الفصل الاول

١-١- المقدمة في الامنية (Introduction):

إن موضوع الأمن في النظم الآلية للمعلومات يعتبر من أكثر المواضيع التي تنال اهتمام الباحثين والمتعاملين مع تلك النظم، لاشك إن انتشار الحاسبات الآلية ودخولها المطرد في إدارة نظم المعلومات المختلفة قد اثر تأثيرا مباشرا في تطوير ورفع كفاءة تلك النظم، لكن يظل هناك سؤالا مطروحا ألا وهو إلى أي مدى يمكن الاعتماد على هذه الحاسبات الآلية في إدارة تلك النظم بصورة دائمة ودقيقة، وعن مدى قدرتها في حماية أسرارنا وخصوصياتنا من الاعتداء[1].

١-٢- امنية الاتصالات

يشمل الأمن هنا التوثق من الطرفيات والمستخدمين وذلك بالتحكم الفيزيائي والتحكم المنطقي بعمل كلمات السر وربطها بنوع الاستخدام وتغييرها من وقت لأخر وبرمجة الطرفيات لتنفصل أليا إذا ظلت دون استخدام لفترة معينة أو إذا اخطأ المستخدم في كلمات عدة مرات.

كذلك يشمل الأمن في نظم الاتصال تسجيل كل الملاحظات في أي طرف ونوع الاستخدام إضافة بالطبع إلى التعرف على الشخص المستخدم عن طريق (رقم التعريف) والتوثق منه بكلمة السر أو البطاقة الممغنطة أو غيرها (التعرف) وربط ذلك بنوع من الاستخدام (الصلاحية) يتم ذلك في الغالب بتركيب أو تصميم نظام المعلومات بطريقة بنائية تكاملية يتم الانتقال فيه من بنية إلى أخرى عن طريق برامج تحكم خاصة تقوم بخزن معلومات عن الشخص الذي دخل إلى هذه البنية وتاريخ ووقت الدخول ونوع الحركة أو الاستخدام الذي قام به. هذه الخاصية متوفرة في كثير

من نظم التشغيل وبالأخص في نظم قواعد المعلومات حيث يشترك عدد ضخم من المستفيدين في التعامل مع قاعدة المعلومات كل في الجزئية والبنية التي تخصه[1].

١--٣- امنية المعلومات و التشفير

سوف نتعامل مع المعلومات بأنها كمية مفهومة لذلك فكل ما يتعلق بها من تأمين سرية هذه المعلومات معتمدا على التشفير يجب أن يكون أيضا مفهوما. أن أمنية المعلومات تعتمد على عدة طرق معتمدة في ذلك على الحالة والمتطلبات من المهم جداً أن يتضح لكافة المشتركين في أمنية المعلومات الأهداف المتعلقة بأمنية المعلومات.

على العموم فان أمنية كل من أنظمة المشاركة الزمنية وشبكات الحاسوب تتألف من ثلاث مكونات:

١-أمنية مركز (أو مراكز) الحاسبات.

٢-أمنية المحطات الطرفية.

٣-أمنية قنوات الاتصال.

تحتاج حماية مراكز الحاسبات لعدد مختلف من مقاييس الأمنية المقياس الأول هو أن المراكز يجب حمايتها من أي كوارث طبيعية مثل الفيضانات، الحريق، الزلازل. الخ. كذلك فان البناية يجب أن تحمى ضد النشاطات الخارجية مثل الهجومات الإرهابية، الاستراق (اختلاس السمع Eavesdropping) الخ، كل هذه المقاييس يمكن أن ينظر لها بأنها أمنية خارجية . الأمنية الداخلية)، على كل حال، تشمل مقاييس حماية تستخدم داخل نظام الحاسبة (مثلا ميكانيكية سيطرة وصول أمينة، أنظمة مراقبة لمحاولات الوصول غير الشرعية، ميكانيكية التعرف على المستفيدومقاييس أخرى تطبق خارج الحاسبة مثل الاختيار المناسب والصحيح للكادر العامل في الحاسبة، حماية فيزيائية لمكونات الحاسبة، إستراتيجية نسخ إضافية مناسبة (Backup)، الخ). أظهرت التجارب أن المحطات الطرفية هي

الأجزاء الأكثر تعرضا للانتهاك من باقي أجزاء الحاسبة. معظم محاولات الوصول غير المشروعة تنشا من المحطات الطرفية. لغرض تقليص فرصة نجاح أي وصول غير شرعي، ويجب وضعها في بنـايات أمينة (هذا الأجراء يؤدي إلى تقوية الأمنية الفيزيائية الجزئية))[1].

يستخدم التشفير لغرض حماية المعلومات التي يمكن أن يتم عليها وصول غير شرعي والتي تكون حالة المقاييس الأخرى للحماية غير كافية. لذلك فان التشفير يمكن تطبيقه لحماية قنوات الاتصال وقواعد البيانات الفيزيائية.

إن العملية الأولية (Primitive) لعلم التشفير هو عملية التشفير (Encryption) وهي عبارة عن عمليات حسابية خاصة تعمل على العبارات (Messages) وتحولها إلى تمثيل لا معنى له لكل الإطراف عدا المستقبل المقصود. إن التحويلات التي تعمل وتؤثر على العبارات هي معقدة الحل (صعبة الحل) بحيث أنها ابعد عن وسائل العدو لإبطال العمل. *عملية* التشفير (Encryption) هي عملية تحويل البيانات إلى صيغة بحيث تكون اقرب إلى عدم الإمكانية القراءة كلما أمكن ذلك بدون معرفة مناسبة (مثلا، وجود مفتاح). إن الهدف من هذه العملية هو ضمان الخصوصية (privacy) وذلك بالاحتفاظ بالمعلومات بصيغة مخفية من أي شخص أخر والذي هو غير الشخص المقصود، حتى أولئك اللذين يملكون وصول إلى البيانات المشفرة. من جانب أخر فان عملية فتح الشفرة (Decryption)هي عكس عملية التشفير، أي أنها عملية تحويل البيانات المشفرة إلى صيغتها الأصلية[2].

كل أنظمة التشفير الحديثة (Cryptosystems) في الغالب وبدون استثناء تعتمد على الصعوبة لعكس (Reverse) تحويل التشفير (Encryption) كقاعدة للاتصال الأمين (Secure Communication). إن التشفير الآن هو أكثر من عملية التشفير وفتح الشفرة. إثبات الشخصية (Authentication) هو جزء أساسي من حياتنا والذي يمثل الخصوصية. نحتاج إلى تقنيات الكترونية لتوفير إثبات الشخصية. يوفر التشفير ميكانيكيات خاصة لمثل هذه الإجراءات. أما التواقيع الرقمية

فإنهـا تقـوم بـربط وثيقـة معينـة إلـى المعـالج بمفتـاح معـين، بينمـا خـتم الوقـت (timestamp) فانـه يـربط الوثيقـة مـع منشـئها فـي وقـت معـين. يمكـن اسـتخدام هـذه التقنيـات التشـفيرية للسـيطرة علـى الوصـول إلـى مشـغل قـرص مشـترك أو أي وسـط أخر.

يـتم اختيـار خوارزميـة التشـفير مـن بـين مجموعـة تحـويلات معكوسـةأو للسـهولة يعـرف نظـام (System). إن العامـل (Parameter) الـذي يختـار تحويـل محـدد مـن هـذه التحـويلات يـدعى مفتـاح التشـفير أو للسـهولة مفتـاح نعنـي بنظـام التشـفير (Cryptosystem) بأنـه عبـارة عـن خوارزميـة، المشـفرة الممكنـة، والمفـاتيح الممكنة.

١ـ٤ـ مقدمة في التشفير

التشـفير عبـارة عـن دراسـة التقنيـات الرياضـية المتعلقـة بعـدد مـن مظـاهر أمنيـة المعلومـات مثـل الوثوقية تكامل البيانات إثبـات شخصيـة الكينونـة (وإثبـات شخصـية مصدر البيانات إن التشفير ليس عبارة عن وسيلة لتزويد أمنيـة المعلومـات فقط وإنمـا عبارة عن مجموعة من التقنيات[2].

فكرة نظـام التشـفير هـي إخفـاء المعلومـات الموثوقـة بطريقـة معينـة بحيـث يكـون معناها غير مفهوما للشخص غير المخـول.

الفصل الثاني

٢-١-تعريف التشفير

التشفير :هو عملية تحويل المعلومات بطريقة ما الى رموز سرية بحيث تصبح محمية من عمليات الوصول غير المرخص بها، أي أن معلومات الرسالة و هذا التحويل C يتم تحويلها إلى رموز مبعثرة لا معنى لها M الواضحة المتناسقة Key انطلاقًا من مفتاح تشفير خاص بعملية التشفير E يتم عن طريق خوارزمية التشفير [2].

٢-٢-

طرق التشفير:

هنالك طريقتان رئسيتان لتشفير المعلومات**[2]**:

١- طريقة التشفير المتناظرة وفيها يكون مفتاح التشفير

متماثل في كلا الطرفين وخوارزمية التشفير مشابهة لخوارزمية فك التشفير.

(E = D , Ke = Kd)

٢- طريقة التشفير غير المتناظرة

وتسمى هذه الطريقة التشفير بالمفتاح العمومي. (KE ≠ D , Ke ≠) وفيها يكون المفتاح العام Ke حيث يسمى مفتاح التشفير .

٢-٣- اهداف التشفير[1]:

١- الوثوقية : هي عبارة عن خدمة معينة تمنع من خلالها معرفة محتويات المعلومات عن جميع المشتركين عدا الأشخاص المخولين بامتلاك هذه المعلومات . يعتبر مفهوم الأمنية (Secrecy) مرادفا لكل من الوثوقية والخصوصية.

٢- تكامل البيانات : عبارة عن خدمة موجهة لاغراض احتواء التغييرات الغير مسموح بها للبيانات ولتحقيق هذا الهدف يجب تمتلك الإمكانية لكشف معالجة البيانات من قبل الأطراف الغير مخولة الإمكانية لكشف معالجة .

٣- إثبات الشخصية: عبارة عن خدمة أو وظيفة تتعلق بتحقيق التعريف هذه الوظيفة تطبق على كل من الأطراف المشتركة عند الاتصال عليها أن تعرف بعضها إلى البعض الأخر . رئيسين هما :

أ - إثبات شخصية الكينونة.

ب - إثبات شخصية مصدر البيانات أن طريقة إثبات شخصية مصدر البيانات تزودنا ضمنياً بتكامل البيانات.

نستنتج من هذا انه في إثبات الشخصية يجب أن يكون ممكنا لمستقبل العبارة أن يتحقق من مصدرها وان العدو يجب ان يكون قادرا على التنكر بأنه شخص معين أخر.

٤-عدم الإنكار : عبارة عن خدمة أو وظيفة والتي تمنع أي كينونة (Entity) من أن ينكر أي تعهد أو عمل سابق تم أجرائه . لذلك عند حصول مثل هذا النزاع بين الأطراف المشتركة في إنكار ما تم اتخاذه من أعمال فيجب توفير وسيلة معينة لحل هذا النزاع. يتم توفر هذه الوسيلة من خلال أجراء معين يتضمن إشراك طرف ثالث موثوق. يجب على المرسل أن لا يكون قادرا على الإنكار الكاذب بعد فترة ويدعي انه قد ارسل عبارة.

ملاحظة: النص الصريح المراد تشفيره يدعى ب plain text والنص المشفر يدعى ب cipher text .

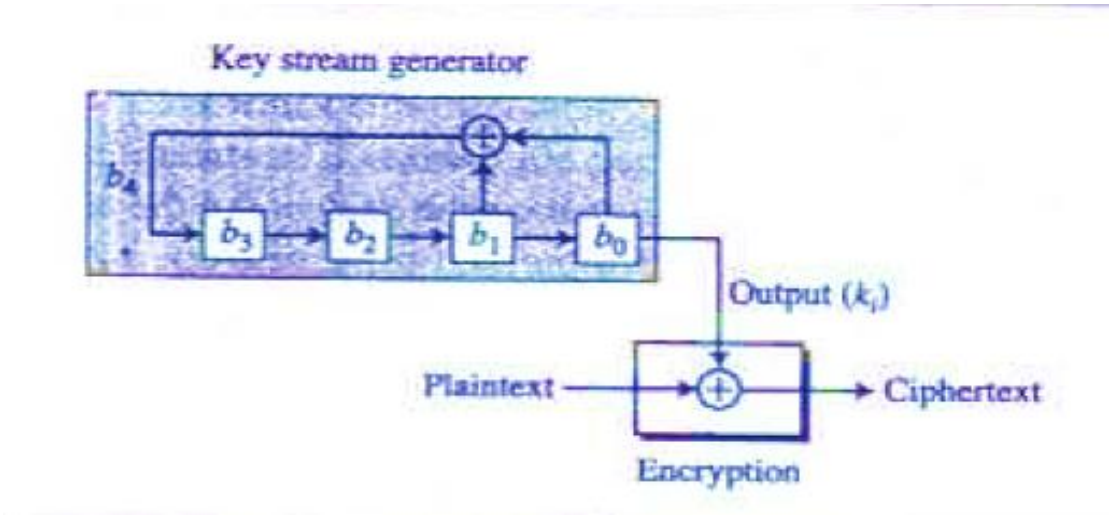
٢-٤-التشفير الانسيابي:

تعتبر أنظمة التشفير الانسيابي أحد أنواع أنظمة التشفير الحديثة المهمة جدا التي تمتاز الأنظمة بأنها الأنظمة الأكثر شيوعا واستخداما في مجال التشفير في الوقت الحاضر لما لها من خصائص مهمة، منها عدم تزايد الأخطاء في حالة وقوعها وسهولة استخدامها في التطبيقات العملية، بالإضافة إلى سرعة تنفيذها. أن أمنية نظام التشفير الانسيابي تعتمد الخوارزمية المستخدمة في توليد سلسلة متتابعة المفتاح. بما أنه توجد خوارزمية محددة لتوليد متتابعة المفتاح ، تكون هذه السلسلة دوريه، لذلك تكون شبه عشوائية وليست عشوائية تماما**[2].**

الصيغة لعامة للتشفير الانسيابي هي n := n1n2 …. ni , where ni Є {0,1} ، مفتاح التشفير k := k1k2k3 … with ki Є {0,1} . ان التشفير وفك التشفير سوف يعطى بواسطة مزج النص الصريح مع المفتاح الانسيابي المتولد باستخدام دالة xor مع ملاحظة ان E هي تشفير و D هي فك التشفير:

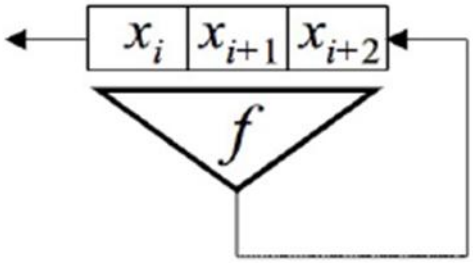
$E^*(k,n) := k \oplus n$, $D^*(k, c) := k \oplus c$

. كما في الشكل (١.٢):



الشكل (١.٢): طريقة التشفير باستخدام المفتاح الانسيابي

يتكون مفتاح التشفير الانسيابي من عدد من المسجلات ، والمسجل عبارة عن عدد من stages كل stage تحتوي على قيمة ثنائية اما صفر او واحد. البيانات المخرجة من المسجل bit واحدة في الوقت الواحد اي سوف تزحف القيم stage واحد كلما خرجت قيمة واحدة، في هذه الحالة سوف يحتاج المسجل الى تغذية ، لإرجاع إملاء المسجل بالقيم بصورة عشوائية والتي تعتمد على طريقة ربط معينة لذلك سوف يستخدم التغذية المرتدة feedback shift register (FSR) والتي تصنف بدالة خطية او غير خطية بالاعتماد على دالة التغذية feedback function. والشكل (٢.٢) يوضح التغذية المرتدة.



الشكل (٢.٢): يوضح التغذية المرتدة.

كما ذكرنا ان المسجل المتحرك shift register يمتلك دالة تغذية مرتدة هذه الدالة تشمل دوال خطية كـ xor, or او دوال بوليانية غير خطية كـ and,not مع استخدام دوال خطية معها لان استخدامها بشكل منفر سوف ينتج مفتاح متكون من اصفار، سيكون موضوع بحثنا حول التغذية المرتدة غير الخطية حيث تعتبر الدوال الاخطية اكثر تعقيد من الدوال الخطية من حيث استرجاع المعلومة من قبل المهاجم. NLFSR (nonlinear feedback shift register) بطول L يتكون من L من (0,1,…,L-1 bits) التي تاخذ مدخل واحد وتعطينا مخرج واحد[2]. ان الدوال غير الخطية سوف تعطي نتيجة المفتاح المتولد يكون فيه عدد الاصفار غير مساوي لعدد الواحدات في المفتاح المتولد[2].

يتم اختيار عدد من stages من المسجل ليتم الربط بينها بدالة بوليانية غير خطية ، يجب ان تحقق الدالة المختارة اعلى دورة ممكنة للمفتاح اي ان اعلى دورة للمفتاح تحسب من المعادلة (2^n-1) حيث n هي عدد stages اي المفتاح لا يتكرر الا بعد اكماله اعلى دورة، وان الربط باستخدام الدوال الاخطية على الاغلب لاتعطي اعلى دورة بسبب العمليات اللاخطية. **<u>ومثال</u>** على هذا:

لنفترض لدينا مسجل من ثلاثة stages كل stage يجب ان تحتوي على قيمة ابتدائية ثنائية والتي يجب ان لا تكون جميعها اصفار من اجل البدئ بحركة المسجل ، حيث ان ال stages التي سوف نختارها لتعطي التغذية المرتدة سوف تدعى بـ متعددة الحدود primitive polynomials سوف نختار متعددة الحدود (**x1 ⊕ not (x3)**) الجدول (١.٢) يوضح النتيجة:

الجدول (٢.١): المفتاح الانسيابي المتولد

n	input	Register state x1 ⊕ x4 * x5	Out put	
0		**101**	**1**	
1	**1**	**110**	**0**	
2	**0**	**011**	**1**	
3	**0**	**001**	**1**	
4	**0**	**000**	**0**	
5	**1**	**100**	**0**	
6	**0**	**010**	**0**	
7	**1**	**101**	**1**	**تكرر المفتاح**
8	**1**	**110**	**0**	
9	**0**	**011**	**1**	
10	**0**	**001**	**1**	
11	**0**	**000**	**0**	
12	**1**	**100**	**0**	
13	**0**	**010**	**0**	

هنا نلاحظ ان المسجل اعطى اعلى دورة وهي 7 .

الفصل الثالث

٣-١- مقدمة في SIMULINK

الـ SIMULINKهو برنامج للنمذجة و المحاكاة و تحليل الانظمة الديناميكية سواء كانت خطية او غير خطية و يقوم أيضا بنمذجة الانظمة سواء فى الزمن المستمر او فى الزمن الغير مستمر [3].

وباستخدام ال SIMULINK يمكنك بناء نماذج من البداية او التعديل على انظمة موجودة بالفعل والفائدة من ذلك هو دراسة خصائص نظام التحكم اوالمنظومة قبل البدء فى التنفيذ حتى نحدد مدى استجابة النظام لما نقوم بعمله والتحكم بيه، وهل نظام التحكم الموجود سيعطى احسن استجابة وأقل اخطاء ام لا ؟

وال SIMULINK ليس قاصرا على التحكم وتطبيقاته وانما يحتوى على مجموعة من الكتل والتى تغطى أغلب تطبيقات الهندسة الميكانيكية والكهربية ,والرياضية.

ويعتبر ال SIMULINKاداة ممتازة لـ Model-Based Design وهذا معناه ان البرنامج ليس فقط قاصرا على الانظمة المثالية ولكن يمكنك ايضا من نمذجة انظمة حقيقة والتى يوجد بها عوامل موثرة لجعلها غير خطية nonlinear مثل الاحتكاك ومقامة الهواء والانزلاق والظواهر الطبيعية الاخرى . كما يوجد فى البرنامج العديد من النماذج لاغلب التطبيقات يمكنك استخدامها او التعديل عليها . والتعامل مع الـ SIMULINK سهل جدا فهو يوفر بما يسمى graphical user interface (GUI) فى بناء النماذج في صفحة النموذج وتقوم بتوصيلها بطريقة سهلة. وبعد بناء النموذج نقوم بتشغيل النموذج لعمل ال simulation ويمكنك اختيار خصائص ال simulation وطريقة التكامل وهذا يكون فى non-real time كما يمكننا ايضا عمل محاكاة للنماذج فى ال real time وهذا باستخدام مجموعة الكتل الموجودة فى البرنامج . ويمكننا التحكم فى ال Simulation من خلال أوامر الماتلاب وهذا يكون مفيد جدا فى حالة الرغبة لعمل Simulation لأكثر من نموذج و ويمكن تخزين النتائج و استخدامها لاحقا[4].

استخدام السميولنك يعتمد على عنصرين للمحاكاة[3]:

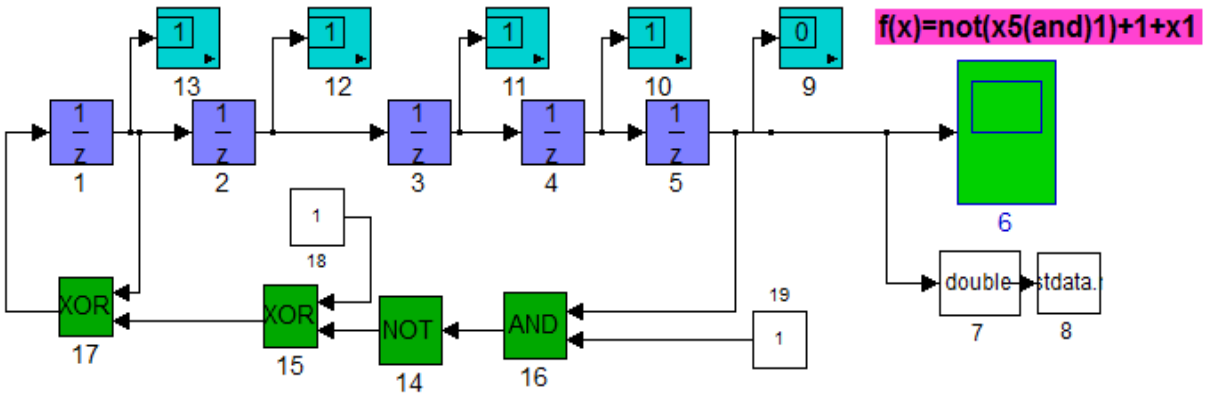
الكتل: وتستخدم الكتل لتوليد لاجراء العمليات مثل الجمع، الخزن، عرض الاخراج الى اخره من العمليات.

الروابط: تستخدم لنقل الإشارات من كتلة إلى أخرى.

لبناء النموذج يجب ان يتسم بتعقيد البناء وسهولة التنفيذ وسرعة الاداء ، حيث ان مولد المفتاح الاخطي هو المولد الذي يستخدم في تنفيذه عمليات منطقية لاخطية وخطية والتي تكون فيه المفتاح الناتج عدد الاصفار غير مساوي لعدد الواحدات.

٣-٢- النموذج المصمم لعملية المحاكاة:

لقد قمنا بتصميم نموذج مولد مفتاح انسيابي لاخطي بواسطة السميولنك كما في الشكل (١.٣) :



الشكل (١.٣): النموذج المصمم

تم محاكاة مولد المفتاح الانسيابي الاخطي والذي ولد سلسلة عشوائية من bits الثنائية والمستخدمة لتشفير النص الصريح، حيث ان المفتاح الانسيابي قد ولد بالاعتماد على محاكاة المسجل والعمليات التي تجري فيه، و تم عرض نتائج التنفيذ عملية المحاكاة أما على شكل مخطط او على شكل قيم مخزونة في مصفوفة او قيم صريحة.الجدول (١.٣) يبين تفصيل الكتل المستخدمة في الشكل (١.٣) :

الجدول (١.٣): الكتل المستخدمة في تصميم مولد المفتاح الانسيابي

الترقيم	رقم الكتلة	وصف الكتلة
١	١-٥	خزان يخزن القيم الثنائية
٢	٦	مخطط رسم
٣	٧-١٣	عرض النتائج
٤	١٤-١٧	دوال منطقية
٥	١٨,١٩	ثوابت وهو (١)

قمنا ببناء مولد مفتاح انسيابي لاخطي مكون من مسجل واحد والذي يتكون من خمسة stages ، حيث اخترنا اصغر مسجل لاخطي وذلك لسهولة قياسه وتتبع أدائه من اجل الحصول على نتائج مضبوطة.

لقد وضعنا القيم الابتدائية لوحدات المسجل هي (11111) ، وكما اخترنا متعددة الحدود التي تعطي اقرب اعلى دورة وهي 31 اي بعد الوقت 31 سوف يتكرر المفتاح بعد الدورة 22 اي افضل قيمة حصلنا عليها من دالة الربط (متعددة الحدود) فقد كانت متعددة الحدود هي (**f(x)=not(x5(and)1)+1+x1**) .

٣-٣- تنفيذ النموذج المصمم لعملية المحاكاة:

بما ان عدد stages في المسجل هي 5 اذن سوف يعطي اعلى دورة للمفتاح هي 31 bits بما ان المفتاح لم يحقق اعلى دورة بسبب استخدام الدوال الاخطية ، فقد تتكرر المفتاح بعد الدورة 23. بعد تنفيذ النموذج حصلنا على المفتاح التالي كما في الجدول (٢.٣) :

الجدول (٢.٣) : المفتاح الانسيابي المتولد

وقت	0	1	2	3	4	5	6	7	8	9	10	11
قيمة	1	1	1	1	1	0	1	0	1	0	0	1

وقت	12	13	14	15	16	17	18	19	20	21	22
قيمة	1	0	0	0	1	0	0	0	1	1	1

الفصل الرابع

٤-١- اختبار نتائج تنفيذ النموذج المصمم:

بعد تصميم النموذج والحصول على المفتاح المتولد يجب معرفة قوة المفتاح وذلك بقياس عشوائيته ، المفتاح المتولد يجب ان يتمتع بعشوائية جيدة وذلك لضمان عدم وضوح البيانات المشفرة والحصول على شفرة جيدة.

هناك مجموعة من الاختبارات يجب اجرائها على المفتاح المتولد وهي[2]:

١. اختبار السلسلة Serial test:

في هذا الاختبار سوف يحدد عدد مرات حدوث القيم 00, 01, 10 and 11 كمتسلسلة جزئية للمتسلسلة العشوائية للمفتاح الانسيابي حيث ان الناتج يجب ان ينحصر مابين $0<x<5.9915$ اي يجب ان لا يتجاوز الحد المطلوب اي ان حد العتبة هو 5.9915.

٢. اختبار التكرار Frequency test:

في هذا الاختبار سوف يحدد عدد مرات حدوث الاصفار والواحدات في المفتاح المتولد ، ان حد العتبة هو 3.8415 ، نستطيع من خلاله معرفة المفتاح الانسيابي المتولد يكون خطي او لاخطي.

٣. اختبار بوكر Poker test:

يستخدم هذا الاختبار لقياس عشوائية المفتاح المتولد من حيث تقسيم المفتاح الى k من المقاطع وحساب مدى تكرار هذه المقاطع في المفتاح المتولد. ان حد العتبة هو 14:0671.

٤. اختبار التنفيذ Run test:

يستخدم هذا الاختبار لقياس عشوائية المفتاح المتولد من حيث عدد مرات تكرار الواحدات والاصفار بعدد معين فيحسب عدد مرات تكرار المقاطع 0 or 00 or 000 و عدد مرات تكرار المقاطع 1 or 11 or 111. ان حد العتبة هو 9:4877.

من اجراء الاختبارات على المفتاح الانسيابي الاخطي المتولد حصلنا على النتائج كما في الجدول (١.٤).

الجدول (١.٤): نتائج اختبار المفتاح الانسيابي الاخطي المتولد

Run test	Poker test	Frequency test	Serial test	Total Length of key	Length of key
3.2474	3.2857	0.3913	0.1542	31	23

لاحظنا من اختبار التكرارات ان عدد الاصفار 10 وعدد الواحدات 13 وهذا يدل على ان المفتاح الانسيابي المتولد لاخطي.

كما ولاحظنا ان نتائج الاختبارات الاربعة لم تتجاوز حد العتبة اي جميعها نتائج جيدة.

٤-٢- الاستنتاج:

نستنتج من العمل الذي قمنا بيه اننا يمكننا توليد مفتاح انسيابي لاخطي واختباره باستخدام بيئة السميولنك، حيث تعتبر بيئة السميولنك بيئة سهلة التطبيق والتنفيذ. واننا ولدنا مفتاح لاخطي باقرب دورة يمكن توليدها من اعلى حد لدورة المفتاح الافتراضية بسبب استخدام الدوال الاخطية ، وان الدوال الخطية تعطينا مفتاح اكثر تعقيدا من الدوال الخطية.

٤-٣- التوصيات:

- استخدام بيئة السميولنك لبناء مفتاح غير متناظر في الانظمة الاخرى.
- تطوير المفتاح الانسيابي الاخطي المصمم باضافة تعقيدات اكثر.

المصادر:

1- تضيف اسم احد المصدرين التي اعطيتك ايها اسم المؤلف اسم الكتاب السنة.

2- Menezes A. and vanOorschot P., Vanstone S. ***"Handbook of Applied Cryptography''*** citeseerx library, 1997.

3- MATLAB/ SIMULINK *"**Simulink ® Getting Started Guide"*** R2013b, 2013.

4- On line MATLAB http://www.mathworks.com/help/simulink.