مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (6) العدد(11) 2022
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (6) No. (11) 2022

"تحسين نظام المصادقة في الحوسبة السحابية "

د. يعرب ديوب *

م. رنا رزوق **

(تاريخ الإيداع 2022/8/22 . قُبِل للنشر في 2022/11/17)

□ ملخّص□

المصادقة في الحوسبة السحابية هي عملية التحقق من هوية المستخدم الذي يقوم بإرسال الرسائل إلى طرف آخر ويستخدم التوقيع الرقمي لضمان هذه العملية والذي يعتمد بشكل رئيسي على عمليتي التشفير و التجزئة . في هذا البحث تم اقتراح نموذج مطور عن خوارزمية التجزئة SHA1 التي تحقق معدل Avalanch effect (أثر الأنهيار) منخفض و كذلك تم اقتراح نموذج مطور عن خوارزمية التشفير RSA يمنع المهاجم من معرفة المفاتيح المستخدمة للتشفير و فك التشفير . حسنت النماذج المطورة عملية المصادقة في الحوسبة السحابية المعتمدة أصلاً على التوقيع الرقمي .

الكلمات المفتاحية : RSA، SHA1، التوقيع الرقمي ، المصادقة ، التشفير ، التجزئة .

* أ.د.م في قسم هندسة تكنولوجيا المعلومات – كلية هندسة تكنولوجيا المعلومات و الاتصالات – جامعة طرطوس– سوريا

**طالبة ماجستير في قسم هندسة تكنولوجيا المعلومات – كلية هندسة تكنولوجيا المعلومات و الاتصالات – جامعة طرطوس– سوريا

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (6) العدد(11) 2022
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (6) No. (11) 2022

" Enhanced authentication system in cloud computing "

Prof. Yaroub dayoub *
Eng. Rana razouq **

(Received 22/8/ 2022 . Accepted 17/11/ 2022)

□ ABSTRACT

Authentication in cloud computing is the process of verifying the identity of the user and uses a digital signature to ensure this process, which depends mainly on the encryption and hashing processes. A developed model has been proposed for the RSA encryption algorithm that is subjected to factorization attack. The developed models have solved the previous problems and thus improved the authentication process in cloud computing that was originally based on the digital signature..

Keywords: RSA, SHA1, digital signature, authentication, encryption, hashing.

* Professor in Department of Information Technology, Faculty of Information and Communication Technology Engineering, Tartous University, Syria.
**Master student at Information Technology Engineering Department, Information and Communication Technology Engineering, Tartous University, Syria.

1- مقدمة :

يشهد العالم اليوم تطوراً سريعاً في وسائل التكنولوجيا و تقنيات التواصل و الاتصال والأمان والذي يقابله في الوقت ذاته تطورا موازياً في وسائل و تقنيات الاختراق و الهجوم.

وقد جعل هذا التطور أمان و حماية بيانات المستخدم المخزنة في السحابة و ملفاته الخاصة أمراً غاية في الأهمية ، و تعددت الأبحاث حول حماية معلومات المستخدم فبعضها أعتبر أن عملية التشفير هي الجزء الأهم في عملية مصادقة المستخدم ، واستخدمت الكثير من الدراسات خوارزمية التشفير RSA بإعتبارها الخوارزمية الأكثر أماناً ، و تطرقت بعض الدراسات لتحسين أداء خوارزميات التجزئة من خلال تقليل الزمن اللازم لتنفيذ الخوارزمية المستخدمة . و بناء نظام مصادقة قوي يعتمد على خوارزمية تشفير و تجزئة قوية .[14] [12] [10]

لم تعالج الدراسات السابقة إنخفاض معامل الأنهيار الذي يعبر عن عدد الخانات التي تعرضت للتغيير في النص المشفر نتيجة تغيير بت واحد في النص الأساسي لخوارزمية SHA1 ما يجعل النص المشفر بهذه الخوارزمية عرضة للهجوم التحليلي حيث يتمكن المهاجم من معرفة النص الأصلي ، كما أن الدراسات السابقة التي تطرقت لعملية التشفير بواسطة خوارزمية RSA(Rivest–Shamir–Adleman) .

لم تعالج إمكانية معرفة المهاجم لمفاتيح التشفير و فك التشفير و التي تمكنه من معرفة النص المشفر . [10][12].

1-1 الحوسبة السحابية:

الحوسبة السحابية هي شكل من أشكال الحوسبة الموزعة التي قد يعمل فيها تطبيق معين على مختلف أجهزة الكمبيوتر المرتبطة في وقت واحد . قدمت الحوسبة السحابية العديد من التسهيلات الغير عادية مثل تخزين كبير السعة و تكلفة تخزين منخفضة و سهولة الوصول.. الخ .[7]

1-2 المصادقة في الحوسبة السحابية :

هي عملية التحقق من هوية المستخدم الذي يقوم بتسجيل الدخول الى الشبكة بإستخدام معلومات سرية خاصة به مثال على ذلك في أنظمة الحوسبة السحابية يقوم المستخدم بتسجيل الدخول عبر إدخال كلمة سر خاصة به وعندما يقوم النظام بالسماح للمستخدم بالدخول إلى الشبكة يعني ذلك أن المستخدم قام في وقت سابق بطلب دخول إلى الشبكة و أدخل كلمة السر الخاصة به هذه لتعبر عن هويته و التي لايجب أن تكون معروفة إلا من قبل المستخدم و النظام الذي يقوم المستخدم بتسجيل الدخول عليه [1].

1-3 التوقيع الرقمي :

يعد التوقيع الرقمي أحد أهم التطبيقات الحديثة لتوقيع الوثائق الإلكترونية بهدف تحقيق الأمان في المعاملات الإلكترونية الرقمية، وهو عبارة عن أرقام ورموز خاصة مشفرة مرتبطة بالرسالة الإلكترونية ، حيث أنها تتيح لمستقبل الرسالة التحقق من الشخص مرسل الرسالة و أنه هو بالفعل الموقع على الرسالة [5].

ولذلك تم استخدام خوارزميات التشفير غير المتناظرة لتحقيق المصادقة و الأمن للرسائل المرسلة عبر الشبكة و يستخدم للمصادقة على صحة مضمون الرسالة والتي قد تكون كلمة سر أو ملف نصي او رمز معين أو بريد الكتروني أو غيرها من وسائل المصادقة و يعتمد على خوارزميات التشفير و التجزئة [11].

2. مشكلة البحث :

تعتمد عملية التوقيع الرقمي لمصادقة المستخدمين بشكل رئيسي على خوارزميات التجزئة و خوارزميات التشفير وتكمن مشكلة البحث في :

1. إنخفاض معدل الإنهيار avalanche effect لخوارزمية SHA-1 .
2. هجوم التحليل إلى عوامل على خوارزمية RSA المستخدمة في التوقيع الرقمي لمصادقة المستخدمين والذي يتمكن من خلاله المهاجم من معرفة مفاتيح التشفير وبالتالي فك التشفير .

3. أهمية البحث :

تكمن أهمية البحث في تحسين أمان عملية المصادقة في الحوسبة السحابية و جعلها أكثر موثوقية وأمان ويصعب على المهاجم معرفة الرسالة الأصلية مما يضمن خصوصية المستخدم الذي يقوم بتسجيل الدخول إلى النظام.

4.أهداف البحث :

تعتمد عملية المصادقة بشكل رئيسي على عمليتي التجزئة و التشفير و يهدف البحث الى تحسين عملية المصادقة بإستخدام التوقيع الرقمي في الحوسبة السحابية وذلك من خلال:

1. تحسين خوارزمية التجزئة SHA-160 وزيادة تعقيدها مما يزيد أمان الخوارزمية .
2. تحسين خوارزمية التشفير RSA مما يزيد من أمان هذه الخوارزمية بزيادة قيمة معامل أثر الإنهيار.
3. تعقيد عملية توليد المفاتيح في خوارزمية RSA .

5. منهجية البحث:

تم إعتماد المنهج الوصفي التجريبي:

تم إقتراح تنفيذ تعديلات على خوارزمية التشفير RSA و خوارزمية التجزئة SHA-160 لتصبح عملية المصادقة أكثر أماناً وقد تم ذلك وفق خطوتين :

الخطوة الأولى :

- إقتراح تعديل على خوارزمية التجزئة SHA-160 مما يجعل هذه الخوارزمية أكثر موثوقية من خلال إختبار معامل الأنهيار.
- إقتراح تعديل على خوارزمية التشفير RSA مما يجعل الخوارزمية أكثر أمانا ضد هجوم التحليل إلى عوامل وذلك بزيادة قيمة معامل الإنهيار .

الخطوة الثانية :

- إجراء تطبيق عملي لخوارزمية SHA-160 المعدلة و خوارزمية SHA-160 الأصلية بإستخدام برنامج الماتلاب و تطبيقهما على 5 ملفات نصية بإحجام مختلفة .

- إجراء تطبيق عملي لخوارزمية RSA المعدلة و خوارزمية RSA الأصلية بإستخدام برنامج الماتلاب و تطبيقهما على 5 ملفات نصية بإحجام مختلفة .

6- خوارزمية التشفير RSA :

تعد من خوارزميات التشفير غير المتناظرة، وذلك لإعتمادها في التشفير على مفتاحين، المفتاح العام للتشفير ويتم توزيعه على جميع المستخدمين في الشبكة والمفتاح الخاص لفك التشفير يمتلكه مستخدم واحد فقط ، تمكن هذه الخوارزمية الطرفين من إجراء الإتصال الآمن في الشبكة و تتضمن خوارزمية التشفير RSA ثلاث خطوات وهي توليد المفاتيح، التشفير، فك التشفير[8][9] :

الخطوة الأولى (توليد المفتاحين العام e و الخاص d في خوارزمية RSA):

1. توليد عددين أوليين عشوائيين نرمز لهما p, q .
2. حساب قيمة المعامل n و الذي يساوي جداء العددين الأوليين p ,q

$$n = p*q \quad (1)$$

3. حساب المعامل $\emptyset(n)$ والتي تحسب من العلاقة (يتم طرح العدد 1 من كل عدد اولي: p−1 و q−1 ثم حساب جدائهما) وفق العلاقة الآتية :

$$\emptyset(n)= (p-1)*(q-1) \quad (2)$$

4. حساب المفتاح العام الذي يستخدم لعملية التشفير بحيث يكون القاسم المشترك الاكبر للمفتاح e و المعامل $\emptyset(n)$ هو 1 :

$$GCD(\emptyset(n),e) = 1 \quad (3)$$

5. حساب المفتاح الخاص d ،والذي يتم حسابه بالإعتماد على قيمة $\emptyset(n)$ ، و تحدد قيمته وفق العلاقة الآتية :

$$d*e = 1 \bmod \emptyset(n) \quad (4)$$

mod تابع باقي القسمة

تقوم الخوارزمية بتجزئة الرسالة الأصلية و لتكن M إلى كتل بيانات كالتالي :

$$M = [m_1 ,m_2 ,.....m_z]$$

حيث z عدد كتل البيانات

m_1 ,m_2 الكتلة الأولى ،..الخ

الخطوة الثانية (عملية التشفير) :

تابع التشفير الرسالة M (يتم رفع الرسالة للأس المفتاح العام e ثم ايجاد باقي قسمتها على المعامل n) وينتج النص المشفر C :

$$C = M^{e} \bmod n \quad (5)$$

الخطوة الثالثة (عملية فك التشفير) :

تابع فك التشفير (يتم فك تشفير الرسالة في الطرف المستقبل وذلك من خلال رفع الرسالة المشفرة C للأس المفتاح الخاص ثم إيجاد باقي القسمة على المعامل n) :

$$M = C^{d} \bmod n \quad (6)$$

يتم تشكيل النص المشفر:

$$C=[c_1,c_2....c_z]$$

حيث $c_1,c_2....c_z$ الكتل المشفرة الموافقة لكتل البيانات $m_1,m_2....m_z$.

في عملية التوقيع الرقمي يتم التشفير بالمفتاح الخاص و فك التشفير بالمفتاح العام (على عكس عملية التشفير في خوارزمية RSA) :

تابع التشفير الرسالة M : $C = M^{d} \bmod n$ (7)

تابع فك التشفير : $M = C^{e} \bmod n$ (8)

7- التجزئة Hashing:

تقوم خوارزميات التجزئة على تحويل النص الاصلي الى أصفار وواحدات وتقسيمه الى أجزاء متساوية ثم يطبق عليه عمليات منطقية مختلفة و توابع رياضية على عدة مراحل للحصول على ناتج هذه العملية وعلى خلاف خوارزميات التشفير فأنه من المستحيل الرجوع الى النص الأصلي [13] .

7-1 خوارزمية التجزئة SHA-160 (Secure Hash Algorithm):

خوارزمية تجزئة تعطي نص مجزء بطول ثابت (160 بت) مهما كان طول الرسالة المراد تشفيرها[4].

خطوات الخوارزمية [3] :

1. يتم استقبال الرسالة المراد تطبيق الدالة عليها و تحويلها لبتات اصفار وواحدات ثم اضافة البت 1 الى بداية الرسالة .
2. يتم اضافة عدد من البتات الاصفار بعد البت 1 بحيث عد البتات المضافة يجعل عدد البتات الكلية للرسالة من مضاعفات 512 .
3. تقسم الرسالة الى بلوكات كل بلوك عبارة عن 512 بت .
4. من اجل كل بلوك : يتم تقسيم البلوك الى 16 كلمة w، يشغل كل منها 32 بت .
5. يتم زيادة عدد الكلمات ليصبح 80 كلمة وفق العملية الاتية :

for (i =16 , i<79 , i++)

$$w[i] = (w[i-3] \text{ xor } w[i-8] \text{ xor } w[i-14] \text{ xor } w[i-16]) \text{ leftrotate } 1 \quad (9)$$

من أجل كل بلوك يتم تطبيق 80 دورة .

مسجلات و بارامترات الخوارزمية :

1. المسجلات A,B,C,D,E :

في الدورة الاولى يتم تمهيد المسجلات بقيم ابتدائية ثابتة ست عشرية :

A= 0x6745230, B=0xefcdab89 ,C=0x98badcfe ,D=0x10325476 ,E=0xc3d2e1f0

وتتجدد قيمة المسجلات في نهاية كل دورة .

2. المسجل W :

وعددها 80 كلمة (في الدورة الاولى تستخدم الكلمة الاولى و w يتم تمهيد هذا المسجل بالكلمة

في الدورة الثانية تستخدم الكلمة الثانية) أي يتم استخدام الكلمة الموافقة لرقم الدورة .

3. المسجل F يأخذ قيم المسجلات B,C,D ويقوم بتطبيق التابع f حسب رقم الدورة :

أول عشرين دورة يتم تطبيق التابع: F_1= (B and C) or ((not B) and D)

ثاني عشرين دورة يتم تطبيق التابع: F_2= B xor C xor D

ثالث عشرين دورة يتم تطبيق التابع: F_3= (B and C) or (B and D) or (C and D)

رابع عشرين دورة يتم تطبيق التابع: F_4= B xor C xor D

4. المسجل K : يخزن قيمة المتغير k التي تتغير حسب رقم الدورة (القيم ثابتة) :

أول عشرين دورة يأخذ المتغير k القيمة : k= 0x5a827999

ثاني عشرين دورة يأخذ المتغير k القيمة : k= 0x6ed9eba1

ثالث عشرين دورة يأخذ المتغير k القيمة : k= 0x8f1bbcdc

رابع عشرين دورة يأخذ المتغير k القيمة : k= 0xca62c1d6

العمليات المنفذة في الخوارزمية بالدورة الاولى :

1. إزاحة محتوى المسجل A نحو اليسار 5 بتات
2. إزاحة محتوى المسجلB نحو اليسار 30 بت
3. التصريح عن متغير t و الذي تحدد قيمته بمجموع القيم الموجودة في المسجلات الاتية :

E,W(i), K, F مضافا إليها ناتج الخطوة رقم 1 والتي هي ازاحة المسجل A نحو اليسار 5 بتات :

t= (A leftrotate 5) +f+e+k+w(i) (10)

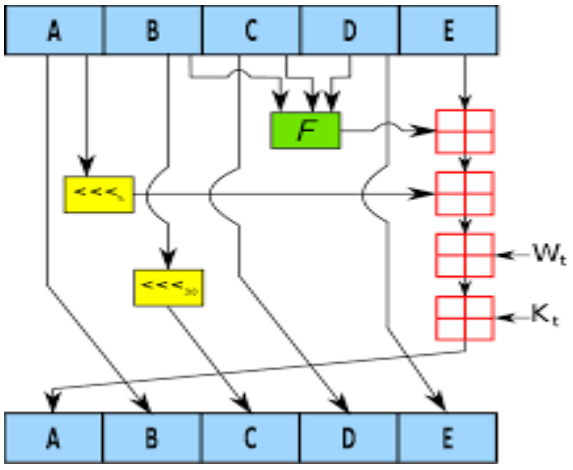
4. تهيئة المسجلات بقيم جديدة :

A= t, B= A , C= B leftrotate 30 , D=C , E=D

في الدورة التالية : يتم تطبيق العمليات ذاتها على القيم المحدثة الموجودة في المسجلات .

تتكرر هذه العملية حتى تنتهي جميع البلوكات حيث أن ناتج التشفير هو القيم الموجودة في المسجلات من اجل آخر بلوك :

النص المشفر = [A B C D E]



الشكل (1) . خوارزمية SHA-160

يوضح الشكل (1) المخطط الصندوقي لخوارزمية SHA-160 الذي يوضح آلية عمل الدورة الواحدة في الخوارزمية .

8- آلية تشكيل التوقيع الرقمي باستخدام خوارزمية RSA [6]:

الخطوة الأولى (توليد مفاتيح التشفير) :

يتم توليد المفاتيح الخاصة والعامة المتعلقة بمستخدمي الشبكة حيث يتم تشفير المفتاح العام الذي سيتم من خلاله فك تشفير التوقيع الرقمي و تشفير الرسالة وفق خوارزمية تشفير وإرسالهم مع التوقيع إلى المستقبل.

الخطوة الثانية (التوقيع الرقمي) :

تتضمن عملية التوقيع المرحلتين الاتيين:

a. المرحلة الأولى: إنشاء ملخص للرسالة Digest Message بإستخدام واحدة من خوارزميات التجزئة Algorithm Hash ،هذا الملخص يتكون من سلسلة من الرموز المرتبطة بالرسالة و بالتالي أي تغيير يطرأ على الرسالة سيؤدي إلى إنشاء ملخص مختلف .

b. المرحلة الثانية: ينتج التوقيع الرقمي بعد تشفير ملخص الرسالة بالمفتاح الخاص وفق تابع تشفير خوارزمية RSA و يتم إرسال التوقيع الرقمي مع المفتاح العام المشفر(وفق خوارزمية تشفير) و الرسالة المشفرة إلى المستقبل .

الخطوة الثالثة (التحقق من التوقيع) :

تتم على ثلاث مراحل :

1- فك تشفير المفتاح العام المشفر المرسل مع التوقيع .

2- فك تشفير الرسالة المرسلة .

3- فك تشفير ملخص الرسالة المشفرة باستخدام المفتاح العام للمرسل .

4- إن المستقبل لا يمكن أن يشتق من الملخص المشفر الرسالة المرسلة، لأن خوارزميات التجزئة ذات اتجاه واحد، لذا يجب عليه أن يقوم بتطبيق خوارزمية التجزئة التي تم استخدامها في مرحلة الإرسال للحصول على ملخص الرسالة من الرسالة التي تم استلامها في الطرف المستقبل.

5 - المقارنة بين ملخص الرسالة في الطرف المستلم وملخص الرسالة بعد فك تشفيره للتحقق من تكامل الرسالة وتوثيقها، ففي حال التطابق بين قيميتي ملخصي الرسالة المرسلة والمستقبلة فإن التوقيع سليم وبالتالي يتحقق مستقبل الرسالة أن الرسالة مرسلة من الشخص المقصود وأنه لم يتم عليها أي تغيير أثناء إرسالها، أما في حالة عدم التطابق فإن الرسالة تعد مرفوضة و أنها تعرضت للتغيير أثناء ارسالها .

9- المصادقة بإستخدام التوقيع الرقمي :

يشير التوقيع الرقمي إلى رمز يُستخدم لمصادقة المستندات التي يتم نقلها عبر الإنترنت .

يعتبر كل توقيع رقمي فريدًا لمستخدم واحد ، مما يعني أنه لا يمكن لأي شخص الحصول على نفس التوقيع مع شخص آخر. باستخدام التوقيع الرقمي ، يمكن لأي شخص التوقيع على وثيقته قبل إرسالها ، وسيتمكن المستلم بسهولة من تأكيد أن المستند ينتمي إلى المرسل. [10]

10- أثر الإنهيار Avalanche Effect :

هو واحد من الخواص المطلوبة في خوارزمية التشفير . اي تغيير خانة واحدة في النص الأصلي أو المفتاح سيسبب تغير ملحوظ لنصف الخانات الناتجة على الأقل في النص المشفر . و هذا الأمر يزيد صعوبة تحليل النص المشفر عند وجود محاولة لهجوم تحليلي على الخوارزمية عن طريق معرفة إحصائيات النص [2] .

و يعبر عن أثر الانهيار بالعلاقة الرياضية التالية :

$$\text{أثر الأنهيار} = \frac{\text{عدد الخانات المشفرة المتغيرة}}{\text{عدد الخانات المشفرة}} * 100\% \qquad (11)$$

11- خوارزمية تشفير RSA المقترحة :

التعديل المقترح على عملية توليد المفاتيح:

1. استخدام أربعة اعداد اولية بدلا من اثنين و هم p,q,r,s:
2. حساب المعامل n وذلك من خلال جداء الأعداد الأولية الأربعة كالتالي :

$$n = p*q*r*s \qquad (12)$$

3. حساب المعامل $\emptyset(n)$ (يتم طرح العدد 1 من كل عدد اولي: p−1 ,q−1 و r−1,s−1 ثم يتم جدائهما) وذلك وفق العلاقة الآتية:

$$\emptyset(n)= (p-1)*(q-1)*(r-1)*(s-1) \qquad (13)$$

4. حساب معامل جديد **z يحسب عشوائياً (من اجل زيادة تعقيد عملية توليد المفاتيح) يقع بين $\emptyset(n)$ و n:**

$$n > z > \emptyset(n)$$

5. حساب معامل جديد $\emptyset(z)$:

$$\emptyset(z) = z - 1 \qquad (14)$$

6. يتم حساب المفتاح العام *e* الذي يستخدم لعملية التشفير بحيث يكون القاسم المشترك الاكبر للمفتاح ***e*** و المعامل $\emptyset(z)$ هو 1 :

$$GCD(\emptyset(z),e) = 1 \qquad (15)$$

7. حساب المفتاح الخاص **d** ، بالأعتماد على قيمة **Ø (z)** والمفتاح العام e وتكون قيمته وفق العلاقة الآتية :

$$d*e = 1 \bmod \emptyset(z) \qquad (16)$$

تقوم الخوارزمية بتجزئة الرسالة الأصلية M إلى كتل بيانات كالتالي :

$$M = [\, m_1 \,, m_2 .. m_z]$$

حيث:

z عدد كتل البيانات

$m_1 \,, m_2 .. m_z$: الكتلة الأولى ، الكتلة الثانية ...الخ

تم التعديل على تابع التشفير :

اذا كانت الكتلة m من الرسالة الأصلية M تمثل عدد زوجي يتم قسمة الكلمة m على العدد 2 ومن ثم رفعها للأس المفتاح وفق التابع :

$$C_i = (m_i / 2)^{e} \bmod n \qquad (17)$$

و اذا كانت الكتلة m تمثل عدد فردي يتم طرح واحد من الكلمة الأصلية ثم قسمتها على 2 وفق التابع التالي :

$$C_i = ((m_i - 1) / 2)^{e} \bmod n \qquad (18)$$

يتم إرفاق متغير k مع كل كلمة يأخذ قيمة 0 اذا كانت الكلمة عدد زوجي و 1 اذا كانت الكلمة عدد فردي .

ويتم إرسال النص المشفر :

$$C=[(c_1 \,, k_1),(c_2 \,, k_2),....(c_z \,, k_z)]$$

عملية فك التشفير :

عند وصول النص المشفر الى المستقبل يقرأ قيمة k :

اذا كانت k = 0 يتم فك التشفيروفق التابع :

$$m_i = (c_i * 2)^{d} \bmod n \qquad (19)$$

اذا كانت قيمة k = 1 يتم فك التشفير :

$$m_i = ((c_i + 1) * 2)^{d} \bmod n \qquad (20)$$

12- التعديل على خوارزمية SHA-1:

تم إضافة تابع وليكن combine يقوم بإستقبال القيم الموجودة في المسجلات B,C,D :

B	C	D
$B_{0,0}$	$C_{0,1}$	$D_{0,2}$
B 1,0	C1,1	D1,2
B 2,0	C2,1	D2,2
B 3,0	C3,1	D3,2

الشكل (2). القيم الموجودة في كل المسجلات B,C,D

يقوم التابع combine بدمج القيم الموجودة في هذه المسجلات :

1. يقوم بتهيئة مصفوفة من ثلاثة أعمدة و أربعة أسطر في كل خلية من المصفوفة يوجد بايت واحد.
2. يتم ملئ المصفوفة بقيم المسجلات الثلاث على الشكل الآتي:

في المصفوفة بشكل أفقي من اليمين الى اليسار .Bاولا: توزع قيم المسجل

.B في الخانة التالية في المصفوفة بعد انتهاء قيم المسجل Cثانيا توزع قيم المسجل

.C في الخانة التالية في المصفوفة بعد انتهاء قيم المسجل Dثالثا : توزع قيم المسجل

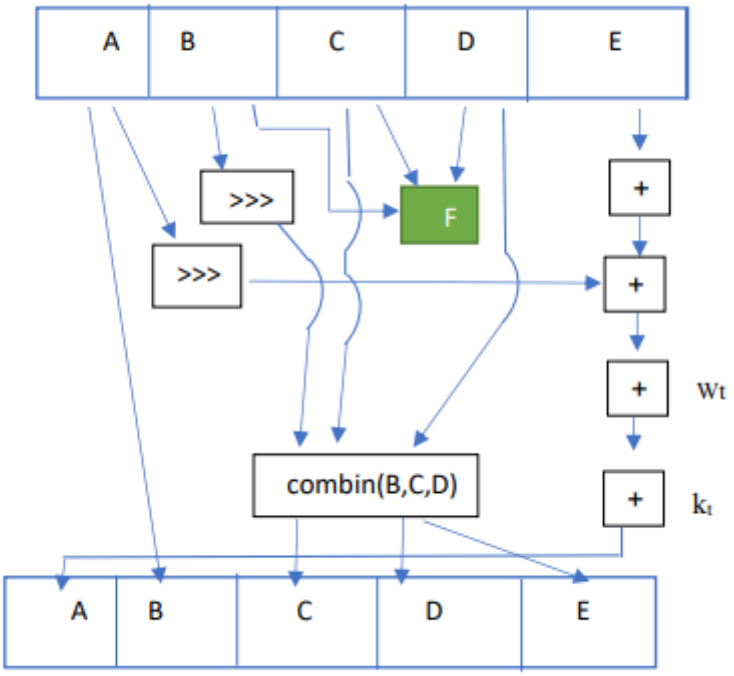
3. إعادة تشكيل قيم المسجلات B,C,D : المسجل B يأخذ قيمه من العمود الأول من اليسار في المصفوفة المتشكلة ، و المسجل C يأخذ قيمه من العمود في المنتصف في المصفوفة ، و المسجل D يأخذ قيمه من العمود الأول بدءاً من اليمين .

B	C	D
B 0,0	C0,1	D0,2
B 1,0	C1,1	D1,2
B 2,0	C2,1	D2,2
B 3,0	C3,1	D3,2

B'	C'	D'
B 2,0	B 1,0	B 0,0
C1,1	C0,1	B 3,0
D0,2	C3,1	C2,1
D3,2	D2,2	D1,2

الشكل (3). دمج المسجلات الثلاث B,C,D

يصبح الشكل العام للخوارزمية :



الشكل (4). مخطط صندوقي للخوارزمية المقترحة

يمثل الشكل (4) آلية عمل الخوارزمية المقترحة من أجل بلوك واحد بوجود التابع combine الذي يقوم بدمج قيم المسجلات الثلاث B,C,D .

13- القسم العملي :

13-1 مقارنة خوارزمية التشفير الأصلية و خوارزمية التشفير المقترحة وفق أختبار معامل الإنهيار:

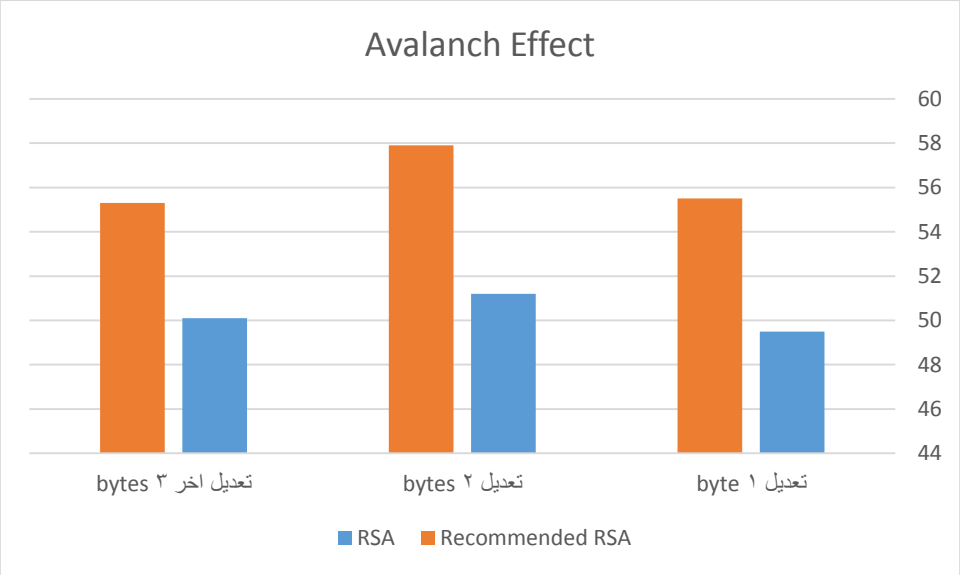
تم أخذ كلمتين مختلفتين في بايت واحد و تطبيق الخوارزمية الأصلية على كل منهما وإظهار نتائج التشفير ثم تطبيق الخوارزمية المقترحة على كل منهما ايضا .

الجدول التالي يظهر نتائج تطبيق اختبار معامل الأنهيار على كل من الخوارزميتين الأصلية و المقترحة بإستخدام برنامج الماتلاب :

Table 1

		Recommended RSA	RSA
Avalanch effect	تعديل 1 byte	55.5	49.5
	تعديل 2 bytes	57.9	51.2
	تعديل اخر 3 bytes	55.3	50.1

من الجدول (1) Table يتبين أن معدل معامل الأنهيار للخوارزمية المقترحة أعلى منه لخوارزمية RSA مما يؤكد أن الخوارزمية المقترحة أكثر أمانا من خوارزمية RSA .



الشكل (5) مخطط بياني يوضح قيم Avalanch Effect لكل من خوارزميتي التشفير الأصلية و المقترحة

يوضح الشكل (5) الفرق بين قيم Avalanch Effect لكل من الخوارزميتين RSA الأصلية و المقترحة في الحالات الثلاث (تعديل بايت واحد ، تعديل 2 بايت ، تعديل 3 بايتات).

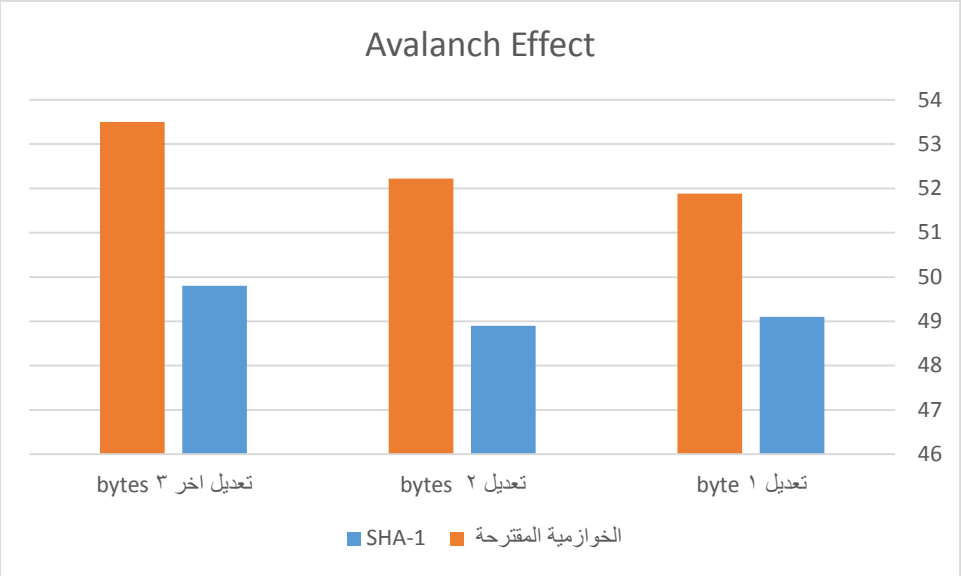
2-13 أختبار خوارزمية التجزئة المقترحة :

: avalanche effect و الخوارزمية المقترحة وفق اختبار SHA-160مقارنة خوارزمية التجزئة الأصلية

تم حساب معامل الأنهيار من أجل خوارزمية SHA-160 و الخوارزمية المقترحة و ذلك في ثلاثة حالات وهي تعديل بايت واحد فقط من الكلمة المراد تطبيق خوارزمية التجزئة عليها، تعديل بايتين من الكلمة ، تعديل اخر ثلاثة بايتات من الكلمة ونلخص النتائج بالجدول Table 2 :

Table 2

	عدد البتات المتغيرة	SHA-1	الخوازمية المقترحة
Avalanch effect	تعديل 1 byte	49.1	51.88
	تعديل 2 bytes	48.9	52.22
	تعديل اخر 3 bytes	49.8	53.5



الشكل (6) مخطط بياني يوضح قيم Avalanch Effect لكل من خوارزميتي التجزئة الأصلية و المقترحة

يوضح الشكل (6) الفرق بين قيم Avalanch Effect لكل من الخوارزميتين SHA-160 الأصلية و المقترحة في الحالات الثلاث (تعديل بايت واحد ، تعديل 2 بايت ، تعديل 3 بايتات).

3-13 اختبار خوارزمية التشفير المقترحة و الخوارزمية الأصلية من حيث زمن التشفير :

يظهر الجدول الآتي الزمن اللازم لعملية التشفير لكل من الخوارزميتين (الخوارزمية الأصلية و الخوارزمية المعدلة) مقدراً بالثانية ، و مقدار الزيادة في زمن فك التشفير للخوارزمية المعدلة عن الخوارزمية الأصلية من أجل خمس ملفات نصية بأحجام مختلفة [32,64,96,128] بايت بإستخدام برنامج الماتلاب نسخة 2013 :

Table 3

حجم الملف (byte)	زمن التشفير للخوارزمية الاصلية RSA	زمن التشفير للخوارزمية المقترحة
32	0.0002	0.0003
64	0.0010	0.002
96	0.005	0.006
128	0.01	0.02

تظهر النتائج في الجدول (3) أن الخوارزمية المقترحة تستهلك زمن تشفير أكثر من الخوارزمية الأصلية عند جميع الملفات النصية المختلفة الحجم وسبب ذلك أن عملية التشفير في الخوارزمية المقترحة أكثر تعقيداً من خوارزمية RSA .

14- الإستنتاجات و التوصيات :

14-1 الإستنتاجات :

1. ارتفاع قيمة معامل الأنهيار في خوارزمية التجزئة المقترحة مقارنة مع الخوارزمية الأصلية SHA-160.
2. ارتفاع قيمة معامل الأنهيار في خوارزمية RSA المقترحة مقارنة مع خوارزمية RSA الأصلية .
3. عملية توليد المفاتيح وعمليتي(التشفير و فك التشفير) في خوارزمية RSA المقترحة أكثر تعقيد من الخوارزمية الأصلية مما يصعب على المهاجم معرفة المفاتيح و فك تشفير الرسالة المشفرة.

14-2 التوصيات :

1. نوصي بتحسين خوارزمية التجزئةSHA1 بإضافة التابع الذي تم اقتراحه في في SHA1 المقترحة .
2. نوصي بتحسين خوارزمية التشفير RSA من خلال اعتماد النموذج المقترح لتوليد المفاتيح و عملية التشفير و فك التشفير .

المراجع :

[1]. Pipkin, Donald, L. Information Security: Protecting the Global Enterprise. Upper Saddle River, NJ: Prentice Hall, 2000.

[2]. Malinowski, C.; and Noble, R. (2007). Hashing and data integrity reliability of hashing and granularity size reduction. Digital Investigation, 4(2), 98-104.

[3]. Locktyukhin, Max (2010-03-31), "Improving the Performance of the Secure Hash Algorithm (SHA-1)", Intel Software Knowledge Base, retrieved 2010-04-02.

[4]. P. Garg and N. Tiwari, "Performance Analysis of SHA Algorithms (SHA-1 and SHA-192): A Review," Int. j .comput. technol. electron. eng., vol. 2, no. 3, pp. 130-132, 2012.

[5]. Zakary Kessler," U.S. Law And Not Technology Is Preventing The Commercial Mortgage Market From Transitioning To A Paperless Emortgage", Journal on Telecommunications and High Technology Law, Volume 11, 2013, pp466.

[6]. Mohamad Ali Sadikin, Rini Wisnu Wardhani, "Implementation Of RSA 2048-Bit And AES 256-Bit With Digital Signature For Secure Electronic Health Record Application", Communication & Information Technology, vol 10, 2016, pp64-65.

[7]. Mrs. S. M. Barhate1 , Dr. M. P. Dhore2, User Authentication Issues In Cloud Computing, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 30. (2016).

[8]. Shireen Nisha, Mohammed Farik, "RSA Public Key Cryptography Algorithm", International Journal of Scientific & Technology Research, Vol 6, ISSUE 07, ISSN 2277-8616, 2017, pp187-188.

[9]. Shivani Sharma, Yash Gupta, "Study on Cryptography and Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol 2, Issue 1, ISSN: 2456-3307, 2017, PP251-525.

[10]. Debabrata Sarddar, Mousumi Biswas, Priyajit Sen and Rajat Pandit, Authentication using Unique Identification Number in Cloud Network using RSA Algorithm, nternational Journal of Grid and Distributed Computing Vol. 10, No. 4 (2017), pp.1-8.

[11]. http://en.wikipedia.org/wiki/digital_signature,2018/5/1

[12]. Gurpreet K. Sodhi, Gurjot s. Gaba, "AN EFFICIENT HASH ALGORITHM TO PRESERVE DATA INTEGRITY", Journal of Engineering Science and Technology Vol. 13, No. 3 (2018) 778 – 789.

[13]. M. Almazrooie, A. Samsudin, A. A. Gutub, M. S. Salleh, M. A. Omer and S. A. Hassan, "Integrity verification for digital Holy Quran verses using cryptographic hash function and compression," J. king Saud Univ. Comput. Inf. Sci., vol. 32, no. 1, pp. 24-34, Jan. 2020.

[14]. S.Hendry Leo Kanickam and Dr. L. Jayasimman "Enhanced Authentication Mechanism to Protect Unauthorized Access in Public Cloud Environment" , Mukt Shabd Journal , Volume IX, Issue IV, ISSN 2347-3150, 2020, pp 414-420.