رفع مناعة AES ضد الهجمات الجبرية باستخدام جداول التبديل المعتمدة على المفتاح ودراسة تأثير هذه الجداول في مناعة AES ضد الهجمات التقليدية

عائدة خالد الجنادي(1) و أنس التارة(2) و جبران جبران(1)

(1) قسم الرياضيات ــ كلية العلوم ــ جامعة دمشق ــ سورية.

(2) قسم الذكاء الصنعي ــ كلية الهندسة المعلوماتية ــ جامعة دمشق ــ سورية.

تاريـــخ الإيداع 2006/03/05

قبل للنشـــر في 2007/02/04

الملخص

بنيت خوارزميات التعمية الحديثة بالاعتماد على الفرضية الآتية: «تعتمد الطرائق التقليدية في تحليل المعميات (التحليل الخطي، التحليل التفاضلي،.....) على خصائص احتمالية تجعل أمن المعمي يزداد بشكل أسي مع عدد دورات المعمي». لذلك فهذه المعميات ليس لها المناعة المطلوبة ضد الهجمات الجبرية التي أصبحت أقوى بعد تطوير خوارزمية XSL. في هذا البحث سوف نقدم بعض الطرائق لرفع مناعة المعمي AES ضد الهجمات الجبرية ثم سندرس تأثير هذا التعديل في مناعة المعمي.

الكلمات المفتاحية: AES، Rijndael، جداول التبديل الديناميكية، الهجمات الجبرية، خوارزمية XSL.

Increasing the immunity of AES against the algebraic attacks by using the dynamic key dependent S-Boxes and studying its effect on AES immunity against the classic attacks

Aeda Janadi[1], Anas Tarah[2] and Jobran Jobran[1]

[1] Department of Mathematics, Faculty of Sciences, Damascus University, Syria.
[2] Department of Aritificial intelligence, Faculty of information Engineering, Damascus University, Syria.

Received 05/03/2006
Accepted 04/02/2007

ABSTRACT

The security of several recently proposed ciphers relies on the fact:" that the classical methods of cryptanalysis (e.g. linear or differential attacks) are based on probabilistic characteristics, which makes their security grow exponentially with the number of rounds".

So they haven't the suitable immunity against the algebraic attacks which becomes more powerful after XSL algorithm. in this research we will try some method to increase the immunity of AES algorithm against the algebraic attacks then we will study the effect of this adjustment.

Key words: AES, Rijndael, Dynamic substitution, Algebraic attacks, XSL algorithm.

المقدمـــة

أدى التطور المستمر في تقنيات جمع المعلومـــات وتخزينهـــا واســـتعادتها وتحليلهـــا وتبادلها وظهور شبكة الإنترنت إلى تزايد عمليات التشارك في المعلومات بـــين شـــركاء العمل على مستويين داخل النظام الواحد أو بين نظم متعددة.

وقد أدى تزايد الاعتماد على الحاسوب في التعامل مع المعلومات إلى التركيز علـــى مدى أمن تقنيات الشبكات التي تتعامل مع هذه المعلومات.

في هذا السياق ظهر العديد من خوارزميات التعمية التي تستخدم لتحويل البيانات مـــن الشكل المقروء إلى الشكل المعمى غير المقروء.

ولعل الخوارزمية الأحدث في هذا المجال هي خوارزمية AES (Rijndael) الفـــائزة في مسابقة المعايير الحديثة للتعمية التي طرحها المعهد الوطني للمعايير والتقنية NIST.

إذ عُدت الخوارزمية الأقوى إلى أن ظهرت خوارزمية XSL (7) التي جعلـــت حـــل جملة المعادلات الجبرية الموصفة لنظام التعمية في AES ممكناً.

في البحث الحالي نقدم تعريفاً عاماً بالهجمات الجبرية ومناعة المعميـــات ضـــد هـــذه الهجمات وبشكل خاص خوارزمية AES التي سنعرض مكوناتها بشيء مـــن التفـــصيل ونطبق تعديلاً على جدول التبديل الخاص بها بهدف زيادة مناعتها ضد الهجمات الجبرية. مع المحافظة على مناعتها ضـــد الهجمـــات الكلاســـيكية (التحليـــل الخطـــي، التحليـــل التفاضلي،.....) وفي النهاية نعرض بعض نتـــائج الاختبـــارات التـــي أجريناهـــا علـــى الخوارزمية بعد التعديل لنقيّم تأثير التعديل في مناعة الخوارزمية ضد الهجمات التقليدية.

1. الهجمات الجبرية:

مقدمة: بنيت المعميات المقدمة مؤخراً من دوال مزج واستبدال تعتمد علـــى جـــداول تبديل صغيرة S-Boxes. وعمل المصممون على تكرار تطبيق هذه الخطوات بالاعتمـــاد على مفاتيح مرحلية يتم توليدها من مفتاح التعمية الأساسي. وتعتمد سريتها على الحقيقـــة الآتية: تعتمد الطرائق التقليدية في تحليل المعميات (التحليل الخطي، التحليـــل التفاضـــلي، .....) على خصائص احتمالية تجعل أمن المعمي يزداد بشكل أسي مـــع عـــدد دورات المعمي (عدد مرات تكرار دوال المعمي).

لكن في عام 2002 قدم Courtois and Pieprzyk في [5] دراســـة لأمـــن لهـــذه المعميات وفق فرضية إضافية: «يمكن توصيف جدول التبديل بشكل كامل بجملة معادلات جبرية وبحيث إن جملة المعادلات هذه صـــحيحة باحتمـــال يـــساوي الواحـــد». وقـــدما خوارزمية أسمياها XSL (7) تستخدم لاستنتاج جملة المعادلات الموصفة للمعمي وحلها.

1.2. تعريف:

هي هجمات يكسر فيها نظام التعمية بواسطة حل جملة المعادلات التي تــصف نظــام التعمية في حقل منته (مثال GF(2)).

وقد طبق مصمما خوارزمية XSL خوارزميتهما علـــى جـــدول تبـــديل Rijndael فاستخلصا 23 معادلة من الدرجة الثانية وبإجمالي 81 تعبيراً مختلفــاً واظهــرا أن هــذه المعادلات مستقلة خطياً. وسنعرض فيما يأتي خوارزمية XSL.

1.3معميات XSL: هي بالتعريف تركيب لـــ N_r مرحلة متماثلة. بالشكل الآتي:

X: المرحلة الأولى I=1 تبدأ بعملية XOR مع المفتاح K_{i-1}.

S: ثم نطبق B جدول تبديل على التوازي كل واحد على s بت.

L: ثم نطبق دالة دمج خطية.

X: ثم نطبق عملية XOR مع المفتاح K_i.

وفق هذا التعريف فإن Rijndeal هـــي حالـــة خاصـــة مـــن XSL-cipher حيـــث $s = 8, B = 4 * Nb$ و $Nb = 4,6,8$. وعندها:

X: المرحلة الأولى i=1 تبدأ بعملية XOR مع المفتاح K_{i-1}.

S: ثم نطبق $B = 4 * Nb$ جدول تبديل على التوازي كل واحد على 8 بت.

L: وهنا لدينا تبديل على مستوى البايت يدعى ShiftRow، يتبع بدالة خطية تـــدعى MixColumn تطبق على التوازي لأجل كل عمود من الـــ $Nb = 4,6,8$ عمود.

X: ثم نطبق عملية XOR مع المفتاح K_i.

1.4.جداول التبديل الممثلة بجملة معادلات معرفة أكثر أو جملة المعادلات خفيفة:

إن الجزء الوحيد غير الخطي من المعميات XSL-Ciphers هو جداول التبديل. لذلك ربما تكون الجزء الأكثر تعقيداً بالنسبة للهجمات الجبرية وفيما يأتي سندرس الخـــصائص العامة لجملة المعادلات الجبرية الممكن استخلاصها من جداول التبديل وتعريف ما يسمى بجملة المعادلات الأكثر تعريفاً أو جملة المعادلات الخفيفة.

ليكن $F : GF(2)^s \rightarrow GF(2)^s$ هو جدول التبديل حيث

$F : x = (x_1, x_2, ..., x_s) \mapsto y = (y_1, y_2, ...y_s)$.

بنيت جداول التبديل في المعميات الجيدة بالاعتماد على دوال بوليانية جيـــدة. بحيـــث تتمتع هذه الدوال بعدد من الخصائص من أهمها أن كل y_i تمثل بكثير حدود ذي درجـــة عالية في x_i. لكن هذا لا يؤكد أنه لا توجد معادلات ضمنية متعددة المتحولات من الشكل $P(x_1, ...x_s, y_1, ...y_s)$ وهي من درجة جبرية منخفضة. مثل هذه المعادلات الضمنية هي الأداة المستخدمة في خوارزمية XSL بهدف كسر المعميات الكتلية.

إن ما يهمنا في هذا النوع من الهجمات لأجل درجة معينة للمعادلاتd (عادة d=2) هو العدد الفعلي لهذه المعادلات r (المعادلات الضمنية).

وهذا العدد r يمكن أن يكون أكبر من s.

كما أننا نهتم بعدد الحدوديات (التعابير) التي تظهر في جملة المعادلات والتي يرمز لها بـ t ويشمل عددها الحدود الثابتة أيضاً. بشكل عام فان:

$$t \approx \binom{s}{d}$$

إذا كان $t << \binom{s}{d}$ نقول: إن المعادلات خفيفة.

إذا كانت $r = s$ فان هذه المعادلات كافية تقريباً لتمثيل جدول التبديل وعندها لأجل كل y سيوجد وسطياً حل واحد، وهكذا إذا كان r>>s . سنقول: إن النظام معروف **أكثر من اللازم**.

1.5.الهجمة MQ على المعميات الكتلية:

لا حظنا سابقاً أنه يمكن تمثيل أي جدول تبديل في معمي كتلي بجملة معادلات جبرية ومن ثم يمكن كتابة المعمي كاملاً كجملة معادلات جبرية. فإذا كانت هذه الجملة تربيعية متعددة المتحولات Multivariate Quadratic ندعو هذا الهجوم بهجوم MQ. وعندها يصبح كسر المعمي عبارة عن مسألة حل جملة المعادلات الممثلة لهذه المعمي من هذه الطرائق خوارزمية XL وخوارزمية XSL.

1.6.المخطط العام لخوارزمية XSL:

يوجد العديد من الطرائق التي يمكن تطبيق هجوم جبري وفقها، فجملة المعادلات يجب أن تكتب بشكل ما بحيث يوجد لها حل وحيد فقط. بالنسبة إلى خوارزمية XSL تعمل على ثلاث مراحل:

كتابة المعمي كجملة معادلات جيدة (أكثر تعريفاً، خفيفة أو كلاهما).

التوسيع إلى نظام أكثر تعريفاً بشكل كبير ليقترب من حد الإشباع بحيث: $\frac{r}{t} \approx 1$.

الوصول إلى الإشباع الكامل أي $\frac{r}{t} = 1$.

حل جملة المعادلات الناتجة.

1.7.مناعة المعميات ضد الهجمات الجبرية:

يعتمد تعقيد الهجمات الجبرية في المعميات الكتلية بشكل كبير على إمكانية استخلاص أكبر عدد ممكن من المعادلات المستقلة خطياً من المعمي ويظهر في [6] أن مسألة تقييم هذه الإمكانية ليست بالمسألة البسيطة حتى لأجل جملة المعادلات الناتجة عن جدول تبديل بسيط في الحقل المنتهي. وحتى الآن لا يوجد توصيف دقيق لما يمكن أن ندعوه خصائص مناعية لجداول التبديل ضد الهجمات الجبرية. لكن بشكل عام فإن معظم الهجمات الجبرية تعتمد على **بساطة** العلاقات الجبرية التي تربط بتات المدخل والمخرج للمكونات اللاخطية (جداول التبديل) في المعميات كما أن الخصائص اللاخطية لجدول التبديل لا تزيد مناعة المعمي ضد الهجمات الجبرية [6].

وفي معرض دراسة Courtois في [6,7] لمعايير ضعف جداول التبديل أمام الهجوم الجبري يوضح أن البحث عن طرائق لزيادة مقاومة نظم التعمية ضد الهجمات الجبرية يأخذ منحيين:

المنحى الأول: البحث عن دوال جبرية ذات خصائص لا خطية عالية توفر مقاومة للهجمات التقليدية (التحليل الخطي، التحليل التفاضلي،.....) بالإضافة إلى تمتعها بخصائص إضافية (لم تحدد بعد) تمكنها من مقاومة الهجمات الجبرية.

المنحى الثاني: استخدام جداول التبديل العشوائية. وهذا المنحى هو مجال بحثنا.

2. خوارزمية AES:

خوارزمية AES[1,2] هي خوارزمية تعمية كتلية ذات طول نص ثابت هو 128 بتاً، وتدعم مفاتيح تعمية ذات أطوال 128، 192,256 بت فقط. والأطوال الأخرى للكتلة أو المفتاح المتاحة في Rijndael غير متاحة في AES. وعلى الرغم مما سبق فغالباً ما يستخدم التعبيران AES و Rijndael بشكل متكافئ.

2.1. الدخل والخرج في Rijndael.

إن الدخل والخرج في Rijndael يفترض أن يكونا متجهتين وحيدتي البعد مؤلفتين من كلمات كل منها ذات 8 بت. الدخل هو كتلة النص الواضح plain text block ومفتاح التعمية key والخرج هو كتلة النص المعمى cipher text block. وفي مرحلة فك التعمية يصبح الدخل هو كتلة النص المعمى cipher text block ومفتاح التعمية key، والخرج هو كتلة النص الواضح plain text block.إن الخطوة في Rijndael تعمل على نتيجة مرحلية ندعوها الحالة state. يمكن تصوير الحالة بأنها مصفوفة مستطيلة من الكلمات،عدد أسطرها أربعة ويرمز لعدد الأعمدة بـ N_b وهو نتيجة قسمة طول كتلة

النص الواضح على 32. وبشكل مشابه ينظم المفتاح في مصفوفة مستطيلة ذات أسطر أربعة وعدد أعمدتها N_k وهو مساوٍ إلى طول المفتاح مقسوماً على 32.

2.2. بنية Rijndael

Rijndael خوارزمية تعمية كتلية تكرارية تستخدم مفتاحاً. وتتألف من تطبيق متكرر لمجموعة معينة من الخطوات على الحالة. عدد الدورات يرمز له بـ N_r ويعتمد على طول الكتلة وطول المفتاح.

2.2.1. التعمية:

تتألف عملية التعمية في Rijndael من الخطوات الآتية:

إضافة مفتاح ابتدائي ويرمز لها بـ AddRoundKey.

مرحلة دورية تتكرر بعدد N_{r-1} مرة.

مرحلة نهائية FinalRound.

يرمز للمفتاح المستخدم في المرحلة الدوريةi بـ ExpandedKey[I]. حيث ExpandedKey[0] يرمز إلى المفتاح الابتدائي المدخل. ويتم حساب مفاتيح التمديد ExpandedKey[i] من مفتاح التعمية CipherKey بعملية التمديد KeyExpansion. ومنه فالشكل العام للخوارزمية هو: Rijndael (State,CipherKey)

```
{
KeyExpansion(CipherKey,ExpandedKey);
AddRoundKey(State,ExpandedKey[0]);
For(i=1;i< N_r ؛i++) Round (State,ExpandedKey[i]);
FinalRund(State,ExpandedKey[ N_r ];
}
```

وسنعرض فيما يأتي الشكل العام للمرحلة الدورية بشيء من التفصيل يرمز لها بـ round. وهي سلسلة من أربع خطوات وتختلف المرحلة الأخيرة قليلاً عن باقي المراحل.كما سنرى أما خطوات المرحلة الدورية فهي:

```
Round(State , ExpandedKey[i])
{
SubBytes(State);
ShiftRows(State);
MixColumns(State);
AddRoundKey(State,ExpandedKey[i]);
```

```
}
```

وللمرحلة الأخيرة الشكل الآتي:

```
Round(State,ExpandedKey[ Nr ])
{
SubBytes(State);
ShiftRows(State);
AddRoundKey(State,ExpandedKey[ Nr ]);
```

2.2.2. فك التعمية:

المدخلات هنا هي النص المعمى ومفتاح التعمية أما المخرجات فهي النص الواضح.

وتأخذ الخوارزمية AES في حالة فك التعمية الشكل الآتي:

```
Inv Rijndael (State,CipherKey)
{
AddRoundKey(state, ExpandedKey[ Nr ])
for i = Nr-1 step -1 downto 1{
InvShiftRows(state);
InvSubBytes(state) ;
AddRoundKey(state, ExpandedKey[i]);
InvMixColumns(state) ;
}
InvShiftRows(state);
InvSubBytes(state);
AddRoundKey(state, ExpandedKey[0]);
}
```

نجد مما سبق أن الخوارزمية مبنية بشكل أساسي على مجموعة من الخطوات سنعرض كلاً منها باختصار مع عرض بسيط للخطوة العكسية المقابلة لها:

2.3. الخطوات المكونة للدورة:

2.3.1. خطوة SubBytes:

إن هذه الخطوة هي الخطوة الوحيدة غير الخطية في الخوارزمية. وتتم على كل كلمة من كلمات الحالة بشكل مستقل. هذه الخطوة هي عملية استبدال كل كلمة من الحالة بالاعتماد على جدول من الرموز يدعى بجدول التبديل S-box. والجدول الخاص بـ Rijndael يرمز له بـ S_{RD} .

وتدعى العملية المعاكسة لعملية SubBytes بــ InvSubBytes وتتم بتطبيق التبديل بالاعتماد على مقلوب جدول الاستبدال الأول والذي يرمز له بـــ S_{RD}^{-1}.

2.3.2. خطوة ShiftRows:

هذه الخطوة هي تحويل على مستوى الكلمة يقوم دورياً بإزاحة أسطر الحالة بقيم مختلفة. أما العملية المعاكسة للعملية السابقة: وتدعى InvShiftRows فهي عملية إزاحة دورية على الأسطر الثلاثة الأخيرة بمقادير محددة.

2.3.3. **خطوة MixColumns**: وهي تحويل يجري على كل من أعمدة الحالة. حيث أعمدة الحالة تعامل كحدوديات على الحقل $GF(2^8)$ ويؤخذ جداؤها كباقٍ للحدودية x^4+1 بحدودية ثابتة c(x).

العملية المعاكسة لــ MixColumns يرمز لها بــInvMixColumns وهي مشابهة لــ MixColumns حيث يحول كل عمود بضربه بحدودية ثابتة d(x) هي مقلوب الحدودية c(x).

2.3.4. الإضافة الدورية إلى المفتاح:

يرمز لهذه الخطوة بـــ AddRoundKey(State,RoundKey). وهي عملية XOR تجرى بين بتات المفتاح الدوري وبتات الحالة. حيث يشتق المفتاح الدوري من مفتاح التعمية بطريقة تدعى ملحق المفتاح.

إن العدد الكلي لبتات المفاتيح الدورية يساوي إلى جداء طول النص الواضح (والتي تساوي إلى طول مفتاح التعمية) بعدد الدورات مضافاً إليها واحد. أما معاكس هذه الخطوة فهي الخطوة نفسها.

2.4. معايير تصميم جدول التبديل في Rijndael ومناعته ضد الهجمات الجبرية:

اختيرت الخطوات المكونة للخوارزمية بحيث تصل إلى القيم الحدية في معايير مناعتها ضد الهجمات التقليدية (التحليل الخطي، التحليل التفاضلي،.....). لكن هذا القول ليس صحيحاً فيما يتعلق بالهجمات الجبرية ويعود السبب في ذلك إلى أن هذا النوع من الهجمات لم يكن خطراً قبل تطوير خوارزمية XSL.

صُمّم S_{RD} بمراعاة المعايير الآتية:

2.4.1. اللاخطية: حيث يجب أن يتمتع S_{RD} بقدر جيد من اللاخطية. وقد استخدم مصمما الخوارزمية جدول تبديل وصل إلى القيمة الحدية في اللاخطية في الحقل $GF(2^8)$ بالاعتماد على دالة المقلوب المتفردة في خصائصها اللاخطية في الحقل $GF(2^8)$ فهي الدالة الوحيدة (حتى الآن) التي توصف بأنها -4 differentially uniform لأجل قيمة زوجية لــ n في الحقل $GF(2^n)$ كما بــرهن علــى ذلــك Kaisa Nyberg في [9]. وتعدُّ هذه الخاصة جوهر قوة المعمي ضد الهجمات التقليدية (التحليــل الخطي، التحليل التفاضلي،.....) لكن لسوء الحظ لا تؤثر هذه الخاصة في مناعة المعمي ضد الهجمات الجبرية [6].

2.4.2.التعقيد الجبري: يجب أن يكون التعبير المعرف لــ S_{RD} معقداً بشكل كاف. وفــي خوارزمية Rijndael بُني جدول تبديل بالدالة المعرفة في الحقل $GF(2^8)$ بالشكل الآتي: $S_{RD}: GF_{2^8} \to GF_{2^8} : S_{RD}[a] = f(g(a)) = f(a^{-1})$ حيث g هي دالة المقلــوب فــي الحقل $GF(2^8)$ و مقلوب العنصر 00 هو نفسه. وأما f فهي الدالة الأفينية القابلة للقلــب المعرفة بالشكل الآتي:

$$b = f(a)$$
$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \\ 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

إن الدالة g توفر اللاخطية للتحويل S_{RD} في حين توفر الدالة الأفينية التعقيد الجبــري المطلوب للتحويل S_{RD}. كما يضاف شرطان يجب أن تحققهما الخطوة S_{RD} وهما:

$$S_{RD}[a] \oplus a \neq 00, \forall a$$
$$S_{RD}[a] \oplus a \neq FF, \forall a$$

نلاحظ أن اختيار الدالة المكونة لجدول التبديل في Rijndael تم فــي إطــار مقاومــة المعمي للهجمات التقليدية لكن البساطة الجبرية لدالة المقلوب في الحقل $GF(2^8)$ تضعف مناعة المعمي ضد الهجمات الجبرية كما ذكر ذلك Courtois في [6,7] .

3. جداول التبديل العشوائية (Random S-Boxes)

تتفق جداول التبديل العشوائية على هدف واحد وهو أن لا تحمل عملية استبدال معينة معلومات عن عملية الاستبدال التالية لها، أو بمعنى آخر أن يتم ترتيب كامل القــيم فــي جدول التبديل و فق آلية عشوائية، بشكل عام لا توجد معايير ثابتة لتوليد جــداول تبــديل عشوائية فهي تختلف باختلاف طريقة التصميم. وإحدى أهم هذه الطرائق وأكثرها شيوعاً

هي استخدام خوارزمية knuth لخلط كامل عناصر جدول التبديل عشوائياً بالاعتماد على المفتاح المرحلي كما في [8] وفي خوارزمية Khufu [10].

في هذه الطريقة يتم بناء جدول تبديل ابتدائي (فعلياً هو جدول تبديل يقابل كل عنصر فيه نفسه) ثم يتم خلط كامل عناصر جدول التبديل بالاعتماد على قيم عشوائية يتم توليدها باستخدام مفاتيح التعمية المرحلية، وفق الخوارزمية الآتية:

```
for i = 1 to 256
sbox[i] := i; /* جدول التبديل الابتدائي*/
for i = 1 to 256
j := RandomInRange (i, 256);
swap (sbox[i], sbox[j]);
end for
```

3.1. مناعة جداول التبديل العشوائية ضد الهجمات التقليدية (التحليل الخطي، التحليل التفاضلي،.....):

درست مناعة جداول التبديل العشوائية من قبل عدد من العلماء الذين أثبتوا القدرة المناعية الجيدة لهذه الجداول ضد الهجمات التقليدية [8]. ومع ذلك فهناك ما يمكن القول عنه تصرف غير نموذجي لجداول التبديل العشوائية فبينما تعدُّ جداول التبديل العشوائية من أسباب قوة المعمي Twofish (حيث ثبت أن استخدام جداول تبديل ثابتة يضعف هذا المعمي) فإنها (أي جداول التبديل العشوائية) عامل ضعف إذا ما استخدمت في حالة المعمي DES [12]. وعليه فقد يكون لجداول التبدل الديناميكية تأثير سلبي في مناعة المعمي، وهذا ما سنختبره من خلال الاختبارات الإحصائية.

4.جداول التبديل الديناميكية

تتألف جداول التبديل الديناميكية [11] من جدول تبديل ثابت قابل للقلب وطريقة ما لتغيير ترتيب القيم داخل الجدول. حيث تخلط محتويات جدول التبديل باستخدام مولد أعداد عشوائية يعتمد على مفتاح التعمية. من الملاحظ أن طريقة بناء جدول التبديل الديناميكي لا تختلف كثيراً عن طريقة بناء جدول التبديل العشوائي وفق خوارزمية Knuth [10]. لكن الاختلاف الأساسي هو في أن جداول التبديل الديناميكية لا تشترط خلط كامل محتويات جدول التبديل بل بعض عناصر جدول التبديل.

5. جدول التبديل المقترح

5.1. معايير تصميم جدول التبديل المقترح:

إن أهداف التعديل الذي نجريه على جدول تبديل Rijndael هي:

أ- رفع درجة مقاومة الخوارزمية للهجمات الجبرية من خلال استخدام جدول تبـــديل متغير بشكل عشوائي.

ب- المحافظة على الخصائص القوية لجدول تبـــديل Rijndael المقاومـــة للهجمـــات التقليدية.

وفي إطار هذه الأهداف اخترنا مكونات جدول التبديل المقترح وفق النقاط الآتية:

ــ في اختيارنا لجدول التبديل الجديد لم نبتعد عن المكونـــات الأساســـية لخوارزميـــة Rijndael بل على العكس حاولنا الإفادة من التركيب القـــوي جـــداً لجـــدول التبـــديل في Rijndael الذي وصل إلى القيمة الحدية في اللاخطيـــة فـــي الحقـــل $GF(2^8)$ وذلـــك للمحافظة على مقاومته العالية للهجمات التقليدية.

ــ اعتمدنا على فكرة جدول التبديل الديناميكي وهي قريبـــة مـــن فكـــرة خوارزميـــة Knuth [22] التي تولد جدول تبديل عـــشوائياً لكـــن هنـــاك فـــرق أساســـي وهـــو أن خوارزميةKnuth في كل عملية خلط تجري عملية swap لكامل عناصر جدول التبـــديل مع قيم عشوائية في حين نحن في كل عملية خلط نقوم بعملية swap للعنـــصر (عنـــصر واحد فقط) الذي استخدمناه للتو مع قيمة أخرى نختارها عشوائياً من جدول التبـــديل. قـــد يقلل هذا الفارق من عشوائية جدول التبديل الذي بنيناه، خصوصاً أننـــا نـــستخدم جـــدولاً معروفاً كجدول تبديل ابتدائي (جدول Rijndael الأصلي) لكننا نعتقد أنـــه كـــافٍ ليرفـــع مناعة جدول التبديل ضد الهجمات الجبرية. لأنه بشكله الحالي (كجدول تبديل دينـــاميكي) يكفي لتعقيد عملية استخلاص وحل جملة المعادلات الجبرية الممثلة للمعمي لسببين:

ــ أصبح لدينا N_{r-1} جدول تبـــديل لأجـــل كـــل بايـــت مـــن الـــنص المـــشفر أي $N_b * 4 * N_{r-1}$ جدول تبديل، بدلاً من جدول تبديل واحد ومن ثم ارتفع عدد المعـــادلات الجبرية الممثلة للمعمي.

ــ إن استخدام المولد العشوائي (في حالتنا دالة مزج وحيدة الاتجاه MD5) في توليـــد جدول التبديل زاد من تعقيد استنتاج المعادلات الجبرية لكل جدول من جداول التبديل.

5.2. **الملامح الأساسية لجدول التبديل المقترح**: يتم توليد جدول التبديل المقترح وفق الخطوات الآتية:

أ. توليد جدول المفاتيح المرحلية حيث لم نغير في طريقة Rijndael لبنـــاء جـــدول المفاتيح الملحقة والتي تستخدم جـــدول تبـــديل Rijndaelالأصـــلي وقـــد أثبـــت مخترعو Rijndael أن هذه الطريقة وصلت إلى القيم الحدية في قوتها[1].

ب. نستخدم المفاتيح المولدة (المرحلية) كبذور لمولد عـــشوائي (دالـــة مـــزج وحيـــدة الاتجاه) لتوليد شريط طوله 128 بتاً نجزئه إلى كلمات طول كل منها 8 بت.

ج. بعد كل عملية استبدال substation سنقوم بإعادة خلط لجزء من محتويات جدول التبديل بالاعتماد على القيم العشوائية المولدة في الخطوة السابقة

5.3. توصيف جدول التبديل العشوائي المقترح:

نفترض أن $w_{j,i}$ هي الكلمة التي سيتم استبدالها و $R_{j,i}$ هي الكلمة العشوائية التي تـم توليدها من المفتاح المرحلي في الدورة (المرحلة)j باستخدام دالة المزج (سنتحدث عنهـا في الفقرة الآتية).

فتجري خطوة الاستبدال substation في التعمية على مرحلتين:

أ- عملية استبدال كما في الحالة الأصلية أي:

$$SubByte(w_{j,i}) = S(w_{j,i}) \quad : 0 \le \mathrm{i} \le 15$$

ب- عملية خلط لقيم جدول التبديل بالاعتماد على قيمة عشوائية R_i

$$Swap(\mathrm{SubByte}(\mathrm{w}_{j,i}), \mathrm{SubByte}(\mathrm{R}_{j,i}))$$

بينما خطوة الاستبدال في فك التعمية تستخدم جدول التبديل الأصليS ومقلوب الجدول Si وهي كما يأتي:

أ- عملية استبدال كما في الحالة الأصلية (باستخدام مقلوب جدول التبديل).

$$InvSubByte(w_{j,i}) = Si(w_{j,i}) \ : 0 \le \mathrm{i} \le 15$$

ب- عمليتا خلط لقيم الجدول الأصلي و جدول المقلوب

$$Swap(InvSubByte(w_{j,i}), InvSubByte(SubByte(R_{j,i})))$$

$$.\ Swap(SubByte(InvSubByte(w_{j,i})), SubByte(R_{j,i}))$$

5.4.الدالة المستخدمة في توليد القيم العشوائية:نستخدم دالـة المـزج MD5 [13] لتوليد شريط عشوائي طوله 128 بتاً لأجل كل مرحلة (دورة). حيـث تكـون الكلمـات المؤلفة لهذا الشريط هي القيم العشوائية المستخدمة في عمليـة الخلـط ونـدخل المفتـاح المرحلي كبذرة لهذه الدالة.

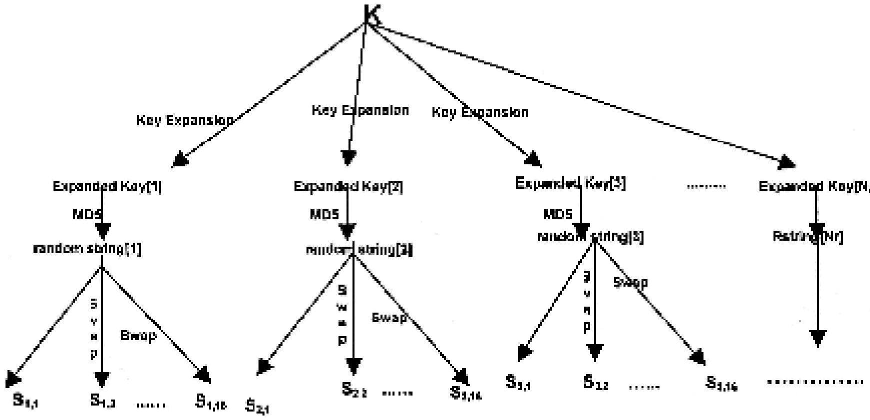
هناك العديد من الاعتبارات التي قادتنا إلى اعتماد MD5 كمولد عشوائي:

1. التكلفة العملياتية المنخفضة لهذه الدالة مقارنة بـدوال المـزج الأخـرى أو حتـى المولدات العشوائية التي لا تعتمد على عملية المزج.
2. السرعة الكبيرة لـ MD5 وما لهذا من تأثير في رفع سرعة عملية التعمية بـشكل عام.
3. نركز في تعديلنا على طول 128 بتاً لمفتاح التعمية، ومن ثم نحتاج أن يكون المولـد العشوائي قابلاً للتعامل مع هذا الطول، وهذا محقق بالنسبة للدالة MD5 التي تأخذ

دخلها كشريط محرفي من أي طول ويكون مخرجها شريطاً محرفياً طوله 128 بتـاً حصراً وهو ما لا يتوافر في بقية دوال المزج.

4. لا تحتاج هذه الدالة أي جداول تبديل كبيرة مما يسهل عملية توظيفها في التطبيقات.

وفيما يأتي مخطط توضيحي لآلية توليد جداول التبديل التي اتبعناها.



خطأ!

عملية توليد جداول التبديل باستخدام قيم عشوائية مولدة من المفاتيح

تقييم تأثير جدول التبديل الجديد

إن تقييمنا هذا سيدرس تأثير جدول التبديل في مناعة الخوارزميـة ضـد الهجمـات التقليدية حيث لا توجد حتى الآن معايير حقيقية عامة لتقييم مناعة المعميات ضد الهجمات الجبرية.

من أهم المعايير التي استخدمت لتقييم الخوارزميات المرشحة لمسابقة AES كـان إجراء اختبارات لتقدير مدى مناسبة هذه الخوارزميات كمولدات أعداد عـشوائية حيـث استخدمت مخرجات هذه الخوارزميات كمدخل لاختبارات إحصائية تقدر حـسابياً مـدى عشوائية هذه المخرجات. وهذه الاختبارات هي مجموعة من 16 اختباراً اقترحها المعهـد الوطني للمعايير والتقنية NIST [3].

الاختبارات الإحصائية للمولدات العشوائية:

هي مجموعة من الاختبارات الإحصائية تجرى على مخرجات المولد العشوائي المراد اختباره. حيث تحسب قيم إحصائية معينة تختلف باختلاف هـدف الاختبـار الإحـصائي. ولتوضيح هذا المعنى سنعرض طريقة إجراء الاختبار الإحصائي **Frequency** بـشكل

تفصيلي ومن ثم نكمل بشكل مختصر بقية الاختبارات مع توضيح بسيط عن هــدف كــل منها.

1. **اختبار (The Frequency (Monobit**: كما ذكرنا سابقاً تجرى هذه الاختبــارات على متتاليات محرفية من مخرجات المولد العشوائي المراد اختبار عشوائيته. ويهدف هذا الاختبار إلى تحديد هل عدد الوحدان والأصفار في المتتالية مطابق لما يمكن توقعه لأجــل متتالية عشوائية حقيقية؟.

توصيف اختبار **Frequency**: يتبع هذا الاختبار التوزيع الطبيعــي نجريــه وفــق الخطوات الآتية :

أ. تحويل الأصفار والوحدان في المتتالية إلى 1+ أو 1- ومن ثم نأخذ مجموع قيم عناصر المتتالية S_n.

ب. نحسب القيمة الإحصائية $S_{obs} = \frac{|S_n|}{\sqrt{n}}$.

ج. نحسب الاحتمال $P = erfc\left(\frac{S_{obs}}{\sqrt{2}}\right)$

د. نعدُّ المتتالية عشوائية عندما $p > 0.01$ أي إن عتبة تحديد عشوائية المتتالية هي 0.01 (بالنسبة لاختبار **Frequency**).

<u>**ملاحظــة**:</u> إن الخطوات السابقة والقيم المحسوبة تختلف من اختبار إلى آخــر بــسبب اختلاف التوزيعات الإحصائية من اختبار إلى آخر باختلاف طبيعة الاختبار وهدفه.

2. **اختبار Frequency Test within a Block**: هدف هذا الاختبار هو تحديد هــل تكرار الوحدان في رزمة من M بت هو M/2 وهي النــسبة المتوقعــة لأجــل متتاليــة عشوائية حقيقية؟.

3. **اختبار The Runs** هدف الاختبار هو تحديد هل عدد الـــ runs للوحدان والأصفار من مختلف الأطوال هو كما يمكن توقعه لأجل متتالية عشوائية؟.

4. **اختبار for the Longest-Run-of-Ones in a Block**: هدف هذا الاختبار هو تحديد هل طول أطول run من الوحدان في المتتالية يتوافق مع ما يمكن توقعــه لأجــل متتالية عشوائية؟.

5. **اختبار The Binary Matrix Rank**: هدف الاختبار هو فحص التبعية الخطيــة بين متتاليات جزئية ذات أطوال ثابتة من المتتالية الأصلية.

6. **اختبار The Discrete Fourier Transform (Spectral)**: هدف هذا الاختبار هو تحديد النماذج المتكررة والقريبة من بعضها بعضاً في المتتالية المختبرة والتي ستحدد الانحراف عن فرضية العشوائية.

7. **اختبار The Non-overlapping Template Matching**: يركز هذا الاختبار على عدد مرات تحقق أحداث نعينها بشكلٍ مسبق. حيث يؤخذ مجال من بتـــات المتتاليـــة ليختبر إن كان يوافق الحدث المحدد مسبقاً في حال تحقق الحدث يبدأ المجال التـــالي مـــن البت الذي المجال الذي تم الانتهاء من فحصه. أي لا يحدث تداخل في المجالات التي يتم فحصها.

8. **اختبارThe Overlapping Template Matching**: يركز هذا الاختبار علـــى عدد مرات تحقق أحداث نعينها بشكل مسبق.الفرق بين هذين الاختبـــارين هـــو أن هـــذا الاختبار يسمح بتداخل المجالات إذ يبدأ المجال التالي من البت الثاني من المجال الذي تـــم الانتهاء من فحصه.

9. **اختبار"Maurer's "Universal Statistical**: يهدف هذا الاختبار إلى تحديـــد إمكانية ضغط المتتالية دون ضياع المعلومات. وتعدُّ المتتاليات القابلة للـــضغط متتاليـــات غير عشوائية. إذ يركز الاختبار على عدد البتات في النماذج المتشابهة في المتتالية.

10. **اختبارThe Lempel-Ziv Compression**: يهدف هذا الاختبـــار إلـــى تحديـــد إمكانية ضغط المتتالية دون ضياع المعلومات. وتعدُّ المتتاليات القابلة للـــضغط متتاليـــات غير عشوائية. إذ يركز هذا الاختبار على عدد النماذج المتمايزة في المتتالية.

11. اختبار The Linear Complexity: يهدف هذا الاختبار إلى تحديد هـــل المتتاليـــة المختبرة معقدة بشكل كافٍ لتعدَّ عشوائية .

12. **اختبار The Approximate Entropy**:إن هدف هذا الاختبار هو مقارنة التكرار في الرزم المتداخلة لطولين متجاورين متعاقبين $(m, m+1)$مقابل النتائج المتوقعة لأجـــل متتالية عشوائية.

13.**اختبار The Cumulative Sums (Cusums)**: هدف هذا الاختبار هو تحديد هل المجموع للمتتاليات الجزئية الحاصل في المتتالية المختبرة هو صغير جداً أو كبيـــر جـــداً بالنسبة إلى التصرف المتوقع لأجل المجموع نفسه في متتالية عشوائية.

14. **اختبار The Random Excursions Variant**: هدف الاختبار هو تحديد هـــل عدد مرات تحقيق عدة نماذج لحدث ما ينحرف عما هو متوقع في المتتالية العشوائية.

15. **اختبارThe Random Excursions**: هدف الاختبار هو تحديد هل عدد مـــرات تحقيق نموذج معين لحدث ما ينحرف عما هو متوقع في المتتالية العشوائية. الفرق بينـــه

وبين الاختبار الذي يسبقه هو تركيز الاختبار السابق على عدة نماذج معاً في حين يركــز الاختبار الحالي على نموذج واحد فقط

16. اختبار **The Serial**: هدف الاختبار هو تحديد هل عدد الأحــداث الـــ 2^m نمــوذج تداخل ذي طول m بت هو تقريباً ما يمكن توقعه لأجل توقعه في متتالية عشوائية.

توصيف البيانات Data Description

يتم اختبار مخرجات الخوارزمية وفق مجموعة الاختبارات الإحصائية السابق ذكرهــا بعد تجميع هذه المخرجات وفق تسعة أنواع من الصياغات المختلفة[4] وهي:

1. Key Avalanche: في هذا النموذج يتم توليد كتلة نــصية تتــألف مــن مجموعــة نصوص معماة تنتج من تعمية نص ثابت لكن باستخدام مجموعة مفاتيح تعمية يختلف كل واحد عن سابقه ببت واحد فقط.
2. Plaintext Avalanche: في هذا النموذج يتم توليد كتلة نصية تتألف من مجموعــة نصوص معماة تنتج من تعمية مجموعة نصوص يختلف كل واحد عن ســابقه ببــت واحد فقط وباستخدام مفتاح التعمية ذاته.
3. Plaintext/Ciphertext Correlation: في هذا النموذج يتم توليد نصوص معماة من نصوص واضحة للعمل على دراسة الارتباط بين أزواج النصوص الواضحة والمعماة.
4. Cipher Block Chaining Mode: في هذا النمط يتم توليد النصوص المعماة وفق نمط السلسلة بمعنى مخرج الخطوة الأولى هو دخل الخطوة الثانية.
5. Random Plaintext/Random 128-Bit Keys يدرس عشوائية النص المعمــى الناتج عن تعمية نص واضح عشوائي.
6. Low Density Plaintext: في هذا النموذج يتم توليد مجموعة نصوص معماة باستخدام مجموعة نصوص واضحة جميع البتات فيها صفرية ماعدا بتاً واحداً يختلف موقعــه مــن نص واضح إلى آخر، في حين يكون مفتاح التعمية ثابتاً لكل نصوص التعمية.
7. Low Density 128-Bit Keys: في هذا النموذج يتم توليد مجموعة نصوص معماة باستخدام مجموعة مفاتيح تعمية جميع البتات فيها صفرية ماعدا بتــاً واحــداً يختلــف موقعه من مفتاح إلى آخر، في حين يكون النص الواضح ثابتاً لكل نصوص التعمية.
8. High Density Plaintext: في هذا النموذج يتم توليد مجموعة نــصوص معمــاة باستخدام مجموعة نصوص واضحة جميع البتات فيها واحدية ماعدا بتاً واحداً يختلف موقعه من نص واضح إلى آخر، في حين يكون مفتاح التعمية ثابتــاً لكــل نــصوص التعمية.

9.High Density 128-Bit Keys: في هذا النموذج يتم توليد مجموعة نصوص معماة باستخدام مجموعة مفاتيح تعمية جميع البتات فيها واحدية ماعدا بتاً واحداً يختلف موقعه من مفتاح إلى آخر، في حين يكون النص الواضح ثابتاً لكل نصوص التعمية.

لأجل كل نوع من هذه الاختبارات توجد عتبة قبول لعدد المتتاليات المرفوضة (أي المتتاليات التي لا تحقق شرط العشوائية بمعنى أنها تتجاوز عتبة القبول a).

تم اختيار العتبة 0.01 لأجل كل الاختبارات وهذا يعني نظرياً أن عدد المتتاليات المرفوضة يجب ألا يتجاوز الواحد لأجل كل 100 متتالية. لكن واقعياً فإن مجموعة البيانات data set المختبرة ستنحرف نتائجها عن القيمة النظرية المذكورة لذلك سنلجأ إلى طريقة تقييم أكثر واقعية نعتمد على مجال ثقة يحدد نسبة المتتاليات التي يجب أن تتجاوز العتبة $a = 0.01$. ويحسب الحد الأقصى لعدد المتتاليات المرفوضة باستخدام الصيغة الآتية:

$$s\left(a + 3\sqrt{\frac{a(1-a)}{s}}\right)$$

حيث: s هي حجم مجموعة البيانات و a هي عتبة قبول المتتالية.

وفيما يأتي جدول لهذه المجالات حسب أحجام مجموعات البيانات المختبرة:

عتبة قبول مجموعة البيانات	عتبة قبول المتتالية	عدد المتتاليات
α= 0.01 with CI	**α= 0.01**	128
4.657	1.28	300
8.170	3.00	384

استراتيجيات الاختبار:

هناك نوعان من استراتيجيات الاختبار:

1- **اختبار الدورة التامة FRT**: يتم تنظيم المخرجات النهائية للخوارزمية المختبرة وفق الأنماط التسعة السابقة ثم جعلها دخلاً للاختبارات الإحصائية الستة عشر.

2- **اختبار الدورات الجزئية PRT**: يتم تنظيم المخرجات المرحلية (بعد كل دورة جزئية) للخوارزمية المختبرة وفق الأنماط التسعة السابقة ثم جعلها دخلاً للاختبارات الإحصائية الستة عشر.

نتائج الاختبارات:

فيما يأتي نتائج الاختبارات الإحصائية على البيانات المولدة وفق 6 طرائق فقط من الطرائق التي سبق ذكرها على أن نستكمل بناء مكتبات بقية الاختبارات لاحقاً.

بفرض:

S: هو عدد المتتاليات التي تجاوزت الاختبار.

F: هو عدد المتتاليات التي لم تتجاوز الاختبار.

C: النتيجة النهائية.

10. الاختبارات التي سنجريها هي وفق 6 أنواع من توصيف البيانات وهي

1. Key Avalanche
2. Plaintext Avalanche
3. Low Density Plaintext
4. Low Density 128-Bit Keys
5. High Density Plaintext
6. High Density 128-Bit Keys

مع ملاحظة أننا سنجري الاختبارات فقط لأجل طول 128 بتاً لكل من النص البسيط ومفتاح التعميـــة.
والاختبارات تتم وفق استراتيجية **الدورة التامة FRT**.

الاختبارات الإحصائية على البيانات المولدة وفق صياغة Low Density 128-Bit Keys

الاختبار الإحصائي: عدد المتتاليات المختبرة في هذا النمط هو 128 متتالية طول كل متتالية 1056896 بت والحد الأدنى المقبول الذي يحدد نجاح الخوارزمية هو أن يكون عدد المتتاليات الفاشلة أصغر أو يساوي 4 متتاليات	اختبار خوارزمية Rijndaelقبل التعديل			اختبار خوارزمية Rijndael بعد التعديل		
	S	F	النتيجة	S	F	النتيجة
Frequency (Monobit) اختبار	127	1	ناجح	128	0	ناجح
Frequency Test within a Block اختبار	126	2	ناجح	126	2	ناجح
Runs اختبار	127	1	ناجح	128	0	ناجح
Longest-Run-of-Ones in a Block اختبار	125	3	ناجح	127	1	ناجح
Binary Matrix Rank اختبار	128	0	ناجح	128	0	ناجح
Discrete Fourier Transform (Spectral) اختبار	128	0	ناجح	125	3	ناجح
Non-overlapping Template Matching اختبار	127	1	ناجح	127	1	ناجح
Overlapping Template Matching اختبار	128	0	ناجح	127	1	ناجح
Maurer's "Universal Statistical" اختبار ناجح	128	0	ناجح	125	3	ناجح
Lempel-Ziv Compression اختبار	- - -	- - - -	- - - - -		- -	- - - -
Linear Complexity اختبار	128	0	ناجح	128	0	ناجح
Approximate Entropy اختبار	128	0	ناجح	128	0	ناجح
Cumulative Sums (Cusums) اختبار	126	2	ناجح	128	0	ناجح
Random Excursions Variant اختبار	127	1	ناجح	127	1	ناجح
Random Excursions اختبار	127	1	ناجح	128	0	ناجح
Serial اختبار	124	4	ناجح	125	3	ناجح

النتيجة: نلاحظ تجاوز المعمي لكل الاختبارات بنجاح إذ لم تتجاوز عدد المتتاليات الفاشلة الأربع لأجل كل الاختبارات الإحصائية.

الاختبارات الإحصائية على البيانات المولدة وفق صياغة Low Density Plaintext:

الاختبار الإحصائي: عدد المتتاليات المختبرة في هذا النمط هو 128 متتالية طول كل متتالية 1056896 بت والحد الأدنى المقبول الذي يحدد نجاح الخوارزمية هو أن يكون عدد المتتاليات الفاشلة أصغر أو يساوي 4 متتاليات	**اختبار خوارزمية Rijndael قبل التعديل**			**اختبار خوارزمية Rijndael بعد التعديل**		
	S	**F**	**النتيجة**	**S**	**F**	**النتيجة**
اختبار Frequency (Monobit)	126	2	ناجح	126	2	ناجح
اختبار Frequency Test within a Block	126	2	ناجح	127	1	ناجح
اختبار Runs	128	0	ناجح	127	1	ناجح
اختبار Longest-Run-of-Ones in a Block	128	0	ناجح	125	3	ناجح
اختبار Binary Matrix Rank	128	0	ناجح	126	2	ناجح
اختبار Discrete Fourier Transform (Spectral)	127	1	ناجح	128	0	ناجح
اختبار Non-overlapping Template Matching	126	2	ناجح	126	2	ناجح
اختبار Overlapping Template Matching	126	2	ناجح	126	2	ناجح
اختبار Maurer's "Universal Statistical"	127	1	ناجح	128	0	ناجح
اختبار Lempel-Ziv Compression	- -	- -	- - - - -		- - -	- - -
اختبار Linear Complexity	128	0	ناجح	128	0	ناجح
اختبار Approximate Entropy	127	1	ناجح	125	3	ناجح
اختبار Random Excursions	127	1	ناجح	127	1	ناجح
اختبار Serial	124	4	ناجح	128	0	ناجح
اختبار Cumulative Sums (Cusums)	124	4	ناجح	126	2	ناجح
اختبار Random Excursions Variant	128	0	ناجح	128	0	ناجح

النتيجة: نلاحظ تجاوز المعمي لكل الاختبارات بنجاح إذ لم تتجاوز عدد المتتاليات الفاشلة الأربع لأجل كل الاختبارات الإحصائية.

الاختبارات الإحصائية على البيانات المولدة وفق صياغة High Density 128-Bit Keys:

الاختبار الإحصائي: عدد المتتاليات المختبرة في هذا النمط هو 128 متتالية طول كل متتالية 1056896 بت والحد الأدنى المقبول الذي يحدد نجاح الخوارزمية هو أن يكون عدد المتتاليات الفاشلة أصغر أو يساوي 4 متتاليات.	**اختبار خوارزمية Rijndael قبل التعديل**			**اختبار خوارزمية Rijndael بعد التعديل**		
	S	**F**	**النتيجة**	**S**	**F**	**النتيجة**
اختبار Frequency (Monobit)	125	3	ناجح	127	1	ناجح
اختبار Frequency Test within a Block	128	0	ناجح	127	1	ناجح
اختبار Runs	127	1	ناجح	128	0	ناجح
اختبار Longest-Run-of-Ones in a Block	128	0	ناجح	128	0	ناجح
اختبار Binary Matrix Rank	128	0	ناجح	127	1	ناجح
اختبار Discrete Fourier Transform (Spectral)	127	1	ناجح	128	0	ناجح
اختبار Non-overlapping Template Matching	128	0	ناجح	128	0	ناجح
اختبار Overlapping Template Matching	128	0	ناجح	126	2	ناجح
ناجح اختبار Maurer's "Universal Statistical"	127	1	ناجح	125	3	ناجح
اختبار Lempel-Ziv Compression	- - -	- -	- - - - -		- - -	- - - - -
اختبار Linear Complexity	126	2	ناجح	127	1	ناجح
اختبار Approximate Entropy	128	0	ناجح	127	1	ناجح
اختبار Cumulative Sums (Cusums)	123	5	فاشل	127	1	ناجح
اختبار Random Excursions Variant	128	0	ناجح	128	0	ناجح
اختبار Serial	128	0	ناجح	127	1	ناجح
اختبار Random Excursions	128	0	ناجح	127	1	ناجح

النتيجة: نلاحظ تجاوز المعمي لكل الاختبارات بنجاح إذ لم تتجاوز عدد المتتاليات الفاشلة الأربع لأجل كل الاختبارات الإحصائية في حين فشلت الخوارزمية الأصلية في تجاوز اختبار **Cusums**.

الاختبارات الإحصائية على البيانات المولدة وفق صياغة High Density Plaintext

الاختبار الإحصائي: عدد المتتاليات المختبرة في هذا النمط هو 128 متتالية طول كل متتالية 1056896 بت والحد الأدنى المقبول الذي يحدد نجاح الخوارزمية هو أن يكون عدد المتتاليات الفاشلة أصغر أو يساوي 4 متتاليات.	اختبار خوارزمية Rijndael قبل التعديل			اختبار خوارزمية Rijndael بعد التعديل		
	S	F	النتيجة	S	F	النتيجة
اختبار Frequency (Monobit)	127	1	ناجح	126	2	ناجح
اختبار Frequency Test within a Block	128	0	ناجح	124	4	ناجح
اختبار Runs	127	1	ناجح	128	0	ناجح
اختبار Longest-Run-of-Ones in a Block	128	0	ناجح	128	0	ناجح
اختبار Binary Matrix Rank	128	0	ناجح	127	1	ناجح
اختبار Discrete Fourier Transform (Spectral)	127	1	ناجح	127	1	ناجح
اختبار Non-overlapping Template Matching	128	1	ناجح	127	1	ناجح
اختبار Overlapping Template Matching	128	0	ناجح	127	1	ناجح
اختبار Maurer's "Universal Statistical"	127	1	ناجح	126	2	ناجح
اختبار Lempel-Ziv Compression	---	--	-----	---	---	---
اختبار Linear Complexity	127	1	ناجح	127	1	ناجح
اختبار Approximate Entropy	128	0	ناجح	127	1	ناجح
اختبار Cumulative Sums (Cusums)	126	2	ناجح	123	5	فاشل
اختبار Random Excursions Variant	128	0	ناجح	124	4	ناجح
اختبار Serial	128	0	ناجح	126	2	ناجح
اختبار Random Excursions	126	2	ناجح	124	4	ناجح

النتيجة: نلاحظ تجاوز المعمي لكل الاختبارات بنجاح ما عدا اختبار **Cusums** حيث بلغت عدد المتتاليات الفاشلة 4<5 .

الاختبارات الإحصائية على البيانات المولدة وفق صياغة 128-Bit Key Avalanche

الاختبار الإحصائي: عدد المتتاليات المختبرة في هذا النمط هو 384 متتالية طول كل متتالية 1048576 بت والحد الأدنى المقبول الذي يحدد نجاح الخوارزمية هو أن يكون عدد المتتاليات الفاشلة أصغر أو يساوي 9 متتاليات.	اختبار خوارزمية Rijndael قبل التعديل			اختبار خوارزمية Rijndael بعد التعديل		
	S	F	النتيجة	S	F	النتيجة
اختبار Frequency (Monobit)	376	8	ناجح	380	4	ناجح
اختبار Frequency Test within a Block	378	6	ناجح	378	6	ناجح
اختبار Runs	378	6	ناجح	378	5	ناجح
اختبار Longest-Run-of-Ones in a Block	382	2	ناجح	382	2	ناجح
اختبار Binary Matrix Rank	381	3	ناجح	382	2	ناجح
اختبار Discrete Fourier Transform (Spectral)	379	5	ناجح	383	1	ناجح
اختبار Non-overlapping Template Matching	384	0	ناجح	383	1	ناجح

اختبار Overlapping Template Matching	384	0	ناجح	379	5	ناجح
اختبار Maurer's "Universal Statistical"	382	2	ناجح	377	7	ناجح
اختبار Lempel-Ziv Compression	----	--	-----	---	--	-----
اختبار Linear Complexity	379	5	ناجح	380	4	ناجح
اختبار Approximate Entropy	378	6	ناجح	378	6	ناجح
اختبار Cumulative Sums (Cusums)	371	13	فاشل	380	4	ناجح
اختبار Random Excursions Variant	351	4	ناجح	365	3	ناجح
اختبار Serial	376	1	ناجح	375	1	ناجح
اختبار Random Excursions	363	2	ناجح	365	2	ناجح

النتيجة: نلاحظ تجاوز المعمي لكل الاختبارات بنجاح إذ لم تتجاوز عدد المتتاليات الفاشلة التسع لأجل كل الاختبارات الإحصائية في حين فشلت الخوارزمية الأصلية في تجاوز اختبار **Cusums**.

الاختبارات الإحصائية على البيانات المولدة وفق صياغة Plaintext Avalanche:

الاختبار الإحصائي: عدد المتتاليات المختبرة في هذا النمط هو 384 متتالية طول كل متتالية 1048576 بت والحد الأدنى المقبول الذي يحدد نجاح الخوارزمية هو أن يكون عدد لمتتاليات الفاشلة أصغر أو يساوي 9 متتاليات.	**اختبار خوارزمية Rijndael قبل التعديل**			**اختبار خوارزمية Rijndael بعد التعديل**		
	S	**F**	**النتيجة**	**S**	**F**	**النتيجة**
اختبار Frequency (Monobit)	381	3	ناجح	379	5	ناجح
اختبار Frequency Test within a Block	379	5	ناجح	380	4	ناجح
اختبار Runs	380	4	ناجح	379	5	ناجح
اختبار Longest-Run-of-Ones in a Block	381	3	ناجح	379	5	ناجح
اختبار Binary Matrix Rank	380	4	ناجح	380	4	ناجح
اختبار Discrete Fourier Transform (Spectral)	379	5	ناجح	381	3	ناجح
اختبار Non-overlapping Template Matching	381	3	ناجح	381	3	ناجح
اختبار Overlapping Template Matching	378	6	ناجح	378	6	ناجح
اختبار Maurer's "Universal Statistical"	380	4	ناجح	382	2	ناجح
اختبار Lempel-Ziv Compression		--	-----			ناجح
اختبار Linear Complexity	377	7	ناجح	383	1	ناجح
اختبار Approximate Entropy	384	0	ناجح	378	6	ناجح
اختبار Cumulative Sums (Cusums)	377	7	ناجح	373	10	فاشل
اختبار Random Excursions Variant	381	3	ناجح	380	4	ناجح
اختبار Serial	380	4	ناجح	378	6	ناجح
اختبار Random Excursions	382	2	ناجح	380	4	ناجح

النتيجة: نلاحظ تجاوز المعمي لكل الاختبارات بنجاح إذ لم تتجاوز عدد المتتاليات الفاشلة التسع لأجل كل الاختبارات الإحصائية.

مناقشة النتائج

من الواضح أن المعمي لم يفقد مناعته بالنسبة للهجمات التقليدية إن لم نقل: إنه حقــق بعض التقدم في بعض الاختبارات. وأما بالنسبة لمناعته ضد الهجمات الجبرية فلم نستطعْ تقييم مدى زيادة هذه المناعة بدقة لعدم توافر معايير قياسية لهذا الأمر، لكن لدينا أســباب

تجعلنا نعتقد أن التعديل الذي قمنا به زاد من تعقيد الهجوم الجبري (ناقشنا هذا الأمر في الفقرة 5.1).

ربما من المفيد دراسة الأثر الدقيق لاستخدام المولد العشوائي (دالة المزج وحيدة الاتجاه) في مناعة الخوارزمية ضد الهجمات وهو أمر نعمل حالياً عليه.

كما أننا قمنا باستخدام جدول تبديل عشوائي (تخلط كامل محتوياته عشوائياً) بدل جدول التبديل الديناميكي الذي استخدمناه في هذا البحث، ونعمل حالياً على دراسة تأثر مناعة الخوارزمية ضد الهجمات التقليدية لنقارن قوة الخوارزمية في الحالات الثلاث (عندما تستخدم جدول تبديلٍ ثابتاً، ثم جدول تبديلٍ ديناميكياً و أخيراً جدول تبديلٍ عشوائياً).

REFERENCES

1. Daemen, J., and Rijmen, V. (2001). "The Design of rijndael AES – The advanced encryption standard", Springer.
2. "Announcing the advanced encryption standard (AES)",Federal Information Processing Standards Publication 197, 2001 URL:http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf
3. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., and Dray, J. (2001)."A statiistiical test suiite for random and pseudorandom number generators for cryptographiic appliicatiions", URL:http://www.csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf
4. Soto, J. (2001). "Randomness testing of the AES candidate algorithms affiliation national institute of standards and technology" URL:http://www.csrc.nist.gov/encryption/aes/round1/r1-rand.pdf.
5. Courtois, N. T., and Pieprzyk, J. (2002). "Cryptanalysis of block ciphers with overdefined systems of equations". URL:http://www.citeseer.ist.psu.edu/courtois02cryptanalysis.html
6. Courtois, N. T., Debraize, B., and Garrido, E. (2002). "on exact algebraic [non-]immunity of s-boxes based on power functions?" URL:http://www.citeseer.ist.psu.edu/courtois05exact.html.
7. Courtois, N. T. (2003). "General principles of algebraic attacks and new design criteria or cipher components" URL:http://www.citeseer.ist.psu.edu/744066.html
8. Keliher, L., and Meijery, y.H. (1996). "A new substitution-permutation network cipher using key-ependent S-Boxes" URL:http://www.citeseer.ist.psu.edu/keliher97new.html.
9. Nyber, K. (1994). "Differentially uniform mappings for cryptography" URL:http://www.citeseer.ist.psu.edu/canteaut97differential.htm.
10. Merkle, R. C. (1989). "A software encryption function" URL:http://www.security-protocols.com/textfiles/cryptography/merkle.txt.
11. Ritter, T. (1990). "Substitution cipher with pseudo-random shuffling: The dynamic substitution combiner" URL:http://www.ciphersbyritter.com/ARTS/DYNSUB2.HTM.
12. Macchetti, M. (2001). "Characteristics of key-dependent S-Boxes: the case of Twofish" URL:http://www.citeseer.ist.psu.edu/macchetti05characteristics.html.
13. Skrenta, R. (1995). "MD5-based random number generator" URL: http://www.pbm.com/dice/random.html.