معمارية مطورة لاستخدام خوارزمية MD5 في التوقيع الرقمي للملفات النصية

Advanced Architecture For Using MD5 Algorithm of Text File Digital Signature

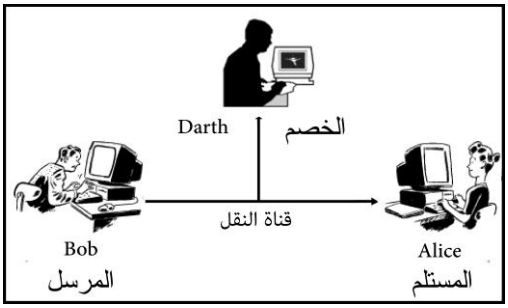
الدكتور
حميد عبد الكريم يونس

الباحث
عبد الكريم حسين عبد الكريم

جامعة البصرة ـ كلية العلوم

1. المقدمة Introduction

عرفت الوثوقية منذ زمن بعيد فمثلا" عندما يرغب شخصان أن يكون بينهما رسول لنقل المعلومات أو المواد فأنهما يقومان بتقسيم عملة نقدية إلى قسمين كل منهما يحتفظ بقسم ويتفقان إذا جرى إرسال شخص يحمل نصف العملة النقدية إلى أحدهما يقوم بمطابقتها مع النصف الآخر للعملة النقدية فإذا تطابقت فإن الشخص المرسل هو شخص موثوق به. هذا ومن الطرائق البدائية للوثوقية هي اتفاق شخصين على كلمة سرية بينهم، وهي تعد وسيلة للتأكد من وثوقية الشخص الحامل للمعلومات. أما في الاتصالات ضمن شبكة الحاسبات فيجب أن نعرف ونملك الطرائق التي من خلالها نتأكد من معرفة هوية الشخص الذي نتعامل معه. نفرض أن المرسل يقوم بإرسال معلومات إلى المستلم من خلال قناة النقل Transmission Channel والواقعة تحت سيطرة الخصم كما في الشكل (1):



الشكل (1): سيطرة الخصم على قناة النقل

فيكون الهدف من الوثوقية معالجة الحالات الآتية:

١- قيام الخصم بإرسال رسالة ليوهمنا بأنها جاءت من شخص مخول.

٢- تغيير محتوى الرسالة.

٣- إنكار المرسل بإرساله الرسالة Source Repudiation.

٤- إنكار المستلم باستلامه الرسالة Destination Repudiation.

ومن هنا يمكن تعريف الوثوقية أنها الأسلوب الذي يستخدم للتأكد من هوية المرسل للرسالة ولذلك من عدم تغير الرسالة أثناء الإرسال بالإضافة لوجوب توفير وسيلة ليتأكد من خلالها المرسل من وصول رسالته إلى المستلم المعني والذي يمكن تحقيقه من خلال قيام المستلم بإرسال اشارة الى المرسل يعلمه بها باستلامه الرسالة [4] [3] [2] [1].

مع انتشار شبكات الحاسبات بشكل كبير في العالم، خاصة وأن هذه الشبكات متصلة مع آلاف من المحطات الطرفية المختلفة، لذا فقد أصبحت مسألة توفير الحماية للمعلومات من المسائل الضرورية والجوهرية في هذه الشبكات. إن عملية تحقيق الحماية تتضمن تحقيق السرية والوثوقية للبيانات. وتقسم الوثوقية إلى جزئين هما:

١- وثوقية المستخدم User Authentication.

٢- وثوقية الرسالة Message Authentication.

إن وثوقية المستخدم يمكن أن تطبق إما بصورة مباشرة بالاستفادة من خصائص معينة موجودة في المستخدم كبصمة الإصبع، وتردد الأمواج الصوتية، وأشكال شبكية العين، وراحة اليد، وتوقيع المستخدم، ونمط الكتابة لدى المستخدم. أو بصورة غير مباشرة عندما يكون لدى المستخدم كلمة سرية خاصة به. أما وثوقية الرسالة فهي مشابهة لوثوقية المستخدم (المطبقة بصورة غير المباشرة) حيث أن كون هذه الطريقة تفرض هيكلة للرسالة معدة مسبقا". وهناك عدة أنواع ومستويات للوثوقية بعض من هذه الأنواع يوفر الوثوقية للرسالة دون الحاجة لتوفير السرية، والبعض الآخر يوفر الوثوقية والسرية معا.

بعد ظهور الاتصالات الإلكترونية في العقود الأخيرة والتطور الواسع في هذا المجال فقد تغيرت الرسائل الورقية التي كانت تتبع في الاتصالات ولمدة طويلة إلى رسائل إلكترونية، فأصبح من الضروري إيجاد تقنية توفر وتضمن السرية للرسائل الإلكترونية بعد أن كان التوقيع الخطي يوفر هذا الجانب. إن تزايد التطور في معالجة المعلومات وتراسلها في أنظمة وشبكات الحواسيب أظهر العديد من الاحتياجات. وبما أن الحاسبات تتعامل مع المعلومات بشكل رقمي، لذلك يجب تحويل التواقيع الخطية إلى أرقام. ومن هنا برزت الحاجة إلى ظهور التواقيع الرقمية كسبيل أمثل لتحقيق هذه الغاية [5] [6].

في عام ٢٠١٠، قدم Li Xiao-fei وآخرون [7] طريقة معدلة لحل ضعف السرية المتولدة بطريقة الجمال للتوقيع الرقمي. يتم ذلك التعديل بإضافة رقم عشوائي إلى الطريقة ليزيد من صعوبة مفتاح فك الشفرة وتحسين السرية. في عام ٢٠١٣، قدم حميد وآخرون [8] خوارزمية لتوقيع ملف نصي. يتم استخدام خوارزمية التشفير RSA الشهيرة ذات المفتاح العام وخوارزميات (SHA-1 و MD5) لإنشاء توقيع رقمي من ملف نصي.

يهدف هذا البحث إلى اقتراح طريقة لتحقيق الوثوقية باستخدام آلية التوقيع الرقمي للملفات النصية وبالاعتماد على خوارزمية الاختزال MD5 بعد إجراء تطوير عليها لجعلها أكثر أمانا بالإضافة الى الاعتماد على خوارزمية التشفير الشهيرة RSA ذات المفتاح العام. ومن أهم مميزات هذا البحث سهولة توليد توقيع رقمي للملفات النصية صعب الكسر التوقيع مما يعطي قوة أمنية مضاعفة وبدرجة تعقيد أقل من الخوارزميات المستخدمة سابقا مع المحافظة على زمن التنفيذ نفسه تقريبا ودون الحاجة إلى أجهزه مادية إضافية مما يعطي قوة وبساطة وأفضلية استخدام على الخوارزميات السابقة.

2. مبادئ أساسية Basic Principles

1.2 التواقيع الرقمية Digital Signatures

يعد التوقيع الرقمي أحد التطبيقات المهمة لأنظمة التشفير اللامتماثل (أنظمة تشفير المفتاح العام). والتوقيع الرقمي لوثيقة ما هو عبارة عن مقطع من البيانات يعتمد على كل من الوثيقة والمفتاح الخاص Private Key للموقع (المرسل للوثيقة)، هذا المقطع من البيانات يجري إضافته إلى الرسالة الإلكترونية لإثبات هوية مرسلها وسلامة محتوياتها خلال عملية إرسالها عبر قناة النقل Transmission Channel ضمن شبكة الحواسيب [1] [6].

1.1.2 صفات التوقيع الرقمي Characteristics of Digital Signature

النقطة الأساسية لاستعمال التوقيع الرقمي هي أنه يمثل الطريقة الرياضية لحل مشكلتين أساسيتين هما:

- تعريف الشخص المرسل للرسالة (وهذه تحل مشكلة تحديد هوية المرسل (IDENTITY PROBLEM)).
- تحدد بسهولة فيما إذا كانت الرسالة قد تعرضت إلى تغيير أثناء الإرسال (وهذه الصفة تحل مشكلة سلامة الرسالة وكمالها (THE MESSAGE INTEGRITY PROBLEM)).

وكذلك بالإمكان استعمال التوقيع الرقمي لحل مشكلة الإنكار لأن الرسالة إذا جاءت من المرسل مع توقيعه الرقمي فأنه لا يمكنه إنكار ارسال الرسالة [10]. ويجب أن تحمل التواقيع الرقمية بعض المواصفات كما تحملها التواقيع اليدوية وهي[9] [11]:

١. الأحادية (UNIQUE): التوقيع الرقمي يمكن أن يولد عن طريق المستخدم (المرسل) فقط.
٢. صعوبة التزوير (UNFORGEABLE): إن عملية توليد توقيع موثوق به من قبل الأشخاص الآخرين الذين يحاولون تزوير التوقيع الأصلي صعبة جداً، وهذا ناتج من أن الشخص المتطفل سيواجه مشكلة رياضية صعبة فيما لو حاول تزوير التوقيع.

٣. سهولة الموثوقية Easy-To Authenticate: يجب أن يحدد المستلم (المستقبل) عائدية التوقيع (أصل كاتب التوقيع) حتى ولو كان بعد وقت طويل.

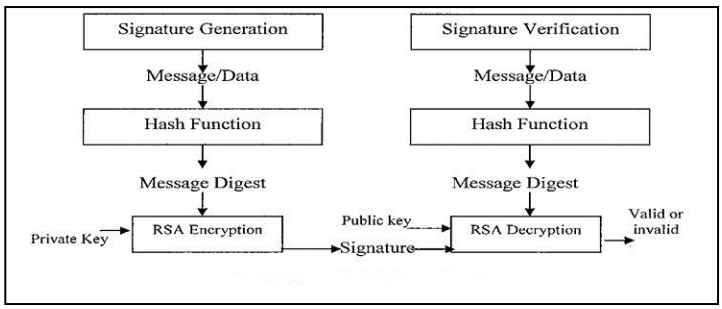
٤. عدم النكران Impossible-To Deny: أي أن الشخص الموقع لا يمكنه رفض أو إنكار توقيعه الصحيح أو عده مزوراً.

٥. سهولة ورخص كلفة التوليد: تعد طريقة توليد التوقيع رخيصة فضلاً عن أنها سهلة التطبيق للمرسل والمستلم.

يجب أن نلاحظ الفرق بين التواقيع اليدوية و التواقيع الرقمية إذ أن التواقيع اليدوية لا تتغير مهما تغيرت الورقة أو الوثيقة المراد توقيعها، ولكن التواقيع الرقمية تكون غير ثابتة وتتغير لأن شكل التوقيع الرقمي يعتمد على محتوى الورقة أو الوثيقة المراد توقيعها وكما يعتمد على المفتاح الخاص للشخص الموقع [12] [2].

2.2 مميزات طريقة التواقيع الرقمية RSA Signature Scheme (RSA)

تعتمد هذه الطريقة في قوتها على صعوبة تحليل الأعداد الكبيرة جداً إلى عواملها الأولية وسُميت بهذا الاسم تبعاً لأسماء مطوريها وهم R. Rivest و S. Shamir و A. Adleman وهي أول خوارزمية مفتاح عام تامة النضج. يبين الشكل (2) وصفا لهذه الطريقة [13].



الشكل (2): طريقة التوقيع RSA

تُستخدم RSA كطريقة للتوقيع الرقمي فضلاً عن كونها نظام تشفير بالمفتاح العام.

من أجل توقيع رسالة ما x يقوم الموقّع Signer باستخدام قاعدة RSA لفك التشفير d_k وهو الشخص الوحيد الذي يستطيع أن يُحدث التوقيع ما دام $d_k = sig_k$ هو سرياً وتستخدم خوارزمية التحقُّق من التوقيع قاعدة RSA للتشفير e_k ، إذ يستطيع أي شخص أن يتحقق من التوقيع مادامت e_k علنية ومن هنا فإن أي شخص يستطيع تزوير التوقيع y على الرسالة x وذلك بحساب: $x = e_k(y)$ ثم حساب: $y = sig_k(x)$.

غير أن استخدام دوال الاختزال الوحيدة الاتجاه One-way Hash Functions مع هذه الطريقة يُبعد هذا النوع من التزوير. تمر عملية التوقيع وفقا لطريقة RSA بالخطوات الآتية:

١- يستخدم المرسل خوارزمية الاختزال Hashing لإنشاء مستخلص الرسالة Message Digest (أو ما يسمى بصمة إصبع Fingerprint).

٢- يحدث بعد ذلك تشفير مستخلص الرسالة والمعلومات الشخصية المتعلقة بالمرسل والطابع الزمني أحياناً Time stamp باستخدام المفتاح الخاص للمرسل ليجري إنشاء التوقيع DS.

٣- تُلحق السلسلة المحرفية المُشفرة نصيا (التوقيع الرقمي DS) بالرسالة ثم يشفّر كل شيء باستخدام المفتاح العام للمستلم.

وبذلك يكون قد حدث التوقيع على الرسالة وتشفيرها وإرسالها إلى الهدف (المستلم).

٤- عند استرداد الرسالة تقوم برمجية التشفير لدى المستلم بفك تشفير الرسالة وذلك باستخدام المفتاح الخاص بهذا المستلم الأمر الذي يؤدي إلى عرض DS والرسالة النصية الصريحة الأصلية.

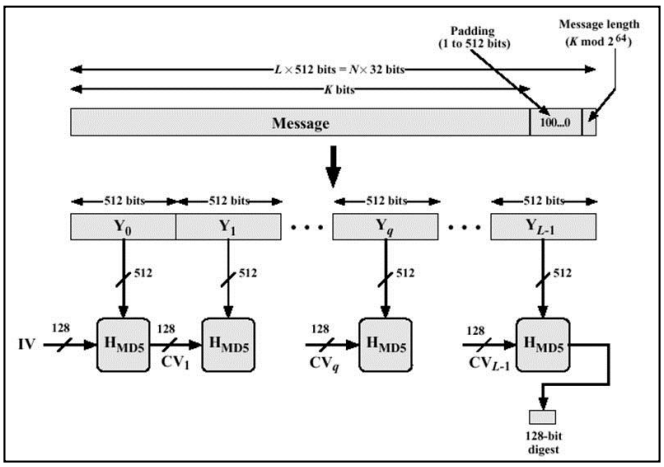
٥- يحدث فك تشفير DS المستخلص من الرسالة باستخدام المفتاح العام للمرسل مما يكشف عن مستخلص الرسالة الأصلية.

٦- باستخدام الخوارزمية نفسها التي يملكها المرسل تقوم برمجية المستلم باستخلاص مستخلص الرسالة المستلمة ثم يقارن هذا المستخلص الناتج مع مستخلص الرسالة الأصلية، إذ يؤكد تطابقهما هوية الشخص المرسل(الوثوقية) وسلامة محتويات الرسالة، كما وتوفر العملية مقياس أمان بميزة عدم التنصل الذي من شأنه أن يمنع إنكار الاشتراك في معاملة رقمية.

3.2 خوارزمية مستخلص الرسالة Message Digest Algorithm (MD5) المطورة.

تتميز هذه الخوارزمية بتحويل الرسالة المدخلة بأي طول إلى بصمة ثابتة ذات طول ١٢٨ بت وقد اقترحنا في هذا البحث تطوير لهذه الخوارزمية لتعطينا بصمة ثابتة ذات طول ١٦٠ بت وفيما يلي تفصيل لطريق عمل هذه الخوارزمية.

تقوم بتقسيم الرسالة إلى كتل بطول 512 bits، الشكل (3) يوضح الهيكل العام لهذه الخوارزمية [1]:



الشكل(3): الهيكل العام لخوارزمية MD5

الخطوة ١: إضافة ثنائيات تكميله: يجري إضافة عدد من الثنائيات بين [1..512] في نهاية الرسالة بحيث يكون طول الرسالة الناتجة من مضاعفات العدد ٥١٢. الثنائيات المضافة له الشكل [1000...].

الخطوة ٢: إضافة طول الرسالة الأصلية: يجري إضافة 64-bit تمثل طول الرسالة الأصلية في نهاية الثنائيات المضافة في الخطوة ١. فإذا كان طول الرسالة k-bit فإننا نضيف القيمة $K \text{ Mod } 2^{64}$. ناتج الخطوتين أعلاه هو رسالة بطول L*512 bits وبالإمكان عدّها مجموعة كلمات بطول 32-bit أي M[0..N-1] بحيث إن N=L*16.

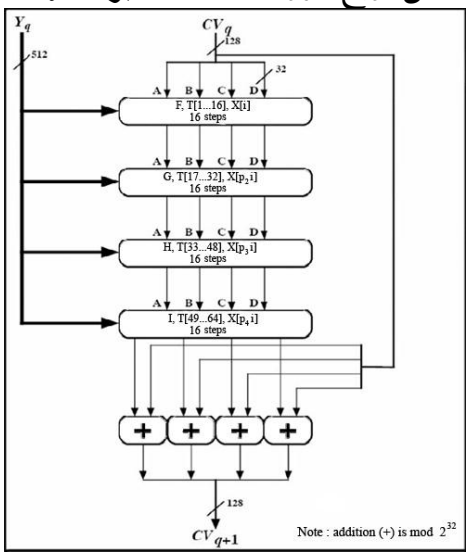
الخطوة ٣: تهيئة المسجلات A, B, C, D يحدث تهيئة هذه المسجلات ذات الطول 32-bit بالقيم الابتدائية الآتية :

A=67452301
B=efcdab89
C=98badcfe
D=10325476

النتيجة النهائية للخوارزمية توجد في هذه المسجلات 128-bit = 4*32-bits .

IV=(ABCD) …(1)

الخطوة ٤: معالجة كتل الرسالة بطول (16-word) 512-bit، هذه الخطوة تمثل قلب الخوارزمية وتتألف من أربع دورات rounds يوضحها الشكل (4):



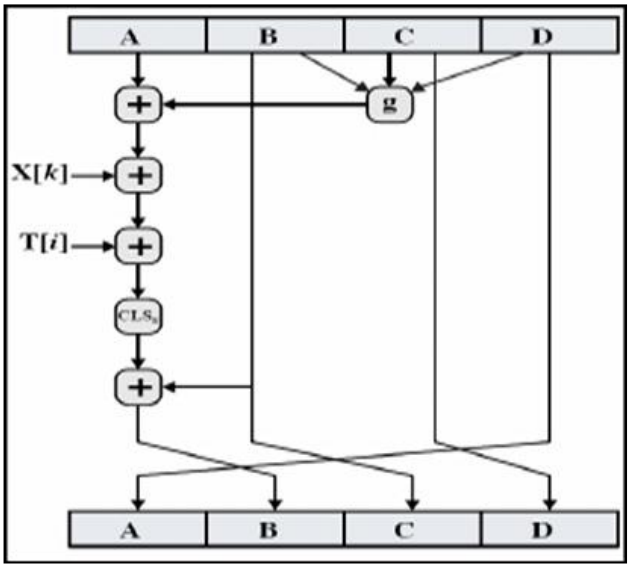
الشكل (4): معالجة كتل الرسالة

ملاحظة: كل دورة لها دالة خاصة بها: F, G, H, I ، كل دورة فيها ١٦ خطوة steps.

في كل دورة round يتم إجراء ١٦ خطوة على المسجلات ABCD بالصيغة الآتية:

$$b=b+ ((a+g (b, c, d) +X[k] +T [i]) <<<s) \quad \ldots(2)$$

كما في الشكل (5) الذي يوضح عمل الخطوة الواحدة:



الشكل(5): الدورة الواحدة لكل دالة

حيث إن g هي إحدى الدوال التالية F, G, H, I كما في الجدول الآتي :

الجدول (1): الدوال المستخدمة في الخوارزمية

Round	Function	g(b,c,d)
1	F(b,c,d)	(b^c) OR (b^d)
2	G(b,c,d)	(b^d)OR (c^d)
3	H(b,c,d)	b XOR c XOR d
4	I(b,c,d)	c XOR (b OR d)

الجدول (2) يوضح قيم T والتي تحسب كما يلي:

$$T(i)=floor(2^{32}*abs(sin(i))) \quad \ldots(3)$$

الجدول (2): قيم المتغير T

T[1] = D76AA478	T[17] = F61E2562	T[33] = FFFA3942	T[49] = F4292244
T[2] = E8C7B756	T[18] = C040B340	T[34] = 8771F681	T[50] = 432AFF97
T[3] = 242070DB	T[19] = 265E5A51	T[35] = 699D6122	T[51] = AB9423A7
T[4] = C1BDCEEE	T[20] = E9B6C7AA	T[36] = FDE5380C	T[52] = FC93A039
T[5] = F57C0FAF	T[21] = D62F105D	T[37] = A4BEEA44	T[53] = 655B59C3
T[6] = 4787C62A	T[22] = 02441453	T[38] = 4BDECFA9	T[54] = 8F0CCC92
T[7] = A8304613	T[23] = D8A1E681	T[39] = F6BB4B60	T[55] = FFEFF47D
T[8] = FD469501	T[24] = E7D3FBC8	T[40] = BEBFBC70	T[56] = 85845DD1
T[9] = 698098D8	T[25] = 21E1CDE6	T[41] = 289B7EC6	T[57] = 6FA87E4F
T[10] = 8B44F7AF	T[26] = C33707D6	T[42] = EAA127FA	T[58] = FE2CE6E0
T[11] = FFFF5BB1	T[27] = F4D50D87	T[43] = D4EF3085	T[59] = A3014314
T[12] = 895CD7BE	T[28] = 455A14ED	T[44] = 04881D05	T[60] = 4E0811A1
T[13] = 6B901122	T[29] = A9E3E905	T[45] = D9D4D039	T[61] = F7537E82
T[14] = FD987193	T[30] = FCEFA3F8	T[46] = E6DB99E5	T[62] = BD3AF235
T[15] = A679438E	T[31] = 676F02D9	T[47] = 1FA27CF8	T[63] = 2AD7D2BB
T[16] = 49B40821	T[32] = 8D2A4C8A	T[48] = C4AC5665	T[64] = EB86D391

الكلمات X[1..16]: تدخل بالبعثرة الآتية:

الجدول (3): بعثرة الكلمات في كل دورة

الدورة	بعثرة الكلمات
Round 1	بدون بعثرة
Round 2	P2(i) = (5i - 4) mod 16
Round 3	P3(i) = (3i + 2) mod 16
Round 4	P4(i) = (7i - 7) mod 16

حيث أن:

s>>>: تدوير نحو اليسار بمقدار s.

X[k]: هي إحدى الكلمات بطول 32-bit من الكتلة المدخلة.

T[i]: الكلمة رقم i من المتجه T.

+ : تعني عملية جمع $\mod 2^{32}$.

$A = (A + AA) \bmod 2^{32}$ …(4),
$B = (B + BB) \bmod 2^{32}$ …(5),
$C = (C + CC) \bmod 2^{32}$ …(6),
$D = (D + DD) \bmod 2^{32}$ …(7).

الخطوة ٥: الإخراج: بعد معالجة جميع الكتل L فان الإخراج هو 128-bit للكتلة الأخيرة.

$MD= CV_{L-1}$ …(8)

إلى هنا تكون خوارزمية MD5 المعروفة قد انتهت ومن هنا تبدأ خوارزميتنا التي أطلقنا عليها(Advanced MD5 (AMD5.

الخطوة ٦: الإخراج في الخطوة ٥ يمثل إخراج خوارزمية MD5 المعروفة بحيث سيكون طول البصمة ١٢٨ بت، وفي هذه الخطوة يكون الإخراج في الخطوة ٥ إدخالاً لهذه الخطوة، ويتم تهيئة خمسة سجلات كالآتي:

A=67452301

B= efcdab89

C=98badcfe

D=10325476

E= c3d2elf0

الخطوة ٧: يتم تطبيق دورة جديدة (أي ١٦ خطوة) على كتلة البيانات الناتجة من الخطوة ٦ مع السجلات الجديدة:

b=b+ ((a+e+g (b, c, d) +X[k] +T [i]) <<<s) ...(9)

باستخدام الدالة K والتي لها الصيغة الآتية:

K (A, B, C) = (a^b) OR (a^c) OR (b^c) …(10)

الخطوة ٨: الإخراج بعد المعالجة يكون الإخراج في السجلات بطول ١٦٠ بت موجودة في السجلات الخمسة.

H=ABCDE …(11)

على سبيل المثال: لو كانت الرسالة المدخلة "Message Digest 5" سيكون اخراج دالة الاختزال MD5 كالآتي:

$(211B88402AC7072606EC70F190BA5DD0)_{Hex}$

بينما سيكون إخراج دالة الاختزال الجديدة AMD5 كالآتي:

$(9E7F36B7083195E3B535027917AC7D078D89E06B)_{Hex}$

3. طريقة التوقيع الرقمي المقترحة Proposed Method of Digital Signature

1.3 توليد التوقيع Signature Generation

في هذه الخوارزمية سيقوم المرسل بتوقيع رسالته باستخدام مفتاحه الخاص ومن ثم إرسال رسالته كما يتّضح بالخطوات الآتية:

١- **اختيار الرسالة (Message Choosing):** يتم هنا تحديد الرسالة المراد توقيعها، وفي بحثنا هذا تكون الرسالة عبارة عن ملف نصي Text File.

٢- **دالة الاختزال (Hash Function):** هنا سنستخدم خوارزميتنا AMD5 لحساب قيمة دالة الاختزال بطول ١٦٠ بت.

٣- **توليد المفتاح (Key Generation):** يجري اختيار المفاتيح طبقا لشروط خوارزمية RSA المعروفة مثل اختيار عددين أوليين p, q وحساب قيم n و e وd حسب المعادلات في خوارزمية RSA.

٤- **قبل التشفير (Pre-encryption):** في هذه الخطوة يتم تهيئة قيمة Hash عن طريق تحويلها إلى متجه من البايتات، يتكون المتجهVec من ٢٠ بايت ومن ثم دمج كل بايتين في بلوك واحد باستخدام المعادلة الآتية:

$$Block= (byte_1 *256) +byte_2 \quad ...(12)$$

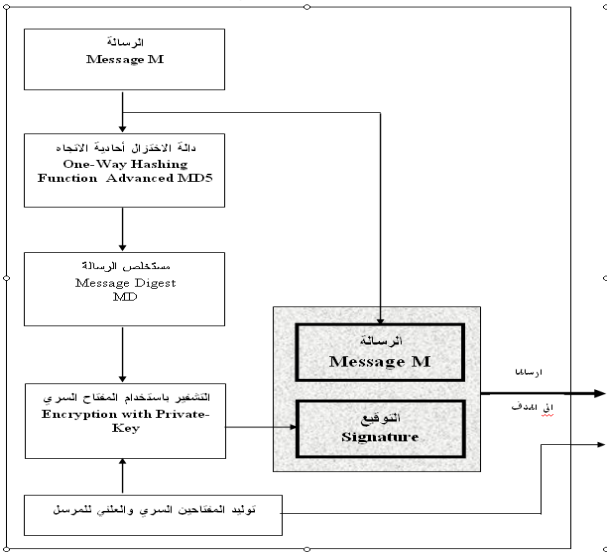
حساب التوقيع (Sign Computation): في هذه الخطوة يستخدم المفتاح الخاص d للمرسل لتشفير كل رقم M في المتجه الناتج من الخطوة السابقة باستخدام المعادلة الآتية:

$$C=M^d \bmod n \quad \ldots(13)$$

وبعده يتم تحويل المتجه الناتج إلى النظام السداسي عشر والذي يمثل التوقيع الرقمي للرسالة.

١- إضافة التوقيع (Sign Appending): يجري هنا إضافة التوقيع الذي حصلنا عليه في أسفل الرسالة.

ويوضح الشكل (6) خوارزمية توليد التوقيع الرقمي:



الشكل (6): عملية التوقيع الرقمي لدى المرسل أو الموقع

2.3 التحقق من التوقيع Signature Verification

١- وثوقية التوقيع (Signature Authentication): يقوم المستلم بفك التوقيع بتحويله من النظام السداسي عشر إلى النظام العشري ومن ثم فك التشفير باستخدام المفتاح العام e باستخدام المعادلة الآتية:

$M=C^e \bmod n$ …(14)

ينتج هنا متجه رقمي نقوم بإعادته إلى البايتات عن طريق المعادلة التالية:

$Byte_1= block/256$ … (15), □

$Byte_2= mod (block, 256)$ ...(16)

النتيجة النهائية لهذه الخطوة تمثل بصمة رقمية متكونة من ١٦٠ بت.

٢- حساب قيمة دالة الاختزال للرسالة المستلمة (Hash Code Computation):

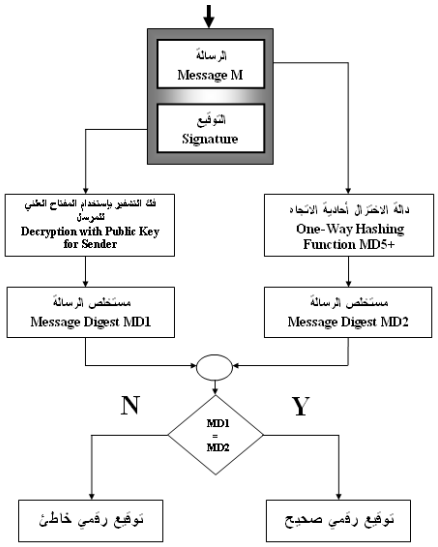
يتم حساب شفرة دالة الاختزال للرسالة المستلمة باستخدام نفس خوارزمية الاختزال المستخدمة في توليد التوقيع وسيكون الناتج بصمة بطول ١٦٠ بت سيتم مقارنتها مع البصمة الناتجة من الخطوة ١ وبعدها سنحصل على النتائج الآتية:

أ- الرسالة لم تتغير أثناء النقل لأن البصمتين متطابقتين.

ب- الرسالة موثوقة لأنه تم فكها باستخدام المفتاح العام للمرسل.

ج- عدم تنصل المرسل بسبب توليد بصمة صحيحة باستخدام مفتاح المرسل العام.

والشكل (7) يوضح خوارزمية التحقق من التوقيع الرقمي:



الشكل (7): عملية التحقق من التوقيع الرقمي لدى المستلم.

4. العمل التجريبي Experimental Results

بعد السرد النظري للطرائق والأساليب شائعة الاستخدام في مجال تحقيق الوثوقية والتكامل للبيانات المرسلة ضمن شبكة الحواسيب، سنناقش هنا بعض التجارب على استخدام الطريقة المقترحة وباستخدام لغة البرمجة MATLAB.

1.4 التجارب

التجربة الأولى Experiment 1

Message Digest 5

في هذه التجربة سيتم توليد التوقيع الرقمي كالآتي. أولاً، سنقوم بحساب قيمة دالة الاختزال وحيدة الاتجاه للنص المدخل باستخدام الخوارزمية المطورة والتي ستكون إخراجها بصمة H ذات طول ١٦٠ بت.

$$H=(9E7F36B7083195E3B535027917AC7D078D89E06B)_{Hex}$$

بعدها سنستخدم المعلمات الآتية لتوليد المفتاح لخوارزمية RSA.

-p=211,q=227,

-Compute n=p*q=211*227=47897.

-Phi=2110*226=476860.

-Select the public key e=65537.

- Compute the private key d by using extended Euclid algorithm. We obtain d=45953.

الآتي:Vec سنحصل على المتجه Pre-encryptionفي خطوة ما قبل التشفير

Vec=[14661, 14150, 13110, 16951, 12344, 13105, 14645, 17715, 16949, 13109, 12338, 14137, 12599, 16707, 14148, 12343, 14404, 14393, 17712, 13890].

بعدها وفي خطوة حساب التوقيع نحصل على التوقيع الآتي:

Sing=(139883B6885A61A0966A01BA0AA46FC299BEB524343 66E354D65E41306ADBA013DBB3D5F44644A5A)$_{Hex}$□

وهنا يتم إضافة التوقيع الناتج في أسفل الرسالة الموقعة قبل إرسالها إلى الهدف.

التجربة الثانية Experiment 2

في هذه التجربة سيتم التحقق من وثوقية الرسالة الموقعة في التجربة الأولى وذلك عن طريق أولاً سنقوم بحساب قيمة دالة الاختزال وحيدة الاتجاه للنص المستلم باستخدام خوارزمية AMD5 والتي ستكون إخراجها بصمة H ذات طول ١٦٠ بت.

H=(9E7F36B7083195E3B535027917AC7D078D89E06B)$_{Hex}$

وستكون قيمة المتجه Vec هي:

Vec=[14661, 14150, 13110, 16951, 12344, 13105, 14645, 17715, 16949, 13109, 12338, 14137, 12599, 16707, 14148, 12343, 14404, 14393, 17712, 13890].

بعدها سنستخدم المفتاح العام e للمرسل لفك شفرة التوقيع المستلم مع الرسالة لغرض التحقق منه عن طريق مقارنة ناتج فك شفرة التوقيع مع قيمة H ناتج خوارزمية AMD5، وهنا سيكون التوقيع صحيح أيّ أنّ الرسالة موثوقة ولم تتغير أثناء النقل بين المرسل والمستلم.

التجربة الثالثة Experiment 3

في هذه التجربة سنستخدم قيمة جديدة للمفتاح العام e للمرسل لفك شفرة التوقيع المستلم مع الرسالة في التجربة الأولى للتحقق من صحة التوقيع. مثلاً لو أخذنا e=65536 فهنا سنحصل على قيمة المتجه Vec التالي لـH كالتالي:

Vec=[16126, 24247, 15518, 13137, 47218, 40652, 22374, 19570, 36362, 4352, 43245, 22366, 25339, 2793, 45429, 11440, 8121, 19827, 43800, 19579].

وهنا نلاحظ ان القيمة الجديدة مختلفة جدا عن القيمة الأصلية وهذا يعني أن الرسالة المستلمة غير موثوقة والتوقيع غير صحيح.

التجربة الرابعة Experiment 4

في هذه التجربة سيتم اختبار حالة تغير قيمة التوقيع الرقمي المولد للرسالة في التجربة الأولى ومدى قابلية الخوارزمية المقترحة على التأكد من وثوقية الرسالة. مثلاً لو كان التوقيع المستلم مع الرسالة كالآتي:

Sing=(139883B6885A61A0966A01BA0AA46FC299BEB524343 66E354D65E41306ADBA013DBB3D5F44644A54)$_{Hex}$

والذي تكون فيه آخر مرتبة قد تغيرت من A إلى 4 فهنا سنحصل على قيمة المتجه Vec الآتي:

Vec=[14661, 14150, 13110, 16951, 12344, 13105, 14645, 17715, 16949, 13109, 12338, 14137, 12599, 16707, 14148, 12343, 14404, 14393, 17712, 12462].

والتي تكون آخر قيمة مختلفة عن القيمة المناظرة لها في المتجه Vec الناتج عن قيمة H للرسالة الأصلية وهذا يعني أن الرسالة غير موثوقة بسبب حدوث تغيير فيها. وهنا تكتشف قوة الخوارزمية في اكتشاف عملية تزوير التوقيع الرقمي للمرسل.

التجربة الخامسة Experiment 5

في هذه التجربة سيتم اختبار مدى حساسية خوارزمية الاختزال المطورة بواسطة تغيير بايت واحد فقط من الرسالة المرسلة إثناء النقل. بعدها سنقارن نتيجة خوارزمية الاختزال في التجربتين (هنا غيرنا فقط الحرف الكبير D إلى الحرف الصغير d).

Message digest 5

سنلاحظ أنّ قيمة دالة الاختزال المطورة ستكون كالأتي:

$$H=(65B314AE55625F8AE36F0CC9DEE6C3E454A4030F)_{Hex}$$

هنا سنلاحظ الاختلاف الواضح جداً بين نتيجة دالة الاختزال في كل من التجربة الأولى والتجربة الخامسة مما يعكس مدى حساسية خوارزمية الاختزال المطورة لأي تغيير حتى وإن كان بسيطاً.

5. مقاييس الأداء Performance Criteria

هنا سيتم توضيح لمتطلبات السرية التي حققتها الطريقة المقترح كما سنوضح نقاط القوة التي تمتعت بها خوارزميتنا مقارنة مع كل من خوارزميتي الاختزال MD5 وSHA-1 لتبيان أفضلية خوارزميتنا المقترحة والتي أطلقنا عليها خوارزمية الاختزال المطورة AMD5 .

1.5 متطلبات السرية Security Requirement

لكي يكون النظام سرياً يجب أن يحقق ما يأتي [14]:

١- يجب على المحلل أن لا تكون لديه القدرة على إيجاد النص الصريح عند معرفته بالنص المشفر وهو ما يعرف بـ Confusion.

٢- يجب على المحلل أن لا تكون لديه القابلية على تحديد خوارزمية فك الشفرة (إيجاد المفتاح) عند معرفته بالنص المشفر حتى لو تمكن من معرفة النص الصريح وهو ما يعرف بـ Diffusion.

2.5 مقاييس شانون Shannon Standards

أقترح شانون خمسة مقاييس لتقييم أنظمة التشفير(Cryptograph Systems)، وهي [13] [15]:

1.2.5 درجة السرية The Degree of Confidentiality

إنّ أي نظام ذي درجة سرية عالية يكون مفضلاً، فإذا كان نظام التشفير قابل

للكسر نظرياً بالإمكان أن يكون غير قابل للكسر عملياً، أي لا توجد تقنية معروفة لتحليل الشفرة لاستعادة النص الصريح أو المفتاح المستخدم في عملية التشفير.

تعتمد خوارزمية الاختزال الجديدة AMD5 على خوارزمية الاختزال MD5 مع استيعاب أفضل الوظائف الممتازة من خوارزمية SHA-1.

بالنسبة لطول البصمة التي تنتجها الخوارزمية فأن خوارزمية AMD5 تنتج بصمة بطول ١٦٠ بت مقارنة مع بصمة بطول ١٢٨ بت التي كانت تنتجها خوارزمية MD5. وهذا يدل على أن الخوارزمية AMD5 حققت زيادة بطول الأمنية بمقدار ٢٥٪ مما يجعلها أكثر قوة وأكثر صعوبة عند الكسر.

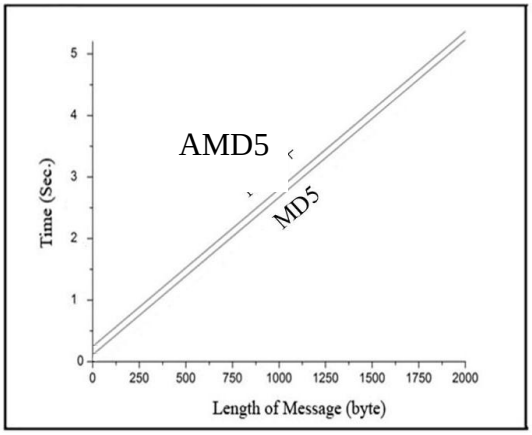
2.2.5 بساطة المفتاح وسهولة تذكره Simple Key and Easy Remember

يفضل أن يكون المفتاح بسيطاً يسهل تذكره، فمن الشائع استخدام أسماء أو مقاطع معينة معروفة لأنها سهلة التذكر وفي الخوارزمية المقترحة هنا يعتمد اختيار المفاتيح على شروط خوارزمية التشفير RSA.

3.2.5 درجة التعقيد لعملية التشفير وفك التشفير The Complexity of The Encryption and Decryption Process

نظام التشفير الجيد يجب أن تكون فيه عملية التشفير وفكّها بسيطة، ولكن عملية تحليل الشفرة يجب أن تكون صعبة وغير ممكنة، أي يجب أن تحدث عملية التشفير وفكّها بوقت كفوء (Polynomial Time).

بينما عملية تحليل الشفرة يجب أن تتم بوقت أسي (Exponential Time). بعد إضافة دالة التوسيع K(X, Y, Z) تحتاج خوارزمية الاختزال AMD5 إلى شرائح زمنية أكثر من خوارزمية الاختزال MD5 في إنفاق زمن الحساب ولكن الفارق الزمني ليس بالفارق الكبير وإنما زمن بسيط جدا ويزداد بزيادة طول الرسالة فهو يزداد بمعدل ثابت مع زيادة زمن الحساب في خوارزمية الاختزال MD5، كما في الشكل (8).



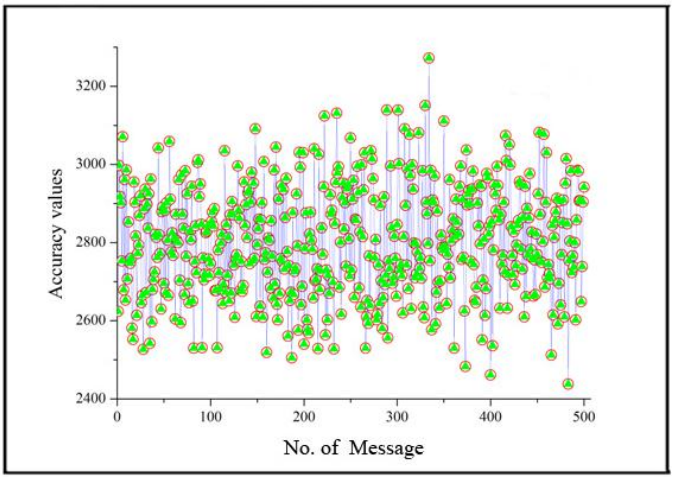
الشكل (8): معدل الزمن نسبة إلى طول الرسالة.

ولكن مقارنة مع خوارزمية الاختزال SHA-1 فأن خوارزمية الاختزال AMD5، وزمن التنفيذ يكون أقل، وكذلك بالنسبة إلى درجة تعقيد النظام فأن درجة تعقيد خوارزمية الاختزال MD5 تساوي 2^{64} وذلك لان الخوارزمية تتكون من ٤ دورات وفي كل دورة ١٦ خطوة و(١٦❖٤=٦٤). بينما خوارزمية اختزال SHA-1 تمتلك درجة تعقيد 2^{80} ولأنها تتكون من ٤ دورات في كل دورة ٢٠ خطوة. أما خوارزمية AMD5 تتكون من ٤ دوارت كل دورة ١٦ خطوة ودورة خامسة للدالة K(X, Y, Z) الموسعة ١٦ دورة وهذا يعني أنّ درجة التعقيد لخوارزمية الاختزال AMD5 تساوي $2^{16}+2^{64}$ ولكن 2^{16} تعتبر قيمة قليلة جداً مقارنة مع 2^{64} لذا تكون القيمة النهائية لدرجة تعقيد خوارزمية الاختزال AMD5 تساوي $2^{64}=2^{16}+2^{64}$ تقريباً.

أما بالنسبة لكسر الشفرة فأن طول البصمة لخوارزمية الاختزال AMD5 هي ١٦٠ بت وهي طول البصمة نفسها التي تنتجها خوارزمية الاختزال SHA-1، لذا يكون لهما درجة التعقيد نفسها في كسر الشفرة وهي 2^{160}، بينما خوارزمية الاختزال MD5 فلها طول بصمة ثابتة بطول 128 بت، وهذا يعني درجة أقل من الخوارزميتين AMD5وSHA-1. وفي هذه النقطة نلاحظ أيضاً الأفضلية لخوارزمية الاختزال AMD5 على نظيراتها.

4.2.5 درجة انتشار الأخطاء The Degree of Errors

في بعض أنظمة التشفير الجيدة فإن ظهور خطأ واحد في الرسالة المرسلة يؤثر في بقية رموز الرسالة عند فك شفرتها فكلما كان النظام أكثر دقة كان أفضل، ونظامنا هذا يتمتع بدرجة دقة عالية جداً. والشكل (9) يوضح درجة الدقة والتي تمثل التطابق بين التواقيع المولدة للرسائل المرسلة والتحقق منها لدى المستلم.



الشكل (9): درجة الدقة للتواقيع المولدة.

5.2.5 قابلية توسع الرسالة Scalability of The Message

قد وضع هذا المقياس لأن بعض أنظمة التشفير يسهل كسرها عندما تكون الرسالة طويلة، لذلك فإن نظام التشفير يجب أن يكون غير قابل للكسر مهما ازداد طول الرسالة. فكلما كانت قابلية النظام لاستيعاب توسع الرسالة أفضل كان هذا نقطة قوة مميزة للنظام. وبما إن خوارزمية الاختزال AMD5 تعتمد في عملها على خوارزمية الاختزال MD5، فهذا يعني انه يستوعب أي رسالة وبأي طول كانت على عكس خوارزمية الاختزال SHA-1 التي من شروطها إن لا يتعدى طول الرسالة 2^{64} بت. وهذا طبعا يعطي أفضلية لخوارزمية الاختزال AMD5 على حساب خوارزمية الاختزال SHA-1.

والجدول (4) يوضح مقارنةً بين خوارزميات الاختزال MD5, AMD5, SHA-1.

الجدول (4): مقاييس الأداء للخوارزميات الثلاث

المقياس		MD5	AMD5	SHA-1
درجة السرية (طول البصمة)		١٢٨ بت	١٦٠ بت	١٦٠ بت
بساطة المفتاح وسهولة تذكره		تعتمد على RSA	تعتمد على RSA	تعتمد على RSA
درجة التعقيد لعملية التشفير وفك التشفير	السرعة	الأسرع	سريعة جداً	الأبطأ
	التعقيد	264	264= 216+264 تقريباً	280
درجة انتشار الأخطاء		لا توجد	لا توجد	لا توجد
طول الرسالة		∞	∞	264

6. الاستنتاجات Conclusions

يمكن تلخيص أهم الاستنتاجات التي تم التوصل إليها من خلال هذا البحث بما يأتي:

١. **جرى تطبيق خوارزمية مقترحة لتحقيق التوقيع الرقمي والحصول على درجة عالية من الأمنية للرسالة الموقعة وكما أعطت هذه الطريقة مستوى عاليا" من الوثوقية وهذا ما تبين لنا في التجارب الأولى والثانية والثالثة.**

٢. **طبقت الخوارزمية المقترحة على أكثر من ٥٠٠ نص ولم تحدث أي حالة تصادم مما يعطي قوة للخوارزمية.**

٣. **تعزيز الطرائق التقليدية المستخدمة في التشفير بخوارزميات حديثة لتحقيق الوثوقية من الأساليب الجيدة في المحافظة على أمنية المعلومات وسريتها فضلا" عن توفير إمكانية كبيرة في تمويه المتطفلين والمحللين للأنظمة الخاصة بطرائق التشفير وتحقيق الوثوقية. علما أن عملية المتطفلين والمحللين يستندون في عملهم إلى طول البصمة التي تنتجها خوارزمية الاختزال لمعرفة وتحديد الخوارزمية المستخدمة لغرض كسرها وبما أن خوارزميتنا تعطي طول بصمة مساوي لخوارزمية الاختزال SHA-1 فهذا يعطي تمويه أكثر للمتطفلين والمحللين في عملية تحديد الخوارزمية المستخدمة.**

٤. الحصول على خوارزمية تعطي درجة الأمنية نفسها لخوارزمية SHA-1 ولكن بدرجة تعقيد أقل وكذلك درجة أمنية أعلى من خوارزمية MD5 العادية مع الحفاظ على الوقت اللازم لتطبيق الخوارزمية والمبين في الشكل (8) [16,17].

٥. كما تتميز الخوارزمية المطبقة بدرجة عالية من الدقة وعدم وجود لأي خطأ في عملية التحقق من التواقيع المولدة كما مبين بالشكل (9).

٦. قابلية الخوارزمية المقترحة على استيعاب الرسائل بأي طول كما بينا سابقا.

المستخلص:

يهتم هذا البحث بدراسة مفهوم الوثوقية والطرائق المستخدمة لتحقيقها، مع التركيز على طريقة التوقيع الرقمي لما توفره هذه الطريقة من مستوى عال من الوثوقية والأمنية للبيانات المنتقلة عبر شبكة الحواسيب فضلاً عن كونها من الطرائق الحديثة في هذا المجال. والتي تستخدم لتحرّي التعديلات غير المرخصة على البيانات ولإثبات هوية الشخص الموّقع للبيانات.

فضلاً عن ذلك فان مستلم البيانات الموقّعة بإمكانه أن يستخدم التوقيع الرقمي كدليل أن البيانات جاءت فعلاً من الشخص المدعى. وهذا ما يعرف بعدم الإنكار لان الموقّع لا يستطيع بسهولة إنكار إرساله البيانات الموقّعة.

قدم هذا البحث طريقة مقترحة لتوليد توقيع رقمي للملفات النصية بالاعتماد على الميزات الموجودة في خوارزمية الاختزال MD5 على خوارزمية التشفير الشهيرة RSA ذات المفتاح المعلن. وقد حققت هذه الطريقة المقترحة درجة كبيرة من الوثوقية والأمنية للرسائل الموقعة المنتقلة عبر شبكة الحواسيب.

Abstract:

This paper aims to study the conceptual of authentication and several methods that begin used to ensure it. More specific, research focuses on one of most important methods which is called *digital signature*. Digital signature mainly consist of two parts, first one is

digital signature generation and verification of digital signature. Digital signature can ensure a high level of authentication and security for data communication. In addition, it is one of the recently used methods for data privacy. Digital signature is normally utilized to seek unauthorized modification that may occur in data, and prove the identity of the sender. Receiver can use the digital signature to ascertain the identity of the sender, so that the sender cannot deny his signature. This is ordinarily called *non-repudiation*.

In this paper, an effective method for digital signature generation has been proposed. This method was utilized to generate digital signature for text file based on modification of MD5 features. RSA, the most widely-used public key cryptography algorithm, was used afterward.

Proposed method presents high level of security and authentication for letters were signed and transferred via computer network.

قائمة المصادر والمراجع

1. Stallings W. , " Cryptography and Network Security Principles and Practice " , Fourth Edition , published by prentice-hall, inc, the united state of America, (2005).
2. Watanabe O., Nakazaki A., Kiya H.,"A scalable encryption method allowing backward compatibility with JPEG2000 images", IEEE International Symposium on Circuits and Systems (ISCAS 2005).Vol. 1, pp. 6324-6327, (2005).
3. Buchmann J., " Introduction to Cryptography", Springer, London, (2004).
4. Pletka R., and Cachin C., "Cryptographic security for a high-performance distributed file system," Research Report RZ 3661, IBM Research, Sept, (2006).

٥- عبد الغني طه ياسين، " الاختراق في شبكة الإنترنت "، المركز القومي للمختبرات الإنشائية، العراق http://internet.arabcomputing.com/haking.html، تم الوصول إليه بتاريخ ١٣ نيسان ٢٠١٢.

6. BAHADORI M. AND ET AL, " A NOVEL APPROACH FOR SECURE AND FAST GENERATION OF RSA PUBLIC AND PRIVATE KEYS ON SMARTCARD ",

PROCEEDINGS OF THE 8TH IEEE INTERNATIONAL NEWCAS CONFERENCE, PP. 265-268, (2010).

7. Li Xiao-fei, Shen Xuan-jing, and Chen Hai-peng, "An Improved ElGamal Digital Signature Algorithm Based on Adding a Random Number", 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2011.

8. Hameed A. Youns, Israa M. Hayder, and Hussain A. Younis, " Create A New Digital Signature Scheme Using Double Hush Function Algorithms", Journal of Kerbala University, Kerbala, Iraq, 2013.

9. Leung K.H. , Ma K.W., Wong W.K. and Leong P.H.W. " FPGA Implementation of A Microcoded Elliptic Curve Cryptographic Processor", IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM), pages 68–76, (2000).

10. Garfinkel S. , Spafford G. , " Unix And Internet Security " , second edition, (1996),

http://www.busan.edu/~nic/networking/puis/ch06-05.htm.

11. Ying C., and Chong F.," An Efficient Implementation of RSA Digital Signature Algorithm ", IEEE International Conference on Intelligent Computation Technology and Automation (ICICTA), Vol. 2, pp. 100-103, (2008).

12. Bagwill R. , Et Al , " Security in Open Systems " , published by computer systems technology u.s. department of commerce & nist , (1994), http://csrc.ncsl.nist.gov/publications/nistpubs/800-7/main.html.

13. Rivest R. L., Shamir A. and Adleman L.,"A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Commun. ACM, Vol 21 , pp. 120-126, April (1978).

14. CHAUM H., ANTWERPEN H.V. "Undeniable Signature", Crypto"89" Springer Verlag, Heidelberg, pp 212-216 (1990).

١٥. توماس، طوم. مركز التعريب والبرمجة. "الخطوة الأولى نحو أمان الشبكات"، الطبعة الأولى – الدار العربية للعلوم، لبنان – بيروت،ص 225-224، (٢٠٠٣).

16. Sallam P. N., , Agrawal J, and Sahu S., "A New Approach 160-bit Message Digest Algorithm", International Journal of Computer Applications, Vol. 38, No. 5, pp. 22-26, January 2012.

17. Ragput D. S., and Jain S. S., "Advanced MD5 Encryption with Extra Compress Function", Journal of Computing Technologies, Vol. 1, Issue 2, June 2012.