بحوث مستقبلية (١٧) ٢٠٠٧
ص ص [١٨١-١٩٧]

دراسة الوثوقية وتحقيقها باستخدام التواقيع الرقمية

بســـام علـي مصطفى[١]
ياسين حكمت إسماعيل[٢]

الملخص

يهتم البحث بدراسة مفهوم الوثوقية والطرائق المستخدمة لتحقيقها، والتركيز على طريقة التواقيع الرقمية لما توفره من مستوى عال من الوثوقية والأمنية للبيانات المنتقلة عبر شبكة الحاسبات فضلا عن كونها من الطرائق الحديثة في هذا المجال . لقد تم تقديم طريقة مقترحة للتوقيع الرقمي بالاعتماد على الميزات والأفكار الجيدة في طرائق تحقيق الوثوقية المستخدمة مسبقا . وتتضمن آلية عمل هذه الطريقة استخدام فكرة دوال التمويه أحادية الاتجاه للحصول على ملخص الرسالة كذلك يتم تضمين فكرة تحقيق الوثوقية باعتماد أنظمة التشفير المتماثل ، والمتضمنة توفير هيكلة معينة للرسالة معدة مسبقا . كما أن عملية التشفير في الطريقة تتضمن إجراء عملية التبديل لحروف الرسالة بحروف ورموز معينة بالاعتماد على الخواص الإحصائية للغة . والطريقة المقترحة هذه توفر مستوى عالياً من العشوائية للنص الناتج وبالتالي تحقق درجة كبيرة من الوثوقية والأمنية للبيانات المنتقلة عبر شبكة الحاسبات ، وتفتح المجال أمام العاملين في القطاعات التجارية والمصرفية عن طريق استخدام الشبكات الإلكترونية من اجل مواكبة التطور العالمي في هذا المجال.

Abstract

This paper deals with studying Authentication conception and the methods which are used to achieve it focusing on Digital Signature method for the high level of Authentication it provides and the secure way of moving data through computer's net. Also, it is considered one of the new methods in the field. The research proposes a method for Digital Signature depending on the right features and ideas of achieving Authentication methods previously used. The mechanism method includes using the idea of a one way hash function to obtain the Message Digest, and also including Authentication inquiry depending on Symmetric Encryption System which includes

(١) مدرس، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

(٢) مدرس مساعد، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

تاريخ الاستـــلام: ٢٠٠٦/٠٤/٢٧
تاريخ قبول النشـر: ٢٠٠٦/٠٧/٠٥

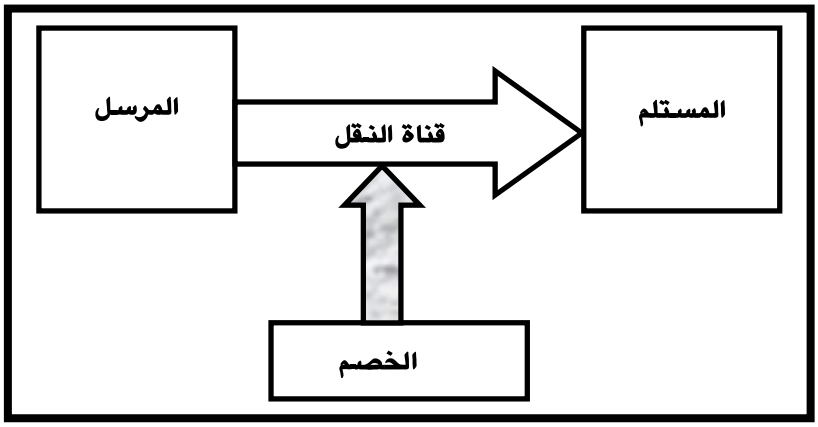
providing specific structure to the message which has been designed before. Encryption process includes the procedure of replacing message letters and symbols depending on the statistical features of English. This method provides high level of randomness to the yield text, hence it achieves high degree of Authentication and will secure the moving data through computer's net. It also opens the way before the workers in banking and the commercial sector through using the electronic Net's to cope with the development in this field .

١. مقدمة :

إن فكرة الوثوقية موجودة منذ قديم الزمان فمثلا" عندما يرغب شخصان في أن يكون بينهما رسول لنقل المعلومات أو المواد فأنهما يقومان بتقسيم عملة نقدية إلى قسمين كل منهما يحتفظ بقسم ويتفقان على أنه إذا أُرسل شخص يحمل نصف العملة إلى شخص يحمل النصف الآخر من العملة فإن الشخص المرسل موثوق به . وكذلك من 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 . وفي الاتصالات الشخصية نحن نميز الأصوات ، والسلوكيات ، والأشكال بينما في اتصالات شبكة الحاسبة نحن لا نملك الدلائل أو الإشارات التي تساعدنا على معرفة هوية الشخص الذي يرغب في الاتصال معنا . [Pfleeger C., 1989:161]

٢. الهدف من الوثوقية (Goal Of Authentication) :

نفرض أن المرسل يقوم بإرسال معلومات إلى المستلم من خلال قناة النقل (Transmission Channel) **والواقعة تحت سيطرة الخصم كما هو موضح بالشكل (١)** .



شكل (١) سيطرة الخصم على قناة النقل

إذ يستطيع الخصم القيام بنشاطات مختلفة على قناة النقل مثل :

١. التصنت والاستماع للمعلومات المرسلة عبر قناة النقل .
٢. منع مرور البيانات .
٣. خزن البيانات وإعادة إرسالها في وقت آخر خلال فترة إرسال كاذبة .
٤. احتمالية انتحال الخصم لشخصية أحد أطراف الاتصال (المرسل أو المستلم).
٥. تغيير محتوى الرسالة بإعادة ترتيب أجزاء مختلفة من الرسالة أو حذفها أو الحشر فيها.

لذلك يجب على المستلم أن يستخدم خدمة الوثوقية لغرض التحقق مما يأتي :

أ . الرسالة أرسلها المرسل الحقيقي .

ب . محتوى الرسالة لم يتغير خلال الإرسال في قناة النقل .

[Schaad A.,1999:5-6] [Jan C.,1998:158-163] [Stallings W.,1999:237-239]

٣. ملخص الرسالة (Message Digest) :

على الرغم من أن التشفير يمنع المتلصِّصين من الإطلاع على محتويات الرسالة ، إلا أنه لا يمنع المخرِّبين من العبث فيها " أي إن التشفير لا يضمن سلامة الرسالة (Integrity) . ومن هنا ظهرت الحاجة إلى البصمة الإلكترونية للرسالة (ملخص الرسالة) ، وهي بصمة

رقمية يتم اشتقاقها على وفقه خوارزميات معيَّنة تُدعى دوالّ أو اقترانات التمويه (Hash Functions) ، إذ تطبِّق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة (سلسلة صغيرة) ، وتُدعى البيانات الناتجة بالبصمة الإلكترونية للرسالة . وتتكوَّن البصمة الإلكترونية للرسالة من بيانات لها طول ثابت تؤخَذ من الرسالة المحوَّلة ذات الطول المتغير. وتستطيع هذه البصمة تمييز الرسالة الأصلية والتعرُّف عليها بدقة ، حتى أن أي تغيير في الرسالة – ولو كان في بت واحد – سيفضي إلى بصمة مختلفة تماماً ، ومن غير الممكن اشتقاق البصمة الإلكترونية ذاتها من رسالتين مختلفتين . ولهذا تعد عملية إيجاد البصمة الإلكترونية للرسالة عملية أساسية في تقنية التواقيع الرقمية (Digital Signatures) .

[Stallings W.,1999:246-249] [Schaad A.,1999:15-16] [Youd D.,1996:1-3]

٤. دوالّ أو إقترانات التمويه (Hash Functions) :

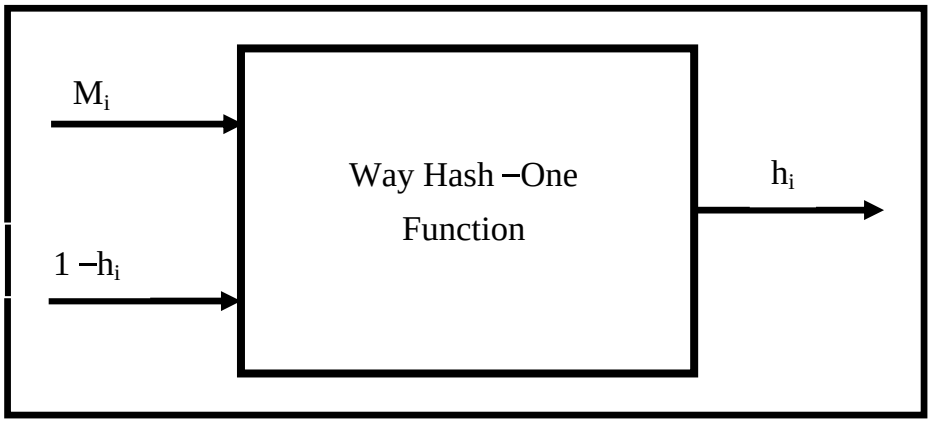
تم استخدام دوال التمويه في مجال علوم الحاسبات لمدة طويلة ، إذ إن دالة التمويه هي دالة رياضية إدخالها عبارة عن سلسلة من البيانات ذات طول متغير تعرف بالصورة الأصلية (Pre-Image) والتي تمثل الرسالة أو البيانات المراد إيجاد قيمة دالة التمويه لها إذ تقوم دالة التمويه بتحويل الطول المتغير (العشوائي) للبيانات المدخلة إلى سلسلة من البيانات ذات طول ثابت (Fixed Length) والتي عادة يكون طولها اصغر من طول البيانات المدخلة . وقد تكون دالة التمويه عبارة عن دالة تقوم باستلام البيانات ذات الطول المتغير وتقوم بإرجاع بايت (Byte) واحد والناتج من إجراء عملية (XOR) لكل بايتات (Bytes) الإدخال . والهدف من دالة التمويه هو تكوين بصمة (سلسلة من البيانات) للبيانات المدخلة إذ إن قيمة البصمة تساعدنا على التحقق من أن رسالتين معينتين تكونان متساويتين إذا كان لهما قيمة دالة التمويه نفسها (البصمة نفسها) . [Gan C.,:1-4] [Migliavacca M.,2004:1-4] [Jan C.,1998:163-164]

٥. دالة التمويه أحادية الاتجاه (One Way Hash Function) :

إن دالة التمويه أحادية الاتجاه لها الكثير من المسميات منها : دالة الكبس (Compression Function) ، دالة الانكماش (Contraction Function) ، ملخص الرسالة (Message Digest) ، فحص التكامل للرسالة (Message Integrity Check (MIC)) ، رمز معالجة الكشف (Manipulation Detection Code(MDC)) ، ومهما

كانت التسمية فان الأساس يعود إلى علم التشفير الحديث . ودالة التمويه أحادية الاتجاه هي الدالة التي تعمل باتجاه واحد فقط فمن السهولة حساب قيمة التمويه (Hash Value) للبيانات المدخلة ، ولكن من الصعوبة الحصول على البيانات الأصلية والتي تم تمويهها (Hashes) إلى قيمة تمويه معينة . ويجب أن تكون دالة التمويه أحادية الاتجاه الجيدة محررة من التصادم (Collision-Free) وهذا يعني انه من الصعب إيجاد مجموعتين من البيانات المختلفة لهما قيمة التمويه نفسها . ومن غير الممكن الحصول على البيانات الأصلية بالاعتماد على قيمة دالة التمويه أحادية الاتجاه . وعلى أساس أن دالة التمويه أحادية الاتجاه بصمة للبيانات فإذا أردت أن تتحقق من أن شخصا" ما لديه ملف معين مشابه للملف الذي لديك ولكن لا ترغب في أن يرسل لك ذلك الملف فباستطاعتك أن تسأله عن قيمة التمويه (Hash Value) فإذا أرسل لك قيمة التمويه الصحيحة فإنك سوف تتأكد من أنه يملك الملف نفسه وهذه العملية مفيدة خاصة في الحوالات المالية .

إن دالة التمويه أحادية الاتجاه تولد قيمة تمويه ذات طول n بإعطائها إدخال ذي طول غير محدد يرمز له بـ m . وثمة إدخالان لدالة الكبس ، الإدخال الأول عبارة عن مقطع (Block) من الرسالة المراد إيجاد التمويه لها في حين إن الإدخال الثاني عبارة عن قيمة التمويه لمقطع سابق ضمن الرسالة (النص) ، آلية عمل دالة التمويه أحادية الاتجاه يمكن توضيحها بالشكل(٢).



شكل (٢) آلية عمل دالة التمويه أحادية الاتجاه

يمثل الإخراج التمويه لمقاطع الرسالة لغاية المقطع الحالي ، والذي هو الإدخال الحالي للدالة ، هذا يعني بان قيمة التمويه (Hash Value) للمقطع M_i من الرسالة هو :

$h_i = f (M_i , h_i\text{-}1)$

إذ إن قيمة التمويه (للمقطع السابق في الرسالة) مع المقطع التالي للرسالة سوف تصبح الإدخال التالي للدالة ، وبالتالي فان قيمة التمويه النهائية للرسالة هي نتيجة دالة التمويه لآخر مقطع في الرسالة .

[Stallings W.,1999:253-256] [Migliavacca M.,2004:1-3] [Gan C.,:1-4]

٦. صفات التوقيع الرقمي :

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 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 من أن الرسالة قادمة منه.

[Pfleeger C., 1989:132-133] [Schaad A.,1999:16] [Jan C.,1998:174]

٧. كيفية إنشاء التوقيع الرقمي والتحقق منه :

إن آلية إنشاء التوقيع الرقمي تتم من خلال الخطوات الآتية :

١. يتم إيجاد ملخص الرسالة (Message Digest) أو ما تعرف بالبصمة الإلكترونية ، وذلك من خلال تطبيق خوارزميات دوال التمويه أحادية الاتجاه (One-Way Hash Function Algorithms) .

٢. يتم إجراء عملية التشفير لملخص الرسالة باستخدام المفتاح الخاص أو السري (Private-Key) للمرسل (للمُوقع) .

٣. يتم إضافة ناتج عملية التشفير إلى الرسالة ومن ثم إرسالها إلى المستلم .

في حين عملية التحقق من التوقيع تتم من خلال الخطوات الآتية :

١. يقوم المستلم بفك التشفير للتوقيع الرقمي باستخدام المفتاح العلني للمرسل ، وبالتالي الحصول على ملخص الرسالة (Message Digest) .
٢. يتم إيجاد ملخص الرسالة للرسالة المستلمة باستخدام دالة التمويه أحادية الاتجاه نفسها والمتغيرات نفسها المستخدمة من قبل المرسل في عملية إيجاد ملخص الرسالة .
٣. يتم مقارنة كلا الملخصين ، فإذا كانا متساويين دل على أن التوقيع الرقمي صحيح ، وإذا كانا غير متساويين دل على أن التوقيع الرقمي خاطئ ، وبالتالي فإن الرسالة المستلمة قد حدث فيها تغيير أثناء إنتقالها في قناة النقل ضمن شبكة الحاسبات ، أو أن الرسالة مرسلة من قبل شخص غير موثوق به .

[Schaad A.,1999:16-19] [Youd D.,1996:1-4] [Jan C.,1998:174-178]

٨. الأفكار المعتمدة من الطرائق السابقة :

بعد الإطلاع على معظم الطرائق والأساليب المستخدمة لغرض توفير الوثوقية والتكامل للبيانات المرسلة ضمن شبكة الحاسبات ، إذ تكون البيانات هنا عرضة لهجوم المتطفل (Intruder) . تم انتخاب مجموعة من الأفكار أو الميزات الجيدة التي تتمتع بها الطرائق المستخدمة آنفا" في هذا المجال ، وتضمين هذه الأفكار كلا" في الطريقة المقترحة وهذه الأفكار هي :

١. فكرة تحقيق الوثوقية باستخدام أنظمة التشفير المتماثل (أنظمة المفتاح السري) والمتضمنة توفير هيكلة معينة للرسالة معدة مسبقا" .
٢. اعتماد فكرة تحقيق وثوقية المستخدم باستخدام كلمة المرور (Password).
٣. اعتماد فكرة ختم الوقت (Time Stamping) .
٤. اعتماد فكرة إيجاد ملخص الرسالة (Message Digest) باستخدام دوال التمويه أحادية الاتجاه (One Way Hash Function) .
٥. اعتماد فكرة أنظمة التشفير التعويضية (Substitution Cipher System) والمتضمنة القيام بعملية التعويض لكل حروف النص الأصلي بحروف ، رموز ، أو أرقام جديدة .

٩. الخوارزمية المقترحة :

أولا" خوارزمية إنشاء التوقيع الرقمي :

تتضمن خوارزمية إنشاء التوقيع الرقمي القيام بالخطوات الآتية :

١. إدخال اسم المستخدم الحالي للنظام وكلمة المرور الخاصة به ، إذ يتم وبالاعتماد على كلمة المرور التي يدخلها المستخدم البحث في قاعدة البيانات والحاوية على أسماء كل الأشخاص المخولين فإذا تم العثور على كلمة المرور المدخلة دل على أن المستخدم هو شخص موثوق به وبالتالي يتم إخراج رسالة تحوي على اسم المستخدم وإلا فسوف يتم الخروج من النظام .

٢. يتم إدخال الرسالة المراد إيجاد التوقيع الرقمي الخاص بها .

٣. يتم إجراء عملية التقطيع (Segmentation) على الرسالة المدخلة إذ يتم تقطيع كل رموز الرسالة ووضعها في مصفوفة أحادية .

٤. يتم حساب عدد الأحرف الأكثر تكرارا وهي (A,E,T,I) ووضع قيم التكرارات في متغيرات معينة .

٥. يتم إدخال تأريخ ووقت إرسال الرسالة (يوم، ساعة، دقيقة، ثانية) وخزنها في متغيرات معينة.

٦. يتم إيجاد ملخص الرسالة (Message Digest) وذلك بالاعتماد على :

A – إيجاد تكرارات الأحرف الإنكليزية كلها والواقعة ضمن المواقع الفردية ، ومن ثم إجراء عملية (XOR) بين كل قيم التكرارات وخزن النتيجة في متغير معين وليكن (Odd) .

B – إيجاد تكرارات الأحرف الواقعة ضمن المواقع الزوجية ، ومن ثم إجراء عملية (XOR) بين قيم التكرارات جميعها وخزن النتيجة في متغير معين وليكن (Even) .

٧. إجراء عملية الحشر (Insertion) لكل المتغيرات أعلاه ضمن هيكلة الرسالة المعدة مسبقا ، كما هو موضح بالجدول (١) ، إذ إن القيم المأخوذة من الرسالة الأصلية يتم عكسها قبل وضعها في مواقعها المخصصة .

٨. إجراء عملية التشفير والمتضمنة القيام بعملية التعويض لأحرف الرسالة الأصلية بأحرف أخرى أو رموز معينة ، وبالاعتماد على إحصائية ترددات أحرف اللغة الإنكليزية ، كما هو موضح بالجدول (٢) ، إن عملية التبديل لأحرف الرسالة تتضمن أيضا إلغاء الفراغات الموجودة بين كلمات الرسالة الأصلية ومقاطعها ووضع فراغات

وهمية بالاعتماد على موقع حرف معين في الرسالة الأصلية مما يزيد من صعوبة عملية التحليل للنص المشفر الناتج . وبالإمكان توضيح عملية التوقيع الرقمي للطريقة المقترحة من خلال المخطط الانسيابي المبين في الشكل (٣) .

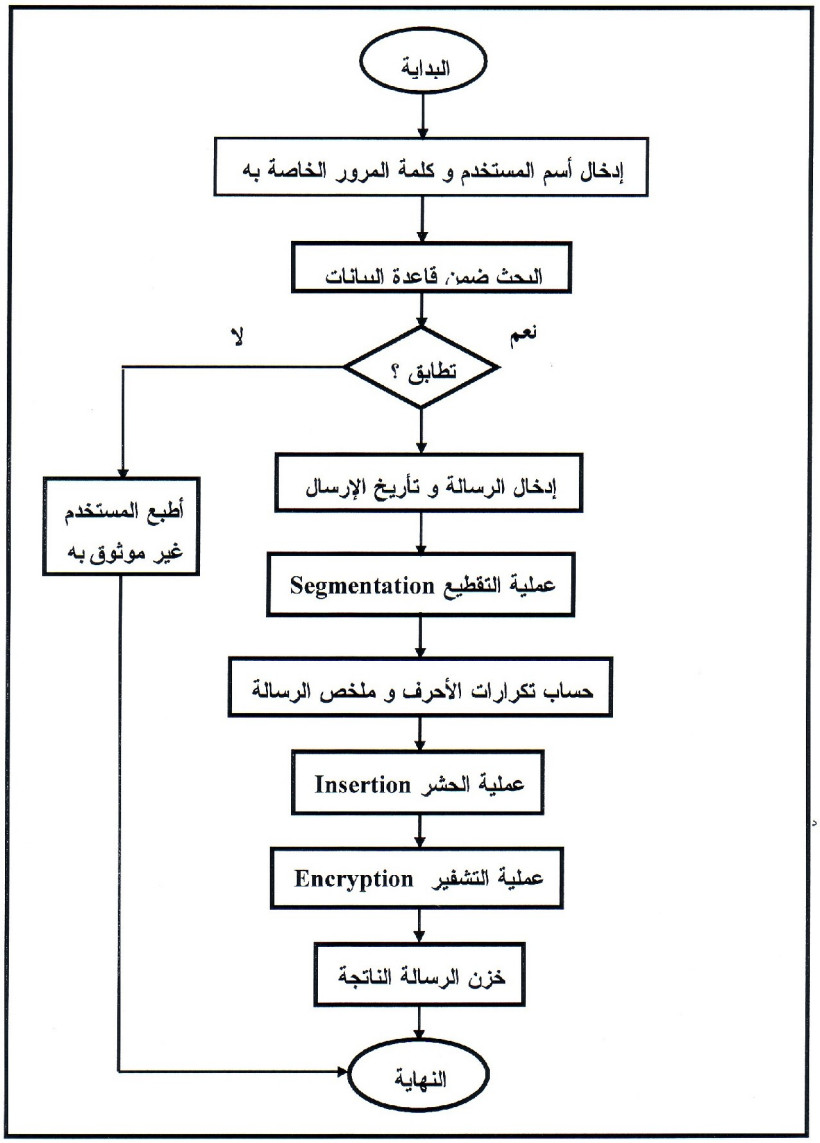
الجدول (١) هيكلية الرسالة الأساسية

Bits	Value	Bits	Value	Bits	Value
1	Message	24	Message	47	Hour
2	Message	25	Message	48	<
3	Message	26	$	49	Day
4	Message	27	E Freq.	50	<
5	Message	28	$	51	<
6	Message	29	+	52	Message
7	Message	30	I Freq.	53	Message
8	Message	31	+	54	Message
9	Message	32	*	55	Message
10	Message	33	T Freq.	56	Message
11	User Code	34	*	57	Message
12	User Code	35	Message	58	Message
13	User Code	36	Message	59	Message
14	User Code	37	Message	60	Message
15	$	38	Message	61	?
16	A Freq.	39	Message	62	Odd
17	$	40	Message	63	?
18	Message	41	<	64	?
19	Message	42	<	65	Even
20	Message	43	Second	66	?
21	Message	44	<	67	Message
22	Message	45	Minute	68	Message
23	Message	46	<	69	Message….etc

الجدول (٢) عملية التعويض لأحرف الرسالة

Message Letters	Substituted by	Message Letters	Substituted by
A	#	**R**	H
E	A	C	R
Space	E	P	C
T	Space	M	P
I	T	Y	M
O	I	B	Y
N	O	K	B
S	N	Z	K
H	S		

أن حساب أعداد الأحرف الأكثر تكراراً يستخدم لتوليد قيمة ملخص الرسالة (Message Digest) والتي سوف يتم حشرها في متن الرسالة المرسلة لغرض التأكد من وثوقيتها ، أما عملية التعويض لأحرف الرسالة تتم مع الأحرف المكررة نفسها من إذ استخداماتها في اللغة الإنكليزية وبالتالي من الصعوبة جدا" على الشخص المتطفل من كسر النص المشفر بالاعتماد على أسلوب التحليل الإحصائي لأحرف النص المشفر.



الشكل (٣) مخطط انسيابي لعملية التوقيع الرقمي في الخوارزمية المقترحة

ثانياً. خوارزمية التحقق من التوقيع الرقمي :

تتضمن عملية التحقق من صحة التوقيع الرقمي القيام بالخطوات الآتية :

١. إدخال اسم المستخدم وكلمة المرور الخاصة بالنظام .

٢. إدخال اسم المستخدم الحالي للنظام وكلمة المرور الخاصة به ، إذ يتم وبالاعتماد على كلمة المرور التي يدخلها المستخدم البحث في قاعدة البيانات والحاوية على أسماء كل الأشخاص المخولين فإذا تم العثور على كلمة المرور المدخلة دل على أن المستخدم هو شخص موثوق به وبالتالي يتم إخراج رسالة تحتوي على اسم المستخدم و إلا فسوف يتم الخروج من النظام .

٣. فتح الرسالة المستلمة والمراد التحقق من صحة التوقيع الرقمي لها .

٤. بالاعتماد على هيكلة الرسالة الثابتة (المعدة مسبقا) يتم سحب قيم المتغيرات جميعها من الرسالة .

٥. إجراء عملية فتح التشفير(Decryption) والمتضمنة القيام بعملية التعويض لأحرف الرسالة ورموزها بأحرف ورموز أخرى (عكس عملية التشفير لدى المرسل) .

٦. إجراء عملية المقارنة والمتضمنة :

A- إظهار تأريخ الإرسال والاستلام ووقتهما.

B- حساب تكرارات الأحرف (A,I,E,T) ومقارنتها مع القيم المرسلة من قبل المرسل ، فإذا تطابقت دل ذلك على عدم احتمالية تعرض الرسالة لعملية الحذف أو الإضافة .

C- حساب ملخص الرسالة بالاعتماد على إجراء عملية (XOR) لقيم تكرارات الأحرف في المواقع الزوجية والفردية للرسالة ومقارنتها مع القيم المرسلة ، فإذا تطابقت القيم دل ذلك على عدم تعرض الرسالة المرسلة لعمليات الإضافة، أو الحذف، أو التبديل .

٧. إجراء عملية المقارنة لرمز المرسل (Sender Code) والذي يمثل كلمة المرور التي أدخلها المرسل ، فإذا تم إيجاد رمز المرسل ضمن قاعدة البيانات دل ذلك على أن المرسل هو شخص موثوق به .

٨. يتم إخراج اسم المرسل والرسالة المرسلة الناتجة من عملية فك التشفير ، وكذلك يتم إخراج نسبة الوثوقية للرسالة بالاعتماد على عمليات المقارنة التي تم إجراؤها أعلاه ، تحدد نسبة الوثوقية ١٠٠٪ أن الرسالة لم يحدث لها أي تغيير وقادمة من جهة موثوق بها. أن نسبة الوثوقية تعتمد على عمليات المقارنة :

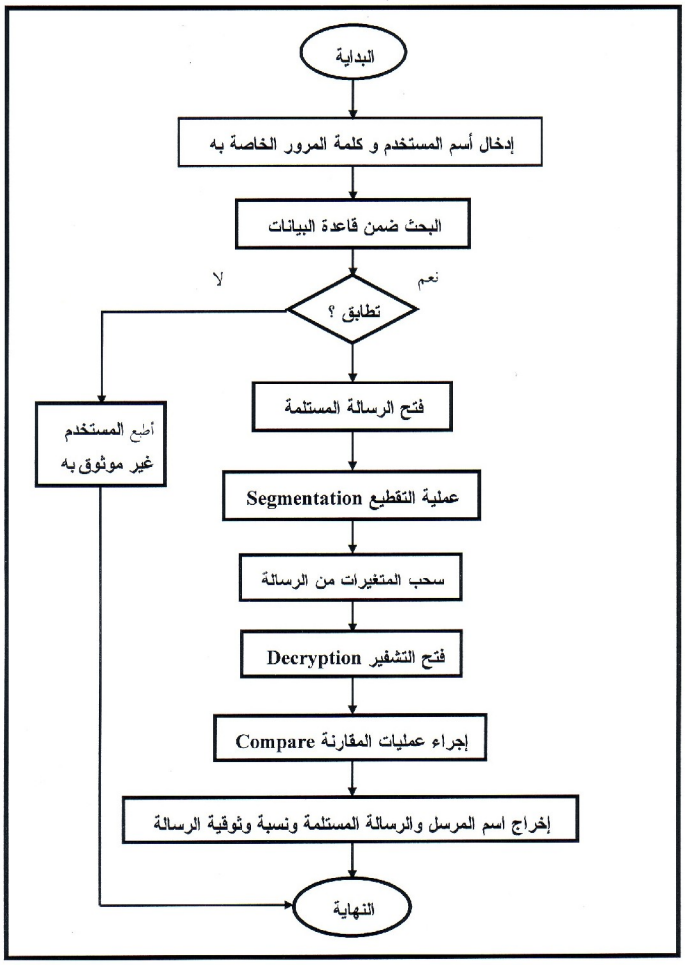
١. إيجاد رمز المرسل ضمن قاعدة البيانات (٢٥٪) .

٢. مطابقة تكرارات الأحرف (A,I,E,T) للرسالة المرسلة مع القيم المرسلة (٢٥٪) .

٣. مطابقة ناتج عملية (XOR) لتكرارات الأحرف الإنكليزية الواقعة في المواقع الفردية في الرسالة المرسلة (odd) مع قيمة (odd) المرسلة (٢٥٪) .

٤. مطابقة ناتج عملية (XOR) لتكرارات الأحرف الإنكليزية الواقعة في المواقع الزوجية في الرسالة المرسلة (even) مع قيمة (even) المرسلة (٢٥٪) .

ويمكن توضيح عملية التحقق من التوقيع الرقمي للطريقة المقترحة من خلال الشكل (٤) .



شكل (٤) مخطط انسيابي لعملية التحقق من التوقيع الرقمي في الخوارزمية المقترحة

١٠. الجانب العملي :

تم في هذا البحث استخدام طريقة مقترحة للتوقيع الرقمي إذ وفرت هذه الطريقة مستوى عاليا" من الوثوقية والأمنية للبيانات المنتقلة ضمن شبكة الحاسبات ، توضح الأمثلة التالية مجموعة من الرسائل قبل إجراء عملية التوقيع الرقمي عليها وبعدها باستخدام الخوارزمية المقترحة :

1.
The original message :
“ authentication is a process by which receiver can verify the message integrity “
The message after digital signature :
“ #rt oas u#7777$9$#enteoit
15+13+yennarihce*14*<<26<14<09<17<<srtswem?3??12?@@m thga oteag#nnapeas emfthaveo#rehavtarahe^ “
2.
The original message :
“Encryption is a process of disguising confidential information in such a way that it's meaning is unintelligible to an unauthorized person . “
The message after digital signature :
“oitcmhroa2222$9$ihce#ente8+9+tdefiennar*17*<<30<44<03<12 <<otntugn?11??2?.eoinhacedakthis u#oueo#ei ealytgtlla otouentegoto#apen' te #s em#we#esruneoteoit #phifotel#t oadtfoireg^ “
3.
The original message :
“A hash function H is a transformation that takes a Variable length Message as input m and returns a fixed-size string , which is called the hash value h (that is, h=H(m)) “
The message after digital signature :
“oufesn#se#4444$18$teseoit 11+13+fno#h e#en*11*<<50<45<09<28<<it #phi?0??1?e.e))p(s=se,nte #s (eseaul#vesn#seas edall#rentesrtswe,egoth neaktn-daxtfe#enohu ahedo#epe ucoten#eag#nnapes goalealy#th#Ve#enab# e #s eo^ “

إذ نلاحظ عملية حشر المتغيرات في متن الرسالة اعتماداً على هيكلية الرسالة المعدة مسبقاً. وتحقق الطريقة المقترحة مستوى عالياً من العشوائية للرسالة الناتجة وكما هو ملاحظ فإن الرسالة الناتجة تحوي على عدد من الأحرف والأرقام والرموز الخاصة المتداخلة فيما بينها موفرة مستوى عالياً من العشوائية ، وبالتالي صعوبة مقدرة المتطفل على تحليل الرسالة وكشف معالمها .

١١. ميزات الطريقة المقترحة :

١. يتم القيام بعملية دمج بين تحقيق الوثوقية للمستخدم وتحقيق الوثوقية للرسالة .
٢. عملية الحصول على التوقيع الرقمي في هذه الطريقة تتضمن إجراء عملية التشفير ليس فقط لقيمة التمويه (Hash Value) بل أيضا" للنص كاملا" .
٣. اعتماد الطريقة على إجراء مجموعة من العمليات السهلة وغير المعقدة ، وعدم احتوائها على عمليات التكرار (Iteration) .
٤. توفير مستوى كبير من العشوائية للنص الناتج ، وبالتالي تحقيق الوثوقية والتكامل والسرية للبيانات المرسلة عبر شبكة الحاسبات .
٥. تتطلب هذه الطريقة وقت تنفيذ قليل نسبيا" .
٦. تتضمن الطريقة إضافة وقت إرسال البيانات عبر شبكة الحاسبات ، وبالتالي أي تأخير في وصول البيانات سوف يدل على احتمالية تعرض البيانات لاعتراض من قبل المتطفل .
٧. تتطلب الطريقة من المستخدم أن يدخل كلمة المرور (Password) إذ تم وضع قناع خاص لإخفاء كلمة المرور أثناء إدخالها بغية تحقيق قدر من الحماية في حال استخدام النظام في المواقع العامة .

١٢. الاستنتاجات :

إن أهم الاستنتاجات التي تم التوصل إليها من خلال هذا البحث ما يأتي :

١. تم تطبيق خوارزمية مقترحة لتحقيق التوقيع الرقمي والحصول على درجة عالية من العشوائية للنص الناتج وبالتالي أعطت هذه الطريقة مستوى عاليا" من السرية والوثوقية .

٢. تعزيز الطرائق التقليدية المستخدمة في التشفير بخوارزميات حديثة لتحقيق الوثوقية من الأساليب الجيدة في المحافظة على أمنية المعلومات وسريتها فضلاً عن توفير إمكانية كبيرة في تمويه المتطفلين والمحللين للأنظمة الخاصة بطرائق التشفير وتحقيق الوثوقية .

المصادر

1. Gan C. ,“ A Study on the md5 hash function and collisions for its iterated compression function , http://www2.elec.qmul.ac.uk/~gan/pdf/hash.pdf .
2. Jan C. A. , (1999) , “ Basic Methods of Cryptogrphy ” , published by cambridge university press .
3. Migliavacca M. , (2004) , “ CS553 Distributed Systems ” , e-mail : migliava@elet.polimi.it, http://sola1.elet.polimi.it/murphy/533/16.security.pdf .
4. Pfleeger C. P. , (1989) , ” Security In Computing ” , the university of tennessee , published by prentice-hall international , inc , printed in the united state of America .
5. Schaad A. , (1999) , ” Anonymous , Authenticated and Nonrepudiable open assessment submission ” , Msc. thesis , department of computer science university of york , e-mail:andreas@cs.york.ac.uk. http://www-users.cs.york.ac.uk/~andreas/thefinalthesis.pdf
6. Stallings W. , (1999) , “ Cryptography and Network Security Principles and Practice ” , second edition , published by prentice-hall , inc , the united state of america .
7. Youd D. ,(1996) , “ What is a Digital Signature ? An Introduction to Digital Signature ” , http://www.youdzone.com/signature.html .