العنوان:	تصميم وتنفيذ مولد تشفير انسيابى جديد مع اختبار مخرجات إحصائيا
المصدر:	مجلة الآداب والعلوم
الناشر:	جامعة المرج
المؤلف الرئيسي:	الحمداني، سيف الدين هاشم قمر
المجلد/العدد:	ع7
محكمة:	لا
التاريخ الميلادي:	2003
الصفحات:	233 - 271
رقم MD:	837801
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	AraBase, IslamicInfo, HumanIndex
مواضيع:	أنظمة التشفير، التشفير الانسيابى، حماية المعلومات، خوارزميات التشفير
رابط:	http://search.mandumah.com/Record/837801

تصميم وتنفيذ مولد تشفير انسيابي جديد مع اختبار مخرجات إحصائياً

□ م. سيف الدين هاشم قمر الحمداني

معهد الدراسات العليا للحاسوب والمعلوماتية

جامعة بغداد

تصميم وتنفيذ مولد تشفير انسيابي جديد مع إختبار مخرجاته إحصائياً

مقدمة: Introduction

إن الحاجة للمحافظة على سرية الرسائل ظلت غير مقدرة لسنين عديدة ، وبالطبع فـإن الناس ما كانوا بطيئوا الإدارك للفوائد التي يمكن أن تكتسب من عملية اعتراض العمليات السرية ، هذا الأمر قاد إلى معركة ساخنة ومستمرة بين صناع الرمز Codemakersومكسري الرمز Codebreaker وحلبة المنازلة لهذه المسابقة هي وسط الاتصالات الذي قد تغير إلى حد بعيد على مدى السنين ، كما أن عملية وصول البرقيات الذي يعتبر فن الاتصالات ، لم يكن كما نعرفه اليوم ، حيث أن المجتمع في الوقت الحاضر متوقف إلى حد كبير على الوسائل الحديثة ذات السرعة والدقة العالية لإرسال الرسائل ، بالاضافة إلى ذلك فإن الأعمال الثابتة الطويلة مثل البريد وخدمات ساعي البريد أصبحت متأخرة في هذا الوقت ، إذ يوجد الآن تلكس وهاتف وتلفزيون وأوساط ذات تقنية عالية وخطوط للمعلومات عالية السرعة وبريد إليكتروني ، وفي العادة فإن الهدف الرئيسي وبشكل مجرد هو إمكانية إرسال الرسائل بأسرع وقت ممكن وبأقل كلفة مادية قدر المستطاع ، وهناك على أية حال عدد من الحالات تكون فيها المعلومات سرية ، لذلك يتم العمل ضمنها على أساس وجود معترض يحتمل أن يكون قادراً على الاستفادة وبشكل كبير جداً من المعرفة المكتسبة بمراقبة دائرة المعلومات المعينة ، وإذا كانت نظم الاتصالات لها القدرة على استعمال الوسائل الغير قابلة للاعتراض لإرسال الرسائل ، فيكون من الواضح أن كل الرسائل التي سترسل ستكون آمنة ، لكن الأشكال الأكثر شيوعاً في نظم الاتصال لا ترضي هذا المتطلب ، والطريقة الأقرب ما يكون لأن تفي بمتطلبات السرية العالية تكون باستعمال ساعي ، ولكن يبقى البطيء الذي يشكل عيباً كبيراً جداً لا يمكن تلافيه ، كذلك الكلفة العالية جداً تشكل العيب الأخر الذي يجب أن يؤخذ بنظر الاعتبار ، وإذا كان عدد الرسائل كبير ، فربما يكون من المحال استخدام هذا الأسلوب ،

والطريقة الوحيدة لوسائل الارسال الغير قابلة للاعتراض هي بإخفاء محتوى كل رسالة وذلك بتحويلها قبل الارسال ، وهذا هو الهدف الأساسي من أنظمة التشفير ، ويسمى هذا الفن أو علم التصميم بمثل هذه الأنظمة بالكتابة السرية Cryptography .

في مثل هذه الحالات ، المشفرون يجب أن يأخذوا بالحسبان الخطوات اللازمة لإخفاء محتوى رسائلهم ، وفي كل الأحوال فإن حجم الحماية المطلوبة سيتغير حسب الحاجة ، إذ أن بعض أنظمة التشفير البسيطة تكون كافية لأن تمنع مستمع عادي من فهم الرسالة ، ولكن في حالات أخرى وعندما تكون المعلومات المرسلة ذات سرية عالية ، في مثل هذه الحالة من الأفضل أن يكون التصميم معقداً جداً بحيث أنها تستعصى حتى على المصمم ذو الخبرة العالية فلا يستطيع استنتاجها.

وهناك ارتباط ثنائي بين أنظمة الاتصالات والأنظمة الأمنية والذي يتضح أكثر عند ملاحظة الهدف الواحد الذي يجمعهما ، إذ أن مصمم نظام الاتصال يهدف لجعل الرسالة واضحة بشكل كبير وفي الاتجاه الصحيح حتى عند محاولة إفساد الإشارة المرسلة بالضوضاء ، ومصمم نظام الأمنية في كل الأحوال يهدف لجعل من المستحيل استعادة الرسالة المرسلة ، حتى عند استلام الإشارة المرسلة بشكل تام (1) ، ولا يفوتنا ذكر أن واحدة من الأهداف الرئيسية لهذا البحث هو تصوير الأنواع المتعددة للحماية المتوفرة والتركيز على الحاجة للمستوى الأمني الذي عرض بالنظام المقترح.

أنظمة التشفير: Cipher systems

مقدمة:

كما هو معروف فإن أنظمة الكتابة السرية Cryptography هي أسلوب خاص لحماية المعلومات المنقولة خلال قنوات الاتصالات التي تستخدم الأسلاك الموصلة Landlines ، وقنوات الأقمار الصناعية Satellites ، ووسائل المايكرويف Microwave ، وتعتبر في بعض

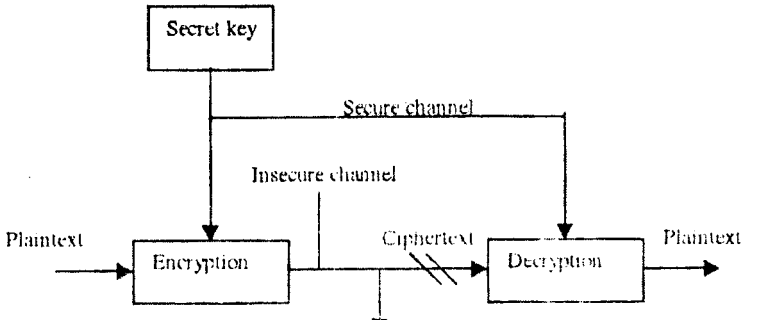
الحالات الطريق الأكثر اقتصاداً لحماية البيانات المخزونة على الأوساط الخازنة ، ويمكن أن تستخدم أساليب الكتابة السرية في تخويل الرسائل Message Authentication والتوقيع الرقمي Digital Signature وتعريف الهوية الشخصية لتخويل نقل الأموال الإلكتروني وصفقات بطاقات الائتمان ، والتشفير هي طريقة عملية لحماية المعلومات التي ترسل خلال قنوات الاتصالات والتي تستخدم الأسلاك الموصلة والأقمار الصناعية ووسائل المايكرويف.

ويمكن تعريف بعض المصطلحات التي تستخدم في نظام التشفير ، وأولها الـ Cyptography التي تمثل العلم الذي يصمم أنظمة التشفير ، ، و Cryptoanalysis وتطلق هذه التسمية على عملية التوصل إلى النص الصريح من النص المشفر من غير معرفة المفتاح السري.(4)

يعرف نظام التشفير على أنه الأسلوب السري في الكتابة ، أي أن تنكر المعلومات السرية بطريقة معينة بحيث يصبح معناها غير واضح إلى الشخص الغير مخول ، إذ تجري مجموعة من التحويلات على النص الصريح للحصول على النص المشفر وتعتمد هذه التحويلات على خوارزمية التشفير بالإضافة إلى المفتاح.

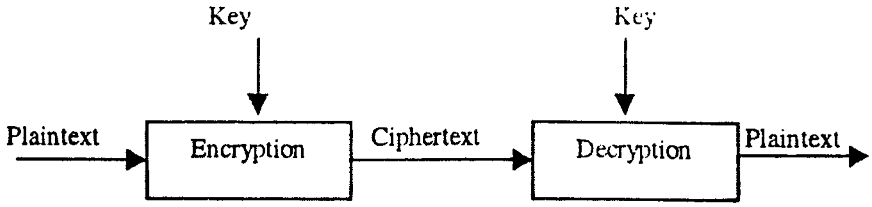
المعلومات المطلوب إخفائها تسمى عادة النص الصريح ، والعملية التي تستخدم لإخفاء النص الصريح تسمى عملية التشفير enciphering or encryption وتسمى الرسالة المشفرة بالنص المشفر ciphertext or cryptogram ومجموعة القواعد التي يستخدمها الشخص المشفر لتشفير النص الصريح تسمى الخوارزمية Algorithm والعمليات التي تتبع في بناء الخوارزمية تعتمد على اختيار المفتاح السري من قبل المشفر ، أما مدخلات الخوارزمية فتتضمن المفتاح السر إضافة إلى الرسالة أو النص الصريح ، وتعرف العملية المعاكسة لعملية التشفير والتي تعتمد على المفتاح السري للتحويل العكسي من النص المشفر إلى النص الصريح تعرف بعملية فك الشفرة deciphering or dcryption (3).

إن أي شخص يعترض النص المشفر لمحاولة كسر النظام يسمى Cryptonalyst ، كما أن مجموعة كل الرسائل المحتملة والتي يستطيع المشفر إرسالها Message space ومجموعة كل عمليات التشفير الممكنة Cryptograms تسمى فضاء عملية التشفير Cryptogram space ومجموعة كل المفاتيح يسمى فضاء المفتاح Key space ، والشكل (1) يمثل التعاريف والمعالجات لنظام التشفير.



الشكل(1) يمثل مخطط نظام التشفير

وبتفصيل أكثر لخوارزمية التشفير والتي تمثل الجزء الأساسي في هذه العملية فهي دالة رياضية تستخدم لعملية التشفر وفك الشفرة ، وبشكل عام توجد هنالك دالتين مترابطتين ، واحدة لعملية التشفير والأخرى لعملية فك التشفير ، فإذا كانت السرية لأي خوارزمية تحدد بطريقة معينة وثابتة يحافظ من خلالها على عمل الخوارزمية بشكل سري ، فإن هذا التحديد للخوارميات أصبح ذا اهتمام تاريخي فقط و لم يعد يتماشى مع معايير اليوم ، إذ أن العدد الكبير أو المجاميع المتغيرة باستمرار من المستخدمين لم يعد بالامكان استخدامهم لها ، إذ أنه بين الحين والآخر يترك مستخدم عمله ومن ثم يجب أن تبدل الخوارزمية بخوارزمية أخرى ، والخ من الأسباب الأخرى التي تقودنا إلى رفض هذا النوع من السرية.



شكل(2) يمثل عمليتي التشفير وفك الشفرة باستخدام مفتاح واحد

نموذج Cryptography وجد حلاًلهذه المشكلة باستخدام مفتاح وليكـــن K ، وهــذا المفتاح يمكن أن يكون واحداً من القيم العديدة المحتملة التي تسمى فضاء المفتاح Key space ، وكلا عمليتي التشفير وفك الشفرة تستخدم هذا المفتاح وكما موضحة في الشكل (2).

ويمكن تعريف الدوال كما يأتي:

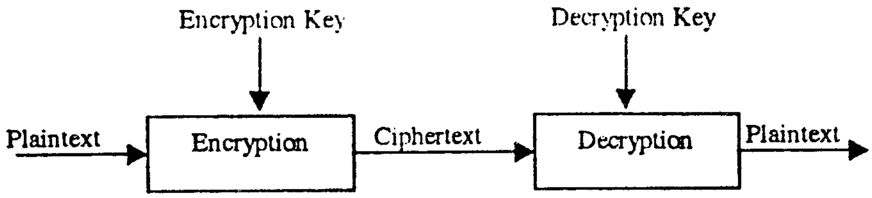
$$E_k(M)=C \quad , \quad D_k(C)=M$$

حيث أن E تمثل عملية التشفير وأن D تمثل عملية فك الشفرة ، وM تمثل الرسالة (النـص الصريح) و C تمثل النص المشفر.

بعض الخوارزميات تستخدم مفتاحاً لعملية التشفير يختلف عن المفتاح المستخدم لعمليـــة فك الشفرة ، وهذا يعني أن مفتاح التشفير وليكن K_1 يختلف عن مفتاح فـــك الشـــفرة K_2 المطابق للمفتاح K_1 ، وتكون الدوال في هذه الحالة كما يأتي:

$$E_{k1}(M)=C \quad , \quad D_{k2}(C)=M$$

$$D_{k2}[E_{k1}(M)]=M$$



شكل (3) يمثل عمليتي التشفير وفك الشفرة باستخدام مفتاحين مختلفين

إن السرية في الخوارزميات المستخدمة تعتمد بشكل أساسي على المفاتيح المستخدمة في عملية التشفير وفك الشفرة ، ولا تعتمد على تفاصيل الخوارزمية ، هذا يعني أن الخوارزمية يمكن أن تكون عامة ومعروفة ، إذ يكون من غير المفيد للمعترض أن يعرف الخوارزمية ما لم يكن يعرف تفاصيل المفتاح المستخدم ، حيث لا يستطيع قراءة الرسالة ، من هنا فإن الـ Cryptosystem هو أي خوارزمية مضافاً إليها كل احتمالات النص الصريح والنص المشفر والمفتاح (3) (7).

الأمنية التامة Perfect Secrecy

الدرجات المختلفة للأمنية تعتمد بشكل أساسي على الخوارزميات المختلفة ومدى صلابتها ومقاومتها للإنكسار ، وإذا كانت الكلفة المطلوبة لكسر أي خوارزمية أكبر من قيمة البيانات المشفرة فإنه يمكن القول وبشكل صريح أن الأمنية جيدة وباحتمال محدد ، وإذا كان الوقت المستغرق لكسر أي خوارزمية أكبر من الوقت المطلوب للمحافظة على سرية البيانات فإن النظام المستخدم هو نظام آمن وباحتمال محدد أيضاً ، كذلك إذا كانت كمية البيانات المشفرة وبمفتاح وحيد أقل من كمية البيانات الضرورية لكسر الخوارزمية فإن الخوارزمية آمنة وباحتمال محدد ، والقول بوجود احتمال محدد للحفاظ على أي شفرة من الكسر أمر ضروري ، لأن الفرصة تبقى موجودة دائماً للإنجازات الجديدة في مجال تحليل الشفرة ، في الاتجاه الآخر

قيمة معظم البيانات تنخفض مع مرور الوقت ، ولابد من الإشارة هنا إلى أن قيمة البيانات يجب أن تبقى أقل من الكلفة المطلوبة لكسر الأمنية. (8)

من المهم الأخذ بنظر الاعتبار السؤال التالي: ما مقدار أمنية النظام التي يجب أن توفر ، وقبل الإجابة على ذلك يجب ملاحظة أن بالإمكان وجود نظامين مختلفين لهما نفس الفرصة للتحليل ، من هنا فإذا تم كسر أي واحد فإن بالإمكان كسر الآخر (3).

تحت افتراض وجود نظامين متشابهين للتشفير R و S ،و إذا وجدت دالة تحويلية خاصة قابلة للعكس f بحيث أن R=f(S) ، فإن f تحول من فضاء الرسالة لـ S إلى فضاء الرسالة لـ R ، ويمكن صياغة ذلك كالآتي: F=S→R ، ومن الواضح إذا تمكن المحلل من كسر S فإنه سيتمكن من كسر R ، حيث أن F^{-1}®=S ، وكذلك يمكن للمحل من كسر S بعد كسر R ومن ثم إجراء عملية التحويل f^{1} ، والطريقة البسيطة للحصول على نصين متشابهين وغير وحيدين تتم بأخذ نظام التعويض الهجائي الأحادي Monoalphabetic substitution للتشفير ومن ثم تغييره باستخدام 26 رمز جديد لهجائية النص المشفر ، فالنص المشفر في كلا الحالتين مختلف ولكن الأسلوب متشابه.

عند مناقشة مقدار الأمنية المطلوبة فيجب تحديد طريقة معينة لقياس هذه الأمنية ، كما يجب أن توضح هذه الطريقة ، وواحدة من القياسات أو الاحتمالات المرغوب فيها لمعرفة مقدار الأمنية هي أن المعترض يجب ألا تكون لديه القدرة على تحليل النص المشفر عند محاولته كل المفاتيح الممكنة ، ولو أن ذلك لا يدل بالضرورة على الأمنية الكافية ، وإذا استخدم نظام التعويض الهجائي الأحادي Monoalphabetic substitution للتشفير (نفس الفرصة لكل المفاتيح) وتحت افتراض أن المحلل استطاع الحصول على 100 حرف ، فإن عليه أن يحاول !26 لكل المفاتيح في كل Nanosecond ، هذا يعني أن عليه محاولة كل المفاتيح الممكنة في 1.23×10^{10} سنة ، ولكنه من المعروف إمكانية استخدام المعلومات الإحصائية المؤكدة لكسر

النظام بشكل سريع ، وتحت افتراض وجود نظام معين وأن لدى المحلل Cryptonalyst الوقت الكافي لكل المحاولات المممكنة ، فهل بإمكان المحلل في هذه الحالة تحديد الرسالة؟ هنا المحلـــل لا يستطيع أن يحدد الرسالة المرسلة لأنه لا يستطيع أن يقرر أي الرسائل هي الرسائل المرسلة وبالتالي تم الحصول على الأمنية المطلوبة.

الأمنية التامة بشكل واضح هي موضوع مرغوب فيه ، وتعني أن المحلـــل مـــا لم يمتلـــك معلومات كافية حول نظام التشفير والمفتاح المستخدم لذا فإنه لا يحصــــل علـــى البيانـــات أو المعلومات المشفرة مهما كان الأسلوب المستخدم لتحليل النص المشفر وهذا يعني أن النظـــام لا يمكن كسره [3].

وفي الحقيقة هناك نظام واحد خاص يمتلك سرية تامة ويستحق الإشارة إليه وهو نظام المرة الواحدة One- time- pad إذ أن عدد المفاتيح الممكنة تأخذ نفس الاحتمالية في هذا النظـــام ويكون طولها على الأقل أكبر من طول الرسالة ، وإذا كـــانت الرســـالة المطلـــوب تشـــفيرها $m=m_1,m_2,m_n$ فإن السلسلة العشوائية المختارة $K_1,K_2,....K_n$ أي أن كل K_1 تختار بطريقة مستقلة عن الأخرى ، إضافة إلى ذلك يجب أن تكون نفس الاحتمالية لكل K_1 تختـــار بطريقة مستقلة عن الأخرى ، إضافة إلى ذلك يجب أن تكون نفـــس الاحتماليـــة لكـــل K_1 المقابل لكل m_1 [3].

تعتبر أنظمة التشفير الإنسيابي أحد أنواع أنظمة التشفير الحديثة المهمة جدا والتي تســـتخدم مفتاحا سريا واحدا في عمليتي التشفير وفك الشفرة ، وتمتاز هذه الأنظمة بأنها الأنظمة الأكـــثر شيوعا واستخداما في مجال التشفير في الوقت الحاضر لما لها من خصائص مهمة ، منها عدم تزايـد الأخطاء في حالة وقوعها وسهولة استخدامها في التطبيقات العملية بالاضافة إلى سرعة تنفيذها.

لقد ظهر هذا النوع من الأنظمة نتيجة الحاجة في الحصول على نظام تشفير عالي الســـرية يماثل نظام فيرنام (one- time- pad system) الذي يعتبر نظام تشفير ذو سرية مثالية ، ولقـد

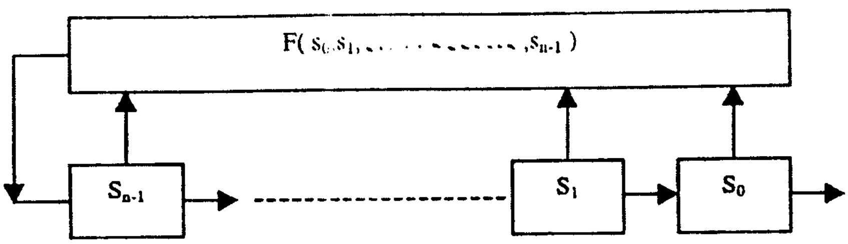
ابتكر هذا النظام سنة 1917 من قبل Joseph Mauborgne and G. Vernam (6) ، ولا يمثل هذا النظام سوى مجموعة كبيرة من الحروف العشوائية والتي لها نفس الاحتمالية في الظهور ، تكتب على ورقة بشكل سلسلة ، وبشكل أكثر واقعية كأنما تكتب هذه الحروف على شـــريط آلة كاتبة مرة واحدة ، والمرسل يستخدم كل حرف من هذا الشريط وبشـــكل مســـتقل عـــن الحروف الأخرى لتشفير حرف واحد فقط من حروف النص الصريح وذلك بجمع هذه الحـروف مع بعضها بمعيار معين ، كما أن كل حرف من السلسلة يستخدم مرة واحدة فقـــط ، فكـــرة استخدام الـــ one- time- pad امتدت بشكل أوسع لتتعامل مع البيانات الثنائية ، أي بـــدلا من استخدام سلسلة عشوائية من الحروف استخدمت سلسلة عشوائية من البيانات الثنائية والـــتي تجمع مع النص الصريح بعد تحويله إلى الصيغة الثنائية بمعيار معين مثل معيار XOR (7).

مستلم النص المشفر يستخدم نفس السلسلة من الحروف العشوائية لفك الرسالة المشـــفرة مرة واحدة ، أي أن كل رسالة مشفرة جديدة تكون لها سلسلة عشوائية جديدة ، من هنا فـــإن المستلم لا يتمكن من حساب نفس السلسلة أو استنتاجها في حالة فقدانها وبالتالي عدم معرفتـــها إلا إذا تم إرسالها والتي تكون عادة طويلة مما قاد إلى أن يكون هذا النظام غير مفيد عمليا.

تطور نظام فيرنام ودرجة أمنيته العالية قاد إلى محاولة الباحثين محاكاة هذا النظام في بعـــض الاتجاهات ، وصولا إلى نظام بمستوى أمن عالي مضمون ، من هنا ظـــهرت أنظمـــة التشـــفير الانسيابي (stream cipher) لتكون مشابهة لهذا النظام بامتلاكها خصائصه الجيدة وتجاوزهـــا مشكلته باستخدام خوارزمية محددة ومفتاح محدد لتوليد سلسلة المفتاح العشوائية.

مسجلات الإزاحة والتغذية المرتدة: Shift Registers and Feedback

إن الفكرة الأساسية من استخدام مسجلات الإزاحة هي توليد سلسلة من الأرقام الثنائيـــة التي يمكن تطويرها وصقلها حسب الحاجة ، ويوجد في الوقت الحاضر مجموعـــة واســـعة مـــن التطبيقات الأساسية المختلفة لمسجلات الإزاحة إما تحت الاختبار أو في الاستعمال الحقيقي.



شكل (4) يمثل مسجل الإزاحة

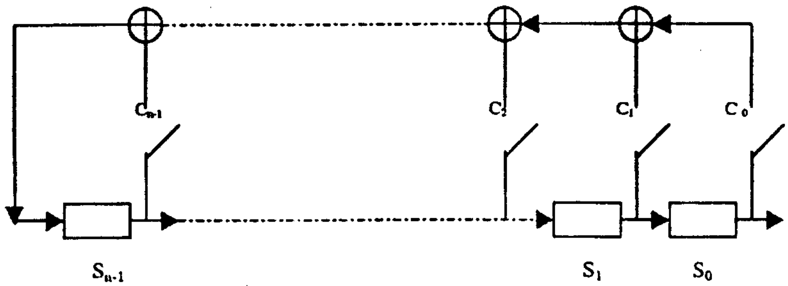
مسجل الإزاحة يحتوي عادة على n عنصر خازن (tube) في الصف وكل عنصر إما on(1) أو off(0) والذي يحرك محتوى كل عنصر خازن إلى العنصر الخازن القادم في حينه ساعة نبض (clock pulse) ، ومسجلات الإزاحة تكون على شكل متجه ثنائي (0 أو 1) بطول n أي n-tube (1).

تسمى الـ n عنصر خازن مراحل مسجل الإزاحة stages ، وفي أي وقت فإن محتوياتها تسمى حالة مسجل الإزاحة state ، كما أن مسجل الإزاحة ذو n مرحلة يمكن أن يكون في إحدى حالاته التي عددها 2^n.

إن الطريق الوحيد الذي يضمن فعالية مسجل الإزاحة هو التغذية المرتدة لحالة مسجل الإزاحة المتكون من n عنصر خازن وفق دالة معينة ، وعندما تتم هذه الإزاحة للمسجل فإن نتيجة الدالة ستحل محل العنصر الخازن الأخير.

مسجل الإزاحة ذو التغذية المرتدة مصمم من جزأين: مسجل الإزاحة ودالة التغذية المرتدة وكما مبين في الشكل (5) ، وفي كل عملية إزاحة فإن bit واحد (الذي يقع في أقصى اليمين) يخرج من مسجل الإزاحة وكل الـ bits الأخرى في مسجل الإزاحة تزحف bit واحد إلى جهة اليمين، كما أن النتيجة التي تظهر من الدالة الناتجة من الـ bits الأخرى في

المسجل تغذى الــ bit الواقع في أقصى يسار مسجل الإزاحـــة ، ويمكـــن ملاحظـــة أن دورة مسجل الإزاحة تعطي طول السلسلة الخارجة من المسجل قبل البدء بالدورة التالية (7). ويمكـــن القول أن هناك نوعين من مسجلات الإزاحة وكما موضحة في المبحثين التاليين:



شكل(5) يمثل مسجل الإزاحة ذو التغذية المرتدة

أولا: مسجلات الإزاحة ذوات دوال التغذية المرتدة الخطية:

إن مسجل الإزاحة ذو الدالة المرتدة الخطية هو أبسط أنواع مسجلات الإزاحة وكما هـــو موضح في الشكل (5) ، فإذا كانت الدالة المرتدة كما مبينة في الصيغة الآتية:

$$F(S_0,S_1, \quad ,S_{n-1})=C_0S_0+ C_1S_1+..........+ C_{n-1}S_{n-1}$$

حيث أن قيم C هي إما 0 أو 1 ، وعملية الجمع هنا تكون بمعيار 2 (XOR) ، فإن مسجل الإزاحة يسمى خطي ، والثوابت $C\ i$ (حيث $i=1,2,.......,n-1$) تســـمى معاملات التغذية المرتدة Feedback coefficients ، وأي n-bit من مسجل الإزاحة الخطـي ذو التغذية المرتدة هو واحد من 2^n-1 من حالات هذا المسجل ، هذا يعني أن أقصى حد لطول دورة السلسلة الثنائية الخارجة من مسجل الإزاحة هو 2^n-1 وأن السلسلة ذات الطول الأعظم تسمى M-sequence.

الحالة الخاصة لمسجل الإزاحة الخطي ذو دالة التغذية المرتدة هي الحالة التي تعطي أعظـــم

دورة للسلسلة الخارجة والتي تعتمد على استخدام متعدد حدود ابتدائي(*) ، كما أن درجة متعدد الحدود الابتدائي تمثل طول مسجل الإزاحة ، وبشكل عام فإنه من غير السهل توليد متعددات الحدود الابتدائية بمعيار 2 (Mod 2) للدرجة المعطاه ، ومثال على ذلك فإن الاعداد التالية (32, 7, 5, 3, 2, 1, 0) يمكن تمثيلها كمتعدد حدود أولي بمعيار 2 وكما يأتي:

$$X^{32} + X^7 + X^5 + X^3 + X^2 + X + 1$$

وهذا يعني أن لدينا مسجل إزاحة مكون من 32 عنصر(32-bits) ، وأن دالة التغذية المرتدة المستخدمة لتوليد القيمة الجديدة تتم بعملية الجمع بمعيار XOR للقيم الواقعة في الموقع الثاني والثلاثين والموقع السابع والموقع الخامس والموقع الثالث والموقع الثاني والموقع الأول مع بعضها ، وهنا فإن دورة مخرجات مسجل الإزاحة ذو دالة التغذية المرتدة ستكون بأعظم طول ، أي أن طول الدورة هو 2^{23}-1.

ثانيا: مسجلات الإزاحة ذوات دوال التغذية المرتدة غير الخطية:

كما لاحظنا في الفقرة أولا السابقة فإن مخرجات مسجل الإزاحة ذو دالة التغذية المرتدة الخطية يمكن تمثيلها بمعادلة خطية ، أي أنه يمكن حلها بسهولة نسبية نوعا ما ، وبالتالي فإنه يمكننا زيادة التعقيد أو تحديد فيما إذا كان الحل ذو تعقيد متزايد بإدخال مفهوم اللاخطية ، وهنا يجب أن نتذكر أنه مهما يأخذ شكل ناتج المتسلسلة فإن كل bit يمكن أن يمثل بمعادلة لعدد من المتغيرات التي تحدد بإيجاد الحالة الأولية للمسجل ، وبالرغم من إمكانية حل مثل هذه المعادلات إلا أن مقدار العمل المطلوب والذي يعتمد على حجم تعقيد الخوارزمية المستخدمة سيكون كبيرا جدا.

تختلف مسجلات الإزاحة ذوات التغذية المرتدة اللاخطية عن ذوات التغذية المرتدة الخطية بكون الأولى تستخدم دوال لا خطية (مثل دالة AND المتمثلة بضرب رقمين ثنائيين) وكما موضحة في الشكل (6) ، ومن المهم أن نحدد هنا بعض المشاكل التي يمكن أن تظهر في المتسلسلة

الخارجة من مسجل الإزاحة ذو دالة التغذية المرتدة اللاخطية وهي:

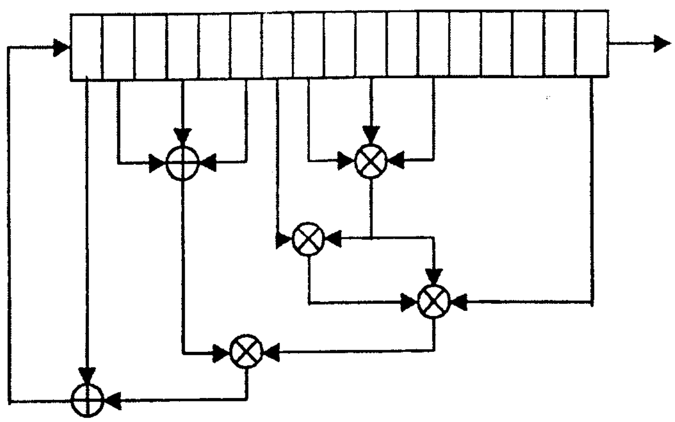
1- من المحتمل أن يكون هناك تحيز في السلسلة الخارجة ، مثلا أن يكون عدد ما موجـود في السلسلة الخارجة من الواحد أكثر من الصفر ، أو عددد مرات الظهور أقل من المتوقعة.

2- أعظم دورة للسلسلة ربما تكون أقل بكثير من المتوقعة.

3- دورة السلسلة ربما تختلف باختلاف القيم الابتدائية.

4- المتسلسلة الخارجة من المولد لربما تظهر بشكل عشوائي لفترة قصيرة ، ثم تستمر بعدها بقيمة مفردة إلى نهاية غير محددة (هذه المشكلة يمكن حلها بسهولة باستخدام XOR للـ bits الواقعة في أقصى اليمين من الدوال اللاخطية) [1]

لذلك من الممكن القول بإمكانية استخدام مسجل الإزاحة ذو دالة التغذية المرتدة اللاخطيـة في تصميم نظام التشفير الإنسيابي ولكن يجب أن يكون بعناية كافية.



شكل(6) يمثل مسجل الإزاحة ذو التغذية المرتدة اللاخطية

تعريف التشفير الإنسيابي: Definition of stream cipher

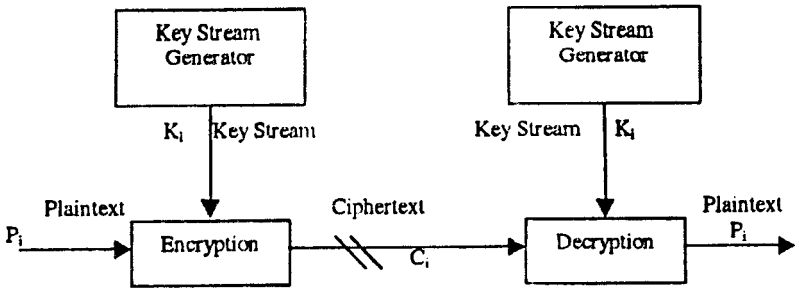
التفشير الإنسيابي هو نظام يتم فيه تغذية خوارزمية معينة بمفتاح سري لتوليد سلسلة غـير

منتهية من الأعداد الثنائية ، ويستخدم التشفير الإنسيابي لتحويل النص الصريح إلى نص مشفر وبالعكس ، أي أنه يحول النص المشفر إلى نص صريح على أن تتم عملية تحويل bit واحد في كل وقت ، وكما مبين في الشكل (7) الذي يوضح مخطط تنفيذي بسيط لعملية التشفير وفك الشفرة باستخدام أسلوب التشفير الإنسيابي ، ومتتابعة المفتاح المولدة (أو السلسلة المولدة) تمثل مخرجات عملية التشفير الإنسيابي من الـ bit: $K_1, K_2, K_3, \ldots K_I$ ، متتابعة المفتاح هذه تجمع بمعيار XOR مع الـ bits الخاصة بالنص الصريح: $P_1, P_2, P_3, \ldots P_I$ لتوليد الـbits التي تمثل النص المشفر وكما موضحة في المعادلة الآتية:

$$C_i = P_i \oplus K_i$$

وللحصول على النص الصريح يتم جمع كل bit من النص المشفر مع الـ bit الذي يقابله من متتابعة المفتاح المولدة وفق معيار XOR لينتج لنا النص الصريح وحسب المعادلة الآتية:

$$P_i = C_i \oplus K_i$$



الشكل(7) يمثل مخطط التشفير الانسيابي

وهنا يجب الانتباه إلى أن سرية النظام تعتمد بالكامل على متتابعة المفتاح المستخدمة في عملية التشفير ، فإذا كانت متتابعة المفتاح المولدة اللامنتهية أصفار فإن النص المشفر الناتج من عملية التشفير سيكون نفس النص الصريح وبالتالي فإن عملية التشفير برمتها تكون غير ذات

جدوى ، إضافة إلى ذلك إذا كانت دورة متتابعة المفتاح المولدة قصيرة كأن تكـــون 16 -bits مثلا ، فإن نظام الأمنية سيكون ضعيفا جدا حيث أن العملية ستكون مشابهة إلى عمليــــة XOR البسيطة ، وفي حالة إعطاء متتابعة المفتاح المولدة مخرجات عشوائية لا منتهية فإن النظام ســيماثل نظام المرة الواحدة (One Time Pad) حيث يعطي سرية تامة [1].

إن سرية التشفير الإنسيابي تقع بين عملية الــ XOR البسيطة ونظام المرة الواحدة (One time pad) ، وعلى أية حال فإن المخرجات المولدة من متتابعة المفتاح تكـــون نفســـها في أي وقت ، من هنا فإن من البديهي إمكانية كسر مخرجات نظام التشفير ، حيث تحت افــــتراض أن شخصا ما يمتلك النص المشفر إضافة إلى النص الصريح ، فإن هذا الشخص بإمكانه وباســـتخدام عملية الجمع للنص المشفر مع النص الصريح وفق معيار XOR استرجاع متتابعة المفتاح ، إضافة إلى ذلك يمكن استخدام خوارزميات معينة لذلك.[2].

نظرية التعقيد: Complexity Theory

تشترط نظرية التعقيد منهجية معينة لتحليل التعقيد الحسابي لتقنيات وخوارزميات أنظمـــة التشفير المختلفة ، وتقارن خوارزميات وتقنيات التشفير وتحدد الأمنية لها ، وتبين نظرية التعقيـــد فيما إذا كان بالاستطاعة كسر النظام ضمن مدة معقولة.

أي خوارزمية تعقيد Algorithm Complexity تحدد بالقوة الحسابية المطلوبة لتنفيذها ، والقوة الحسابية لأي خوارزمية غالبا ما تقاس بمتغيرين هما: T الذي يمثل تعقيـــد الوقـــت (أي الوقت اللازم لتنفيذ الخوارزمية) و S الذي يمثل تعقيد المجال Space (أو الذاكرة المطلوبـــة) ، وكل من T و S يعبر عنهما كدالتين مشتركتين لـــ n ، حيث n تمثل حجم المدخلات.

بشكل عام التعقيد الحسابي لأي خوارزمية يعبر عنه بالرمز O الذي يمثل درجــــة أهميـــة التعقيد الحسابي من حيث كبره ، وكمثال على ذلك إذا كان تعقيد الوقت للخوارزميه المعطـــاه هو $4n^2+7n+12$ ، فإن التعقيد الحسابي من الدرجة n^2 ويعبر عنه $O(n^2)$ [10].

قياس تعقيد الوقت هو نظام مستقل ، من هنا فليس بالضرورة معرفة الوقت المضبوط للعمليات المتنوعة ، أو عدد الـ bits المستخدمة لتمثيل المتغيرات المختلفة أو حتى سرعة المعالج processor ، فربما هناك كومبيوتر 50% أسرع من كومبيوتر آخر ولكن أهمية التعقيد لأي خوارزميه تبقى نفسها.

الخوارزميات تصنف طبقا إلى تعقيدا الوقت والمجال ، وأي خوارزمية تكون ثابتة إذا كان تعقيدها غير معتمد على n أي: $O(1)$ ، وأي خوارزمية تكون خطية إذا كان تعقيد الوقت هو $O(n)$ والخوارزميات يمكن بالطبع أن تكون تربيعية quadratic وتكعيبية cubic وهكذا ، وكل هذه الخوارزميات هي متعددات حدود Polynomial ولها التعقيد $O(n^m)$ ، حيث أن m ثابت ، والخوارزمية المصنفة طبقا إلى التعقيد الذي يتطلب وقتا يعبر عنه بمتعدد الحدود Polynomial time complexity تسمى Polynomial-time algorithim، كما أن الخوارزميات التي تمتلك التعقيدات $O(t^{f(n)})$ حيث أن t ثابت أكبر من 1 وأن f(n) تمثل دالة متعدد حدود لـ n تسمى هذه الخوارزميات بالخوارزميات الأسية exponential والخوارزميات الأسية التي لها مجموعات جزئية تمتلك تعقيدات معينة ولتكن $O(C^{f(n)})$ حيث أن c ثابت و f(n) أكبر من 1 وأقل من الخطي تسمى superpolynomial [10] ، وبشكل مثالي يمكن القول بأن الخوارزميات التي تحتاج إلى وقت تنفيذ يعبر عنه بدلالة دالة أسية هي خوارزميات غير كفء ، أما الخوارزميات التي تحتاج إلى وقت تنفيذ يعبر عنه بدلالة دالة متعددة حدود فهي خوارزميات كفء. [1]

التعقيد الخطي: Linear Complexity

يعرف التعقيد الخطي على أنه طول أقصر مسجل إزاحة ذو دالة تغذية مرتدية خطية يستخدم لتوليد سلسلة ثنائية تحاكي مخرجات المواد المطلوب حساب درجة تعقيده.

يعتبر التعقيد الخطي من المقاييس المهمة المستخدمة في تحليل وكسر مخرجات مسجلات

الإزاحة ذوات دوال التغذية المرتدية الخطية ، فإذا كان التعقيد الخطي لسلسلة معينة n فإن معرفة 2n مرتبة ثنائية متلاحقة من ممتابعة المفتاح المولدة تكون كافية لكسر النظام ، حيث عن طريقها يمكننا استنتاج بقية متتابعة المفتاح ، لذلك كلما كان التعقيد الخطي كبيرا كلما حصلنا على درجة سرية أكبر وذلك لأنه يتطلب معرفة جزء كبير من متتابعة المفتاح ، ولحساب التعقيد الخطي لسلسلة ثنائية يمكن استخدام خوارزمية Berlekamp-Massey.

مناعة الارتباط: Correlation immunity

قام مصممو أنظمة التشفير الإنسيابي محاولة لإعطاء درجة عالية للتعقيد الخطي بجمع مخرجات العديد من المتسلسلات في أسلوب لا خطي ، والخطر الذي ظهر نتيجة اتباع هذا الأسلوب تمثل في كون واحد أو أكثر من مخرجات مسجلات الإزاحة ذوات دوال التغذية المرتدة الخطية ترتبط بعلاقة مع متسلسلة المفتاح المولدة الناتجة من هذا الأسلوب اللاخطي ويمكن استخدام هجوم الأرتباط لكسر هذا النظام وقد أوضح Thomas Siegenthaler (9) أن مناعة الارتباط يمكن تعريفها بدقة حيث تمثل توزان بين مناعة الارتباط والتعقيد الخطي.

من هنا ظهرت الفكرة الأساسية التي وقفت خلف هجوم الارتباط والتي تكمن في تحديد بعض الارتباط بين جزء من مدخلات الدالة اللاخطية (مخرجات مسجلات الإزاحة الخطية) وبين مخرجات متتابعة المفتاح المولدة ، وبالاستناد على هذا الارتباط أصبح من الممكن معرفة بعض من مخرجات مسجلات الإزاحة الخطية والتي تعتبر جزء من مفتاح النظام باستخدام تقنية فرق تسد والتي سميت بهجوم الارتباط ، وهذا يعني التقليل من عدد المحاولات لإيجاد مفتاح النظام عند وجود ارتباط بين مدخلات ومخرجات الدالة اللاخطية التي استخدمت في تجميع مخرجات مسجلات الإزاحة الخطية ، إذ يمكننا معرفة كل مسجل إزاحة بشكل مستقل عن بقية المسجلات ، أي مبدأ فرق تسد ، أما إذا تم تجميع مخرجات مسجلات الإزاحة الخطية باستخدام دالة لا خطية وعندما لا يوجد أي ارتباط بين متتابعة المفتاح وبين أي مجموعة من مسجلات

الإزاحة الخطية ، يكون مولد متتابعة المفتاح الذي يمتلك هذه الصفة ذات أعظم درجة لمناعة الارتباط ولا يمكن مهاجمته باستخدام هجوم الارتباط.

مفهوم العشوائية: The Concepts of kandomness

المشكلة المهمة والرئيسية في هذا الموضوع هي كيفية تحديد معنى العشوائية ، وهنا يجب الانتباه لأنه لا يمكن أن تعرف العشوائية ما لم تقدم مصطلحات أكثر ويعرف المفهوم الإحصائي لدالة الارتباط الذاتي ، فإذا كانت S تمثل أي سلسلة ، فإن الجريان run هو عبارة عن سلسلة من العناصر المتماثلة المتتالية التي لا تسبق ولا تتبع بنفس الرمز ، وكمثال على ذلك 0111001 التي بدأت بجريان مكون من 0 واحد ، وتحتوي أيضا على جريان مكون من ثلاثة من 1 وجريان مكون من أثنين من 0 وفي النهاية يود جريان مكون من 1 فقط ، والجريان المكون من 0 يسمى فجوة gap ، بينما الجريان المكون من أ يسمى كتلة block [3].

لتكن S_t سلسلة ثنائية ذات دورة P ، يكون $S_m+P=S_m$ لأي قيمة للعدد m ، ولأي عدد ثابت t ، فبالإمكان مقارنة العناصر الأولى من السلسلة S والتي عددها P مع S_t ، أي السلسلة بعد تزحيفها لليسار t مرتبة ثنائية ، فإذا كان A يمثل عدد المواقع التي تكون فيها السلسلتين متشابهتين ، و D (D=p-A) تمثل عدد المواقع التي تكون فيها السلسلتين غير متشابهة ، فإن دالة الارتباط الذاتي C(t) Autocorrelation function هي:

$$C(t)=(A-D)/p$$

ومن الواضح أن $C(t)=C(t+p)$ لكل قيم t ، لذلك فإن قيمة يجب أن تحقق الشرط $0 < t < p$ وعندما $t=0$ يكون هناك ارتباط ذاتي داخل الطور in phase autocorrelation ، حيث في هذه الحالة يكون $A=p$ و $D=0$ لذلك $C(0)=1$ لكن عندما تكون $t\neq0$ يكون هناك ارتباط ذاتي خارج الطور Out of phase autocorrelation.

وتتصف السلسلة شبه العشوائية الدورية بطول دورة P بما يأتي:

1- إذا كانت P عدد زوجي فإن عدد ما موجود في السلسلة من الواحد يساوي عدد الأصفار ، وإذا كان عدد فردي فإن عدد ما موجود في السلسلة من الواحد أكثر أو أقل بمقدار واحد عن عدد الأصفار.

2- حيث أن الجريان run يمكن تعريفه على أنه سلسلة من العناصر المتلاحقة المتشابهة فإن نصف الجريانات بطول 1 وربعها بطول 2 ، وبشكل عام $1/2^i$ من الجريانات بطول i.

3- دالة الارتباط الذاتي خارج الطور ثابتة.

الصفات أعلاه ليست دائمة التحقق ، ولكن عندما تقترب السلسلة بعد اختبارها من هذه الصفات فإن ذلك مؤشر على اقترابها من العشوائية المثلى وعامل الخطأ أو مستوى المعنوية يستفاد منه لتقدير درجة الاقتراب من العشوائية.

الاختبارات الإحصائية للعشوائية: Statistical Tests of randomness

هناك العديد من الاختبارات الاحصائية لفحص مدى عشوائية السلسلة الثنائية والتي تسمى اختبارات العشوائية المحلية Local randomness tests ، لكونها تختبر مقطعا واحدا (دورة واحدة) من السلسلة الثنائية ، وفي البداية يجب تحديد درجة النجاح والفشل للإختبارات ، لذلك تم استخدام قيم احصائية مخصصة لسلاسل العشوائية واعتبرت درجة النجاح على أنها 95% والتي تكون مساوية إلى $(100-\alpha)\%=(100-5)\%$ حيث α تسمى المستوى المميز للأختبار ، ويكون الاختبار ناجحا عندما تكون قيمته أقل أو مساوية إلى قيمة X^2 حيث أن X^2 تمثل القيمة الجدولية عند المستوى المميز α % لتوزيع مربع كاي(*) ، والاختبارات الإحصائية مبينة في المباحث الآتية(**):

أولا: اختبار التردد: frequenency test

في السلسلة الثنائية العشوائية نتوقع أن يكون نصف عناصرها الثنائية واحد والنصف الأخر يكون صفر ، لذلك يعتمد هذا الاختبار على عدد الأصفار n_0 وعدد ما موجود من الواحد n_1 في السلسلة المولدة بطول n والمراد اختبارها ، والمعادلة المستخدمة في هذا الاختبار هي:

$$.x^2 = \frac{(n_0 - n_1)^2}{n}$$

يكون الأختبار ناجحا إذا كان $x^2 \le 3.84$ وذلك لأنه لدرجة حرية واحدة يكون $x^2{}_{0,05} = 3.84$ والتي يمكن إيجادها من جدول كآي.

ثانيا: اختبار التسلسل Serial test

يعتمد هذا الاختبار على تردد المقاطع الثنائية (11 , 00 , 10 , 01) في السلسلة بطول n، ويعطي دلائل فيما إذا كانت المراتب الثنائية في السلسلة لا تعتمد على سابقتها ، إذا كانت n00 تمثل تردد المقطع 00 ، وأن n01 تمثل تردد المقطع 01 و n11 تمثل تردد المقطع 11 ، فإن المعادلة المستخدمة في هذا الاختبار هي:

$$.x^2 = \frac{4}{n-1}\sum_{i=0}^{1}\sum_{j=0}^{1}(n_{ij})^2 - \frac{2}{n}\sum_{i=0}^{1}(n_i)^2 + 1$$

ويكون الاختبار ناجحا إذا كان $x^2 \le 5.99$ ، وذلك لأنه لدرجتي حرية يكون $x^2{}_{0.05} = 5.99$ ، ويمكن اعتماد درجة حرية 3 وبالتالي تتم المقارنة على ضوء قيمة $x^2{}_{0.05}$ التي تساوي 7.81.

ثالثا: اختبار بوكر: Poker Test

إن مبدأ هذا الأختبار هو تقسيم السلسلة الثنائية ذات الطول n والمراد اختبارها إلى F

من الكتل طول كل منها m ، ومن ثم دراسة هذه الكتل ، فإذا كانت $F=(n/m)$ فإن المعادلة المستخدمة في هذا الإختبار هي:

$$.x^2 = \frac{2^m}{F} \sum_{i=0}^{m} \frac{(x_i)^2}{\binom{m}{i}} - F$$

حيث أن x_i يمثل عدد الكتل المحتوية على i من الوحدات و m-i من الأصفار ، وأن $\binom{m}{i}$ تمثل معاملات binomial ، ويكون هذا الاختبار ناجحا عند المستوى المميز α % إذا كانت قيمة الاختبار أقل أو مساوية إلى القيمة الجدولية لتوزيع مربع كاي ولدرجة الحرية $.2^m-1$

رابعا: اختبار الجريان: Run Test

يعتمد هذا الاختبار على حساب ترددات الكتل ضمن السلسلة الثنائية بطول n ، فإذا كانت r_{0I} يمثل عدد الفجوات بطول i و r_{1i} عدد الكتل بطول i وكانت r_0 و r_1 تمثل عدد الفجوات والكتل بالتعاقب ، يكون:

$$.r_0 = \sum_{j=1}^{n} r_{0j} \qquad r_1 = \sum_{j=1}^{n} r_{1j}$$

كذلك

$n_{01}= r_0-1$ or r_0

$n_{10}= r_1-1$ or r_1

$n_{00}= n_0-r_0$ $n_{11} = n_1 - r_1$

أما المعادلة المستخدمة في هذا الاختبار فهي:

$$.t_0 = \left[\sum_{j=1}^{r_0} (r_{0_j} - \frac{n}{2^{2+i}})^2 \, 2^{2+i} \right] \Big/ n$$

$$t_1 = \left[\sum_{j=1}^{r_1} (r_{1_j} - \frac{n}{2^{2+i}})^2 \, 2^{2+i} \right] \Big/ n$$

وعدد درجات الحرية المستخدمة مع t_0 و t_1 مساوي إلى قيمة طول أطول فجوة وطول أطول كتلة بالتعاقب.

ولا يمكن تطبيق هذا الاختبار إلا بعد إجتياز السلسلة اختبار التسلسل وبهذا نعرف أن عدد كل من الفجوات والكتل لم يتجاوز الحد المقبول ، فعند اجتياز السلسلة الثنائية هذا الاختبار يكون نصف عدد الفجوات (الكتل) بطول 1 ، وربعها بطول 2.

خامسا: اختبار التطابق الذاتي: Autocrrelation Test

لو كانت السلسلة المراد اختبارها هي $a_1\, a_2 \ldots.. a_n$ يكون:

$$A(d) = \sum_{i=1}^{n-d} a_i \cdot a_{i+d} \qquad ,0 \le d \le n-1$$

$$A(0) = \sum_{i=1}^{n} a_i = n_i$$

فإذا كانت السلسلة تحتوي على n_0 من الأصفار و n_1 من الوحدات ، فإن الكمية المتوقعة لـ $A(d)$ حيث $d \neq 0$ هي:

$$\mu = \frac{n_1^2 (n-d)}{n^2}$$

ويكون الاختبار ناجحا إذا كانت $x^2 \le 3.841$ لكل قيم d ، حيث أن x^2 يمكن حسابه كما يأتي:

$$x^2 = \frac{(A(d)-\mu)^2}{\mu}$$

تصميم وتنفيذ خوارزمية تشفير إنسيابي جديد:

Design and Implementation new algorithm stream cipher

أولا: مقدمة:

المشكلة الأساسية التي تظهر عند تصميم مولد التشفير الانسيابي أنه في سياق الآلية ذات الحالة المحددة يجب أن يؤخذ بنظر الاعتبار عند إيجاد الحالة التالية للدالة ومن ثم المخرجات إن يعطي المصمم ضمانة بتحقيق المتطلبات الأساسية للتشفير من حيث طول الدورة وزيادة التعقيد الخطي والمناعة العالية للأرتباط وأن يضمن خصائص التوزيع المنتظم ، والتصميم وفق معايير الأداء الأساسية هذه بالطبع ستقود إلى عدم إمكانية تحليل مثل هذا المولد ، كما أن بناء نظام التشفير الإنسيابي ذا الأمنية الضرورية مرتبط بشكل كبير باستخدام التحويلات اللاخطية والتي تزيد من التعقيد لعملية التحليل ، وعندما تستخدم الآليات الخطية داخل خارطة التصميم اللاخطية للنظام لتوليد متتابعة المفتاح ، فإن مثل هذا التصميم يعتبر جيدا وكفئ ضد أي هجوم يمكن أن يحدث ، وفي هذا السياق فإن من الملائم تقسيم المولد إلى جزأين الأول يسمى الجزء الخطي Linear part والثاني يسمى جزء التوحيد اللاخطي Nonlinear combining part ، الجزء الأول يتحكم بحالة السلسلة الخارجة من المولد واستجابتها لشروط السلاسل من حيث كبر طول الدورات والخصائص الإحصائية الجيدة ، وكمثال على ذلك فإن الجزء الخطي هذا يمكن أن يحتوي على مجموعة من مسجلات الإزاحة ذوات دوال التغذية المرتدة الخطية التي تعطي أكبر دورة ، وبشكل مغاير فإن الجزء الثاني من المولد أي جزء التوحيد اللاخطي مختص بزيادة معنوية التعقيد الخطي لمتتابعة المفتاح المولدة للحفاظ عليها ضد أي هجوم خطي ومن غير أن تهدم خصائص التوزيع الجيدة التي زودت بها من الجزء الخطي.

ثانيا: أهداف التصميم: The design Objective

أقترح Madryga (*) عدة أهداف لخوارزميته لضمان الأمنية التامة وبعض من هذه الأهداف المقترحة اعتمدت في التصميم المقترح في هذا البحث لملاءمتها لهذا التصميم ، ومعظم هذه المقترحات هي:

1- النص الصريح لا يمكن الحصول عليه من النص المشفر بدون استخدام المفتاح.

2- عدد العمليات المطلوبة لتحديد المفتاح من جزء أو عينة من النص الصريح أو النص المشفر يساوي حاصل ضرب مجموع العمليات المطلوبة لفك شفرة معينة مع عدد الاحتمالات الممكنة للحصول على مفتاح التشفير.

3- معرفة الخوارزمية لا يؤثر على قوة نظام التشفير (كل الأمنية يجب أن تبقى في مفتاح).

4- تغيير bit واحد في المفتاح يؤدي إلى تغيير جوهري في النص المشفر المقابل لنفس النص الصريح.

5- المجموعة المتكررة من الـ bit في النص الصريح يجب أن تحجب كليا في النص المشفر.

6- طول النص المشفر يجب أن يكون مساوي إلى طول النص الصريح.

7- يجب ألا توجد أي علاقة بين أي من المفاتيح المحتملة والنص المشفر.

8- أي مفتاح يجب أن يعطي تشفيرا قويا (أي لا يوجد مفتاح ضعيف)

9- طول المفتاح والنص يجب أن يكون قابلاً للتعديل لكي يقابل التغير في متطلبات الأمنية.

10- يجب أن تكون للخوارزمية القدرة على العمل بكفاءة في البرمجيات (في الحاسبات الكبيرة والحاسبات الصغيرة والحاسبات المايكروية) ، وفي الدوائر المتقطعة discrete logic.

ثالثا: وصف الخوارزمية: Description of the Algorithm

الخوارزمية المصممة هنا تتألف من جزئين كما موضحة في الشكل (8).:

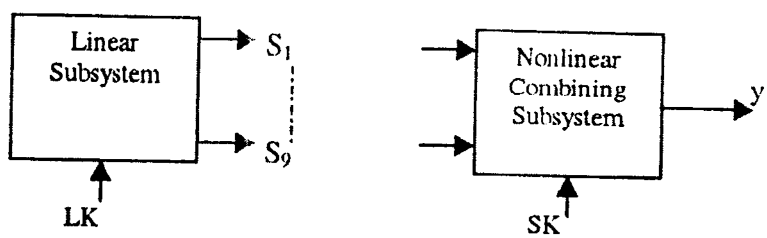
1- النظام الخطي الجزئي. Linear subsystem

2- نظام التوحيد اللاخطي الجزئي Nonlinear combining subsystem

يتألف النظام الخطي الجزئي من ثلاثة مجموعات مكونة من مسجلات إزاحة هي:

- مجموعة الاختيار (choosing group CG): وتتألف من خمسة مسجلات إزاحة.
- مجموعة التدوير (Rotation group RG): وتتألف من ثلاث مسجلات إزاحة.
- مسجل التوجيه (Directive register DR): ويتكون من مسجل إزاحة واحد.

مسجلات الإزاحة للمجموعات الثلاثة السابقة الذكر تكون ذات أطوال أولية مع بعضها البعض ، ودالة التغذية المرتدة لكل مسجل إزاحة تكون خطية وتعطي سلسلة بأعظم طول دورة ، والجدول (1) يوضح ذلك.

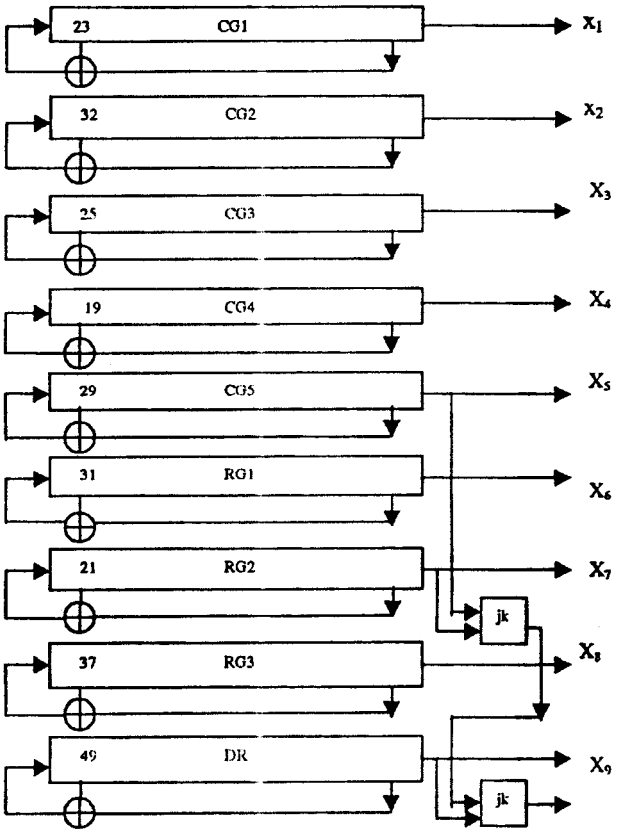


شكل(8) يمثل مخطط مولد التشفير الانسيابي المقترح

تملئ مسجلات الإزاحة هذه بسلسلة من الأرقام الثنائية bits المأخوذة من المفتاح السري (LK) الذي سيناقش لاحقا.

No.	Length	Tabbing stages
CG1	23	23,5
CG2	32	32,7,6,2
CG3	25	25,3
CG4	19	19,5,2,1
CG5	29	29,2
RG1	31	31,3
RG2	21	21,2
RG3	37	37,6,4,1
DR	49	49,25

جدول(1) يصف أطوال المسجلات وتحديد مواقع الربط للتغذية المرتدة



شكل(9) يمثل مخطط الجزء الخطي للمولد المقترح

لتصميم نظام التوحيد اللاخطي الجزئي (F) أخذت بنظر الاعتبار المتطلبات الآتية:

1- F تنقل الخصائص الإحصائية لدورات متسلسلات الجزء الخطي إلى متتابعة المفتاح المولدة ، معنى ذلك عندما تكون السلسلة الداخلة ذات خصائص جيدة فإن ذلك سينعكس إيجابيا على السلسلة الخارجة.

2- F تعظم دورة متتابعة المفتاح المولدة المتصلة بدورات المتسلسلات الخارجة من الجزء الخطي.

3- F تعظم التعقيد الخطي لمتتابعة المفتاح المتصلة بالتعقيدات الخطية للمتسلسلات الخارجة من الجزء الخطي.

4- لا تسمح F بأي تسرب ، فذلك يعني أن أي هجوم مباشر على الانظمة الفرعية للجزء الخطي من المفتاح الانسيابي المولد يجب أن يفشل.

5- تكون F سهلة وسريعة التنفيذ.

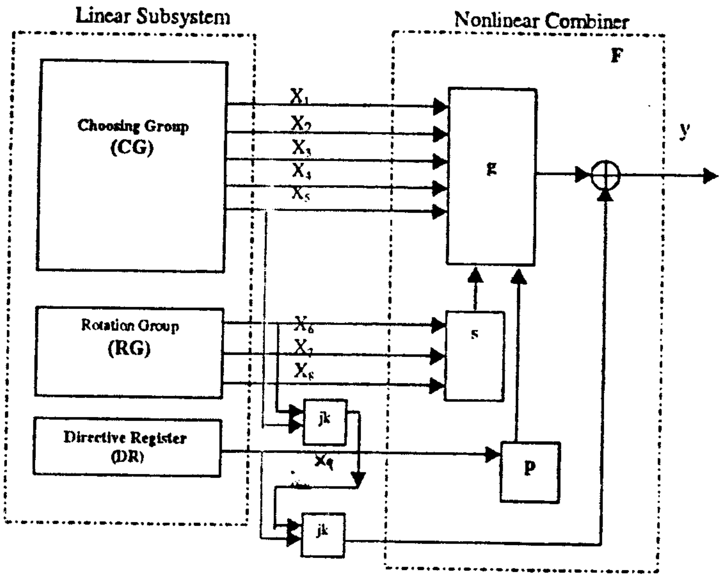
في مولد التشفير الانسيابي المقترح جزء التوحيد اللاخطي F أفترض كدالة Boolean من نوع: $F:B^9 \rightarrow B$

والذي يوضح بالصيغة الآتية:

$$y_I=(g_i(x_{1j}, x_{2j}, x_{3j}, x_{4j}, x_{5j}, S_j(x_{6j}, x_{7j}, x_{8j}), P_j(x_{9j}), JK\ x_{sj}\ JK\ x_{7j}\ JK\ x_{9j})$$

حيث أن Jk يمثل نطاط flip-flop من نوع jk وأن Y_I تمثل مخرجات الدالة عند الزمن j و gi تمثل دالة توحيد لأي 5-bit ، وتعمل كحاوية container لـ 32-bit التي تمثل الحالة الابتدائية للمفتاح السري (SK) ، ومدخلات الدالة هي ثلاثة مجموعات ، الأولى $(x_{1j}, x_{2j}, x_{3j}, x_{4j}, x_{5j})$ تعتبر كعنوان لموقع معين (cell) في الحاوية ، والمجموعة الثانية $(x_{6j}$ $x_{7j}, x_{8j})$ والتي رمز لها s تعمل مخرجاتها على تحديد مقدار التدوير ، والمجموعة الأخيرة التي يرمز

لها P ، تتكون من الـــ bit x_{91} فقط حيث تحدد مخرجاتها اتجاه التدوير ، وأهمية الدالتين s و P تكمن في زيادة مناعة الارتباط.



شكل(10) خوارزمية مولد التشفير الانسيابي الجديد

رابعا: هيكلة المفتاح Key Structure

تضمن المولد المقترح مفتاحين سريين هما:

- مفتاح الجلسة Session Key: تولد هنا bits-32 عشوائيا (من قبل المستخدم) وبنفس النسبة للظهور بالنسبة للـــ 0 أو 1 ، أي باحتمال 0.5 لكل منهما ، وهذا المفتاح يمكـــن أن يستخدم لتشفير مجموعة من الرسائل ، وعدد هذه الرسائل يعتمد على طبيعتها ، ولذلـــك يمكن تغييرها دوريا.

- المفتاح الخطي Linear Key: و يتكون مـــن 266 bits (38 ASCII character) تستخدم كحالة أولية لمحتويات مسجلات الإزاحة ذوات التغذية المرتدة الخطية المتضمنـــة في

الجزء الخطي من المولد ، وهذا المفتاح يجب أن يغير مع كل رسالة.

خامسا: التهيئة الأولية للمولد والتشغيل:

Initiglization for generaton and Operation

العملية الأولى لخوارزمية المولد تبدأ بتحويل المفتاح الخطي (38 characters) Linear Key من الـ ASCII إلى الثنائي binary ومنه نحصل على 266-bits كنتيجة لهذا الاتحويل ، وهذه الـ bits تستخدم لتغذية الحالة الأولية للمسجلات CG1 إلى CG5 ومن ثم RG1 إلى RG3 و أخيرا DR على التوالي.

عملية توليد متتابعة المفتاح تبدأ بإيجاد 5-bits من الـ CG كعنوان لمفتاح الجلسة Session Key والذي يبقى في الحاوية g ، ثم أن محتويات الحاوية g تدور قبل إيجاد القيمة أو الـ bit المحدد ، وعملية التدوير تعتمد على مخرجات الدالة S والتي تحدد كم موقع يمكن أن تدور ، أما مخرجات الدالة P فتحدد اتجاه التدوير (0 تدوير نحو الأعلى و 1 تدوير نحو الأسفل) ، ويستخدم الـ bit الخارج من CG5 مع الـ bit الخارج من RG2 كمدخلات إلى نطاط flip-flop أخر من نوع JK ومخرجات هذا النطاط تكون كمدخلات مع الـ bit الخارج من DR إلى نطاط flip- flop آخر من نوع jk أيضا ، وأخيرا فإنه يتم إيجاد الـ bit الخارج من المولد بالجمع بمعيار 2(XOR) لمخرجات الحاوية g ومخرجات النطاطات للمسجلات DR و RG2 و CGR وهذه العملية تكرر لتوليد متتابعة المفتاح وحسب طول النص الصريح أو النص المشفر.

سادسا: التقدير والاختبار: Evaluation and Test

تم في هذا المبحث اختبار التصميم المقترح ولحظ فيما إذا كان ملائما لتوليد سلاسل تشفير انسيابي واعتمدت لهذا الغرض ثلاثة مقاييس لتحديد فيما إذا كانت المتسلسلات الخارجة جيدة أم لا ، وهذه المقاييس هي التعقيد الخطي ومناعة الارتباط والاختبارات الاحصائية.

أختيرت معمارية هذه الخوارزمية لكي يماثل فيها حجم تعقيدها الخطي LC حجم التعقيد الخطي لأي نظام أخر محصن ضد هجمات الارتباط ، ذلك يعني:

$$LC \approx 2^{302}$$

وهذه القيمة اشتقت من الحقيقة التي تقول أن التعقيد الخطي LC_i لأي مولد جزئي يمكن أن يعطي بالصيغة الآتية:

$$LC = \prod (LC_i)$$

ومنه يمكن ملاحظة:

$$LC = \prod_{k=1}^{9} (2^{L_k} - 1) \approx 2^{266}$$

وذلك لأن الاختيار لمسجلات الإزاحة ذوات التغذية المرتدة الخطية كانت ذات أطوال أولية فيما بينها ، مما نتج عنه الحصول على أعظم طول دورة ممكنة ، وفي الجانب الأخر فإن التعقيد للجزء اللاخطي يتكون من ثلاثة دوال هي p, s, g والتي نستطيع حسابها كالآتي:

$$LC_2 = \prod_{k=1}^{3} 2^{L_k} = 2^{36}$$

لذلك يكون التعقيد الخطي لكل المولد LC

$$LC=(LC_1)(LC_2) \approx 2^{302}$$

وكلما كبير حجم التعقيد الحسابي سيكون من غير الممكن الهجوم على مثل هذا المولد حيث تحت افتراض أن الكمبيوترات العملاقة supercomputer تنجز 10^{10} عملية في كل ثانية فإن $2^{266} = 1.186 \times 10^{80}$ عملية تحتاج إلى 3.760×10^{62} سنة لتحليلها.

وحقيقة أن السبب الأساسي لتضمين جزء التوحيد اللاخطي في المولد لاعطاء المولد مناعة عالية ضد الارتباط ، هذا يعني أن الخوارزمية المستخدمة هنا تمتلك أمنية كافية ضد هجوم الارتباط ، ويتضح ذلك جليا بوجود تسع متسلسلات تبتدأ من X_1 وتنتهي بـ X_9 للمولدات

الخطية الجزئية التي تكون مستقلة وغير متطابقة إحصائيا (i.i.d) مع مخرجات المولـــد المقـترح كما أنها مستقلة بعضها عن بعض أيضا ، كل ذلك قاد إلى القول بأن الولد المقترح من الدرجة 9th لمناعة الارتباط ، والجدول (2) يمثل هذه الحقيقة بوضوح ، والذي يتضمن قيم الارتباطـات لكل مسجل مع متابعة المفتاح المولدة ، فيما يبين الجدول (3) قيم الارتباطات للمسجلات فيمـا بينها ، وقد تم حساب هذه الارتباطات باستخدام المفتاح LKs (مع الأخذ بنظر الاعتبـــار أن المفتاح الجلسة SK نفسه) ، وقد تم توليد 1000000-bits كمخرجات من المولد لكل مفتـاح وأخضعت لحساب مناعة الارتباط ، وكانت المفاتيح المستخدمة كالآتي:

SK : (01001100011100011110000011111101)
LK1: (ABCDEFGHIJKMNOPQRSTUVWXYZABCDEFGHIJKL)
LK2: (AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA)
LK3: (KKLLMMNNOOPPQQRRSSTTUUVVWWXXYYZZYYAABBCC)

ومن الواضح أن المفاتيح المستخدمة أخذت كمفاتيح ضعيفة ، وكـــانت نتـــائج مناعـــة الارتباط جيدة مما يدل على أن المولد المقترح يحقق المواصفات الجيدة لتصيمم المولدات.

No.	Correlation by using LK1	Correlation by using LK2	Correlation by using LK3
CG1	0.494	0.491	0.493
CG2	0.490	0.492	0.492
CG3	0.495	0.493	0.492
CG4	0.517	0.49	0.474
CG5	0.492	0.49	0.491
RG1	0.490	0.492	0.490
RG2	0.494	0.491	0.493
RG3	0.492	0.493	0.492
DR	0.492	0.493	0.492

جدول(2) يوضح الارتباط بين المولدات الخطية الجزئية ومتابعة المفتاح المولدة

LK1	CG2	CG3	CG4	CG5	RG1	RG2	RG3	DR
CG1	0.504	0.500	0.499	0.498	0.498	0.500	0.501	0.502
CG2		0.501	0.500	0.502	0.502	0.549	0.496	0.498
CG3			0.500	0.480	0.499	0.513	0.453	0.520
CG4				0.500	0.498	0.500	0.500	0.500
CG5					0.501	0.533	0.455	0.460
RG1						0.499	0.500	0.499
RG2							0.520	0.467
RG3								0.530

جدول(3) يوضح الارتباطات بين كل مسجلي إزاحة مع بعضهما باستخدام المفتاح LK1

LK2	CG2	CG3	CG4	CG5	RG1	RG2	RG3	DR
CG1	0.501	0.501	0.501	0.499	0.498	0.502	0.501	0.499
CG2		0.500	0.499	0.497	0.500	0.501	0.498	0.501
CG3			0.540	0.520	0.499	0.493	0.455	0.465
CG4				0.540	0.500	0.533	0.520	0.479
CG5					0.501	0.499	0.520	0.499
RG1						0.498	0.501	0.500
RG2							0.493	0.467
RG3								0.457

جدول(4) يوضح الارتباطات بين كل مسجلي إزاحة مع بعضهما باستخدام المفتاح LK2

تحققت مناعة الارتباط هذه بواسطة الدالتين P, S لأن التأثير على محتويات الدالة g يختلف من وقت لآخر (ذلك يعني أن محتويات الموقع المعين عند الزمن t يختلف عن محتوياته عند الزمن t+1) وباستخدام نفس المفاتيح (SK, LKs) وباستبعاد تأثير الدالتين p , s وجد أن الارتباط يبدو واضحا وكما مبين في الجدول (5).

سابعا: الاختبارات الإحصائية: Statistical Tests

ظهر أن التصميم المقترح يمتلك خصائص إحصائية جيدة ، ويتضح ذلك جليا من خلال النتائج الجيدة للأختبارات الإحصائية الخمسة التي استخدمت في هذا البحث وكما موضحة في الجدول (6).

No.	Correlation by using LK1	Correlation by using LK2	Correlation by using LK3
CG1	0.502	0.520	0.506
CG2	0.508	0.518	0.498
CG3	0.515	0.638	0.440
CG4	0.580	0.416	0.525
CG5	0.627	0.450	0.474
RG1	0.492	0.491	0.491
RG2	0.467	0.497	0.531
RG3	0.305	0.266	0.489
DR	0.356	0.567	0.538

جدول(5) يوضح الارتباط بعد استبعاد تأثير الدالتين s و p

Test		LK1	LK2	LK3	Pass value
Frequency test		1.01	1.205	0.840	Must be ≤3.84
Run test	T0	3.249	9.125	6.645	Must be≤12.309
	T1	3.917	5.765	9.889	
Poker test		4.320	4.800	10.040	Must be ≤11.1
Serial test		2.646	2.960	6.160	Must be ≤7.81
Auto- correlation test	Shift 1	2.273	0.253	0.485	Must be ≤3.84
	Shift 2	0.363	2.00	0.362	
	Shift 3	0.505	1.742	3.722	
	Shift 4	0.167	0.167	1.500	
	Shift 5	1.274	0.011	2.368	
	Shift 6	1.532	0.043	2.723	
	Shift 7	0.011	1.301	0.011	
	Shift 8	0.174	2.130	0.391	
	Shift 9	0.275	0.840	1.857	
	Shift 10	0.178	0.378	2.178	

جدول(6) نتائج الاختبارات الإحصائية للمولد المقترح

المقارنة مع بعض الأنظمة المعروفة:

Comparison with some Known systems

لمقارنة مولد التشفير الإنسيابي المقترح في هذا البحث مع المولدات المعروفة ، فقد تم تطبيق نفس المفتاح المستخدم في المولد المقترح مع مولد جيف Geffe generator [2] ، ومولد بلس

Pless generator [3].

وتحت افتراض أن مولد جيف متكون من نفس المسجلات الثلاثة الأولى للمولد المقترح ، وأن مولد بلس متكون من المسجلات الثمانية الأولى من المولد المقترح ، ومخرجات هذين المولدين اختبرت اعتمادا على التعقيد الخطي ومناعة الارتباط والاختبارات الاحصائية:

التعقيد الخطي لهذين المولدين يمكن حسابها كما يأتي:

$$LC = \Sigma LC_i$$

حيث أن i يمثل عدد الأنظمة الجزئية المعتمدة ، ومن الصيغة أعلاه نستطيع حساب التعقيد الخطي للمولد وكما يأتي:

$$LC_{Geffe} = 2^{23} + 2^{32} + 2^{25} = 1.0009\ 2^{32}$$

وبنفس الطريقة نجد التعقيد الخطي لمولد بلس حيث ظهر أنه:

$$LC_{Pless} = 1.051\ 2^{37}$$

والجداول (7) و (8) و (9) و (10) أثبتت أن المخرجات كانت ذات سلوك إحصائي جيد بالنسبة إلى مولد جيف وعلى العكس بالنسبة لمولد بلس ، ولكن مناعة الارتباط كانت ضعيفة لكلا المولدين مقارنة مع النتائج التي أظهرها المولد المقترح.

No.	Correlation by using LK1	Correlation by using LK2	Correlation by using LK3
LFSR1	0.499	0.496	0.501
LFSR2	0.750	0.749	0.751
LFSR3	0.750	0.751	0.750

جدول(7) يوضح الارتباطات لمولد جيف

No.	Correlation by using LK1	Correlation by using LK2	Correlation by using Lk3
LFSR1	0.591	0.592	0.592
LFSR2	0.407	0.407	0.409
LFSR3	0.595	0.592	0.593
LFSR4	0.408	0.408	0.410
LFSR5	0.589	0.593	0.592
LFSR6	0.408	0.408	0.408
LFSR7	0.594	0.589	0.589
LFSR8	0.408	0.409	0.410

جدول(8) يوضح الارتباطات لمولد بلس

Test		LK1	LK2	LK3	Pass value
Frequency test		0.006	0.117	0.973	Must be ≤3.84
Run test	T0	10.100	21.139	12.303	Must be≤22.078
	T1	21.471	18.462	10.977	
Poker test		4.292	4.434	6.973	Must be ≤11.1
Serial test		0.569	6.905	1.946	Must be ≤7.81
Auto- correlation test	Shift 1	0.001	2.426	0.702	Must be ≤3.84
	Shift 2	1.971	0.002	0.376	
	Shift 3	3.036	0.110	0.045	
	Shift 4	1.011	0.112	1.459	
	Shift 5	1.000	0.313	1.482	
	Shift 6	1.058	0.317	1.490	
	Shift 7	0.026	0.718	0.713	
	Shift 8	2.190	1.089	2.080	
	Shift 9	3.685	0.069	1.031	
	Shift 10	1.714	0.511	2.936	

جدول(9) نتائج الاختبارات الإحصائية لمولد جيف

Test		LK1	LK2	LK3	Pass value
Frequency test		0.225	1.901	0.92	Must be ≤3.84
Run test	T0	89.669	95.235	92.707	Must be≤22.078
	T1	70.041	47.503	60.562	
Poker test		10.529	10.720	6.725	Must be ≤11.1
Serial test		6.999	4.516	0.277	Must be ≤7.81
Auto- correlation test	Shift 1	2.070	0.929	0.188	Must be ≤3.84
	Shift 2	0.493	0.001	0.829	
	Shift 3	0.357	0.640	2.532	
	Shift 4	4.111	4.711	4.379	
	Shift 5	0.172	0.629	0.028	
	Shift 6	0.169	0.597	0.029	
	Shift 7	0.313	0.137	0.052	
	Shift 8	1.989	5.823	0.023	
	Shift 9	2.657	1.998	1.135	
	Shift 10	0.400	0.548	0.144	

جدول(10) نتائج الاختبارات الإحصائية لمولد بلس

الاستنتاجات:

تم الحصول خلال العمل في هذا البحث على بعض الاستنتاجات التي يمكن إجمالها في النقاط الآتية:

1- حيث أن دوال التوحيد اللاخطية تحافظ على التعقيد الخطي ومناعة الارتباط والخصائص الإحصائية ، إلا أنها في بعض الأحيان تفشل في المحافظة عليها ، وكما يبدو ذلك واضحا في مخرجات مولد جيف وبلس حيث فشلت في بعض هذه الاختبارات.

2- المولد المقترح أخذ بنظر الاعتبار مجموعة مخرجات مسجلات إزاحة ذات التغذية المرتدة الخطية كعنوان إلى موقع معين ، كما استخدم مخرجات مسجلات أخرى للتدوير سواء للأعلى أو للأسفل ، مما أعطى مولد كفء ، حيث أن المخرجات حافظت على التعقيد الخطي ومناعة الارتباط والخصائص الاحصائية الجيدة.

3- استبعاد عمليتي التدوير والتوجيه في جزء التوحيد اللاخطي قاد إلى زيادة الارتباط بين مخرجات المولد ومخرجات مولدات الإزاحة ذوات دوال التغذية المرتدة الخطية ، وذلك يدل على أهمية هذين الجزئيين للحفاظ على مناعة الارتباط.

4- الاستقلالية بين مخرجات مولدات الإزاحة ذات التغذية المرتدة الخطية مع بعضها قاد إلى الحصول على تعقيد عالي جدا (حيث أن التعقيد ينتج من حاصل ضرب طول دورات المسجلات مع بعضها).

المصادر: References

المصادر العربية:

(1) الحمداني ، وسيم عبد الأمير عواد ، وسن شاكر ، **أنظمة التشفير الإنسيابي ، بغداد 1997.**

(2) عبد السلام ، أياد عبد القهار ، **"تحليل كمي وتصميم جديد لمولـــد تشـــفير إنسيابي"** ، رسالة ماجستير في علوم الحاسبات ، كلية العلوم ، جامعة بغداد ، 1999.

المصادر الأجنبية:

(3) Berker th and Fipiper, "Cipher system the protection of commu Northwood books" (1982).

(4) Diffiew. And M.E. Hellman, "Privacy and Authentication An introduction to cryptography" Proc. IEEE, vol. 67, pp. 379-427, March (1989).

(5) Henkel W., "Another description of the Berlkamp-Massy algorithm" IEEE Proceedings, vol. 136, June (1992).

(6) Meyer, Carl th, "Cryptographyanew dimension in computer data security". John Wiley & Sons Inc (1982).

(7) Chneier, Bruce, "Applied Cryptography, second edition protocols, algorithms and source code in C" John wiley & Sons Inc. (1996).

(8) Shannon, C. E. "communication theory of security systems", Advanced technology seminars Obere Waidstrasse 17 Zurich, Switzerland (1987)

(9) Siegen thaler, Correlation Immunity of Nonlinear Combining Function for Cryptographic Applications. Advanced technology seminas, Obas, waidstrasse 17 zurich, switzerland (1987).

(10) Weggerer I, "The complexity of Boolean function", B. G. Teubner, Stuttgart, and John Wiley & Sons, Inc. (1987).