العنوان: تصميم خوارزمية تشفير كتلية جديدة عالية السرية
المصدر: المجلة العراقية لتكنولوجيا المعلومات
الناشر: الجمعية العراقية لتكنولوجيا المعلومات
المؤلف الرئيسي: نجار، يحيي
مؤلفين آخرين: شعار، محمود(م. مشارك)
المجلد/العدد: مج6, ع2
محكمة: نعم
التاريخ الميلادي: 2014
الصفحات: 8 - 24
رقم MD: 707793
نوع المحتوى: بحوث ومقالات
قواعد المعلومات: HumanIndex
مواضيع: الخوارزميات (برمجة)، التشفير (برمجة)، التشفير الكتلى
رابط: http://search.mandumah.com/Record/707793

تصميم خوارزمية تشفير كتلية جديدة عالية السرية

يحي نجار*، محمود شعار*، سلام رزوقي مهدي**

*قسم هندسة الحواسيب كلية الهندسة الكهربائية والإلكترونية جامعة حلب

** طالب دراسات عليا (دكتوراه)

الملخص

تعتبر خوارزمية تشفير (Twofish) من الخوارزميات القوية للغاية وذات بُنية معقدة إلى حد ما وتتخللها معظم عمليات توزيع وتبديل البيانات ويمكن تنفيذها بسهولة. مفاتيح خوارزمية Twofish متغيرة الأطوال (192، 128 أو 256 بت)، وجدول المفاتيح فيها يتولد مرة واحدة ويتكرر استخدامه في تشفير كل كتل الرسالة مهما كان عددها وهذا يقلل من سرية التشفير. في هذا البحث تناولنا تصميم جديد لخوارزمية Twofish بمفهوم جديد والمتمثل بالتغيير الدائم في عملية التشفير وعملية توليد مفاتيح التشفير لكل كتلة. يعد هذا المفهوم جديد وغير مطروق في كافة خوارزميات التشفير الكتلي المعروفة، ويعتمد على توليد دائم للمصفوفات MDS (Maximum Distance Separable) و (Reed Solomon) SR الداخلة في عملية التشفير وعملية توليد المفتاح كل حسب عملها. لقد تمكنا من استخدام تشفير جيف Geffe الانسيابي في توليد المصفوفات MDS وRS ليصبح لكل كتلة صريحة مصفوفات ومفاتيح جديدة تختلف من كتلة إلى أخرى، مما يكسب الخوارزمية حماية ضد العدو. أخيرا هذه الخوارزمية تعمل تقريبا كخوارزمية One- Time Pad.

1. المقدمة

إن المعلومات المحفوظة بشكل يدوي يمكن حمايتها بإخفائها بمكان آمن مقفل بمفتاح لا يملكه إلا المخولين بالاستخدام. ولكن ماذا عن المعلومات المحفوظة في أجهزة الحاسوب؟ وماذا عن المعلومات المنقولة عبر شبكات الحاسوب؟

لذلك لابد من حماية المعلومات والبيانات بحيث تكون غير قابلة للتحوير والتحطيم وغير قابلة للإفشاء والتشويش بصورة متعمدة أو غير متعمدة، وبالتالي لابد من وجود طرق تؤمن نقل وتخزين البيانات والمعلومات المتضمنة تشفير وإخفاء محتويات الرسالة وتحويلها إلى شكل آخر قبل الإرسال أو التخزين(1، 2).

2. التشفير

التشفير هو مجموعة التحويلات التي تجري على النص الصريح للحصول على النص المشفر. هذه التحويلات تشمل خوارزمية التشفير بالإضافة إلى المفتاح. يعتبر التشفير الانسيابي والتشفير الكتلي أهم أنواع التشفير الحديث المستخدم في يومنا هذا (1، 3).

2-1. التشفير الانسيابي Stream Cipher

التشفير الانسيابي هو أحد أهم طرق التشفير الحديثة ويستخدم في الغالب في مجال الاتصالات. وتتكون معظم أنظمة التشفير الانسيابي من مجموعة مسجلات إزاحة ذات تغذية خلفية خطية (Linear Feedback Shift Register)، ويتكون كل مسجل إزاحة من مجموعة من النطاطات (Flip- Flops) كل منها تسمى بمرحلة (Stage)، وبعدد هذه المراحل يتحدد طول مسجل الإزاحة ودرجة تعقيده وهنا يبرز لنا مفهوم مهم هو المكافئ الخطي (Linear Equivalence) والذي يعرف على أنه أقل طول لمسجل الإزاحة المستخدم في توليد المتتابعة. ويمكن إشراك معظم هذه المراحل بوساطة دالة تدعى دالة التغذية المرتدة (Feedback Function). وفي كل نبضه (Pulse) تزاح محتويات المسجل. وأيضا تدخل في تكوينه دوال ربط خطية ولا خطية مختلفة تستخدم للربط بين مسجلات الإزاحة لغرض الحصول على متتابعة ذات دورة طويلة وخصائص عشوائية جيدة وتعقيد خطي كبير لضمان السرية العالية في التشفير. حيث يتم فيها التشفير (بتا بعد بت) بدالة متغيرة زمنيا. من الخوارزميات المهمة في التشفير الانسيابي خوارزمية تشفير جيف Geffe's Algorithm وتتكون هذه الخوارزمية من ثلاث مسجلات إزاحة مختلفة الطول والقاسم المشترك الأكبر بين أطوالها هو واحد ودالة التغذية المرتدة لكل مسجل إزاحة هي دالة خطية (4، 5).

2-2. التشفير الكتلي Block Cipher

أنظمة التشفير الكتلي هي أحد نماذج التشفير المتماثل (المتناظر) الحديث والتي تستخدم مفتاح واحد فقط للتشفير ولفك التشفير. يتم في هذا النوع من التشفير تقسيم النص الصريح إلى مقاطع أو كتل Blocks بأطوال ثابتة واستخدام دالة واحدة لتشفير كل مقطع من هذه المقاطع لينتج كتلة النص المشفر. في عام 1994 طرح Bruce Schneier في هذا الحقل خوارزمية Blowfish كبديل عن خوارزمية DES القياسية. وقد كان هدفه من هذه الخوارزمية هو تحقيق معايير السرعة في التطبيق وصغر الحجم وسهولة الدراسة والتحليل. وأخيرا مستوى الأمن المتغير وحسب طول المفتاح المستخدم ويصل حتى 488 بت (6، 7).

2-2-1. خوارزمية (Twofish) في التشفير الكتلي

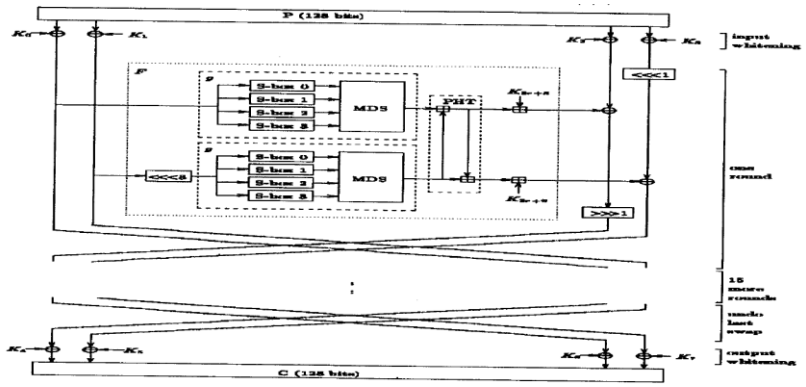
في 15 حزيران عام 1998 نشر العالم Bruce Schneier وخمسة علماء (J.Kelsey, D. Whiting, N. Ferguson, D. Wagner, C. Hall) خوارزمية Twofish وشاركوا بها في مسابقة اختيار مقياس التشفير المتقدم AES (Encryption Standard Advanced). وقد أصبحت الخوارزمية واحدة من الخوارزميات الخمس التي وصلت إلى النهائيات المعتمدة عالميا. وتعتبر خوارزمية Twofish في التشفير الكتلي من أفضل الخوارزميات الحديثة لما تمتاز به من قوة في السرية، وإن الذي جعل الخوارزمية مميزة وقوية هو اعتمادها على صناديق التوزيع S-boxes وتعقيد جداول

المفتاح وإن أقوى محللي الشفرات استطاع من كسر 5 دورات من خوارزمية Twofish من خلال اختيار 2^{22} نص صريح و 2^{51} محاولة. وآخر مقارنة نشرتها إحدى المجلات العلمية في أيار 2011 حصلت خوارزمية Twofish على المرتبة الأولى من حيث القوة والسرية. صمم Bruce Schneier مع سبعة علماء خوارزمية Three fish معتمدين على Skein Hash Function من عائلة تختلف عن ما هو في خوارزمية Twofish وبدون استخدام S-Boxes، وعدد أكبر من الدورات لكنها فشلت أمام محللي الشفرات كما أعلن عن ذلك في أكتوبر عام 2010 حيث استطاعوا من كسرها من خلال بعض دوراتها (2، 7، 8).

2-2-2. هيكلة خوارزمية (Twofish)

تتكون خوارزمية (Twofish) من جزئيين رئيسيين هما جزء معالجة النص المطلوب تشفيره (Encryption Algorithm) وجزء معالجة وجدولة المفتاح الداخل في عملية التشفير (Key Scheduling).

الشكل رقم (1) يبين نظرة عامة لخوارزمية Twofish في التشفير الكتلي.

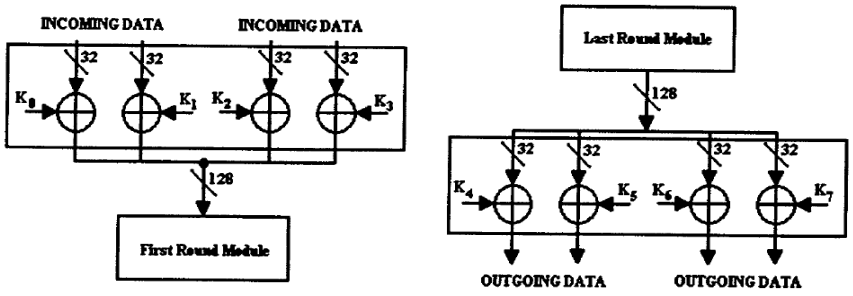


الشكل رقم (1) يمثل الهيكل الكامل لخوارزمية Twofish

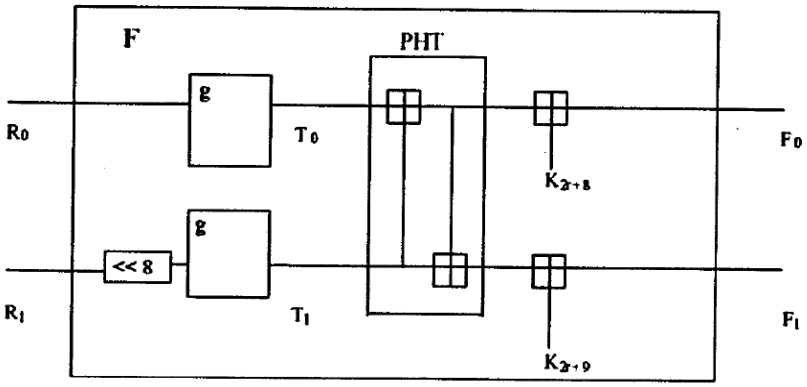
في هذه الخوارزمية يُقسم النص المطلوب تشفيره إلى كتل حجم الكتلة الواحدة 128 بت. إما المفتاح فإنه متغير الطول حيث يمكن أن يكون 128، 192 أو 256 بت ولا يوجد مفتاح ضعيف في هذه الخوارزمية. تستخدم هذه الخوارزمية هيكلية فستل (Feistel Structure) الشائعة والمستخدمة نفسها في خوارزمية تشفيرDes وهي طريقة عامة لإجراء تحويلات وتبادل في دالة (وتسمى عادة F-Function) وهي أساس التشفير الكتلي وصممها Horst Feistel. تستخدم هذه الخوارزمية 16 دورة (Feistel) في مدخلات التشفير ومخرجات فك التشفير. وكما نلاحظ في الشكل رقم (1) أن عملية التشفير تتضمن عدة مراحل هي مرحلة اختيار الكتلة بطول 128 بت من النص المراد تشفيره. ومرحلة الإدخال input .Whitening ومرحلة الست عشرة دورة 16 round ومرحلة الإخراج output Whitening. وأخيرا مرحلة النص المشفر بطول 128 bits.

الشكل رقم (2) يوضح نظرة سريعة لمرحلة تبييض الإدخال ومرحلة تبييض الإخراج قبل أول وبعد أخر دوره.

الشكل رقم (2) يوضح مرحلة التبييض للإدخال والإخراج



والجزء المهم في خوارزمية Twofish هو الدالة f التي تشكل المحور الرئيسي لكل دوره من دورات عملية التشفير الست عشرة دوره. الشكل رقم (1، 3) يبين وظيفة الدالة F والتي تعتمد على المفاتيح الفرعية والرسالة ويكون حجم المفاتيح المدخلة 64 بت، وهذا يعطي 2^{64} تبديل في كل دورة. وتجري في الدالة F عدة عمليات وتعتمد هذه العمليات على ثلاثة عناصر هي المدخلات والتي تمثل R0 وR1 وبطول 32 بت لكل واحدة (النصف الأيسر من الكتلة المطلوب تشفيرها بطول 128 بت)، والعنصر الثالث هو r رقم الدورة.



الشكل رقم (3) الدالة F

$T_0=g\,[R_0)$ $T_1= g\,[<<<\ 8\ R_1]$

$F0= [T_0+ T_1+ K_{2r+8}] \text{ Mod } 2^{32}$ $F1= [T_0+ 2T_1+ K_{2r+9}] \text{ Mod } 2^{32}$

الداخل الأول للدالة g هو R0 ويكون مخرج g هو T0. الداخل الثاني للدالة g هو R1 بعد أن يزاح إلى اليسار 8 بت (8<<<) ليخرج T1. النتائج T0, T1 تمر مجتمعة عبر PHT ويضاف لها مفتاحان K2r+8 وK2r+9 لينتج F1, F0 كما هو موضح بالشكل رقم (3). النابجان F1, F0 هو ناتج الدالة F. سوف نتطرق لاحقا على تفاصيل دقيقة وجديدة للدالة g[8,7,2].

3. الاختبارات الإحصائية لدرجة العشوائية في المتتابعات الثنائية

هناك عدد كبير من الاختبارات الإحصائية لفحص مدى عشوائية النص المشفر عن النص الصريح. وأهم خمسة طرق اختبار معتمدة هي الاختبار الترددي (Frequency Test) يتم في هذا الاختبار فحص عدد الواحدات والأصفار بحيث لا يختلف كثيرا عن n/2 وتستخدم لذلك المعادلة التالية: $x^2=(n0-n1)^2/n$، حيث أن n0 هو عدد الأصفار و n1 هو عدد الواحدات في المتتابعة n. لكي تجتاز المتتابعة هذا الاختبار يجب أن تكون قيمة ($x^2\leq 3.84$)، (حسب جدول مربع كاي عند $x^2_{0.95}$، ودرجة حرية=1). والاختبار الثاني هو الاختبار التسلسلي (Serial)، والغرض منه هو التأكد من أن قيمة كل موقع ضمن المتتابعة مستقلة عن القيمة السابقة لها. ويعتمد هذا على تردد المقاطع الثنائية في المتتابعة n ويقاس بتطبيق المعادلة التالية:

$$x^2=4/(n-1)\Sigma(i=0\ To\ 1)\ \Sigma(j=0\ To\ 1)\ (nij)^2/n^*\ \Sigma(i=0\ to\ 1)\ (ni)^2+1$$

حيث n11,n10,n01,n00,n1,n0 هو تردد 11,10,01,00,1,0 على التوالي ويكون الاختبار ناجحا إذا كانت قيمة ($x^2\leq 5.99$) و(حسب جدول مربع كاي عند $x^2 0.95$ ودرجة حرية=2). الاختبار الثالث هو اختبار بوكر (TEST POKER) يحدد هذا الاختبار استقلالية المقاطع فيما بينها وبطول معين ويعتمد المعادلة التالية

$$x^2=2^m/F\sum_{i=0}^{m}\frac{(xi)2}{(mi)}-F$$

Fi هي عدد المقاطع التي تحوي i من الواحدات وm-i من الأصفار. لنجاح الاختبار يجب أن تكون قيمة x^2 أقل من أو تساوي قيمة مربع كاي عند درجة حرية (m-1).

والاختبار الرابع هو اختبار الجريان (Runs Test) الذي يعتمد على حساب ترددات المقاطع للوحدات المتشابهة (الكتل أو الفجوات) ضمن المتتابعة بطول معين. وباستخدام نفس المعادلة المستخدمة في الاختبار التسلسلي يكون الاختبار ناجحا إذا كانت قيمة $x^2\leq 5.99$ و(حسب جدول مربع كاي عند $x^2_{0.95}$ ودرجة حرية 2). والاختبار الأخير هو اختبار الارتباط الذاتي (Autocorrelation test)، يعتمد هذا الاختبار على عدد التطابقات والاختلافات لكل إزاحة (d) بالنسبة للمتتابعة. لو كانت المتتابعة (n) هي a1,a2....an فإن

$$A(d)=\Sigma_{(i=0\ to\ n-d)}ai\ ai+d;\ 0\leq d\leq n-1$$
$$A(0)=\Sigma_{(i=0\ to\ n)}\ ai\ \Sigma_{(i=0\ to\ n)}ai$$

لو كانت المتتابعة (n) تحوي (n0) من الأصفار، (n1) من الواحدت، فالقيمة المتوقعة ل A(d) حيث ($A(d)\neq 0$) تكون: $x^2=ni^2(n-d)/n^2$ يكون الاختبار ناجحا عند ($x^2\leq 3.84$) و(حسب جدول مربع كاي عند $x^2_{0.95}$ ودرجة حرية 2) [9، 10].

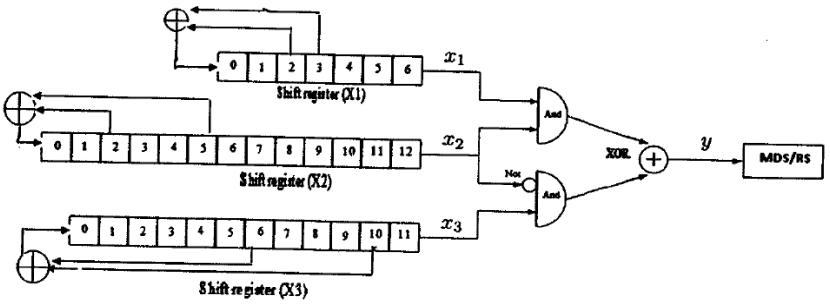
4. تطوير خوارزمية Twofish

سوف نشرح في هذا البند (البند 4) تطوير خوارزمية Twofish وتبيان الفرق بين الجديدة المتطورة والأصلية. من المعروف لنا أن المصفوفة MDS والمصفوفة RS تدخلان في عملية التشفير وتوليد جدول المفتاح في خوارزمية Twofish. وتكونان ثابتتين ومعلومتين للجميع، ولكن في بحثنا جعلناهما سريتين ومتغيرتين ومعتمدتين على المفتاح السري الرئيسي للخوارزمية، وتتولد كل منهما بواسطة خوارزمية جيف الانسيابية ولكل كتلة يراد تشفيرها (128 بت) لها مصفوفة تختلف عن مصفوفة تختلف عن مصفوفة الكتلة الأخرى، وهناك جدول للمصفوفات MDS وRS مولد بواسطة تشفير جيف الانسيابي والمفتاح السري الرئيسي، يحدد في هذا الجدول المصفوفتين MDS وRS والكتلة المقابلة لهما من النص الصريح وبطول 128 بت. وتُنفذ خوارزمية Twofish الجديدة والمتطورة بنفس خطوات تنفيذ خوارزمية Twofish الأصلية والموضحة بالشكل رقم (1) ولكن هنا تكون المصفوفات MDS وRS متغيرة من كتلة إلى أخرى وبالتالي فإن عملية التشفير وعملية توليد المفتاح تكون متغيرة في كل كتلة. وتتم عملية التشفير المتطورة بأخذ النص الصريح المراد تشفيره وطوله 128 بت ويقسم إلى أربع كتل طول كل كتلة 32 بت. في خطوة الإدخال input whitening تعالج المدخلات مع أربع كتل المفتاح السري (k3,k2,k1,k0) بعملية (xoRed) كما في الشكل (1 و2). تتبعها المرحلة التالية مرحلة 16 دورة والتي تبدأ من نتائج المفاتيح k0,k1,k2,k3 في الجهة اليمنى واليسرى لتكون النتيجة كمدخلات للدالة F، وأحد هذين المدخلين يزاح إلى اليسار بطول 8 بت (8<<<). الدالة g تتكون من أربعة بايت (wide Key) يعتمد على صناديق التوزيع s(s-boxes)، والمصفوفة (Maximum Distance Separable) MDS. أن المصفوفة MDS والمتولدة بواسطة تشفير جيف الانسيابي والمفتاح السري لكل كتلة يراد تشفيرها كما في الشكل (4) توضع هذه المصفوفة في جدول يحدد فيه تسلسل الكتلة المقابلة لها من النص الصريح. ويتم من خلال هذه المصفوفة عملية خلط خطي لمخرجات الصناديق. وبعدها يتم إدخال النتيجتين من الدالة g إلى PHT (Pseudo-Hadamand Transform) كما في الشكل (3) ويعامل الناتج مع كلمتي المفتاح k_{2r+8}, k_{2r+9} ومن ثم تعامل النتيجتين بعملية (XORed) إلى الجزء الناتج من عمليات مرحلة الإدخال input whitening والتي تم معالجة واحدة منها مع المفتاح k_2 وثم تدوير أو إزاحة النتيجة إلى اليمين بمقدار 1 بت (1<<<). من جانب آخر تدور أو تزاح نتائج المفتاح K3 مع جزء الكتلة المطلوب تشفيرها إلى اليسار بمقدار 1 بت (1>>>) وبعدها تعالج نتيجة المفتاح مع النتائج الخارجة من الدالة F بعملية الإضافة XORed. وبهذه تكون الدورة الأولى من الست عشر دورة قد انتهت ثم الخطوة التي تليها يتم فيها عملية تبديل الجزء الأيمن بالأيسر ويكون كمدخل للدورة التالية. بعد تنفيذ كل الدورات وصولا إلى الدورة رقم 16 يتم تغيير أو تبديل الجزء الأيسر بالأيمن والأيمن بالأيسر (switching) وتكون النتائج قد وصلت إلى

مرحلة الإخراج بعد إجراء عملية XORed بين النتائج الأربع والكلمات المفتاحية k_4,k_5,k_6 and k_7 لينتج النص المشفر (الكتلة المشفرة) بطول 128 بت.

4-1. التوليد الدائم والمتغير للمصفوفات MDS وRS بواسطة نظام التشفير جيف

لقد اعتمدنا التشفير الانسيابي في تطوير خوارزمية Twofish وذلك باستخدام خوارزمية جيف الانسيابية (وبمسجلات ذات أطوال اختيارية) في توليد دائم ومتغير للمصفوفتين MDS وRS الداخلتين في عملية التشفير وتوليد المفتاح في خوارزمية Twofish. وخوارزمية جيف تتكون من ثلاث مسجلات إزاحة بأطوال مختلفة، x1=7,x2=13,x3=12 والقاسم المشترك الأكبر لهم هو 1، [gcd(x1,x2,x3)=1] ودالة التغذية المرتدة لكل مسجل إزاحة هي دالة خطية تعطي أعظم دوره طولها $4259852415=(2^7-1)\ (2^{13}-1)\ (2^{12}-1)$. وتربط بين مسجلات الإزاحة دوال ربط AND وXOR وعملية النفي NOT كما هو موضح بالشكل (4). x1 و x2 وx3 هي نواتج مسجلات الإزاحة وتخرج من هذا الربط الدالة y اللاخطية كما هي موضحة بالشكل (4) أعلاه. ويمكن أن نعبر عن هذه العمليات بالمعادلة التالية: $y=(x1 \wedge x2) \otimes (\neg(x2) \wedge x3)$ تولد خوارزمية جيف المصفوفات MDS و RS الجديدة، وتوضع في جدول يحدد المصفوفات والكتل المقابلة لها. وأن هذه المصفوفات تستخدم في عملية التشفير وعملية توليد مفاتيح متغيرة تستخدم في خوارزمية Twofish



وتعتبر الأساس في تصميم جديد لخوارزمية Twofish.

4-2. تأثير تغيير المصفوفة MDS على المفاتيح التي تعتمد على S-Box

من المعروف أن جدول S-Box هو جدول يقودنا إلى عمليات توزيع غير خطية تستخدم في أغلب خوارزميات التشفير الكتلية. وهناك أربعة أنواع من المفاتيح تعتمد على S-Box– وهذه الأنواع جديدة بعض الشيء في التشفير. وأن ناتج الأربع الصناديق S-Box المختلفة يشكل مدخلات للمصفوفة MDS في الدالة g، التي تظهر مرتين في الدورة الواحدة، وأن المصفوفة MDS ثابتة في تشفير Twofish ولكن في بحثنا هذا تمكنا من توليد مصفوفة جديدة لكل كتلة الشكل رقم (4) يوضح المخطط الكامل لخوارزمية جيف التشفير السري. وبذلك يكون تأثير المصفوفة في عملية التشفير وتوليد المفتاح تأثيرا متغيرا من كتلة إلى أخرى وهذا يؤدي إلى وجود عملية تشفير مختلفة ومفتاح جديد

مختلف من كتلة إلى أخرى. في خوارزمية Twofish كل صندوق S-Box يحتوي على ثلاثة تباديل 8 by 8 بت تختار من مجموعتين من التباديل الممكنة q0, q1. التباديل qi تتضمن العديد من العمليات المنطقية كما في الشكل رقم (5، 6) وأيضا qi يعتمد في حسابه على الجداول الموجودة في الشكل رقم (6) والذي يحدد قيم (t0,t1,t2,t3)، والمتمثلة 4 بت لكل قيمة (i=0,1). إن كل من q0, q1 يتكونان من هيكل موحد يختلف فقط في جداول في الشكل (6). الشكل (6) يمثل هيكل لكل الصناديق S-Box إن التباديل qi التي تجري عليها عمليات XOR مع المفاتيح الفرعية S0, S1 وسوف نشرحها لاحقا. نعتبر إن X هي الإدخال وأن y هي الإخراج، المعادلات التالية تعبر عن العمليات التي يمثلها الشكل رقم (6) وهيكلية الصناديق S(S-Box) موضحة في الشكل (5).

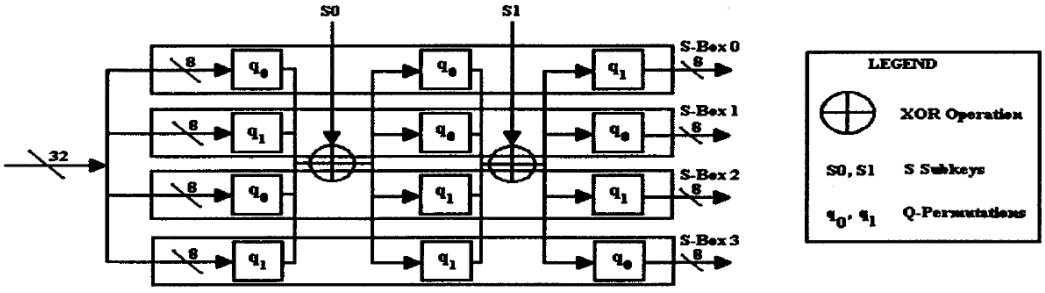
First the byte is split into two nibbles a0, b0

a0, b0= [x/16], x mod 16

a1-a0+b0, b1= a0+ right rotate by one bit (b0, 1)+ 8a0 mod 16

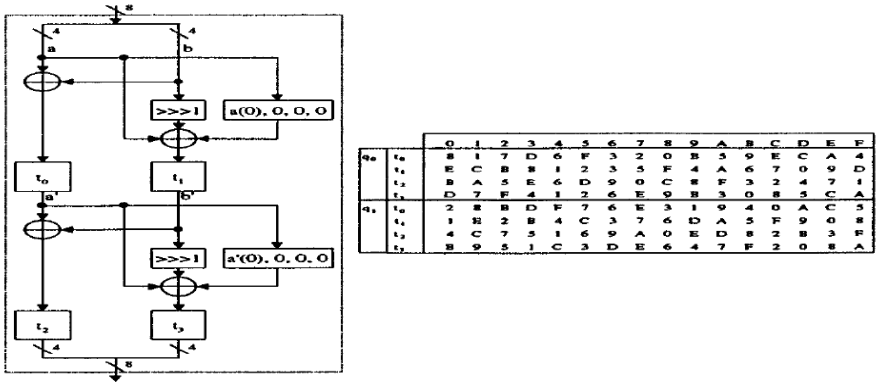
a2, b2= t0 [a1], t1 [b1], a3= a2+b2

b3= a3+ Right rotate by one bit (b_2,1)+ 8_{a2} mod 16



a_4, b4-$t_2[a_3]$,$t_3[b_3]$, y=$16b_4$+a_4

الشكل رقم (5) يوضح اعتماد المفاتيح على صناديق التوزيع S-Box



الشكل رقم (6) يوضح التباديل q0 و q1 والصناديق S-Box

3-4. عمل المصفوفة المتغيرة Maximum Distance Separable (MDS)

المصفوفة MDS هي مصفوفة تباديل 4 by 4 بايت كما هو مبين بالشكل رقم (7)، وهو الشكل الثابت للمصفوفة في خوارزمية Twofish والذي سوف نتعامل معه كنموذج لتنفيذ الخوارزمية.

مدخلات المصفوفة 32 بت وهي مخرجات S-Boxes ويمكن أن نعبر عن هذه المدخلات بمتجه (vector) طوله 4، [y0, y1, y2, y3] وأن كل yi يمثل بايت واحد وبضرب هذا المتجه بالمصفوفة MDS (4*4) وبمعيار الحقل $GF(2^8)$ نحصل على المتجه $[z_0, z_1, z_2, z_3]$ الذي يمثل ناتج من الدالة g كما موضح بالشكل رقم (7).

$$MDS = \begin{bmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{bmatrix}$$

$$\begin{bmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} \cdot & \cdots & \cdot \\ \vdots & MDS & \vdots \\ \cdot & \cdots & \cdot \end{bmatrix} \cdot \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

الشكل رقم (7) يوضح مدخلات ومخرجات الدالة g بواسطة المصفوفة MDS

لو فرضنا أن خوارزمية جيف ولّدت لنا المصفوفة MDS بصيغتها الموجودة بالشكل (7)، فإن المعادلات التالية تمثل كيف وماذا ينتج من الدالة g:

$z_0 = y_0*01 + y_1*EF + y_2*5B + y_3*5B$
$z_1 = y_0*5B + y_1*EF + y_2*EF + y_3*01$
$z_2 = y_0*EF + y_1*5B + y_2*01 + y_3*EF$
$z_2 = y_0*EF + y_1*01 + y_2*EF + y_3*5B$

أن y3, y2, y1, y0 بايتات على التوالي من كلمة إدخال طولها 32 بت وأن البايت y3 هو البايت الأكبر أهمية. لقد تعاملنا مع الشكل العام للمصفوفة وكما قلنا أننا سوف نولد مصفوفة خاصة لكل كتلة بطريقتنا الجديدة.

4-4. العلاقة بين المصفوفة MDS المتغيرة وتحويلات هادا مارد The Pseudo Hadamard (PHT) Transforms

تحويلات هادا مارد PHT تحتوي على عمليتي إضافة ضمن الحقل 2^{32} Module. إن الحقل 2^{32} Moduleيقبل الكلمتين الناتجتين من المصفوفة MDS المتغيرة (المتولدة بواسطة تشفير جيف) وطول الواحدة 32 بت، وتخرج (PhT) أيضا كلمتان بطول 32 بت، والعملية سهلة وسريعة كما هي موضحة المعادلات التالية والشكل (2).

$$F0 = [T_0 + T_1 + K_{2r+8}] \bmod 2^{32} \text{ and } F_1 = [T_0 + 2T_1 + K_{2r+9}] \bmod 2^{32}$$

حيث F1, F0 هي مخرجات الدالة F. والمفتاحان k2r+9, K2r+8 يضافان إلى الكلمتين بطول 32 بت الناتجتين من تحويلات هادا مارد PHT وبمعيار ^{32} 2Modulo، وأن r يمثل عداد للدورات الست عشرة في تشفير Twofish.

5-4. جداول المفتاح Key Schedules المتغيرة

تعني جداول المفتاح العمليات التي تجري على المفاتيح من تحويل وتدوير وتغيير بتات المفتاح المستخدم في عملية التشفير لبناء خورازمية تشفير Twofis الكتلية لتكون أكثر قوة وعالية السرية.

خوارزمية Twofish تحتاج أن تكون مفاتيحها معقدة وغير سهلة التحليل عصية الكسر من قبل محللي الشفرات. جدول المفاتيح يولد ويجهز 40 كلمة مفتاح $k_0, k_1 ..... k_{39}$ ومعتمدا على صناديق التبديل S-Boxes ودالة g (g-function)، وأن الدالة g تعتمد بعملها على المصفوفتين RS(Reed solomon) و MDS. المعروف أن المصفوفتين RS و MDS تكونان ثابتين في خوارزمية Twofish الأصلية في كافة الدورات والكتل. في هذا البحث تناولنا تصميم جديد لخوارزمية Twofish بمفهوم جديد والمتمثل بالتغيير الدائم في عملية التشفير وعملية توليد مفاتيح التشفير لكل كتلة حيث هذا المفهوم ينتج عنه مبدأ جديد غير مطروق في كافة خوارزميات التشفير الكتلي المعروفة ويعتمد على توليد دائم للمصفوفتين MDS و RS الداخلتين في عمليتي التشفير وتوليد المفتاح. لقد تمكنا من استخدام تشفير جيف Geff الانسيابي في توليد المصفوفتين MDS و RS الداخلتين في توليد جدول المفتاح الذي يعتمد في عملية تشفير الرسالة الصريحة ليصبح لكل كتلة صريحة مصفوفات جديدة ومفاتيح مختلفة من كتلة إلى أخرى. وتقسم مفاتيح التشفير في خوارزمية Twofish إلى نوعين هما: S-Keys و K-keys.

4-5-1. تغير المفتاح S-keys

طول المفتاح في خوارزمية Twofish متغير يمكن أن يكون 128، 192 أو 256، أما في طريقتنا فإن المفتاح يمكن أن يأخذ أحد الأطوال أعلاه ولكن تمكنا من توليد مفتاح متغير لكل كتلة (بالإضافة إلى تغيير طول المفتاح فإن البيانات التي يتألف منها المفتاح ومتغيره من كتلة إلى أخرى). وتستخدم نفس خطوات توليد المفتاح في خوارزمية Twofish الأصلية ولكن باستخدام مصفوفات (MDS وRS) متغيرة في كل كتلة. لو فرضنا أن طول المفتاح الرئيسي المستخدم في هذه الخوارزمية 128 بت يستخدم لتوليد مفتاحين s_0 و s_1 بطول 32 بت والذي يضاف إلى صناديق التوزيع S-Box بعملية XOR المنطقية في عملية تشفير وفك شفرة كل دورات خوارزمية Twofish الست عشرة ويمكن الرجوع إلى الشكل رقم (6) لبيان ذلك. وأن كلا المفتاحين يمكن الحصول عليهما من حاصل ضرب مصفوفة RS المبينة في الشكل رقم (8) والمفتاح العام 128 بت ضمن حقل غاليلو 2^8، يبين الشكل (8) والشكل (9) تفاصيل هذه العملية.

$$RS = \begin{pmatrix} 01 & A4 & 55 & 87 & 5A & 58 & DB & 9E \\ A4 & 56 & 82 & F3 & 1E & C6 & 68 & E5 \\ 02 & A1 & FC & C1 & 47 & AE & 3D & 19 \\ A4 & 55 & 87 & 5A & 58 & DB & 9E & 03 \end{pmatrix}$$

الشكل رقم (8) المصفوفة RS

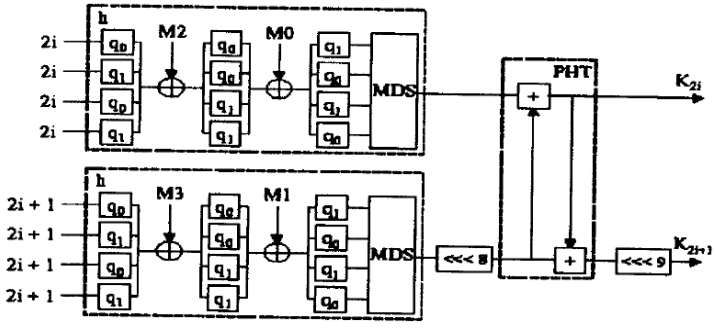
$$\begin{bmatrix} s_{i,0} \\ s_{i,1} \\ s_{i,2} \\ s_{i,3} \end{bmatrix} = \begin{bmatrix} \cdot & \cdots & \cdot \\ \vdots & RS & \vdots \\ \cdot & \cdots & \cdot \end{bmatrix} \cdot \begin{bmatrix} m_{8i} \\ m_{8i+1} \\ m_{8i+2} \\ m_{8i+3} \\ m_{8i+4} \\ m_{8i+5} \\ m_{8i+6} \\ m_{8i+7} \end{bmatrix}$$

الشكل رقم (9) يوضح عملية توليد المفتاحين S0 و S1

حيث i هو عداد يأخذ القيمتين 0 أو 1 التي تشير إلى S_0 أو S_1 وأن القيم $[S_{i,3}\ S_{i,2}\ S_{i,1}\ S_{i,0}]$ أجزاء كل جزء مكون من 8 بت تكون المفتاح Si بطول 32 بت ($s_{i,3}$ هو البايت الأكثر أهمية)، و $[m_{8i+7}\ m_{8i+6}\ \ldots\ m_{8i+1}\ m_{8i}]$ أجزاء من 8 بت للجزء الواحد تكونت من المفتاح الرئيسي 128 بت. أن S-Keys تستخدم S_0 and S_1 في S-Boxes والتي تزيد من قوة الخوارزمية خلال الدورات. وكما ذكرنا سابقا أن المصفوفة RS تتولد من جديد لكل كتلة بواسطة خوارزمية جيف في التشفير الانسيابي لنحصل على مفاتيح جديدة متغيرة في كل دورة ولكل كتلة.

2-5-4. **المفاتيح K-Keys المتغيرة (توليد متغير للمفاتيح K- keys)**

في خوارزمية Twofish الأصلية تكون المفاتيح نفسها في تشفير كل الرسالة مهما كان عدد كتل هذه الرسالة. بطريقتنا تكون المفاتيح متغيرة لكل كتلة. يوجد 40 مفتاح ذات طول 32 بت خلال الست عشرة دورة في خوارزمية Twofish، ثمانية منها $k_7,\ldots k_1,k_0$ تستخدم في إدخال وإخراج مراحل التبييض كما مبين في الشكل(1). أما المفاتيح الباقية وعددها 32 مفتاح ($k_8, k_9,\ldots, k_{39}$) من K-Keys فإنها تتولد بنفس طريقة التشفير الرئيسية ولكن الاختلاف فقط هو لأنه لا يوجد مفتاح يضاف بعد تحويل هادا مارد PHT والإزاحة بمقدار 8 بت تتم بعد الدالة g الثانية بدلا من قبلها، وأيضا هناك تدوير أو إزاحة بمقدار 9 بت بعد الإخراج الثاني من PHT كما مبين في الشكل (10). هذه المفاتيح المتولدة تكون متغيرة حسب الكتلة والمصفوفات المقابلة في التشفير وفك الشفرة وتغطي كافة 16 دورة وعلى دالتي g. و PHT.



الشكل رقم (10) يوضح العمليات الرئيسية في توليد المفاتيح K-keys

المفاتيح M_0 ,M_1, M_2, M_3 مشتقة من المفتاح الرئيسي 128بت وعلى التوالي وكل مفتاح طوله 32 بت وأن M_3 هو المفتاح الذي بتاته الأكثر أهمية في بتات المفتاح الرئيسي و M_0 الأقل أهمية. والعداد i هو متغير يأخذ القيم من 0 إلى 19 ويستخدم لتوليد المفاتيح الفرعية K_0,.. ,K_{38}, K_{39} كما مبين في (10).

6-4. نظرة موجزة في التصميم الجديد لخوارزمية Twofish Twofish

خوارزمية Twofish قوية جدا وذات هيكلية معقدة ولكنها سهلة التنفيذ وتمتاز بقلة الفرق بين عملية التشفير وفك الشفرة وتشترك بنفس دوال عملية توليد المفتاح بفارق بسيط. لا تحتاج إلى مساحة تخزين كبيرة في ذاكرة RAM عند تنفيذها. جدول المفاتيح في الخوارزمية هو أيضا يعطي قوة إضافية إلى سرية خوارزمية Twofish ويتم حساب المفاتيح بطريقة مقاربة إلى طريقة التشفير وذلك باعتماده على بعض المصفوفات وبعض العمليات المنطقية مثل XOR. من مقاييس شانون في التشفير المثالي هو التشويش والعشوائية وهذا يتم بانتشار عناصر الرسالة عند تشفيرها وضياع كل خواص الربط بين الرسالة قبل وبعد التشفير. ولكي نزيد من قوة خوارزمية Twofish علينا أن نزيد من درجة العشوائية وذلك بانتشار الرسالة في النص المشفر، وقد استطعنا في بحثنا هذا أن نزيد من عشوائية عملية التشفير وعملية توليد المفاتيح وذلك بتوليد مفاتيح مختلفة لكل كتلة يراد تشفيرها ويمكن أيضا لكل دورة في نفس الكتلة.

في خوارزمية تشفير Twofish الأصلية يتم توليد نوعين من المفاتيح S و K (أربعة مفاتيح هي S_0, S_1, S_2, and S_3 والنوع الآخر 40 مفتاح هي (K0, K1, ..., K39) يتم تطبيق هذه المفاتيح نفسها على الرسالة مهما كان عدد كتلها. ولكن في بحثنا تمكنا من تصميم جديد للخوارزمية وتحسينها بطريقة جديدة وذلك بتوليد مستمر للمصفوفة MDS والمصفوفة RS الداخلتان في توليد هذه المفاتيح بواسطة تشفير جيف الانسيابي وبهذا يصبح لكل كتلة صريحة يراد تشفيرها مفتاح مستقل عن الكتل الباقية. بهذا نكون زدنا من سرية التشفير وقوته أمام المهاجم والعدو وأصبح من الصعب جدا كسرها. لكسر شفرة Twofish بالطريقة الأصلية نحتاج إلى وقت يتناسب مع طول المفتاح (128 بت)، أما لكسر خوارزمية Twofish بطريقتنا الجديدة نحتاج وقت لكسر مفتاح كل كتلة بقدر الوقت الكافي لكسر خوارزمية Twofish الأصلية، وهذا يعني أننا نحتاج إلى وقت مضاعف بقدر عدد كتل الرسالة، سنوضح ذلك لاحقا. لا نحتاج إلى مساحة تخزين في الذاكرة RAM كبيرة عند تنفيذ الخوارزمية بطريقتنا ولا إلى معالجات سريعة، لأنه لم تجر تغيير بحيث يحتاج المساحة الكبيرة والسرعة العالية بل يمكن أن تنفذ على معالجات البنتيوم و RAM بحجم 8 ميكا، وأكيد هذا لا شيء اليوم ونحن نتكلم بمعالجات سريعة تفوقه بآلاف المرات البنتيوم ويصل حجم RAM إلى 8 كيكا. في طريقتنا الجديدة تم اختيار طول مناسب لمسجلات الإزاحة المستخدمة في خوارزمية جيف بحيث تعطي طول دورة كبيرة جدا تكفي لإرسال رسائل كثيرة وطويلة بدون تكرار السلسلة المتولدة. يتم إدخال الرسالة المطلوب تشفيرها في

خوارزمية Twofish بعد تقسيم الرسالة إلى كتل طول الواحدة 128 بت، وأيضا يتم اختيار المفتاح ويكون هنا طوله 128 بت ليولد منه المفاتيح من نوع S و K وأيضا نأخذ منه وبصورة مباشرة الحالات الابتدائية لمسجلات الإزاحة كل حسب طوله. يتم حساب المصفوفات MDS و RS باستخدام خوارزمية جيف كما يلي:

Algorithm for calculate RS matrix used Geffe generator system

- **INPUT: initial value for three LFSR (linear Feedback Shift Register) X1, X2, and X3, (1≤X1≤127) (1≤ X2≤8191), (1≤ X3≤ 4095).**
- **OUTPUT: the result of f-function used to generate the new value for the MDS/RS matrix.**
- **PSEUDO-CODE:**

1. Initial value for the registers X1, X2, X3;
2. For i=0 to 3, for j=0 to 7, RS(i,j)= (0,0)
3. {

عملية توليد المصفوفات MDS و RS بواسطة خوارزمية جيف

Encryption Algorithm

1. Input: Plaintext split into four 32 bits words (R0,R1,R2,R3), 32 bit key subkeys S, K.
2. X0=R0 ⊕ K0, X1=R1 ⊕ K1, X2=R2 ⊕ K2, X3=R3 ⊕ K3.
3. For i=0 to 15 {
4. T_0=g(R0), T_1=g(<<<R1). Where g represents a function using S-box.
5. RS[i] = Geffe Generate
s_0=RS *(m0,..,m7); s_1=RS*(m8,…,m15). Where m0,…, m15.which derived directly from the main key (M).
6. MDS[i] = Geffe Generate
Subkey S_0, S_1 and MDS S-box multiplying by the MDS matrix.
7. F0=T_0+T_1+K_{2r+8}Mod 2^{32}.
8. F1=T_0+2T_1+K_{2r+9}Mod2^{32}.
9. R2=>>>1(F0⊕R2); R3=F1⊕(<<<R3).
10. X0 ⟷ R2; R1 ⟷ R3
11. }
12. Output: Ciphertext in C0, C1, C2, C3;
C0=R2⊕K4, C1=R3⊕K5, C2=R0⊕K6, C3=R1⊕K7.

Decryption Algorithm

Decryption is similar to encryption the same structure but the subkeys are applied in reveres order. Also the replacements by the following:
R2=F0⊕(<<<1R2)
R3=>>>1(F1⊕R3)

خوارزمية التشفير وفك التشفير في طريقة Twofish الجديدة

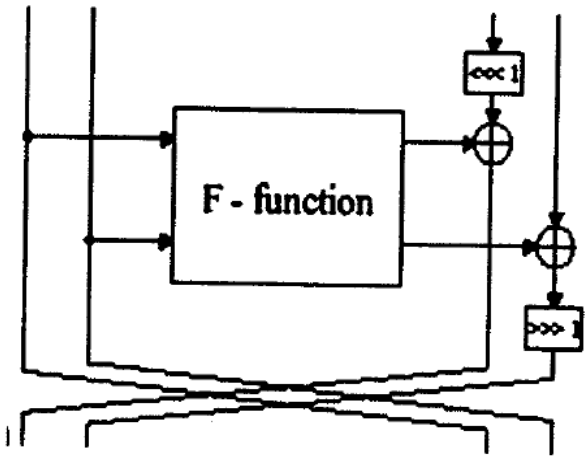
7-4. مستوى تعقيد خوارزمية Twofish الجديدة

تعد كل خوارزميات التشفير المولدة رياضيا قابلة للكسر نظريا. لكن ما يميزها عن بعضها هو الزمن اللازم لعملية الكسر، هذا الزمن الذي يتبع إلى الطاقة الحسابية المتوافرة لدى محلل الشفرة وإلى أهمية المعلومة مع الزمن. فيمكن للمهاجم أن يستخدم الأسلوب العشوائي لكسر التشفير، أي التجربة والخطأ وفي هذه الحالة يكون عدد الاحتمالات التي يجب تجربتها هي 2^{128} محاولة في حالة كان طول المفتاح المستخدم هو 128 بت، وهذا يساوي $3.4*10^{38}$ محاولة تقريبا. فإذا استطاع المهاجم تجربة

مفتاح كل 1 مايكرو ثانية فالوقت المطلوب لتجربة جميع المفاتيح سوف يكون زهاء 10^{25} سنة. أما في حال استخدام المعالجة المتوازية باستخدام عدة معالجات تقوم كلها بمعالجة المشكلة آنيا، فإن المعالج الواحد الذي يستطيع معالجة مفتاح واحد كل 1نانو ثانية (إذا كان ذلك ممكنا) تستطيع تجربة تقريبا 10^{14} مفتاحا في اليوم الواحد أي إنها تحتاج تقريبا إلي 10^{24} يوم لتجربة جميع المفاتيح. وهذا يعني إننا نحتاج إلي 10^{24} معالج يعمل على التوازي بهذا المعدل حتى يتم إنجاز الكشف خلال يوم واحد وبالطبع إنجاز مثل هذه الآلة مستحيلا في الوقت الحالي. إن التعقيدات التي ذكرت كانت من أجل مفتاح واحد يستخدم لتشفير كتلة واحدة من الرسالة، أما في الخوارزمية Twofish الجديدة هنا فإن المفتاح يتغير بشكل دائم مع تشفير كل كتلة، لذلك لفك شفرة رسالة طولها N كتلة نحتاج إلى $N*2^{128}$ محاولة وتقريبا $N*10^{25}$ سنة لتجربة جميع المفاتيح وكسر الرسالة وأيضا نحتاج إلى وقت وجهد ليس بالسهل لمعرفة المصفوفة MDS والمصفوفة RS لأنهما تولدان بواسطة تشفير جيف القوي والسري وليس بالسهل كسره ومعرفتها ولا ننسى أنهما يتولدان ببيانات مختلفة لكل كتلة يراد تشفيرها. وهذا الأمر ليس سهلا إن لم يكن مستحيلا.

5. فك تشفير خوارزمية Decryption Twofish Algorithm Twofish

فك الشفرة الناتجة من خوارزمية Twofish فإن كتلة البيانات المشفرة يجب أن تدخل أولا إلى خوارزمية فك الشفرة ونفس المفتاح المستخدم خلال التشفير يجب أن يستخدم في التحليل كل حسب دورته. تمتاز خوارزمية Twofish بتغير بسيط بين عملية التشفير وفك الشفرة وذلك باستخدام نفس الهيكلية. تتم عملية فك الشفرة بإدخال النص المشفر ويستخدم المفتاح الجزئية $K_4,....,K_7$ في مرحلة تبييض الإدخال والمفاتيح الجزئية $K_0,....,K_3$ تستخدم في مرحلة تبييض الإخراج. أما في حالة الست عشرة دورة فإنها تستخدم المفاتيح $K8, K_9,....., K_{39}$ ولكن بعكس الترتيب أي أنه في الدورة الأولى يستخدم المفاتيح K_{39}, K_{38} والدورة الأخيرة نستخدم المفاتيح K9, K8 مع معكوس كل من المصفوفة MDS والمصفوفة RS. أما عملية XOR وعملية الإزاحة التي تتم في عملية التشفير فإن الشكل (11) التالي يوضح ذلك.



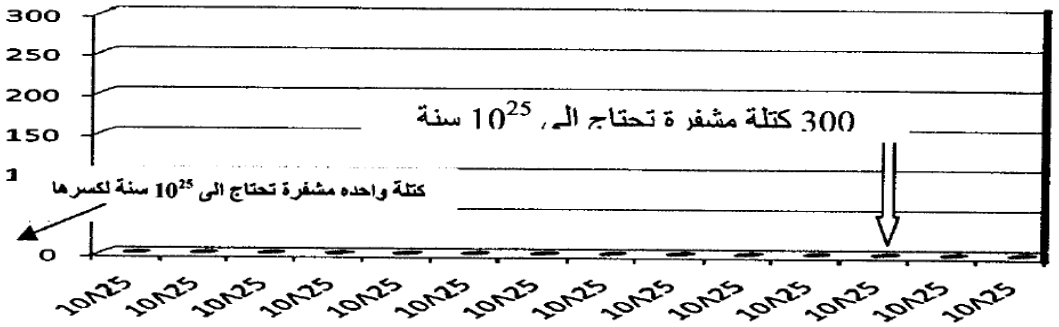
الشكل رقم (11) فك تشفير خوارزمية Twofish الكتلية Decryption Twofish Algorithm

6. النتائج والمناقشة

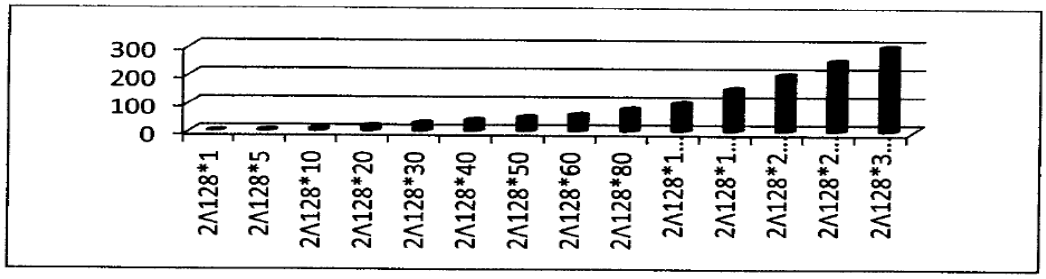
لقد حققت خوارزمية Twofish الجديدة وباستخدام مفتاح طوله 128 بت نتائج على مستوى السرية والعشوائية أفضل بكثير من الخوارزمية الأصلية بعد استخدام خوارزمية جيف في التشفير الانسيابي لتوليد المصفوفة RS في توليد مفاتيح التشفير، ويمكن ملاحظة ذلك في الجدول (1). وطبقا للجدول رقم (1) حققت خوارزمية التشفير Twofish الكتلية نجاحا في الاختبار الترددي والتسلسلي واختبار الجريان. وأما خوارزمية Twofish الكتلية المتطورة فقد حققت أكبر نجاح وأفضل نتائج وذلك باجتيازها لأكثر الاختبارات الإحصائية حيث اجتازت الاختبار الترددي والاختبار التسلسلي واختبار الجريان إضافة إلى اجتيازها اختبار بوكر وبنجاح ونتائج تفوق نتائج خوارزمية Twofish الأصلية وبنسب عالية وواضحة (النص الأكثر عشوائية هو الذي يجتاز أكثر الاختبارات العشوائية ويكون ذات عشوائية مقبولة إذا اجتاز على الأقل ثلاث اختبارات). وكما ذكرنا سابقا إذا كان طول المفتاح 128 بت وطول الرسالة المطلوب تشفيرها 300 كتلة وإذا افترضنا وقت تجربة المفتاح الواحد هو 1 مايكرو ثانية، فنحتاج إلى 2^{128} محاولة لكسر هذا التشفير و 10^{25} سنة لكسر الرسالة في تشفير Twofish الأصلية كما مبين في الشكل (12). أما عند تشفيرها بطريقتنا الجديدة فنحتاج إلى $300*2^{128}$ محاولة وبزمن $300*10^{25}$ سنة لكسر هذه الشفرة، الشكل رقم (13 و 14) يبين ذلك. وهذا يدل على أن خوارزمية Twofish المتطورة أفضل وأقوى سرية وصعبة الكسر من قبل المخربين.

جدول رقم (1) نتائج الاختبارات الإحصائية

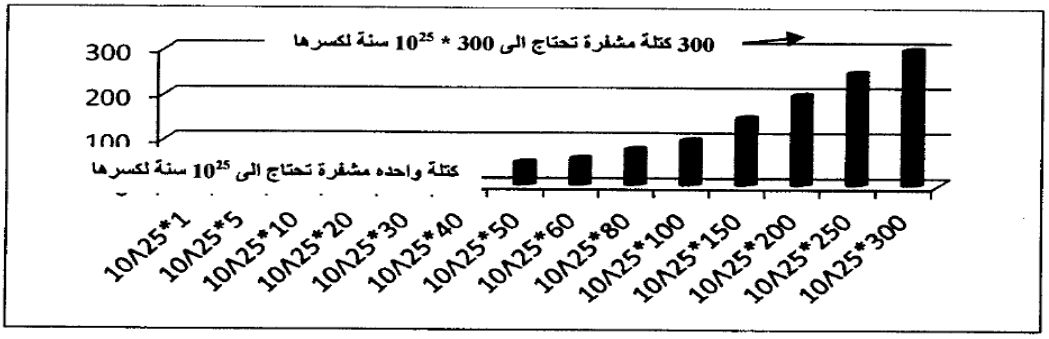
TESTS	ORIGINAL	NEW	TESTS the LIMITS
Frequencey1	3.81254	0.1225	Must be less than 3.84
Serial	-130.749832	-123.8495	Must be less than 5.99
Poker	20.70841	-1.793855	Must be less than 11.07
Runs	3.07755	-1.86374	Must be less than 5.99
Autocorrelation Shift by 1	42.99288	14.53962	Must be less than 3.84
Autocorrelation shift by 2	43.89572	11.37488	Must be less than 3.84



الشكل (12) يوضح العلاقة بين عدد الكتل وعدد السنين أو عدد المحاولات لكسر شفرة توفش الأصلية



الشكل رقم (13) يوضح العلاقة بين عدد الكتل وعدد المحاولات لكسر شفرة توفش الجديدة



الشكل رقم (14) يوضح العلاقة بين عدد الكتل وعدد السنين لكسر شفرة توفش الجديدة

المصادر

1. CHISTOPHER PAAR, 2003 "Applied Cryptography and Data Security", Department of Electrical En g. and information Science. Germany, Internet paper http://www.crypto_rub.de.
2. ساري الخالد، 2011، "التعمية الأساسيات– الخوارزميات– التطبيق"، طبع بمطبعة دار الخرقي دمشق– سوريا الطبعة الأولى.
3. الأستاذ الدكتور وسيم الحمداني، الدكتورة وسن، 1997 "التشفير والتشفير الانسيابي" الجامعة التكنولوجيا بغداد العراق.
4. Prof. BART PRENEEL, 15 September 2010, "Stream Ciphers: Past, present and future", Katholieke Universiteit Leuven, COSIC, International ISC Conference on information Security and Cryptography 2010 (ISCISC'10).
5. PATRIK EKDAHL and THOMAS JOHANSSON, 2000, "A New Version of the Stream Cipher SNOW", Dept, of Information Technology, Lund University, P.O. Box 118, 221 00 Lund, Sweden
6. CHRISTOPHER SIVEIRA, May 1, 2003 "AES: the new key on the block", Internet paper. http://www.nist.gov/aes.
7. GREGOR LEANDER, May/June 2011, "Lightweight Block Cipher Design", DTU Mathematics, Denmark ECRYPT II.
8. LARS R. KNUDSEN, 2000 "Trawling Twofish (revisited)", Dept, of Informatics University of Bergen, report.
9. JUAN SOTO and LAWRENCE BASSHAM, March 28, 2002.report, "Randomness Testing of the Advanced Encryption Standard Finalist Candidatesl", Computer Security Division, National Institute of Standards and Technology.
10. YUE WU, JOSEPH P. NOONAN, and SOS AGAIAN, April 2011, "NPCR and UACI Randomness Tests for Image Encryption", Member, IEEE, Journal of Selected Areas in Telecommunications (JSAT).