علم التشفير:

هو علم واسع جداً ، حيث يضم كل من علم كتابة الشفرة ، وعلم تحليل الشفرة ، وهذا العلم مأخوذ من الكلمة اليونانية (KRYPTOS) وتعني(مخفي) والكلمة (LOGOS) وتعني (كلمة) وكلاهما يعنيان مصطلح (الكلمة المخفية) ويتضمن مايأتي [5].

1. 2. 2. 1 علم تحليل الشفرة :

هوعلم التقنيات الرياضية المستخدمة لفتح منظومة التشفير, وقراءة المعلومات أو العبارات للنص المشفر بدون معرفة المفتاح وعادةً نبدأ بالنص المبهم ، ثم يتم إرجاعه إلى النص الصريح[3][5].

1. 2. 2. 2 علم كتابة الشفرة :

هو فن دراسة وتصميم أنظمة وتقنيات التشفير التي تقوم بإخفاء المعنى الحقيقي أو الأصلي للمعلومات ، ويضم فرعين أساسيين هما الترميز والتشفير ، وكلاهما قابل للتطبيق في مجالات متعددة (الاتصالات السرية ، الخزن ، الإرسال ألبرقي(التلغراف)). وعند الاتصال ، نبدأ بالنص الصريح للرسالة ، ثم يتم خلط الرسالة فتتحول إلى نص مشفر بواسطة نظم الترميز أو التشفير [5][6].

1. 2. 2. 2. 1 الترميز :

هي مجموعة من القوانين التحويلية التي تحدد العلاقة بين عناصر المعلومات الأصلية وعناصر المعلومات المرمزة أو العلاقة بين أبجديتين مختلفتين[5].

1. 2. 2. 2. 2 التشفير :

يعرف التشفير بأنه عملية تحويل البيانات من هيأتها الطبيعية إلى هيأة أخرى غير قابلة للفهم عبر عمليات خوارزمية معقدة بهدف حماية البيانات أو إرسالها لأطراف أخرى بطريقة آمنة تضمن أن لا يقوم بالاطلاع على هذه البيانات سوى الأشخاص المخولين ولكي يتمكنوا من قراءة محتواها فيجب عليهم أولاً القيام بفتح تشفير تلك البيانات أو المعلومات ، حيث إن فتح التشفير هي عملية إرجاع البيانات أو المعلومات من هيأتها المشفرة إلى هيأتها وطبيعتها الأصلية لقراءة محتواها ، وذلك لا يتم إلا بمعرفة المفتاح المستخدم في عملية التشفير، وبناء" عليه فإن ذلك يمنع كل من لا يملك المفتاح من قراءة ومعرفة محتوى البيانات أو المعلومات المشفرة . الشكل(1−3) يبين نظام التشفير[6]. حيث ينقسم نظام التشفير الى قسمين :

أولاً: خوارزمية التشفير :

هي مجموعة من العمليات التي تهدف الى تحويل النص الصريح الى نص مشفر .حيث ان أمنية أنظمة التشفير الحديثة تعتمد على مفتاح التشفير(k) , ولكل منها مجال التي يمكن ان

يأخذها المفتاح ويسمى فضاء المفتاح . وتعتمد قوة وفعالية التشفير على عـاملين أساسـيين:
1.الخوارزمية 2. طول المفتاح . فإذا كانت M هي فضاء الرسالة و C هـي فضـاء الرسـالة المشفرة و K هي فضاء مفتاح التشفير فأن خوارزمية التشفير (E) فتكون كمايأتي :

$$Ek : M \quad C = Ek(m) = c \quad \ldots\ldots\ldots(1.1)$$

$$k \epsilon K \ , \ m \epsilon M \ , \ c \epsilon C$$

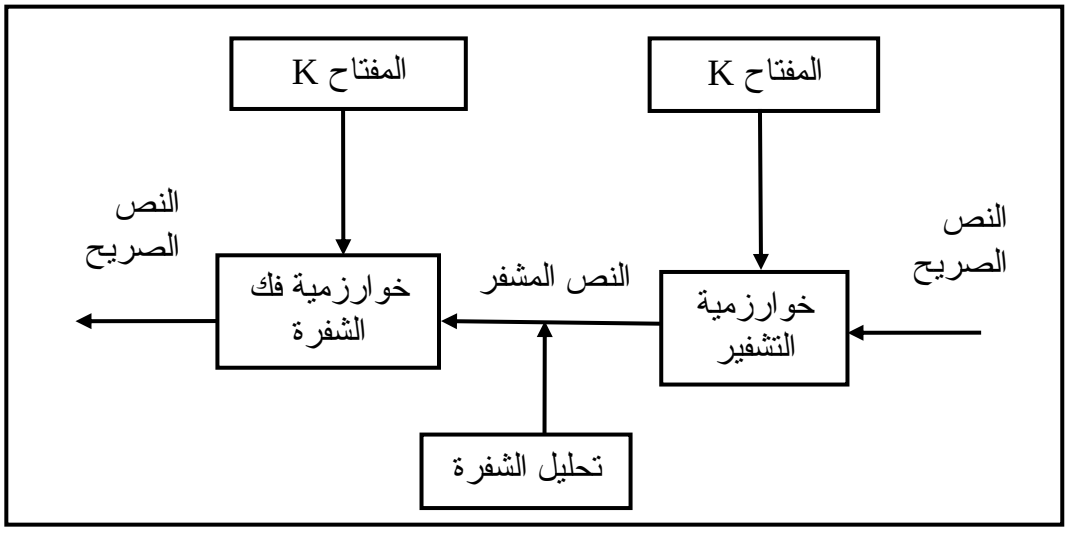
ثانياً: خوارزمية فك التشفير :

هي العملية المعكوسة أي تحويل الرسالة المشفرة الى شكلها الأصلي[3] [5] [7].

اما خوارزمية فك التشفير(D) فتكون كمايأتي :

$$Ek^{-1} = Dk$$

$$Dk(c) = Dk[Ek(m)] = m \quad \ldots\ldots\ldots\ldots\ldots(1.2)$$



الشكل(1-2) نظام التشفير[7]

الفصـــــل الثاني

RSA

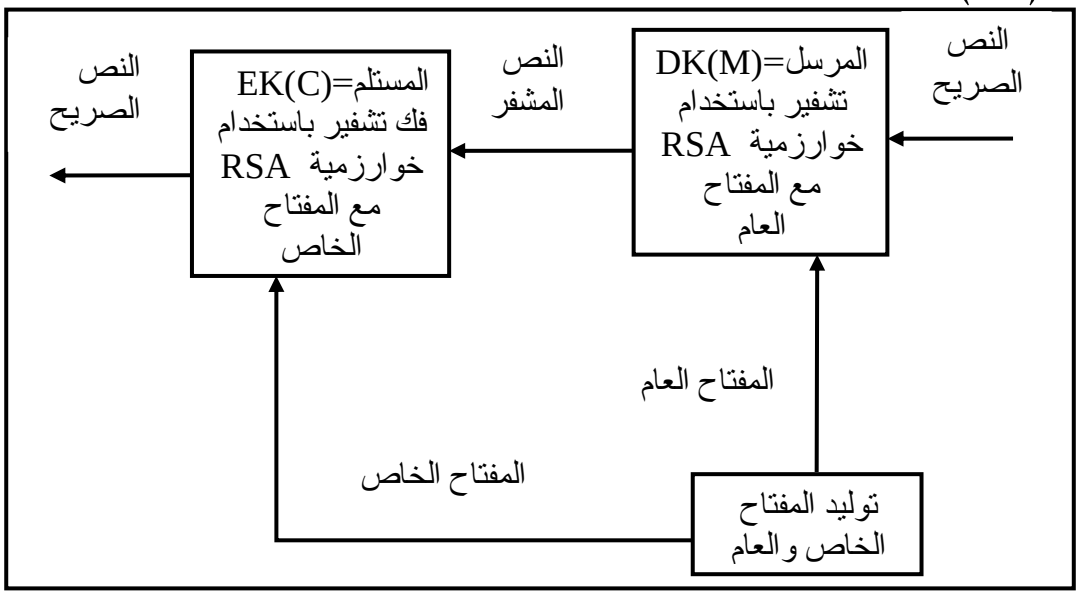
2. 1 المقدمة :

شكَّل الحاسوب في بدايات ظهوره وسيلةً جديدة للاتصالات الآمنة ، وفك تشفير الرسائل . واحتكرت الحكومات في حقبة الستينيات حق التشفير وفكه ، وفي أواخر الستينيات ، أسَّست شركة (IBM) مجموعةً تختص بأبحاث التشفير ، ونجحت هذه المجموعة في تطوير نظام تشفير أطلقت عليه اسم لوسيفَر ، طَوَّر ثلاثة أساتذة جامعيون نظامَ تشفير آخر أطلقوا عليه اسم (RSA) Rivest- Shamir- Adelman ، ويستخدم هذا النظام زوجاً من المفاتيح مفتاح عام ، ومفتاح خاص بدلاً من استخدام مفتاح واحد فقط . وهو نظام للتشفير بواسطة مفتاح عام المعروف بكونه مناسب للتّوقيع بالإضافة إلى التشفير، ومستخدم في بروتوكولات التّجارة

الإلكترونيّة على نطاق واسع ، ويُعْتَقد أن تكون مضمون على أساس أنه يوجد مفاتيح طويلة بشكل كاف واستعمالَ أحدث التطبيقاتِ إذ تم اكتشافه في العام 1970 ويعد هو نظام يوفر كل من الأمنية والتواقيع الرقمية باعتمادها على التعقيد لمسألة تحليل عوامل الإعداد الصحيحة [3][6][11] [12] .

2.2 التشفير اللامتماثل – المفتاح العام :

ينهض التشفيراللامتماثل على أساس استخدام زوج من من المفاتيح . وهذا المفتاح الزوجي يشتمل على مفتاح العام ومفتاح الخاص.وتقتصر معرفة العامة على مفتاح العام بينما يبقى المفتاح الخاص سريا ويحتفظ في سرية. يقوم المرسل بتشفيررسالة بالمفتاح العام للمستقبل الرسالة ويفك المستقبل الرسالة بمفتاحه الخاص وخوارزميات التشفير بالمفاتيح اللامتماثلة التي أطلق على اسم مخترعيها , تستخدم عادة مفاتيح تتراوح أطوالها من 512 الى 1024 بت أو في بعض الأحيان 2048بت وهي RSA(Rivest- Shamir- Adelman) وكما موضحاً في الشكل(2−1)[6][13] .



الشكل (2−1) أنظمة التشفير اللامتماثل (خوارزمية RSA)[6]

2.3 فوائد المفتاح العام(التشفير اللامتماثل) [11]:

- ❖ استخدام أكثر من مفتاح عام وبذلك يكون العدو أمام صعوبة أخرى في معرفة أي المفاتيح العامة مستخدمة في التشفير والتي كان سابقاً يعدها معلومة جاهزة ولا يفكر في إيجاد الحلول
- ❖ باستخدام أكثر من مفتاح عام سيكون للمرسل أكثر من مفتاح خاص وهذا يزيد من أمنية طرق تشفير المفتاح العام في حالة اكتشاف أو ضياع احد المفاتيح الخاصة.

❖ التفكير بجدية في تقوية بروتوكول توزيع المفاتيح العامة بسبب تزايد عددها ,غير أن عدد المشتركين يكون عادة قليلاً في التطبيقات الحساسة ومن ثم لا توجد مشكلة ذات شأن تنجم عن ذلك.

❖سيكون هناك تغييراً في مفهوم المفاتيح العامة المستخدمة في طرق تشفير المفتاح العام بحيث يصبح هناك مفتاح خاص مع مفتاح عام سري وليس مفتاحاً عاماً غير سري .

4.2 نظام إدارة المفاتيح :

تستخدم البنية التحتية للمفاتيح العامة Public key infrastructure (PKI) لتنفيذ نظم التشفير اللامتماثل والوظائف الرئيسية التي تدعمها هذه البنية هي [13] [14] :

- توليد زوج من المفاتيح الفريدة (مفتاح العام + مفتاح الخاص) , تخصيص زوج لكيان وتخزين المعلومات الضرورية لإدارتها حفظ المفاتيح كأضابير, لاسترجاعها او إذا طلبت السلطات القضائية الإعلان عنه .
- إدارة الشهادات الرقمية , انشاء شهادات تجديد , او التوقيع عليها او إصدارها , أو التحقق منها أو الغاؤلها .
- نشر المفاتيح العامة الى الجهات الطالبة , والمرخص لها كذلك .
- اعتماد المفاتيح العامة(التواقيع على الشهادات الرقمية).

5.2 مدخل إلى نظرية الإعداد :

- **الأعداد الأولية:**

لاَتملك سوى قاسمين الواحد الصحيح والعدد نفسه مثلا الإعداد {2 , 3 , 5 , 7 } أعداد أولية . تشكل الأعداد الأولية مركز نظرية الأعداد [3] .

- **تحليل الأعداد الأولية إلى عواملها :**

تحليل العدد n هو عملية كتابته على شكل ناتج مجموعة من الأعداد الصحيحة مضروباً مع بعضها $n = a \times b \times c$.التحليل الأولي إلى عوامل هو كتابة العدد على شكل أعداد أولية مضروبة مع بعضها مثلا العدد $91 = 7 \times 13$ [15] .

- **الأعداد الأولية النسبية :**

يمكن تعريف العددين الصحيحين(أنهما أوليان نسبياً) أوليان فيما بينهما إذ ان العامل المشترك لهما هو الواحد فقط. مثلا 8 و15 أوليان نسبياً وذلك لأن عوامل العدد 8 هي {1, 2, 4, 8 } وعوامل العدد 15 هي {1, 3, 5, 15 } مما يعني عدم وجود عدد مشترك بخلاف الواحد بينهما[3].

- **القاسم المشترك الأكبر(GCD) [3]:**

إذا كان لدينا عددين (a , b) والقاسم المشترك D فان العددين a , b تقبل القسمة على D بدون باقي إي: a mod D and b mod D=0

- مثال: القاسم المشترك الأكبر للعددين 10و15 هوالعدد 5 , GCD(10,15)=5و إذا كان a , b عدد أوليين Prime Numbers فان : GCD(a , b)=1

- **نظرية فيرمات:**

تنص على انه إذا ان هناك عدد أولي P وكان GCD له مع عدد صحيح a يساوي واحد , أي ان a , p أوليان فيما بينهما أو أوليان نسبياً، فإن : $a^{p-1} \bmod p = 1$ تستخدم هذه النظرية في خوارزميات إنشاء المفتاح العام [9] .

- **دالة توشنت أويلر ø(n) :**

عند عمل إجراءات حسابية موديلو(mod) n عدد عناصر هذه المجموعة هي n-1 من 0 حتى n-1 والمجموعة (المقلصة) المنقصة هي مجموعة الأعداد الأولية نسبياً مع n . دالة أويلر هي عدد العناصر الأولية نسبيا مع n ويرمز لها بالرمز ø(n). ولحساب دالة اويلر للعدد الصحيح n أو عدد الإعداد الأولية النسبية ل n فانه : إذا كان n عدد اولياً فان ø(n)= n-1 , وإذا كان p و q فان ø(n) = (p-1)*(q-1) وهما الطريقتان اللتان أثبتهما اويلر لحساب قيمة دالته ، وذلك بالاستعانة بنظرية فيرمات [9] [16] .

- ø(37) = 36 , (37 is a prime)
- ø(21) = (3–1)×(7–1) = 2×6 = 12 , (21= 3 * 7)

- **نظرية اويلر[9]:**

وقد ولد اويلر نظرية اويلر بتطبيق نظرية توشنت اويلر على نظرية فيرمات ، تنص نظرية أويلر على

$a^{ø(n)} \bmod N = 1$, where GCD (a , N) = 1 .....(2.1)

- a=3 , n=10 , Ø (10)=4 , 3^4=81,81 mod 10=1 .
- a=2 , n=11 , Ø (11)=10 , 2^{10}=1024, 1024 mod 11=1 .

6.2خطوات عمل الخوارزمية لطريقة RSA [17]:

خطوة1) توليد عددين أوليين كبيرين عشوائياً p , q متباعدين عن بعضهما.

خطوة2) حساب قيمة n . $n = p * q$.....(2.2)

خطوة3) حساب قيمة Ø(n) . $Ø(n) = (p-1)(q-1)$ .....(2.3)

خطوة4) اختيـــار عدد صحيح عشوائياً e , عن طريق المعادلة الاتية :

$1 < e < Ø(n)$ حيث أن

$GCD (e , Ø(n)) = 1$ بحيث أن .....(2.4)

خطوة5) حساب قيمة d . $d = e^{-1} \bmod Ø(n)$ .....(2.5)

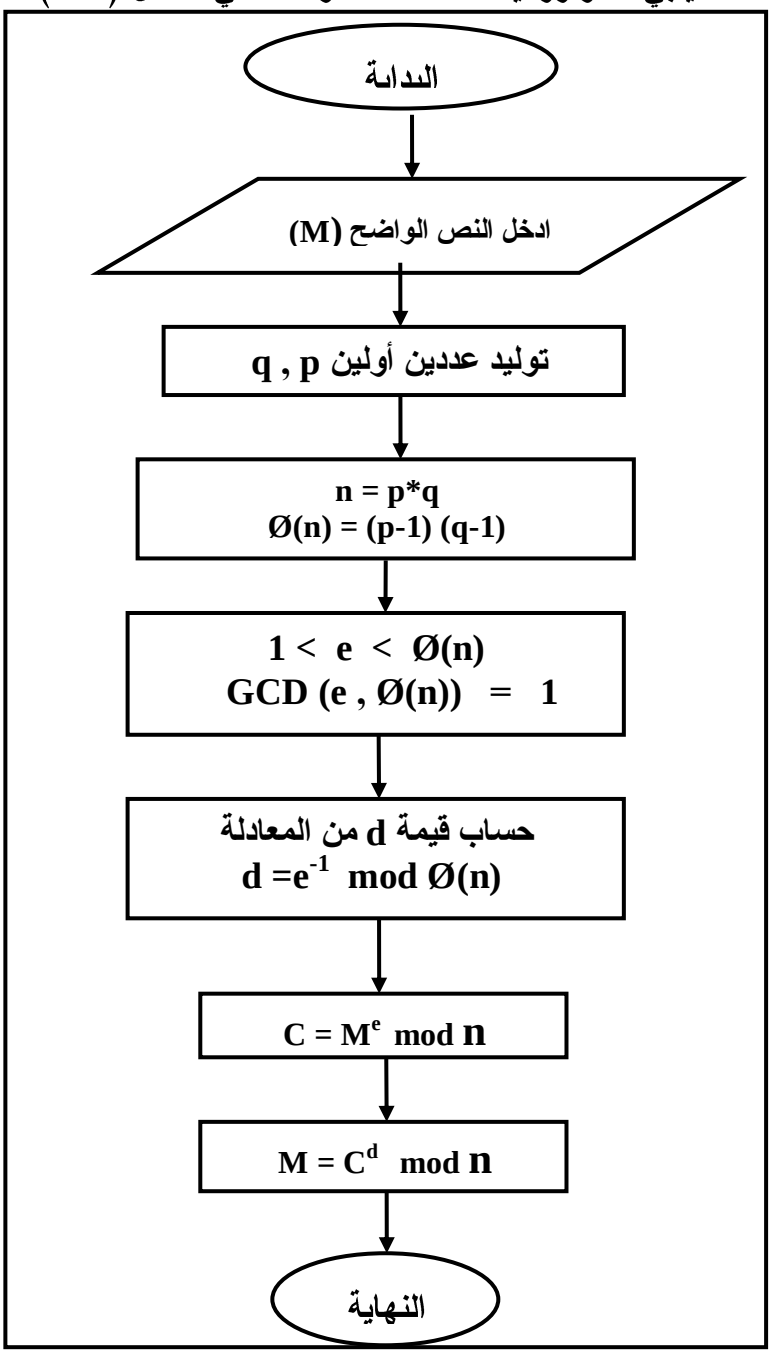
خطوة6) تشفير النص يستخدم المفتاح العام هو (e , n) = KU عن طريق المعادلة

الآتية: $c = m^e \bmod n$……(2.6)

خطوة7) فك الشفرة يستخدم المفتاح الخاص هو KR=(d , n) عن طريق المعادلة الآتية: $m = c^d \bmod n$……(2.7)

حيث ان :e يطلق عليها أس التشفير و d أس فك الشفرة في حين n يطلق عليها المعامل.

1.6.2 المخطط الانسيابي للخوارزمية RSA كما موضحا في الشكل (2-2):



الشكل (2-2) خوارزمية RSA **[11]**

الفصل الثالث

الخوارزمية الجينية

1.3المقدمة :

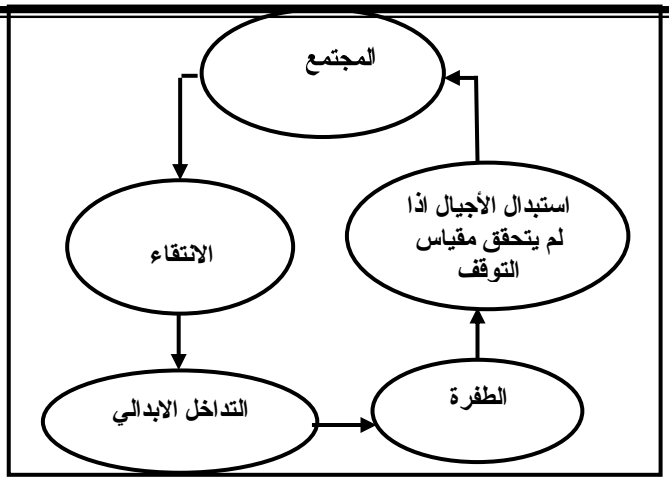
تعد الخوارزمية الجينية أحد أساليب الذكاء الاصطناعي وهي من الأساليب الحديثة، كما إنها واحدة من خوارزميات البحث العامة المعتمدة على آلية الانتقاء الطبيعي ونظام الجينات الطبيعية، ان فكرة العمل للخوارزمية الجينية تعتمد بشكل دقيق على أفكار الهندسة الوراثية والتي تتميز بالإنتاج المقصود للمجموعات الموروثة بهدف تكوين أفراد ذات صفات جيدة، وعلى هذا الأساس تقوم الخوارزمية الجينية بانتخاب الحلول الأفضل من بين عدد كبير من الحلول وإجراء بعض التداخلات والتبديلات بين هذه الحلول بهدف تكوين حلول أفضل. اختصرت الخوارزمية الجينية الكثير من الجهد والزمن المطلوبين لدى مصممي الأنظمة والبرامج ، وذلك من خلال إيجادها خوارزمية عامة يُعتمد عليها في حل مختلف أنواع المسائل، بدلاً من بناء خوارزمية خاصة لكل مسألة، مع مراعاة التغيرات اللازمة التي تتناسب مع خصوصية كل مسألة من حيث حجم ونوع البيانات المستخدمة وطبيعة دالة الهدف والقيود لكل مسألة [20] [21] [22] [23].هنالك العديد من البراهين النظرية والعلمية على إمكانية الخوارزمية الجينية على أجراء البحث الجيد لأغلب المسائل المعقدة . وتختلف الخوارزميات الجينية عن طرائق البحث التقليدية كالآتي[24] :

3.2 مجالات استخدام الخوارزمية الجينية[22][25]:

استخدمت الخوارزمية الجينية في العديد من المجالات منها: (التحليل العددي والأمثلية، ومعالجة الصور، ومسائل الأفضلية المركبة مثل مسألة البائع المتجول، وتطبيقات الشبكة العصبية، ومسائل التشفير وكسر الشفرة).

3.3المخطط العام للخوارزمية الجينية:

تتضمن الخوارزمية الجينية عدداً من الخطوات الأساسية ، هذه الخطوات ثابتة لمختلف المسائل ولكل التطبيقات ويكون الاختلاف في أسلوب صياغة كل خطوة من هذه الخطوات و تطبيقها حسب المسألة أو مجال تطبيقها . إن خطوات هذه الخوارزمية تكون مترابطة بعضها مع البعض الآخر ، ولا يمكن تطبيق هذه الخوارزمية على أية مسألة ما لم تطبق جميع هذه الخطوات وإلا تفقد الخوارزمية الجينية قيمتها و فائدتها في إيجاد أو تحسين الحل كما موضحا في الشكل (3-1)[21][25].



الشكل (3−1) يوضح المخطط العام للخوارزمية

4.3خطوات عمل الخوارزمية الجينية [25][26] :

خطوة1) البداية:إنشاء جيل عشوائي يتكون من n من الكروموسومات(الحلول المناسبة للمسالة) .

خطوة2) دالة التقييم : حساب دالة التقييم F(x) لكل كرموسوم x في الجيل.

خطوة3) مجتمع جديد: توليد جيل جديد بتكرار الخطوات الآتية إلى أن يكتمل الجيل ، وتتضمن:

- الاختيار: يتم اختيار اثنين من الكروموسومات والدين من المجتمع الابتدائي استنادا إلى دالة اللياقة (أفضل القيم التي لها فرص اكبر للاختيار).
- التداخل الابدالي : إجراء إحدى عمليات التعابر للحصول على الذرية ويكون بين كروموسومين.
- الطفرة: مع احتمالية وجود الطفرة يتم عمل الطفرة للسلف الجديد بموقع معين في الكروموسوم، وتجري بين الجينات في الكروموسوم الواحد.
- الاستبدال: عملية وضع السلف الجديد المتكون في الجيل الجديد للحلول محل المجتمع الابتدائي.
- الاختبار: عند تحقق شرط التوقف، فإن الخوارزمية الجينية تتوقف وتعيد الحل الجيد
- الدورة : يتم الرجوع إلى الخطوة 2 .

إن كل تكرار لهذه العملية يسمى بالجيل ، وبعد نهاية التنفيذ يقوم الباحث بتقديم تقرير عن الحقائق التي تم التوصل إليها.

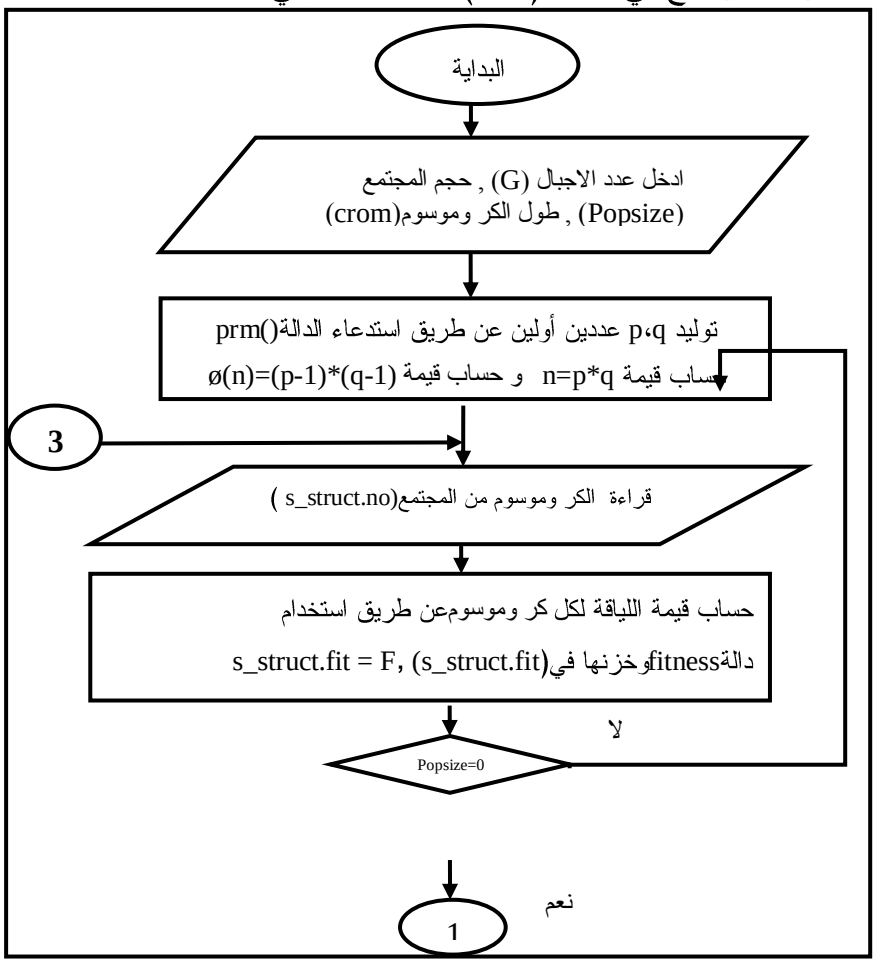
الفصل الرابع

الجانب التطبيقي والعملي

1.4تمهيد:

بعد إلقاء الضوء على مفهوم التشفير وشفرة RSA والخوارزمية الجينية الاطلاع على ميزات وخصائص كل نوع ، فقد خصص هذا الفصل لبيان كيفية إيجاد المفتاح العام لشفرة

RSA باستخدام الخوارزمية الجينية وخزن المفاتيح العامة والخاصة(e,n),(d, n) في الدليل المستخدم(ورقة العمل) واستخدام الدليل للتشفير وفك الشفرة من خلال الاتصال بالدليل للتزويد بالمفاتيح RSA وكما موضح في الشكل(4-1) مخطط تفصيلي لبناء الدليل:



الشكل (4-1) مخطط تفصيلي لبناء الدليل

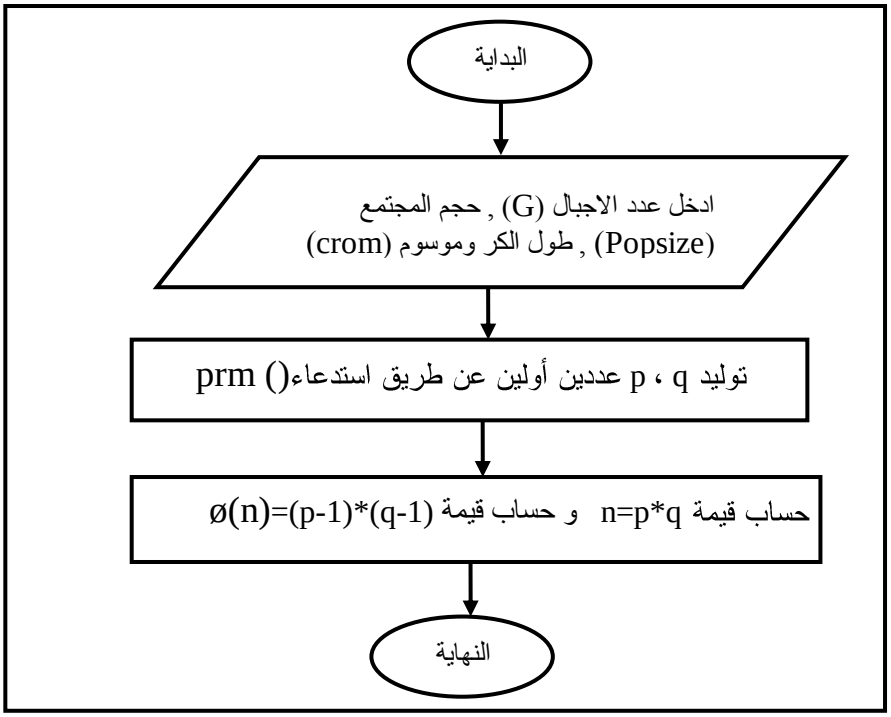
2.4 بناء الدليل:

بعد توضيح المخطط العام لبناء الدليل , سوف نتناول شرح كيف تم بناء الدليل باستخدام الخوارزمية الجينية.

1.2.4 الإدخالات:

من المعروف إن الخوارزمية الجينية تعتمد على عدد الأجيال وعدد الأفراد وطول الكروموسوم في كل جيل , وسوف يتم إدخال عدد الأجيال والأفراد وطول الكروموسوم من خلال لوحة المفاتيح , وإن خوارزمية RSA تعتمد على قيمتي q، p عددين أولين يتم توليدهم

بشكل عشوائي من خلال استدعاء دالة () prm بعد ذلك يتم حساب قيمتي n,ø(n), n = p*q,(p-1)*(q-1)=ø(n).وكما موضح في الشكل(4-2).



الشكل(4-2) الإدخالات النظام

2.2.4 مجتمع ابتدائي:

يتم في البداية توليد مجتمع ابتدائي من الأفراد ، إن إنشاء الجيل الابتدائي يعد نقطة الانطلاق في حل المسألة ،أن عملية بناء الجيل الابتدائي تتم بطريقة عشوائية ، وتم ذلك برمجياً عن طريق استخدام دالة توليد القيم العشوائية (rand) والتي تأتي بقيم عشوائية من الذاكرة تتراوح بين الصفراوواحد، ويكون عدد أفراد المجتمع مختلفاً من مسألة إلى أخرى بالاعتماد على إدخاله عن طريق لوحة المفاتيح ,ويتم خزن هذه القيم في(s_struct . no).

3.2.4 التحويل من الصيغة الثنائية:

بما أن الجيل الأولي العشوائي المتكون بالصيغة الثنائية (الترميز الثنائي) ، فلابد من تحويله إلى صيغة يسهل التعامل معها تم تحويل كل فرد أو كروموسوم إلى عدد صحيح .

4.2.4 تقييم أفراد المجتمع :

بعد أن تم توليد المجتمع الابتدائي،وتحويل قيمته إلى قيم صحيحة، سيجري تقييم كل فرد من أفراده من خلال تطبيق دالة تقييم(FitnessFunction).سوف يتم حساب قيمة اللياقة

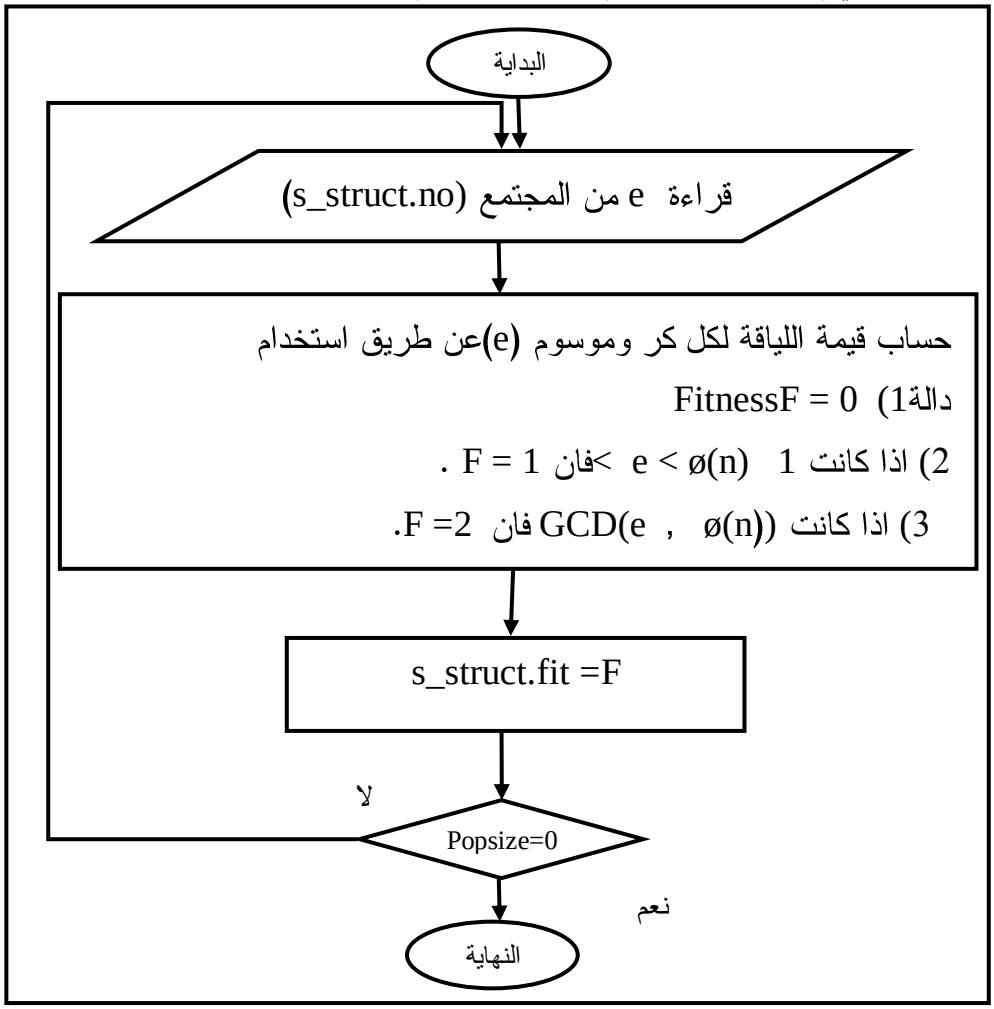
لكل كروموسوم(حيث ان الكروموسوم يعد بمثابة e) بالشكل الآتي, وكما هو موضح في الشكل(4-3).

1) F = 0 .

2)اذا كانت 1 <e< ø(n) فان F = 1 .

3) اذا كانت GCD(e,ø(n)) فان F =2.

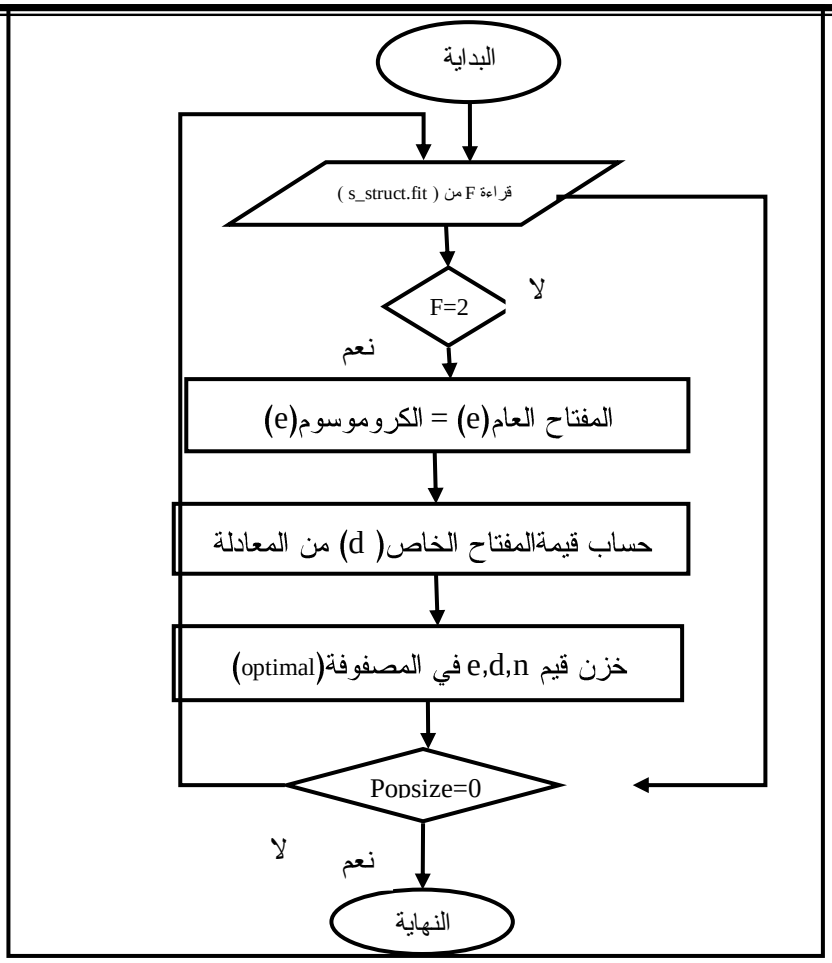
4) سوف يتم خزن F في(s_struct.fit) (struct.fit = F) .



الشكل(4-3) تقييم أفراد المجتمع

5.2.4إيجاد المفاتيح العامة والخاصة (e , d):

بعد تقييم كل فرد من أفراده من خلال تطبيق دالة تقييم (Fitness Function),سوف يتم إيجاد المفاتيح العامة والخاصة (e , d) من خلال تطبيق دالة(btodFunction) اذ يتم الانتقاء أفضل فرد في المجمع (F=2) سوف تكون قيمة المفتاح العام(e) وحساب قيمة (d)المفتاح الخاص من خلال المعادلة $d = e^{-1} \bmod Ø(n)$ وخزن القيم (e, d , n) في المصفوفة(optimal) .كما هو موضح في الشكل(4-4).



الشكل(4-4)إيجاد المفاتيح العامة والخاصة

6.2.4الانتقاء :

كما مر ذكره في الفصل الثالث ، فثمة طرق متعددة للانتقاء ، وفي هذا البحث تم انتقاء المجموعات لاختيار أفراد من الجيل الحالي لإنتاج جيل جديد , وتم ذلك عن طريق بناء الدالة(Functionselect) .اذ ينتقى فردين مختلفين عشوائياً ، ويفوز أفضلهما.

7.2.4 التداخل اوالتزوج:

بعد أن تم اختيار الأفراد من الجيل الابتدائي ليكون لها دور في توليد الجيل الآتي ، تبدأ عملية التزاوج ، حيث يقوم كل فردين بتكوين فردين جديدين ضمن المجتمع الجديد ، وتم في هذا البحث التداخل الابدالي ذو نقطة القطع الواحدة ، حيث تم توليد رقم عشوائي واعتماده كإزاحة ضمن الكروموسوم يتم عندها إجراء عملية التداخل الابدالي(التزاوج) ,وتم ذلك عن طريق بناء الدالة (Functioncrossover).

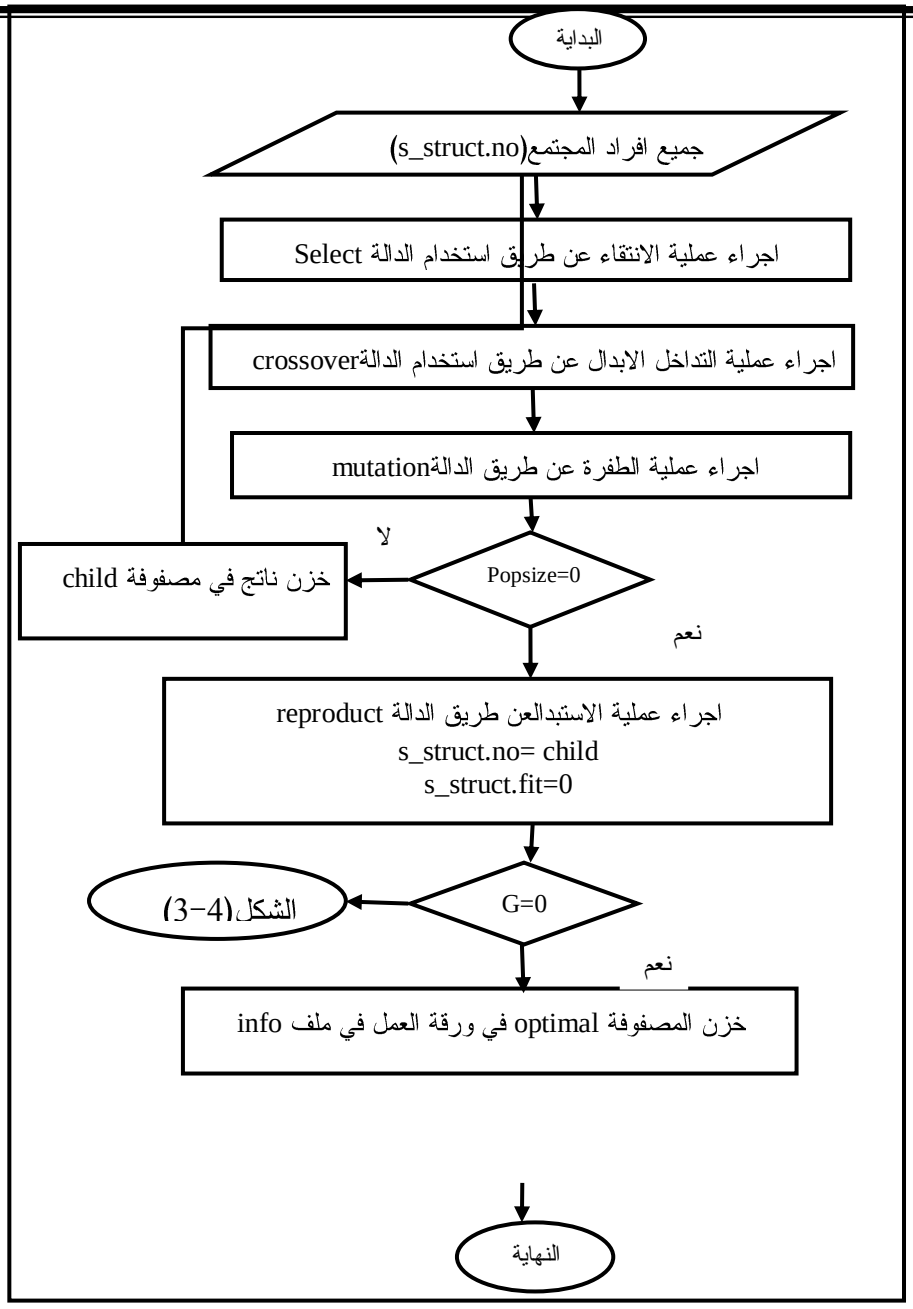
8.2.4 الطفرة:

بعد عملية التزاوج يأتي دور الطفرة في تغيير النتائج التي نتجت من عملية التزاوج وقد تم استخدام عكس قيمة الجين وتستخدم هذه الطريقة في حالة الترميز الثنائي لكروموسوم إذ يتم

اختيار موقع معين في الكروموسوم وعكس قيمته عن طريق دالة (Functionmutation). وذلك لتوسيع حيز الحلول الممكنة والمتمثل بتكوين أكبر عدد ممكن من المقاطع المختلفة ضمن الجيل ويتم خزن الأبناء في المصفوفة child كما هو موضح في الشكل(4-5).

9.2.4الاستبدال:

سوف يكون ناتج الأبناء جيل أباء للجيل القادم وتم ذلك عن طريق بناء الدالة (Functionreproduct) سوف تقوم بالإحلال ناتج المصفوفة child إلى s_struct.no وكما هو موضح في الشكل(4-5)(s_struct.no= child) وتصفير s_struct.fit=0 لتقييم الكروموسومات من جديد والعمليات التي تليها عند عدم الانتهاء من عدد الاجيال وعند الانتهاء من عدد الأجيال سوف يتم خزن المصفوفة optimal في ورقة العمل باسمinfo.اي يتم خزن المفاتيح العامة(e) والخاصة(d) والمعامل(n), في هذه الحالة تم بناء دليل من مفاتيح شفرة RSA وأصبحت مفاتيح جاهزة للتشفير وفك الشفرة .

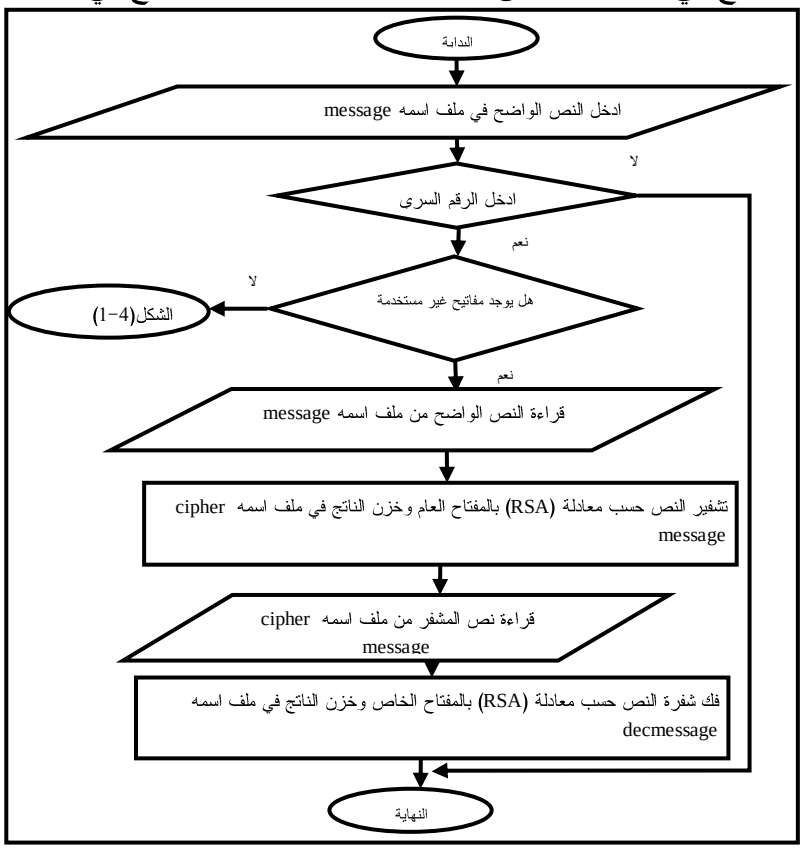


الشكل(4-5) الانتقاء والتداخل والطفرة والاستبدال

3.4 التشفير وفك الشفرة:

بعد الانتهاء من تكوين الدليل سوف تكون جاهزة للاستخدام عند طلب المستخدم للمفاتيح العامة والخاصة فعند ذلك تطلب المفاتيح من الدليل في حالة إدخال الرقم السري بشكل صحيح ووجود مفاتيح غير مستخدمة . يزود المستخدم هذه المفاتيح مرة واحدة للتشفير وفك الشفرة ولا يزود مرة أخرى وفي حالة الانتهاء المفاتيح سوف يتم تكوين الدليل من جديد وتزويد المستخدمين بالمفاتيح .وعند الحصول على المفاتيح سوف يتم قراءة النص الواضح من ملف

اسمه"message" ويشفرالملف حسب معادلة التشفير(RSA) بالمفتاح العام ويخزن نص المشفر في ملف اسمه"cipher message" ,ثم بعد ذلك سوف نقرأ نص المشفرمن ملف المشفر"ciphermessage" ,ولفك شفرة الملف حسب معادلة فك التشفير(RSA) بالمفتاح الخاص وتخزن الناتج في ملف اسمة"decmessage" .وكما هو موضح في الشكل(4-6).



الشكل(4-6) تشفير وفك الشفرة

الفصل الخامس

الاستنتاجات والتوصيات

1.5الاستنتاجات:

هنالك عدة استنتاجات في هذه البحث منها :

1) بناء دليل من المفاتيح لشفرة (RSA) سوف تكون جاهزة للاستخدام عند طلب تنفيذ التشفير وفك الشفرة بالسرعة الممكنة مباشرة عند طلب التشفير بدون الانتظار توليد المفاتيح (RSA) فهذا يأخذ وقت ولاسيما في حالة وجود أكثر من طالب للمفاتيح .
2) استخدام الخوارزمية الجينية لإيجاد قيمة المفتاح العام(e) أفضل من طرق التقليدية يتم إيجاد عدة قيم للمفتاح العام(e) في آن واحد بدلاً من استدعاء البرنامج لكل توليد (e).

3) بعد تطبيق الخوارزمية الجينة لإيجاد قيمة المفتاح العام(e) وجد أن هناك عدة قيم للمفتاح العام(e) لنفس قيمة (n) كما موضحاً في الجداول في فصل الرابع لذا تعد أفضل من الطرق التقليدية لأن الطرق التقليدية تقوم بإيجاد المفتاح العام(e) واحدة لكل n.

4) من خلال تطبيق البرنامج في توليد بناء الدليل وجدنا أنه عندما يكون عدد الأجيال وحجم المجتمع كبيراً وقيمة n كبيرة حصلنا على عدد كثير من المفاتيح .وعندما يكون عدد الأجيال وحجم المجتمع صغيراًوقيمة n صغيرة حصلنا على عدد قليل من المفاتيح.كما يمكن القول أن كلما كانت قيمة (n) كبيرة حصلنا على نتائج أفضل, وكما أوضحنا في الفصل الرابع .

5) تشفير أسئلة الامتحانات الوزارية والكتب الرسمية وإرسالها عبر الشبكة وفك الشفرة عند المستقبل أفضل وامن من الطرائق التقليدية .

2.5 التوصيات:

من خلال هذه الدراسة والنتائج التي تم الحصول عليها نوصي بما يأتي:

1) ان يكون البرنامج مربوط على الشبكة, ويكون الدليل هوالخادم ومن خلاله يتم تزويد المستخدمين بالمفاتيح .

2) استخدام الخوارزمية الجينية لإيجاد e, q , p في نفس الكروموسوم بدلا من e .

3) زيادة عدد البايت للكروموسومات .

4)استخدام الخوارزمية الجينية في تحليل شفرة RSA .

5) وضع أمنية أعقد لقاعدة بيانات (ورقة العمل) .

6) تشفير أسئلة الامتحانات الوزارية والكتب الرسمية من خلال المفتاح العام لكل محافظة وإرسالها مباشرة الى مراكز الامتحانية ولكل مركز امتحاني يكون له مفتاحه الخاص لفك التشفير أسئلة .

7) انه بالامكان تطوير البحث ليضم عدد اكبر من الادله .

8) لغرض التشفير قد تكون هناك حالات شاذة .

الهوامش و المصادر

1.مركز التميز لأمن المعلومات (علم التشفير أو التعمية (cryptography).
http://www.boosla.com/showArticle.php?Sec=Security&id=62update:2012/11/1

2.كلمة المرور والتشفير.
http://www.mediafire.com/?i41htzu6wuza4qh
update:2o12/11/15

3 .علاء حسين الحمامي , سعد عبد العزيز العاني ,2007 , "تكنولوجيا أمنية المعلومات وانظمة الحماية" ,دار وائل للنشر .

4.رشا عواد حسن الجبوري،2011،"تصميم وتنفيذ نظام هجين لتشفير وإخفاء الملف النصي في بروتوكولات الصوت عبر الانترنت " ، رسالة ماجستير،كلية علوم الحاسبات والرياضيات،جامعة الموصل، العراق.

5. ميلاد جادر سعيد جلميران ،2003،" تشفير النصوص العربية باستخدام شفرة مورس"، رسالة ماجستير،كلية علوم الحاسبات والرياضيات،جامعة الموصل، العراق .

6. ياســـين حكمت إسماعيل العبيدي ، (2004)، "دراسة الوثوقية وتحقيقها باستخدام التواقيع الرقمية"، رسالة ماجستير،كلية علوم الحاسبات والرياضـــــــيات،جامعة الموصل، العراق.

7.ساهرة عبيد سعد ، (2007)، "اعتماد التغيرات الحرفية والثنائية لتشفير المعلومات", جامعة البصرة/كلية العلوم/قسم الحاسبات .

8.شامل قيس إبراهيم الأمين ، (2011) ، " تصميم وتمثيل نظام برمجي أمني بالاعتماد على قزحية العين والقنوات المخفية", رسالة ماجستير, كلية علوم الحاسبات والرياضـــــــيات ، جامعة الموصل , العراق.

9. William Stallings, 1999," Cryptography And Network Security Principles And Practice ", SecondEdition , published by prentice-hall , inc, the united state of America.

10.مركز التميز لأمن المعلومات (الكتابةالمشفرة (Cryptography))
http://coeia.edu.sa/images/Articles/new/cry.pdf
update: 2012/11/24

11. ندى بدر جراح , 2009 ,"تقنيات التشفير في التبادل التجاري الالكتروني" , كلية الإدارة والاقتصاد، جامعة البصرة, مجلة ميسان للدراسات الأكاديمية ,المجلد (7) , العدد(14), العراق.

12."ENCRYPTION"
http://www.vc4arab.com/showthread.php?t=1175
update: 2012/11/30

13.سولانغ غيرناوي–هيلي, 2006,"دليل الأمن السيبراني للبلدان النامية", طبع في سويسرا (جينف)
http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-a.pd
update:2012/11/24

14.RSA Laboratories , 2000,"(FAQ) Frequently Asked Questions about Today's Cryptography", Version 4.1, Publisher: RSA Security Inc.

15.RSA Laboratories ,2006 , "RSAES-OAEP Encryption SchemeAlgorithm specification and supporting documentation" , RSA Security Inc. ,Bedford MA 01730 USA .

16. Joachim Rosenthal, 2004/05, Cryptography

http://translate.google.iq/translate?hl=ar&langpair=en%7Car&u=http://en.wikipedia.org/wiki/RSA
update:2012/11/30
17.Pekka Riikonen,2002," RSA Algorithm" .
http://iki.fi/priikone/docs/rsa.pdf
update:2012/11/30
18.RSA Algorithm Example
http://www.cs.utexas.edu/~mitra/honors/soln.html
update:2012/12/12
19.تاج الدين جركس, عدنان معترماوي, غسان ناصر,2007, أمان طرائق التواقيع الرقمية,**مجلة** جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الهندسية , المجلد (29) , العدد (1) , العراق .
20.أسماء صلاح الدين سليمان الحداد, 2010," استخدام الخوارزمية الجينية في دراسة التوازن للألعاب ذات المجموع غير الصفري", رسالة ماجستير،كلية علوم الحاسبات والرياضيات،جامعة الموصل ,العراق .
21.غصون سالم بشير,2003,"استخدام الخوارزمية الجينية في مطابقة الصور", رسالة ماجستير, كلية علوم الحاسبات والرياضـــــيات ، جامعة الموصل,العراق.
22.همســـــة معـــن محـمـــد ثـابـــت,2005 ," بعض تطبيقات الخوارزمية الجينية في حل مسائل الأمثلية", رسالة ماجستير, كلية علوم الحاسبات والرياضـــــيات ، جامعة الموصل,العراق.
23. Randy L. Haupt& Sue Ellen Haupt, 2004 , "PRACTICAL GENETIC ALGORITHMS" ,Second Edition,A John Willey &Enetic Sons, Inc., Publication, the united state of America.
24. محمد ناظم داؤد المولى,2007 ,"تقطيع صور أورام الدماغ ممثلة بالخوارزميات الجينية", رسالة ماجستير, كلية علوم الحاسبات والرياضـــــيات ، جامعة الموصل,العراق.
25.فرح سعد نشاط الجلبي,2009 , " استخدام الخوارزمية الجينية في تقدير معلمة توزيع بولتزمان المتمثل بمعلمة RNA", رسالة ماجستير, كلية علوم الحاسبات والرياضـــــيات ، جامعة الموصل ,العراق.
26. هنـــاء محمد عصمان محمد,2012, "تحقيق وتطبيق نظام كشف وتصنيف التطفل المعتمد على الخوارزمية الجينية على بيانات NSL-KDD", رسالة ماجستير, كلية علوم الحاسبات والرياضيات ، جامعة الموصل, العراق.
27. شهلة حازم احمد محمد خروفة,2005," استخدام الخوارزمية الجينية المهجنة لتصنيف صور الأقمار الصناعية", رسالة ماجستير, كلية علوم الحاسبات والرياضـــــيات ، جامعة الموصل,العراق.
28.HartmutPohlheim, 2006, " Genetic and Evolutionary Algorithms: Principles, Methods and Algorithms. Genetic and Evolutionary Algorithm".
http://www.geatbx.com/docu/algindex.html
28. لغة Matlab
http://ele-maga.com/vb/showthread.php?t=171
update:2012/12/22