مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الأساسية المجلد (29) العدد (4) 2007
Tishreen University Journal for Studies and Scientific Research- Basic Sciences Series Vol. (29) No. (4) 2007

دراسة تحليلية ومقارنة لأشهر خوارزميات التعمية المتناظرة

الدكتور محمد حسن [*]
الدكتور معتصم شفا عمري [**]
بسيم برهوم [***]

(تاريخ الإيداع 23 / 5 / 2007. قُبِل للنشر في 2007/7/24)

□ الملخّص □

مع دخول الحواسيب ونظم المعلومات جميع ميادين الحياة المعاصرة، أصبح أمن المعلومات من المتطلبات الأساسية لبناء منظومة أتمتة حاسوبية (كالنظم المصرفية، والتجارة الإلكترونية، والنظم الإدارية، وغيرها)، وتعدّ خوارزميات التعمية المتناظرة النواة الأساسية لأية منظومة حماية، لذلك فإن عملية اختيار خوارزمية التعمية المتناظرة (المتماثلة) ذات السوية الأمنية العالية والأداء الأفضل مهمة صعبة، ومن هنا فقد ركزنا في بحثنا هذا على تقديم نتائج دراسة مقارنة لأهم خوارزميات التعمية المتناظرة، إذ يتناول هذا البحث دراسة تحليلية ومقارنة لأشهر خوارزميات التشفير المتماثل العالمية Rijndael، Mars، IDEA، Blowfish، (حيث أن خوارزمية Rijndael هي المقياس الدولي الحالي للتشفير AES) وذلك من خلال مقارنات جديدة تشمل أهم النواحي النظرية والعملية التطبيقية للخوارزميات المذكورة من حيث الأمن ومستوى الأداء، وصولاً إلى استخلاص معايير مناسبة للاستخدام في بيئات مختلفة تمنع استغلال الثغرات الأمنية.

الكلمات المفتاحية: خوارزميات التعمية (التشفير)، التعمية الرزمية، التعمية المتناظرة (المتماثلة)، أمن المعلومات، المقياس الدولي للتشفير AES، تحليل خوارزميات التعمية.

[*] رئيس قسم الرياضيات – كلية العلوم – جامعة تشرين – اللاذقية – سورية.
[**] باحث رئيسي في المعهد العالي للعلوم التطبيقية والتكنولوجيا – دمشق – سورية. ورئيس أقسام علم الحاسوب وهندسة البرمجيات ونظم المعلومات – كلية تكنولوجيا المعلومات– الجامعة الدولية الخاصة للعلوم والتكنولوجيا IUST– درعا– سورية.
[***] طالب ماجستير – معلوماتية – كلية العلوم – جامعة تشرين – اللاذقية – سورية.

مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الأساسية المجلد (29) العدد (4) 2007
Tishreen University Journal for Studies and Scientific Research- Basic Sciences Series Vol. (29) No. (4) 2007

An Analytical Studies and Comparison of Symmetric Block Cipher Algorithms

Dr. Mohamad Hassan [*]
Dr. Moutasam Shafa Amry [**]
Baseem Barhoum [***]

(Received 23 / 5 / 2007. Accepted 24/7/2007)

□ ABSTRACT □

Computers and information systems involve all areas of contemporary life. Therefore, information security has become a fundamental requirement for building any network application or automation system (banking, e-commerce, and administrative systems, ERP, etc.). The asymmetric algorithms are the core of any protection system. So the selection of a good asymmetric algorithm, with high security and performance, is a difficult, but important task.

This search focuses on the best known algorithms to provide an analytical and comparative study of the most important asymmetric encryption algorithms, implemented in some protocols and organizations (e.g. Rijndael-AES, Mars, IDEA, and Blowfish). The comparisons include the most important aspects of new theoretical and practical applications of the algorithms listed in order to draw the appropriate standards for use in different settings to prevent the exploitation of the security gaps. We provide a short review of each algorithm, types of attacks on symmetric algorithms, security evaluation, performance and timing comparison.

Keywords: Encryption Algorithms, AES, Symmetric Encryption, Information Security, Cryptanalysis.

[*] **Professor, Department of Mathematic, Faculty of Sciences ,Tishreen University, Lattakia, Syria.**
[**] **Professor, Higher Institute for Applied Sciences and Technology, Damascus, Syria & Head of the Computer Science and Software Eng. Departments, Faculty of IT, IUST University, Daraa, Syria.**
[***] **Postgraduate Student, Informatics Department, Faculty of Science ,Tishreen University, Lattakia, Syria**

مقدمة:

يعدّ التوجه حالياً نحو الاعتماد على نظم المعلومات والشبكات الحاسوبية في جميع الميادين الاقتصادية والاجتماعية والعسكرية وحتى الشخصية منها. ولتأمين الخصوصية والأمن للمعلومات المخزنة أو المتبادلة عبر الشبكات السلكية واللاسلكية لا بد من استخدام تقانات التعمية. إذ لا يمكن للمؤسسات المالية التعامل فيما بينها أو مع زبائنها دون تأمين المستوى اللازم من الحماية، ولا يمكن بناء نظم التجارة الإلكترونية E-Commerce أو تقديم الخدمات عبر منظومات الحكومة الإلكترونية E-Government دون توفير مستوى الأمن المطلوب. وتعدّ خوارزميات التعمية ذات المفتاح الوحيد أو المتناظرة (Symmetric Algorithms) من أهم البنى التي تدخل في تصميم نظم الحماية. ولا تعتبر الخوارزميات المتناظرة حديثة العهد بل هي مفهوم قديم للحماية، إلا أنها تتطور مع الزمن، وبحسب متطلبات وحاجات الاستخدام. لقد شهد العقدان الأخيران اهتماماً كبيراً من قبل المؤسسات البحثية والمعيارية في تطوير وتصميم العديد من خوارزميات التعمية المتناظرة الحديثة، وبرزت في الوجود عدة خوارزميات للتعمية المتناظرة اعتمدت الهيئات الدولية بعضها مثل AES، إلا أن بعض المؤسسات والجهات العلمية والتجارية اعتمدت خوارزميات أخرى في تطبيقاتها. ومع الانتقال السريع إلى أتمتة أمور الحياة اليومية أصبح لزاماً علينا أن نخوض في تفاصيل علم التعمية (التشفير) من أجل الحفاظ على استقلالية أمنية مقبولة، ومن أجل مجابهة المشاكل التي ستظهر بشكل أساسي من الاستخدام المكثف للتقانات الجديدة سواء على المستوى الفردي أو المؤسساتي (مثل: التقنيات المصرفية وتقنيات الاتصالات، والبريد الإلكتروني، والتجارة الإلكترونية وكذلك خدمات الحكومة الإلكترونية). من هنا تبرز أهمية البحث في مجال التشفير ومنهجيته وخوارزمياته وتحليلها بشكل علمي دقيق يخدم عملية الوصول إلى استخدام فعال وآمن لتلك المشفرات التي لا يخلو منها أي جهاز الكتروني حديث أو تطبيقات عصرية لخدمات الحاسوب والاتصالات، ثمّ العمل على سد الثغرات الأمنية المقصودة أو غير المقصودة التي تحويها هذه المشفرات من خلال تصنيف المعلومات في مستويات أمنية مناسبة وإيجاد المشفر المناسب للعمل في كل مستوى ومجال، وبناء الخبرات المحلية في هذا المجال.

أهمية البحث وأهدافه:

تبرز أهمية البحث في دراسة واختيار المشفرات المناسبة التي تعتمد الخوارزميات المتناظرة لبناء القدرة التحليلية والمعرفة العلمية السليمة لطرق تصميم هذه الخوارزميات، وتقدم الدراسة المقارنة نتائج تساعد الجهات الراغبة في اختيار نظام التعمية المناسب من حيث خصائصه وتوافقه مع البيئة والحاجات والأغراض العملية المطلوبة (مستوى السرية والأداء والسرعة والسهولة)، مع إبراز بنية و آلية عمل أهم وأحدث هذه النظم، ممّا يسمح بتطويرها مستقبلاً لتحقيق الاستقلالية الأمنية بالاستغناء عن الأنظمة الأمنية الجاهزة المستوردة. ويهدف البحث بشكل أساسي إلى:

1- إجراء دراسة شاملة لأهم خوارزميات التعمية المتناظرة.
2- استعراض أنواع الهجوم التي تتعرض لها نظم التعمية.
3- دراسة مستوى الأمن في كل من الخوارزميات التي تم انتقاؤها في هذا البحث.
4- دراسة مستوى أداء كل منها.
5- مقارنة النتائج واستخلاص مزايا ونقاط الضعف في كل منها و شروط عملها و قواعد الحماية اللازمة.

وتكمن أهمية البحث في تقديم دراسة شاملة تصبح مرجعية للجهات الراغبة في مقارنة خصائص خوارزميات التعمية المتناظرة الحديثة، واختيار الأنسب في تطبيقاتها وكذلك بناء الخبرة الوطنية في هذا المجال. جرى هذا

البحث في مخابر المعهد العالي للعلوم التطبيقية والتكنولوجيا بدمشق وفي كلية العلوم بجامعة تشرين خلال العام 2006-2007.

أولاً: دراسة خوارزميات التعمية المتناظرة:

يتألف نظام التعمية المتناظر Symmetric Cipher System بشكل عام من ثلاثة مكونات أساسية، وهي: (1) خوارزمية تعمية encryption algorithm و(2) خوارزمية فك التعمية decryption algorithm و(3) خوارزمية توليد المفاتيح الجزئية، أو ما تعرف بخوارزمية توسعة المفتاح key expansion algorithm، وهي الخوارزمية التي تقوم بتوليد مفاتيح جزئية من المفتاح الذي يدخله المستثمر أو ما يعرف بالمفتاح السري، بحيث يتم من خلال هذه المفاتيح الجزئية التأثير على كل خانة من الخانات الثنائية bits للنص في كل دورة (تكرار Iteration) من التكرارات المعتمدة في بنية خوارزمية التعمية/أو فك التعمية.

من أهم معاملات التعمية المتناظرة: (1) طول المفتاح الذي تدعمه الخوارزمية، (2) وحجم الكتلة (الحزمة) Block size الذي تعمل عليه الخوارزمية سواء في التعمية أو في فك التعمية، (3) العدد الفعلي للتكرارات في بنية الخوارزمية. وتختلف خوارزميات التعمية المتناظرة عن بعضها في هذه البنود الثلاثة إضافة إلى البنية الداخلية لتوابع الاستبدال والتحويل الداخلة في صلب تصميمها. وقد اخترنا مجموعة من أشهر الخوارزميات المتناظرة في هذه الدراسة، وهي الخوارزميات التالية: خوارزمية بلوفيش Blowfish و خوارزمية IDEA، وخوارزمية مارس Mars، إضافة إلى خوارزمية ريجندايل Rijndael، وسوف نبين لاحقاً أسباب اختيارنا لهذه الخوارزميات دون غيرها للدراسة والمقارنة، وسوف نبين كذلك مزايا وخصائص كل منها.

توجد العديد من الدراسات التي تقوم على دراسة خصائص خوارزمية معينة، أو اختيار بعض من هذه الخوارزميات للمقارنة في بعض خصائصها، كالسرعة في التنفيذ، أو حجم الذاكرة المطلوب للخوارزميات المختارة ولهدف معين، ولكن لا توجد حتى الآن دراسة شاملة تقارن الخوارزميات المختارة معاً، لذلك هدفنا في هذا البحث إلى تقديم دراسة مقارنة شاملة لهذه الخوارزميات معاً، علماً أن جميع هذه الخوارزميات قد اعتمدت في الواقع العملي للحماية، بشكل أو بآخر بناء على رغبة بعض الجهات التجارية ووجهة نظرها الخاصة أو في بنى نظم تعمية شبكية معيارية.

1- خوارزمية ريجندايل Rijndael

لقد اخترنا خوارزمية ريجندايل Rijndael من ضمن الخوارزميات التي نقوم بتقييمها لأنها الخوارزمية المعيارية الحديثة، والتي أطلق عليها فيما بعد اسم AES: Advanced Encryption Standards، إذ اعتمدت عالمياً لأن تكون المعيار التجاري كخوارزمية للحماية من قبل NIST في الولايات المتحدة الأمريكية، وتمت التوصية بها أوروبياً للتعمية من قبل NESSIE: New European Schemes for Signature)، (Integrity and Encryption، وكذلك من قبل CRYPTREC الهيئة المسؤولة في اليابان. وتعود تسمية الخوارزمية إلى أسماء مصمميها Rijndael (Rijmen&Daemen) [1].

وهي خوارزمية حزمية Block Cipher تعمل بطول مفتاح وطول حزمة متعددين (128، 192، 256) خانة ثنائية، وتعتمد شكلياً المصفوفات في خطوات عملها [1]، وتقوم على تكرار عدة خطوات عدداً من المرات (عدد التكرارات تابع لطول المفتاح ولطول حزمة النص) وعدد التكرارات في الخوارزمية هو:

- 10 تكرارات إذا كان طول كل من المفتاح والحزمة 128 خانة ثنائية.
- 12 تكرار، إذا كان طول المفتاح أو طول الحزمة 192 خانة ثنائية.
- 14 تكرار، إذا كان طول المفتاح أو طول الحزمة 256 خانة ثنائية.

وبشكل عام تتكون خوارزمية Rijndael من قسمين أساسين هما:1- **معالجة ثمانيات النص (استبدال وإزاحة ومزج استبدالي وإضافة المفتاح الخاص بالمرحلة).2- معالجة عملية توليد المفاتيح المستخدمة في مراحل الخوارزمية من المفتاح الأساسي.** وتميزت هذه الخوارزمية باعتمادها على مفهوم جبر المصفوفات في عملها وبعدم الاعتماد في تكراراتها على مبدأ Feistel 2 Network المعتمد في أغلب خوارزميات التعمية المتناظرة.

1-معالجة ثمانيات (Bytes) الحزمة: تعمل الخوارزمية في معالجة ثمانيات الحزمة بحسب الخصائص التالية:

- طول الحزمة (16أو 24 أو 32) ثمانية (Bytes) تتوزع ضمن مصفوفة من أربعة أسطر وعدد من الأعمدة يتناسب مع طول الرزمة، كما في الشكل التالي:

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$

الشكل رقم (1) يبين توزيع ثمانيات الدخل في خوارزمية Rijndael

هذا التنوع في طول الحزمة يجعلها مناسبة للتطبيقات المختلفة سواء بشكل برمجي أو عتادي.

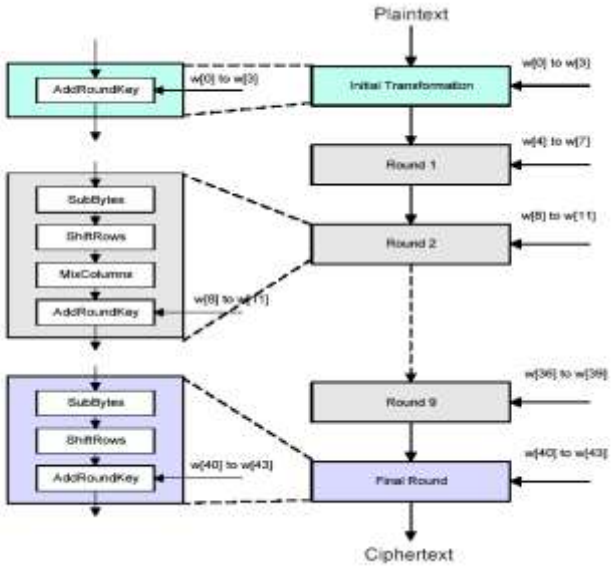
- وتعتمد في تصميمها على عدد من التكرارات، وكل تكرار مؤلف من أربع مراحل هي:

1. مرحلة الاستبدال على مستوى الثمانية (ByteSub) باستخدام صندوق التعويض S-box: وهو تابع غير خطي.
2. مرحلة الإزاحة في الأسطر ShifRow وهي عملية نثر داخلية للأعمدة
3. مرحلة المزج في الأعمدة MixColumn وذلك باستخدام ضرب عمود بمصفوفة استبدال محددة تودي إلى النثر ضمن الأعمدة.
4. مرحلة مزج الحزمة مع المفتاح الجزئي: وذلك في عملية جمع منطقي X-or لعناصر مصفوفة النص وعناصر مصفوفة المفتاح، أي AddRoundKey إذ تبدأ به الخوارزمية وتنتهي معه أيضاً.

أما في عملية فك التشفير وفق خوارزمية Rijndael، فنستخدم نفس الخطوات السابقة مع عكس تتاليها، مع استبدال مصفوفة مزج الأعمدة MixColumns بعكسها واستبدال الصندوق S-box بعكسه، ويبين الشكل رقم (2) المخطط العام للخوارزمية.

1- مصفوفة المفتاح ومصفوفة النص بأربعة أسطر وعدد أعمدة متغير وتابع لطول المفتاح وطول الحزمة.

2 -Feistel Network (استخدام نصف حزمة البيانات من أجل تعديل النصف الأخر من الحزمة ومن ثم مبادلة النصفين).



الشكل رقم (2) يبين الشكل العام لخوارزمية AES

2-توليد المفاتيح الجزئية Key Schedual: تعتمد خوارزمية توليد المفتاح في Rijndael على مفتاح أساسي مكون من 128خانة ثنائية 3 يتوزع ضمن مصفوفة بأربعة أسطر وأربعة أعمدة، وتتم عملية توليد 10 مفاتيح فرعية لاستخدامها في مراحل الخوارزمية، وذلك من خلال سلسلة من عمليات الاستبدال والنثر4 على المصفوفات الأساسية و المفتاح الأساسي مع اعتماد صناديق تعويض محددة.

2- خوارزمية بلوفش BLOWFISH:

تعدّ هذه الخوارزمية من الخوارزميات التي تتمتع بسهولة في التنفيذ البرمجي والعتادي وذات سوية أمنية وسرعة أداء عالية. وهي معتمدة حالياً في نواة نظام التشغيل Linux، وتعتبر نواة لخوارزمية 5Twofish التي ظهرت بديلاً عنها فيما بعد، و هي خوارزمية تشفير حزمية بطول 64 خانة ثنائية للحزمة الواحدة وتعتمد على مفتاح متغير الطول. كما أنها تعتمد على مبدأ Feistel Network في التصميم وتتكون من 16 تكراراً، وكذلك تعتمد تقنية التبييض (Whitening)6 في بدء ونهاية الخوارزمية، ومصممة من شقين أساسيين هما: **1- معالجة الرزم. 2- توليد المفاتيح الجزئية اللازمة انطلاقاً من المفتاح السري.**

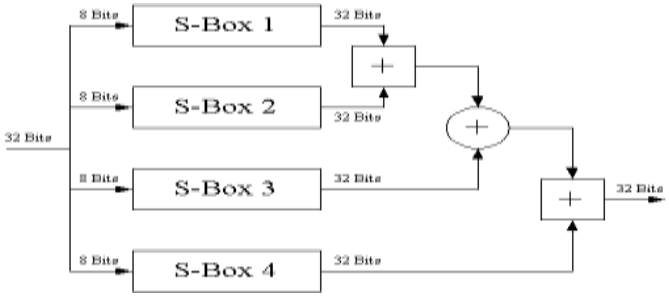
1- معالجة الرزم في خوارزمية بلوفش: تقوم خوارزمية Blowfish بتشفير البيانات وفق مخططFeistel Network في التصميم، ويعتمد تابع التحويل F في كل تكرار على عمليات استبدال باستخدام أربعة صناديق تعويض مدروسة بحيث تحقق النثر بشكل جيد، ومخارج هذه الصناديق مترابطة بعمليات الجمع، والجمع الثنائي X-or كما يبينه الشكل التالي:

3 – المفتاح بطول 128 أو 192 أو 256، ولنعتبر الحالة الأولى من أجل التوضيح.

4 – نثر الخانات الثنائية الزائدة من النص الأصلي في مختلف أنحاء النص المشفر باستخدام التبديل وتغيير المواقع لمنع المهاجم من الحصول على استنتاجات منطقية من خلال دراسة النص المشفر

5- خوارزمية حزمية متطورة تعمل على حزمة من 128 bit وطول مفتاح متغير ومكونة من 16 تكرار، وقد رُشحت لتكون معيارية

6 – مزج المفاتيح الفرعية مع حزمة البيانات في الخطوتين الأولى والأخيرة من الخوارزمية.

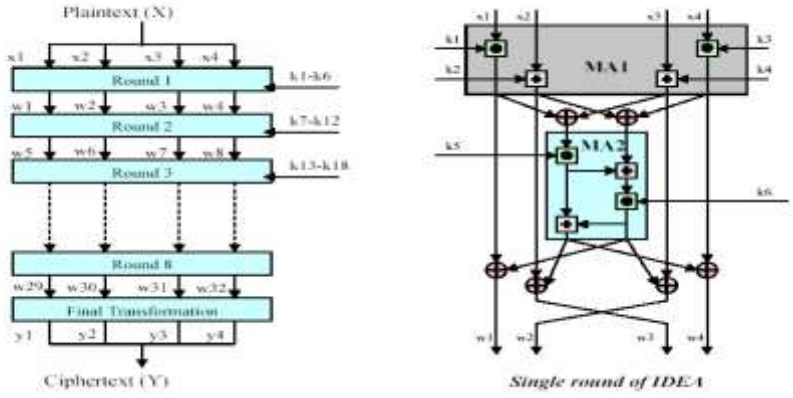


الشكل رقم (3) يبين الشكل البنية الداخلية للتابع F في خوارزمية Blowfish

2- توليد المفاتيح الجزئية Key Schedual: تستخدم خوارزمية بلوفش 18 مفتاحاً جزئياً كل منها مؤلف من 32 خانة ثنائية تحسب قبل البدء بعملية معالجة الرزم والتشفير. وتولد هذه المفاتيح من خلال توليد مصفوفة المفاتيح الجزئية اعتماداً على المفتاح الأساسي وإجراء مجموعة من عمليات النثر والاستبدال باعتماد مجموعة محددة من صناديق الاستبدال (التعويض) بحيث يحوي كل صندوق 256 عنصر كل منها مؤلفٌ من 32-bits. لمزيد من المعلومات حول الخوارزمية يمكن الإطلاع [2, 3] .

3- خوارزمية IDEA

تم اختيار هذه الخوارزمية لكونها تمتاز بطريقة مختلفة وجديدة لاستخدام مبدأ Feistel Network إذ تمزج جميع الكتل الجزئية ضمن تكرار واحد، ومن ثَمّ اختصرت عدد التكرارات المطلوبة للوصول إلى السوية الأمنية في التعمية، وهي الخوارزمية الأولى التي استخدمت التوابع الرياضية كالجمع والضرب في بنية تابعها الاستبدالي والتي اعتمدت فيما بعد في الخوارزميات الأخرى، وهي أول خوارزمية رشحت خلال التسعينات لتكون مقترحاً لخوارزمية معيارية إذ أطلق عليها أسم PES Proposed Encryption Standard، وتعتبر IDEA خوارزمية حزميه بطول 64 bit للحزمة الواحدة، وتعتمد بشكل أساسي على مبدأ التشويش ومبدأ النثر، وتصميمها يقوم على مزج بين ثلاث زمر جبرية الجمع الثنائي($\oplus$)، والجمع بالمقاس(2^{16} Mod) + ،والضرب بالمقاس($2^{16}+1$ Mod) $\otimes$ وتمثل العمليات الثلاثة السابقة صندوق تعويض الخوارزمية، وتطبق ،على حزم جزئية بطول 16خانة ثنائية، وتعتمد هذه الخوارزمية على مفتاح أساسي بطول128 خانة ثنائية كما أنها تستخدم للتشفير ولفك التشفير، وقد صممت بمراحلها وتعديلاتها من قبل كل من Xuejial Lai و James Massey في عام 1991 وهي مسجلة في أوربا وفي الولايات المتحدة الأمريكية، ولكن يمكن استخدامها مجاناً لأغراض متعددة ويمكن الحصول على رخصة استخدام تجاري لها.



الشكل رقم (5) يبين مخطط خوارزمية IDEA، والبنية الداخلية لتكرار واحد ضمن الخوارزمية

توليد المفاتيح الجزئية Key Schedual:كما ذكرنا سابقاً تعتمد الخوارزمية على مفتاح أساسي بطول 128 خانة ثنائية، ومن هذا المفتاح الأساسي يتم توليد 52 مفتاحاً فرعياً بطول 16 خانة ثنائية لكل مفتاح، تستخدم كل مرحلة من مراحل الخوارزمية الثمانية 6 مفاتيح فرعية وأربعة مفاتيح لإجراء تحويل الخرج النهائي. أما عملية توليد المفاتيح الفرعية فتتم على الشكل التالي: 1- يقسم المفتاح الأساسي المكون من 128 خانة ثنائية إلى 8 مفاتيح فرعية طول كل منها 16 خانة ثنائية، نستخدم منها6 مفاتيح في المرحلة الأولى والمفتاحين P_7 و P_8 في المرحلة الثانية.

2 – يزاح المفتاح الأساسي دورانيا نحو اليسار بمقدار 25 بت.

3- نكرر الخطوة الأولى فنحصل على ثمانية مفاتيح فرعية جديدة، نستخدم منها أربعة مفاتيح في المرحلة الثانية وتبقى أربعة مفاتيح للمرحلة الثالثة وهكذا.

4 – نكرر الخطوة 2 بإزاحة المفتاح الأساسي يساراً بمقدار 25 خانة ثنائية وتقسيمه إلى ثمانية مفاتيح، وهكذا حتى نهاية المرحلة الثامنة من الخوارزمية. للمزيد من المعلومات عن بنية الخوارزمية [2].

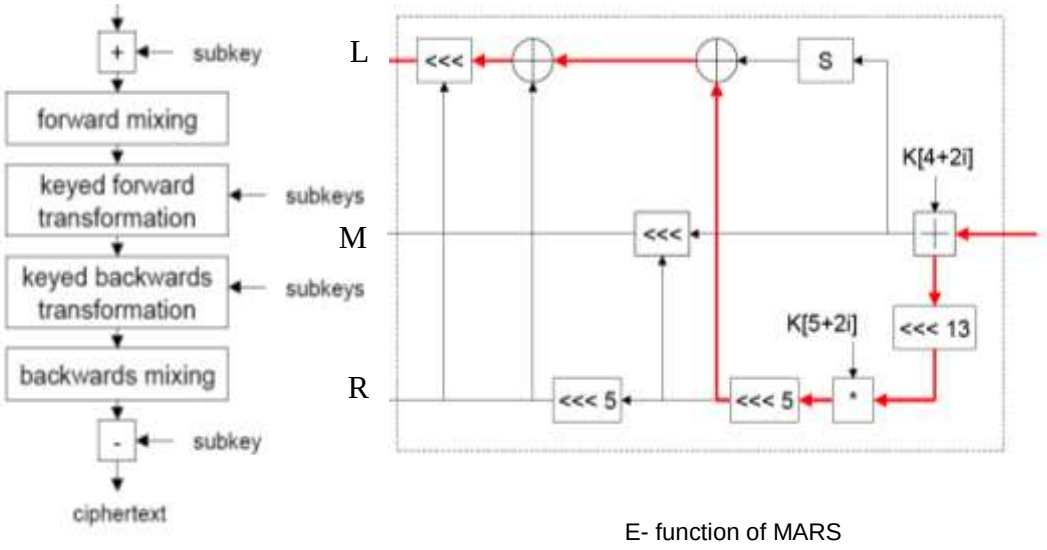
4- خوارزمية MARS

هي إحدى الخوارزميات التي رشحت لتكون خوارزمية معيارية دولية، كما أنها مصممة بشكل يمكنها العمل على حواسيب اليوم وعلى حواسيب ذات معماريات أكثر تطوراً، وتجمع هذه الخوارزمية بين السرعة والقوة والمرونة، هي خوارزمية حزمية تعمل على حزمة بطول 128 خانة ثنائية مقسمة إلى أربع كلمات بحجم 32 خانة ثنائية للكلمة الواحدة، وتعتمد الخوارزمية طول مفتاح متغير، وهي مشفر متماثل بحيث غالباً ما يكون النصف الأخير من التكرارات صورة عكسية للنصف الأول،. تلعب مجموعة التكرارات الأولى والأخيرة دوراً مختلفاً عن دور مجموعة التكرارات الوسطى، وتعتمد مبدأ Feistel Network. وتستخدم الخوارزمية عمليات الجمع + والطرح – والجمع الثنائي $\oplus$ لمزج قيم كلمات البيانات مع قيم كلمات المفتاح، وعمليات جدولية لزيادة درجة أمان الخوارزمية، إذ يُستخدم جدول S-box مكون من 512 كلمة مكونة من 32 خانة ثنائية أو جدولين كل منهما يحوي 256 كلمة من 32 خانة ثنائية ويجب اختيار الصندوق S-box بشكل جيد لتحسين أداء الخوارزمية ولاسيما في وجه الهجوم التفاضلي. تتكون خوارزمية Mars من قسمين أساسيين:

1- معالجة الرزم في خوارزميةMARS: وتتضمن التحويلات الأمامية والخلفية وتتكون هذه الخطوة من 16تكراراً من التحويلات المزودة بمفاتيح، و16 تكراراً مزج دون مفاتيح تُنجز بشكل يضمن التشفير وفك التشفير بنفس القوة، حيث أول ثمانية تكرارات تكون من النمط الأمامي (Forwards) والثماني تكرارات الأخرى من النمط الخلفي (Backwards). وتستخدم مصفوفة المفتاح الموسع وتتكون من 40 كلمة كل منها بطول 32 خانة ثنائية.كما تستخدم صندوق تعويض S-box مكوناً من 512 كلمة كل منها بطول 32 خانة ثنائية ونرمز لأول 256 خانة ثنائية من الصندوق بالرمز S_0 ولآخر 256 خانة بالرمز S_1.

2- توليد المفاتيح الجزئية Key Schedual: يتم ترتيب المفتاح في مصفوفة []K مكونة من n كلمة وكل كلمة مكونة من 32 خانة ثنائية وبحيث $4 \leq n \leq 39$. نوسع هذه المصفوفة إلى مصفوفة []K تحوي 40 كلمة كل منها مكونة من 32 خانة ثنائية وبشكل يضمن لنا أن كلمات المفتاح المستخدمة في عمليات الجداء في التشفير يجب أن تحقق الخاصتين الآتيتين: (a) الخانتان الثنائيتان الأقل قيمة(الواقعتان في اليمين) في كل كلمة هما واحد واحد (11)، (b) لا تحوي أية من كلمات المفتاح عشر واحدات متتالية أو عشرة أصفار متتالية.

الشكل التالي يبين البنية العامة لخوارزمية MARS:



الشكل رقم (6) يبين البنية العامة لخوارزمية MARS والتابع E.

لمزيد من المعلومات يمكن الإطلاع [4]. يمكننا استنتاج خلاصة دراسة الخوارزميات وتلخيص هذه الخوارزميات من حيث المواصفات الأساسية لكل منها ومبدأ عملها في الجدول التالي:

الجدول رقم (1) يبين مقارنة عامة للبنية الأساسية للخوارزميات المدروسة، ومبدأ عمل كل منها.

الخوارزمية	طول الحزمة	طول المفتاح	عدد المفاتيح الفرعية	طول المفتاح الفرعي	عدد التكرارات	مبدأ العمل
MARS	128بت 32 X 4*	متغير7	1 موسع	n كلمة*** ب 32 bit	32	Fiestel وتستخدم المصفوفات في التشفير وفي إعداد المفتاح
RIJNDEAL	متغير8	متغير9	متغير10	متغير11	متغير12	المصفوفات حيث توزع حزمة النص والمفتاح على شكل مصفوفة من أربع أسطر وأعمدة (4,6,8)
BLWOFISH	64 بت	متغير13	18	32 بت	18	شبكة Fiestel مع تطبيق تابع يتضمن تعويض يعتمد على المعطيات والمفتاح ومن تبديل يعتمد على المفتاح
IDEA	64بت** 4 X 16	128بت	52	16 بت	8	مزج زمر جبرية تستخدم العمليات $\oplus, \otimes, +$

7. من 128 bit إلى 1248 bit.

*** حيث 39=> N >=4، يتم توسيعه إلى 40 كلمة من 32 بت

*- طول حزمتها 128 بت مقسمة إلى أربع أجزاء بطول 32 بت للجزء.

8- طول الحزمة 128 أو 192 أو 256 بت.

9- طول المتاح 128 أو 192 أو 256 بت.

10- تابع لطول المفتاح ولطول الحزمة ويساوي عدد التكرارات.

11- تابع لطول المفتاح ولطول الحزمة (عدد أعمدة مصفوفة المفتاح وعدد أعمدة مصفوفة الحزمة).

12- تابع لطول المفتاح ولطول الحزمة (10 أو 12 أو 14 تكرار).

13- يمكن أن يصل طول المفتاح حتى 448 بت.

**- طول حزمتها 64 بت مقسمة إلى أربع أجزاء بطول 16 بت للجزء.

بعد أن تم استعراض بنى وخصائص الخوارزميات سوف نستعرض بعض أنواع الهجوم الحديثة التي يمكن أن تتعرض لها خوارزميات التعمية الحزمية المتناظرة.

ثانياً: أنواع الهجوم على الخوارزميات Types of Attacks

لمعرفة سوية الأمن لدى أي من خوارزميات التعمية، لابد من استعراض وتعريف الطرق الحديثة للهجوم والتي يمكن أن تتعرض لها أية من هذه الخوارزميات، إضافة للأنواع التقليدية القديمة والمعروفة مثل (الهجوم بالنص المشفر المختار Chosen - Ciphertext Attack والهجوم بالنص الواضح المختار Chosen-Plaintext Attack والهجوم التفاضلي Differential Cryptanalysis والهجوم التفاضلي المختزل Truncated-Differential Attack والهجوم التحليلي التفاضلي المستحيل Impossible Differential Cryptanalysis Attack والهجوم التخطيطي المتناثر الموسع XSL: Extended Sparse Linearization وهجوم جدولة المفاتيح Key Schedule Attack)[14]

1. **<u>الهجوم الزمني Timing attack:</u>**

هجوم فعال ضد العمليات التي تُنجز بقيم مختلفة من الزمن ،ويستخدم المعايير الزمنية في أثناء تنفيذ الخوارزمية من أجل الحصول على معلومات عن المفاتيح ويستغل خصائص الخوارزمية والأشكال التنفيذية المرتبطة مع تلك الخصائص من أجل صد هذا الهجوم، ويجب الحرص على أن تحدث كل عملية ضمن التشفير وفك التشفير بقيمة زمنية واحدة [7]، ومن الوسائل الهامة للدفاع في وجه هذا الهجوم حذف التفرعات من البرنامج التنفيذي.

2. **<u>هجوم القوى (الطاقة) Power attack:</u>**

فعال ضد العمليات التي تستخدم كميات مختلفة من الطاقة وذلك اعتماداً على نماذج الضعف التدريجي للطاقة التي يمكن أن تُنفذ حسب موقع العملية وظروفها[7]، إذ أن الطاقة المستهلكة وعدد الواحدات في المفتاح الفرعي يعطيان معادلة تتضمن متحولا ت مستقلة تعبر عن ثنائيات المفتاح الأساسي. لصد هذا النوع من الهجمات نستخدم مبدأ التوازن البر مجي (Software balancing) وذلك لجعل الطاقة الكلية المستهلكة في حالة تعادل، ونحصل على التوازن البرمجي بترتيب البيانات المعالجة بعملية أساسية واحدة بشكل متقارب زمنياً قدر الإمكان لأن ذلك يقلل معلومات الارتباط بين الثنائيات Bits. ويكون هذا الهجوم فعالاً أمام العمليات التي تستهلك قوى مقنعة (Masked)[15] عند تنفيذ العملية مرتين، لذلك يجب أن يكون استهلاك الطاقة غير مرتبط مع بيانات المفتاح أو مع بيانات الدخل والخرج.

---

[14] أنواع معروفة من الهجمات التقليدية التي تتعرض لها خوارزميات التشفير، حيث كل نوع منها يعمل وفق أسلوب محدد ومعطيات معينة مثل (النصوص الواضحة والمشفرة والاختلافات بين النصوص والاختلافات المستحيل حدوثها إضافة إلى الاحتمالات المرافقة)

15 يقصد بالأقنعة سلاسل عشوائية من ال bits المولدة لتتحد مع بيانات الدخل وبيانات الخرج

ثالثاً: تقييم خوارزميات التعمية Symmetric Cipher Algorithms Evaluation

سوف نعتمد في تقييم خوارزميات التعمية المختارة في هذه الدراسة المقارنة على التقييم الأمني لكل منها وإجراء المقارنات على النتائج، إضافة إلى تقيم الأداء وإعطاء النتائج لكل منها ومن ثم نخلص إلى التوصيات والنتائج.

1. التقييم الأمني لخوارزميات التعمية Security Evaluation

يعتبر مستوى الأمن العامل الأهم في عملية تقييم خوارميات ونظم التعمية (المشفرات) ويتضمن مدى مقاومة المشفر لأنواع الهجوم ومدى عشوائية الخرج، ثمّ نسبة الأمن الذي يحققه مقارنة مع باقي المشفرات. ويتعلق أمن الخوارزمية بعوامل عديدة منها: عدد تكرارات الخوارزمية، والعمليات الرياضية والمنطقية التي تعتمدها الخوارزمية في بنيتها.

علاقة الأمن بعدد التكرارات في الخوارزمية: عند تعديل عدد التكرارات في خوارزمية يعني أننا نحصل على خوارزمية جديدة لذلك فإن الهجوم على خوارزمية بعد تقليص عدد تكراراتها لا يعطي بالضرورة أي مؤشر أمني حقيقي عن الخوارزمية بأدوارها الأساسية الكاملة. لكن من أهم مقاييس الهامش الأمني لخوارزمية ما هو أن يكون العدد الكلي لتكرارات الخوارزمية أكبر من عدد التكرارات التي تمت مهاجمتها. بشكل عام فإن أي هجوم يحتاج إلى دعائم أساسية هي المعلومات والذاكرة والمعالجة. بناءً على ما تقدم تمكنا من سبر نتائج الهجمات المتنوعة التي بينتها الدراسات والأبحاث الأخيرة على هذه الخوارزميات، ضمن شروط منها عدد محدد من التكرارات وأطوال المفاتيح المختلفة، نبين هذه النتائج في الجدول التالي، مع توضيح لمقدار الذاكرة اللازمة لشن كل هجوم والعدد المتوقع للعمليات اللازمة لذلك، للمزيد [7].

الجدول رقم (2) يلخص أحدث الهجمات على الخوارزميات المدروسة على عدد محدود من التكرارات ومتطلباتها

التكرارات الأساسية	المرجع	التكرارات وطول المفتاح	الهجوم	متطلبات الهجوم(نص)	الذاكرة اللازمة للهجوم (byte)	عدد العمليات اللازمة للهجوم
MARS 16 تكرار 16 مزج	[7]	**11 C**	Amp.Boomerang	2^{63}	2^{70}	2^{229}
	[7]	*6 C, 6 M	Amp.Boomerang	2^{69}	2^{73}	2^{197}
Rijndael (128)10 (192) 12 (256) 14	[7]	4 5 6	Truncated Diff Truncated Diff Truncated Diff	2^{9} 2^{11} 2^{32}	بسيطة بسيطة $7*2^{32}$	2^{9} 2^{40} 2^{72}
	[7]	(192) 7 (256) 7 (256) 8	Truncated Diff Truncated Diff Truncated Diff	$19*2^{32}$ $21*2^{32}$ 2^{128}-2^{119}	$7*2^{32}$ $7*2^{32}$ 2^{101}	2^{155} 2^{172} 2^{204}
	[7]	(192) 7 (256) 7	Truncated Diff Truncated Diff	2^{32} 2^{32}	$7*2^{32}$ $7*2^{32}$	2^{184} 2^{200}
	[7]	(256 ،192) 7	Truncated Diff	2^{32}	$7*2^{32}$	2^{140}
IDEA (128)8	[8] [8]	3 3.5	Differential Truncated Diff	2^{29} 2^{56}	لا تتوفر معلومات	2^{44} 2^{67}
Blowfish 16	[2]	(196,128)7	Differential	** 2^{58}	لا تتوفر معلومات	لا تتوفر معلومات

* (Core Cryptographic) C تخفيض عددا لتكرارات المزودة بمفتاح من 16 تكرار إلى 6 و (Mixing)M تخفيض تكرارات المزج الأمامي والخلفي من 16 تكرار إلى 6 .

ومن هنا يمكن تعريف الهامش الأمني بما يلي:

الهامش الأمني: يعرف الهامش الأمني من خلال نسبة العدد الأدنى من التكرارات اللازم لتحقيق الأمن في خوارزمية مقابل العدد الكلي لتكرارات الخوارزمية، فمثلاً إذا كان عدد التكرارات اللازم لتحقيق الأمن M=10 تكرارات وعدد التكرارات الكلي R= 12، عند ذلك يكون الهامش الأمني S= 20 % وذلك حسب العلاقة التالية: S= [100 – (R / M)*100] ومن ثمّ يمكن القول إنّ الفرق بين الحد الأدنى

من متطلبات الخوارزمية (عدد تكرارات، إزاحات، مزج، طول مفتاح، طول حزمة، صناديق تعويض ثابتة ومتغيرة، بيئة التنفيذ ،..الخ.) لتحقيق الأمن وبين كامل معطيات الخوارزمية يمثل الهامش الأمني.من هنا فإن الهامش الأمني لكل خوارزمية مرتبط بشكل مباشر مع عدد التكرارات المنفذة**16**. للمقارنة بين الهوامش الأمنية لهذه الخوارزميات، نقدم فيما يلي عدد التكرارات (الكلية والدنيا اللازمة لتحقيق الأمن والمهاجمة) والهامش الأمني المرافق لها، وذلك من أجل مفتاح تعمية بطول 128 بت.

الجدول رقم (3) يبين الهوامش الأمنية للخوارزميات المدروسة

الخوارزمية	R عدد تكرارات الخوارزمية	M1 العدد الأصغر من التكرارات اللازمة لتحقيق الأمن	M2 عدد التكرارات المفضلة من أجل الهجوم	S1 الهامش الأمني المرتبط مع M1	S2 الهامش الأمني المرتبط مع M2
Rijndael	10	8	6	%25	%66
Mars	32	20	12	%60	%166
IDEA	8	4	3	%100	%166
Blowfish	16	8	6	%100	%166

وكنتيجة لذلك يمكن أن نخلص إلى ما يلي:

لم تثبت الدراسات حتى الآن حقيقة الهامش الأمني لـ MARS وذلك بسبب بنية الخوارزمية المعقدة واحتوائها على نوعين مختلفين من التكرارات، إضافة إلى إمكانية وجود مفاتيح ضعيفة.

كما أنه من الصعب مهاجمة Blowfish بعد التكرار السادس، إلا بعد حذف عمليات التبييض وبأثر لا يتجاوز أثر الهجوم بالبحث الشامل. بالنسبة لـ Rijndael، فكما تبينه نتائج الأبحاث المبينة في الجدول رقم (2) إنّ هناك نتائج متباينة في محاولة كسر هذه الخوارزمية باستخدام التحليل التفاضلي المختزل ضمن تكرارات لا تتجاوز الثمانية. أما بالنسبة لخوارزمية IDEA فلم تبين الأبحاث أية محاولة للهجوم في عدد تكرارات تتجاوز 3 تكرارات [2] وذلك بسبب الطريقة التي اعتمدها مصمموها في تعديل مبدأ Feistel Network وتطبيقها في المزج المباشر على مستوى التكرار الواحد.

** بين Serge Vaudenay أنه باستخدام صناديق تعويض معلومة و r مرحلة فإن التحليل التفاضلي يمكنه الحصول على مصفوفة المفاتيح باستخدام 2^{8r+1} نص واضح مختار، وينخفض إلى 2^{8r+1} باستخدام مفاتيح توليد ضعيفة. لكن كل ذلك مع عدد منخفض من المراحل (8 مراحل أو أقل).

16- التكرارات العادية للخوارزمية أو التكرارات المعدلة.

علاقة الأمن بالعمليات الرياضية والمنطقية المستخدمة في بناء خوارزميات التعمية:

من الجدير بالذكر أن العمليات الرياضية والمنطقية وعمليات الجدولة والإزاحة والتعويض الداخلة في بنية خوارزمية التعمية أو في بنية خوارزمية توسيع المفتاح لنظام التعمية المتناظر تشكل عناصر قوة أو ضعف في الخوارزمية لذلك نستعرض هنا تحليلاً لهذه العمليات وأثرها على الخوارزمية.

تعتبر هذه العمليات فعالة بشكل عام أمام أنواع الهجوم التقليدية القديمة المعروفة(بالنص المشفر المختار،أو النص المعمى المختار والتفاضلي و...)، وإن لم تكن كذالك فإنه يمكن زيادة فعاليتها من خلال أسلوب ترتيبها واستخدامها، وفيما يلي توضيح لفعالية هذه العمليات أمام أنواع من الهجمات الحديثة المفترضة وهي هجوم الطاقة والهجوم الزمني التي تعتبر من أهم الهجومات وخاصة في حال استخدام الخوارزميات في التطبيقات الحديثة التي تعتمد البطاقات الذكية.

أ- **العمليات الجدولية (Table lookup)**: غير معرضة للكسر أمام الهجوم الزمني المفترض، وتملك مقاومة فعالة أمام هجوم الطاقة (القوى) وذلك من خلال حسن استخدام العناوين ومتمماتها.

ب – **عمليات الإزاحة والتدوير الثابتة (Fixed shifts / rotation)**: غير معرضة للكسر أمام الهجوم الزمني وتملك إمكانية دفاع فعالة أمام هجوم القوى وذلك من خلال استخدام محتويات المسجل ومتمماتها [17].

ج- **العمليات البوليانية (المنطقية)**: غير معرضة للكسر أمام الهجوم الزمني المفترض. يمكنها الصمود والدفاع في وجه هجمات القوى وذلك باستخدام المتممات.

ء – عمليات الجمع والطرح (Addition / Subtraction): من الصعب على هذه العمليات إلى حد ما الدفاع أمام الهجمات الزمنية أو هجمات القوى.

هـ- عمليات التضاعف والقسمة والإزاحة والتدوير غير الثابتة (Var.shi / ult-Div، rot): الخوارزميات التي تحتوي على هذه العمليات تصمد بصعوبة شديدة أمام الهجمات الزمنية وهجمات القوى. ولكن لم يتم حتى الآن التعرف على أية هجمات فعالة في المجالات التطبيقية، وإنما كل ذلك بمعنى الإمكانية النظرية في وجه أنواع من الهجمات الافتراضية.

نقدم فيما يلي ملخصاً للعمليات المستخدمة بشكل أساسي من قبل خوارزميات التشفير المتماثل المعنية في هذا البحث.

الجدول رقم (4) يبين العمليات المستخدمة في كل من الخوارزميات المختلفة

الخوارزمية	العمليات المستخدمة					
	Tab lo جداول التعويض	FixShi-Rot الإزاحة والتدوير[18]	VarShi-Rot الإزاحة والتدوير[19]	Logic منطقية	Add - Sub الجمع والطرح	Mul - Div المضاعفة والقسمة
Rijndael	نعم	نعم	لا	نعم	لا	لا
Mars	نعم	نعم	نعم	نعم	نعم	نعم
IDEA	لا	لا	لا	نعم	نعم	نعم
Blowfish	نعم	لا	لا	نعم	نعم	لا

[17] – السجل الذي يحوي مقدار الإزاحة ومقدار التدوير.

[18]– عمليات ثابتة.

[19] – عمليات مرتبطة (غير ثابتة).

بناءً على ما تقدم يمكن ترتيب وتقييم مستوى الأمن ضد الهجوم الزمني وهجوم القوى في الخوارزميات المدروسة، وذلك بناء على تأثير ما تستخدمه من عمليات ضمن بنيتها التصميمية، كما يلي:

1 – خوارزمية ريجندال، تتمتع بمناعة عالية ضد هذين الهجومين وذلك نتيجة لعدم استخدامها أية من العمليات التي تضعفها (الجمع والطرح أو التقسيم أو الضرب أو العمليات المنطقية بشكلها البسيط).

2 – خوارزمية بلو فيش blowfish بسبب استخدامها لعمليات الجمع والعمليات المنطقية.

3 – خوارزمية IDEA وذلك بسبب العمليات التي تستخدمها كما هو واضح في الجدول (4).

4 – والأخيرة تصنف فيها خوارزمية Mars لاستخدامها عمليات الجمع والضرب والإزاحة الثابتة إضافة إلى العمليات المنطقية ومن ثمّ فهي الأكثر تعرضاً لكلا الهجومين مقارنة بباقي الخوارزميات.

2. تقييم الأداء Performance Evaluation:

يجب ملاحظة العلاقة الهامة بين عدد التكرارات وسرعة التنفيذ وبين عدد التكرارات والأمن، ثمّ بين سرعة التنفيذ والأمن الذي تحققه الخوارزمية وأنه لا يمكن النظر إلى سرعة التنفيذ دون النظر إلى الأمن، وحجم كلمة الحاسوب المستخدمة (8 خانة ثنائية أو 16 خانة ثنائية أو 32 خانة ثنائية أو 64 خانة ثنائية) واللغة المستخدمة[20] إضافة إلى معماريات الحاسوب ومميزاته والعمليات التي تدعمها هذه المميزات. كل ذلك يلعب دوراً عند الحديث عن الأداء، إضافة إلى التكلفة الزمنية والمادية ومدى أهمية كل منهما في الحالة الراهنة. بشكل عام يشمل الأداء فعالية الحسابات عند استخدام المعماريات والصيغ المختلفة ومتطلبات الذاكرة، إضافة إلى قيود التنفيذ البرمجي والإنجاز العتادي، إلى جانب متطلبات الترخيص.

تم تنفيذ اختبارات لقياس سرعة أداء كل من الخوارزميات وحصلنا على النتائج الموضحة في الجدول التالي:

الجدول رقم (5) يبين نتائج اختبار سرعة التنفيذ للخوارزميات

الخوارزمية	السرعة (**Mega bytes / Sec**)
IDEA	10.8
RIJNDAEL(256-bit)	14.02
BLOWFISH	14.53
MARS	25.97

لدى التمعن في النتائج نلاحظ أن خوارزمية Mars هي الأسرع في التنفيذ، يليها Blowfish و Rijndael ، أما خوارزمية IDEA فهي الأقل سرعة وأداء خلال الاختبارات التي جرت ضمن بيئة عمل واحدة.

الاستنتاجات والتوصيات:

من خلال الدراسة التحليلية والمقارنة للخوارزميات السابقة يمكن تلخيص النتائج على الشكل الأتي:

A-خوارزمية Mars:

- تدعم أطوال كبيرة للمفاتيح أكثر من 256 خانة ثنائية ونظرياً يصل إلى 1248 bit.
- بشكل عام تتمتع بسرعة وأداء عالي، ويمكن أن تُنفذ بشكل أفضل على حواسيب مزودة بدعم لعمليات التضاعف والدوران.

[20]– بعض لغات البرمجة تسمح باستخدام الإمكانيات التي يوفرها المعالج.

- تُنفذ بشكل جيد على معماريات بـ 32 خانة ثنائية، وعلى معماريات تدعم عمليات الإزاحة غير الثابتة
- يتراجع مستوى تنفيذها على معماريات غير مدعمة بالاحتياجات المطلوبة.
- كما أن التنفيذ العتادي ضمن البطاقات الذكية أسرع من التنفيذ البر مجي للخوارزمية.
- النسخة الأساسية من الخوارزمية لا تعمل بشكل جيد مع البطاقات الذكية بسبب حاجتها للتوليد الآني للمفاتيح وهذا ما تفتقده الخوارزمية، وتحتاج إلى متوسط كبير من الذاكرة ROM، أما مشكلتها مع الـ RAM فقد تم تجاوزها في النسخة المعدلة.
- يتراجع مستواها الأمني كثيراً أمام الهجوم الزمني وهجوم القوى.
- تحليل الخوارزمية صعب نسبياً ضمن مخطط زمني محدود.
- لا تدعم التنفيذ المتوازي بشكل جيد إلا عند توفر بعض الاحتياجات الإضافية لها والتي تدعم عملياتها المختلفة.

B. خوارزمية Rijndael:

- تُنفذ بشكل ممتاز من خلال المعماريات والصيغ المختلفة.
- تحتاج كمية بسيطة من الذاكرة لذلك تُنفذ بشكل جيد في مجال العتاد وفي البيئات ذات الذاكرة المحدودة.
- يتم تجهيز المفتاح بسرعة عالية.
- تدعم وبشكل جيد التنفيذ المتوازي للتعليمات في المعالجات الحديثة [6].
- تدعم أطوال مفتاح وأطوال حزم تزيد عن 32 بت.
- تتمتع بمناعة عالية ضد الهجوم الزمني وهجوم القوى.
- يفضل الابتعاد بهامش أمني عن التكرار السادس في حال استخدام مفتاح بطول 128 وعن التكرار الثامن في حال استخدام مفاتيح أطول من ذلك.

C. خوارزمية IDEA:

- عدد التكرارات المستخدمة قليل مقارنة مع باقي الخوارزميات وذلك بسبب اعتمادها تعديل مبدأ Fiestel etwork.
- ذات أداء منخفض نسبياً مقارنة مع باقي الخوارزميات.
- محدودة طول الدخل بـ 64 خانة وطول مفتاح بـ 128 خانة ثنائية.
- ذات سوية متواضعة أمام الهجوم الزمني و هجوم القوى.
- تتمتع بسوية أمنية عالية ضد الهجوم التفاضلي.
- يمكن استخدامها من أجل عدد مراحل أقل من 8 (ضمن مجالها الأمني) للحصول على سرعة أعلى.
- تدعم التوازي العتادي أكثر من دعمها لعمليات التوازي البرمجي.

D. خوارزمية Blowfish:

- ذات سرعة مثالية في التطبيقات التي لا يتغير فيها المفتاح بوتيرة عالية (الاتصالات).
- تعمل على معالجات صغرية ذات 32 bit بسرعة 26 دور ساعة من أجل تشفير كل بايت.
- تزداد سرعتها إذا ما نُفذت تعليماتها بشكل مباشر دون استخدام الحلقات.
- يمكن حساب مفاتيحها مسبقاً بهدف الحصول على سرعة أعلى.
- تواجه الهجوم الزمني وهجوم القوى بشكل مقبول.

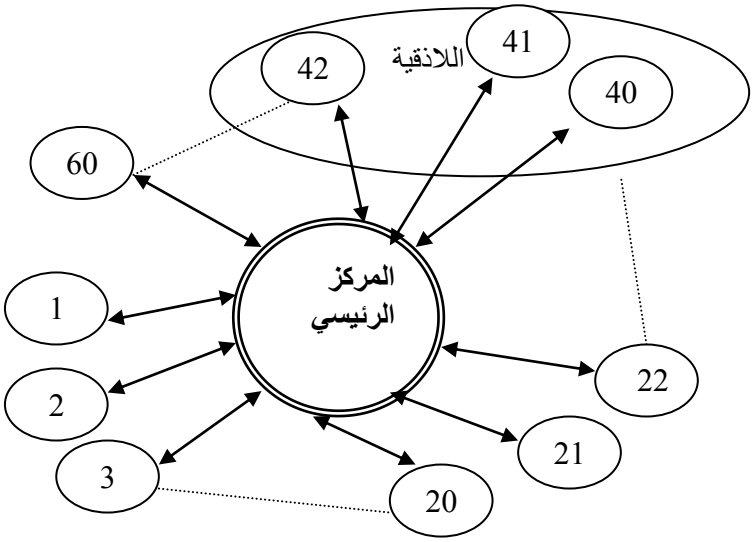
- بالاعتماد عليها تم بناء خوارزمية Twofish ذات الإمكانيات المتقدمة في مجال الأمن والأداء.

تطبيق عملي:

سنشير فيما يلي إلى مثالين من الواقع العملي.

1- الهيكلية الأمنية في المصرف التجاري السوري:

من خلال زيارتنا لفروع المصرف التجاري السوري باللاذقية علمنا أن المصرف التجاري السوري يتكون من المركز الرئيسي بدمشق ومن حوالي 60 فرعاً منتشرة في المناطق المختلفة وموصولة مع المركز الرئيسي على شكل شبكة نجمية كما هو موضح بالشكل التالي:



الشكل رقم(7) يبين البنية التنظيمية الأمنية للمصرف التجاري السوري

كما أن الفرع (3) في المصرف التجاري السوري باللاذقية يضم حوالي 30 جهاز حاسوب من أنوع مختلفة وموصولة بشبكة محلية وهذه الشبكة موصولة مع مخدم في المركز الرئيسي عن طريق خطوط من أنواع مختلفة وسرعات نقل مختلفة يتم من خلالها إرسال واستقبال البيانات، ومن خلال دراستنا لواقع العملية المصرفية تبين لنا أن المشاكل التي تعاني منها هذه الافرع متعددة، نأخذ منها الجانب التالي:

المشكلة الامنية الناتجة عن البنية التنظيمية لهذه الأفرع

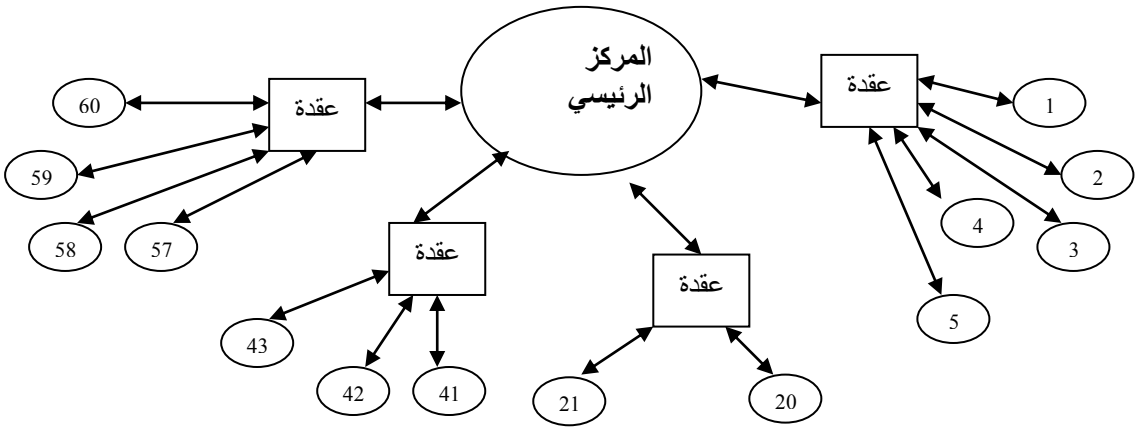
يبين الشكل (7) أن كل فرع يتصل مباشرة مع المركز الرئيسي ولذلك فإن كل عملية مصرفية في أي من الأفرع تتم عن طريق المركز الرئيسي وهذا يعطي الفرصة لمهاجمة البيانات وتزويرها من خلال مراقبة الحزم الصادرة والواردة بكثافة عالية من وإلى المركز الرئيسي ودراسة التقاطعات بين هذه الحزم المشفرة ثم وصول المهاجم إلى هدفه[21] من خلال الحصول على بعض خانات المفتاح المستخدم. ولحل هذه المشكلة نقترح وضع عقد وصل في مناطق

[21]- قد تكون الآن المشاكل الأمنية بسيطة ولكن ستظهر مشاكل أمنية متعددة وكبيرة مع توسع العمليات المصرفية في البنك.

مناسبة ومن ثم يتم وصل الأفرع مع العقدة المناسبة ووصل العقد مع المركز الرئيسي كما هو موضح بالشكل رقم (8) وهذا يمكننا من استخدام مستويين من أمان خوارزميات التشفير. المستوى الأول مابين الأفرع والعقد ويستخدم خوارزميات تشفير ذات أمان جيد وسرعة عالية وتسمح بالتغيير الدوري لمفتاح التشفير 128 - Rijndael، والمستوى الثاني مابين العقد والمركز الرئيسي ويستخدم خوارزميات ذات سوية أمنية عالية وسرعة عالية وتتناسب مع تغيير المفتاح دورياً مثل خوارزمية 256 -Rijndael.

2- **مشكلة أرسال استحقاقات العاملين في جامعة تشرين من رواتب وغيرها إلى المصرف التجاري:**

في نهاية كل شهر يتم إيصال جداول مستحقات العاملين بجامعة تشرين إلى المصرف التجاري بطريقة قديمة، حيث يتم تخزينها على بواسطة تخزين خارجية وترسل بواسطة شخص محدد (وفق ما أفادنا به مدير الدعم الفني في المصرف) وهذا ماينعكس سلباً على وصول المستحقات لأصحابها بشكل مناسب زمنياً، إضافة إلى كون هذا الأسلوب غير متناسب مع البيئة التقنية الحديثة التي يعشها العالم الان، إضافة إلى الجهود المبذولة بشكل مستمر من أجل ذلك، حيث لايتم ارسالها بشكل الكتروني خشية من العقبات الأمنية التي قد تعترضها. **نقترح لحل هذا الموضوع** استخدام خوارزمية Blowfish – لكونها الأكثر ملاءمة للعمل على معالجات صغرية ، ومع ملاحظة أن المدة الزمنية اللازمة لبقاء هذه البيانات مشفرة هي مدة قصيرة نسبياً ولانحتاج للتغيير المستمر في المفتاح المستخدم، كما أنه يمكننا استخدام الخوارزمية (في حالتنا هذه) بعدد تكرارات منخفض يحقق الهامش الأمني القياسي الوارد في الجدول (3) لتشفير هذه البيانات وارسالها واستخدام نفس الخوارزمية ونفس المفتاح في الطرف الاخر لفك تشفير البيانات، ومن ثمّ يصبح كل ما هو مطلوب في نهاية كل شهر إدخال مفتاح التشفير من قبل المعتمد في الجامعة وضغط مفتاح الارسال، وعندها يمكن تفعيل الحسابات مباشرة دون الانتظار مدة 24 ساعة بعد وصول البيانات كما هو حادث الان.



شكل رقم (8) يبين البنية التنظيمية الأمنية المقترحة للمصرف التجاري السوري

الاستنتاجات والتوصيات:

يعتبر هذا البحث نواة في دراسة واختبار المشفرات التي تعتمد الخوارزميات المتناظرة، وذلك بهدف بناء القدرة التحليلية والمعرفة العلمية السليمة لطرق تصميم هذه الخوارزميات، وتقدم الدراسة المقارنة نتائج تساعد الجهات الراغبة في اختيار نظام التعمية المناسب، والاستفادة منها في التطوير المستقبلي أو تصميم خوارزميات جديدة لتحقيق

الاستقلالية الأمنية بالاستغناء عن الأنظمة الأمنية الجاهزة المستوردة، لذلك نوصي الجهات الوطنية بالعمل على إنشاء فرق علمية متخصصة في دراسات وتحليل وتصميم نظم التعمية لبناء النظم الوطنية الخاصة في أمن المعلومات مع الأخذ بالاعتبار النقاط التالية – كنتائج لهذه الدراسة – لتصميم خوارزمية تعمية متناظرة:

a. الابتعاد قدر الإمكان عن التفرعات في البرامج التنفيذية للوقوف في وجه الهجوم الزمني.
b. تجنب استخدام خوارزميات تعتمد على عمليات من الصعب صمودها أمام الهجمات المذكورة.
c. ننصح باستخدام خورازمية Rijndael بشكلها البرمجي وبمفاتيحها المتعددة الأطوال.
d. تجنب استخدام أنظمة التشفير العتادي المستورد قدر الامكان وذلك بسبب الأبواب الخلفية المزروعة فيه.
e. في حال التطبيقات التي تعتمد البطاقات الذكية في التشفير يجب اختيار البطاقة الذكية المناسبة.
f. استخدام التوازن البرمجي من خلال استخدام المتممات حتى عندما يكون مجموع القوى مبدداً و فعالاً من أجل عمليات معينة تضعف قوتها تدريجياً، حيث يتم تمديد طول بعض العمليات من خلال تنفيذها مرتين باستخدام المتممات مرة ثانية.

المراجع:

1-DAEMEN,J ; RIJMEN,V, *The Design of Rijndael AES – Advanced Encryption Standard*, Springer-Verlag,2002,238,
22.4.2007< http://en.wikipedia.org/wiki/Advanced_Encryption_Standard >

2- SCHNEIER ,B, *Applied Cryptography*. Second Edition, John Wiley & sons, 1996 ,894,
24.4.2007 <http://www.schneier.com/blowfish.htm>.

3- SCHNEIER ,B, *Fast Software Encryption* ,Cambridge Security Workshop Proceedings (December 1993),Springer – Verrhg, 1994, 191-204.

4- BURWICK,C; COPPERSMITH,D;et al, *MARS-a Candidate for AES*, IBM Corporation ,1998 ,4-62, 15.3.2007<http://www.research.ibm.com/security/mars.pdf >.

5- VAUDENAY, S, *On the Weak Keys of Blowfish*., in Fast Software Encryption (FSE'96), LNCS 1039, Springer-Verlag, 1996, 27-32

6- NICOLAS,T;COURTOIS,C;PIEPRZYK,J, *Cryptanalysis of Block Ciphers With Overdefind Systems of Equations*, Asiacrypt 2002, 1-35.

7- NECHVATAL, J; Barker, E; et al; *The Development of The Advanced Encryption Standard (AES)*; Report on Computer Security, Division information Technology Laboratory, National Institute of Standard and Technology Administration (NIST), U.S. Department of Commerce, October 2,2000, 7-111,
11.4.2007 < http://citeseer.ist.psu.edu/cachedpage/382178/19 >.

8- SHEN,H,*International Data Encryption Algorithm*,CS-627-1,Fall,2004, 2-11.