مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الهندسية المجلد (29) العدد (1) 2007
Tishreen University Journal for Studies and Scientific Research- Engineering Sciences Series Vol. (29) No. (1) 2007

أمان طرائق التواقيع الرقمية

الدكتور تاج الدين جركس*
الدكتور عدنان معترماوي**
غسان ناصر***

(تاريخ الإيداع 4 / 10 / 2006. قبل للنشر في 2007/3/18)

□ الملخّص □

تعتبر التواقيع الرقمية إحدى أهم التطبيقات الحديثة للتعمية ومن أهم تقنيات تحقيق الأمان في المعاملات الإلكترونية الرقمية التي تتزايد أهميتها باستمرار في عصر الحوسبة والمعلوماتية.

يهدف هذا البحث إلى دراسة مقارنة لأمان طرائق التواقيع الرقمية وذلك بعد دراسة التواقيع الرقمية ومتطلباتها وأنواعها وطرائقها.

يتضمن البحث دراسة أمان أهم طرائق التواقيع الرقمية التي تقوم على خوارزميات المفتاح العام المبنيّة على أسس رياضية مختلفة وسنختار من أجل ذلك طريقتين مستخدمتين لإنشاء تواقيع المرة الواحدة و طرائق أخرى تقوم على مسألة اللوغاريتم المقطَّع بالإضافة إلى طريقة تقوم على مسألة تحليل الأعداد الكبيرة جداً إلى عواملها الأولية.

كما يتضمن البحث اقتراح توصيات مناسبة لتحسين الأمان.

الكلمات المفتاحية: الأمان– التوقيع الرقمي– المصادقة– عدم التنصل– طرائق التوقيع الرقمي– التواقيع الرقمية غير القابلة للإنكار – التواقيع الرقمية المنيعة على الإخفاق – توابع التهشير وحيدة الاتجاه.

* أستاذ في قسم هندسة الاتصالات والالكترونيات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.
** مدرّس في قسم هندسة الاتصالات والالكترونيات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.
*** طالب ماجستير في قسم هندسة الاتصالات والالكترونيات – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين– اللاذقية – سورية.

مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الهندسية المجلد (29) العدد (1) 2007
Tishreen University Journal for Studies and Scientific Research- Engineering Sciences Series Vol. (29) No. (1) 2007

Security of Digital Signature Schemes

Dr. Tajedin Jarkas*
Dr. Adnan Matarmawi **
Ghassan Nasser ***

(Received 4 / 10 / 2006. Accepted 18/3/2007)

□ ABSTRACT □

Digital signatures is one of the most important new applications for cryptography and the most important technique of achieving security in digital transactions. Its importance increases continuously in the age of computing and informatics.

This paper studies the security of digital signature schemes after studying the digital signatures and its requirements, types and schemes.

The paper includes studying the security of the most important digital signature schemes, which depend on the public-key algorithms that are based on several mathematical bases.

We will select for that two schemes used to produce one-time signatures and other schemes that depend on discrete logarithm problem, in addition to one scheme that depends on factoring very great numbers.

The paper also includes suggestions for suitable recommendations to improve the security of digital signature schemes.

Keywords: Security, Digital Signature, Authentication, Non-repudiation, Digital Signature Schemes, Undeniable Signature Scheme, Fail-Stop Signature Scheme, One-way Hash Function.

* **Professor, Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen, Lattakia, Syria.**
** **Assistant Professor, , Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen, Lattakia, Syria.**
*** **Postgraduate Student, , Department of Communication Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen, Lattakia, Syria.**

مقدمة:

يعتبر الأمان أحد التحديات الرئيسة التي تواجهها المراسلات الالكترونية عبر الشبكات الحاسوبية المختلفة، ومن هنا كان الاهتمام الكبير بإيجاد تقنيات تستطيع تحقيق متطلبات الأمان الرئيسة الآتية:

السرية (Confidentiality) – التكاملية (Integrity) – المصادقة (Authentication) – عدم التنصل (Non-repudiation) – الجاهزية (Availability) – والتحكم بالوصول (Access Control).

إن الهدف من طرائق التواقيع الرقمية هو إنشاء التواقيع الرقمية التي يمكن لها أن تحقق ثلاثة متطلبات من متطلبات الأمان الرئيسة وهي: المصادقة – التكاملية – وعدم التنصل.

لقد جاء التوقيع الرقمي ثمرة من ثمار التطور الهائل في العمل على تقنيات التعمية (Cryptography) حيث يوفر مجموعة من القدرات الأمنية يصعب تنفيذها بأي طريقة أخرى.

سيتم في هذا البحث التعرف على التواقيع الرقمية ومتطلباتها وأنواعها وطرائقها.

كما ستتم دراسة الأمان في أهم طرائق التواقيع الرقمية التي تقوم على خوارزميات المفتاح العام المبنية على أسس رياضية مختلفة وسيتم اختيار طريقتين مستخدمتين لإنشاء تواقيع المرة الواحدة و بعض الطرائق التي تقوم على مسألة اللوغاريتم المقطَّع وأخرى تقوم على مسألة تحليل الأعداد الكبيرة جداً إلى عواملها الأولية.

كما سيتم في نهاية البحث اقتراح توصيات مناسبة لتحسين الأمان في طرائق التواقيع الرقمية.

تم إجراء هذا البحث في قسم هندسة الاتصالات والالكترونيات في كلية الهندسة الميكانيكية والكهربائية في جامعة تشرين في الفترة الواقعة بين 30 / 01 / 2006 م و 30 / 09 / 2006 م.

أهمية البحث وأهدافه:

تكمن أهمية البحث في أهمية الأمان بشكل عام الذي يعتبر أحد التحديات الرئيسة التي تواجهها المراسلات الالكترونية عبر الشبكات الحاسوبية المختلفة وفي أهمية التوقيع الرقمي بشكل خاص كإحدى أهم تقنيات تحقيق الأمان الذي يبدو من التقنيات الأساسية التي ستحدد مستقبل المعاملات الالكترونية.

تتلخص أهداف البحث في التعرف على التواقيع الرقمية ومتطلباتها وأنواعها وطرائقها وفي دراسة الأمان في أهم طرائق التواقيع الرقمية التي تقوم على خوارزميات المفتاح العام المبنيّة على أسس رياضية مختلفة واقتراح توصيات مناسبة لتحسين الأمان في طرائق التواقيع الرقمية.

طريقة البحث:

يبدأ البحث بالتعرف على التواقيع الرقمية ومتطلباتها وأنواعها وطرائقها بالإضافة إلى مصطلحات الأمان.

ثم ينتقل إلى دراسة أمان أهم طرائق التواقيع الرقمية التي تقوم على خوارزميات المفتاح العام المبنيّة على أسس رياضية مختلفة حيث ستتم دراسة:

1- طريقة توقيع لامبورت (Lamport Signature Scheme)

– طريقة توقيع بوس– تشاوم (Bos - Chaum Signature Scheme)

وهما طريقتان بسيطتان لإنشاء تواقيع المرة الواحدة.

2- طريقة توقيع تشاوم – فان انتويربن غير القابل للإنكار
(Chaum - van Antwerpen Undeniable Signature Scheme)
- طريقة توقيع فان هيست وبيدرسن المنيع على الإخفاق
- (Van Heyst and Pedersen Fail - stop Signature Scheme)
- طريقة توقيع الجمال (El-Gamal Signature Scheme)
- معيار التوقيع الرقمي DSS (Digital Signature Standard)

كطرائق تواقيع رقمية تعتمد في قوتها على صعوبة حل مسألة اللوغاريتم المقطَّع.

3- طريقة التوقيع RSA (RSA Signature Scheme) كطريقة توقيع رقمي تعتمد في قوتها على صعوبة تحليل الأعداد الكبيرة جدا إلى عواملها الأولية.

ثم مناقشة جوانب الأمان المختلفة (محاسن وعيوب) في طرائق التواقيع الرقمية الواردة في البحث ومن ثم الاستنتاجات والتوصيات بالإضافة إلى قائمة بأسماء المراجع التي يستند إليها البحث.

ما هو التوقيع الرقمي ؟

التوقيع الرقمي هو المكافئ الرقمي للتوقيع اليدوي وهو تقنية مصادقة (Authentication Technique) تتضمن تدابير لمنع الإنكار سواء من قبل المصدر (المرسل) أو من قبل الوجهة (المستلم) كما يمكن أن تتضمن تدابير لفحص تكاملية الرسالة ويجب أن يحقق الخواص التالية:

1- القدرة على التحقُّق من الموقِّع ومن تاريخ وزمن التوقيع.
2- القدرة على مصادقة المحتويات في أي وقت كان.
3- يجب أن يكون التوقيع قابلاً للتحقُّق من قبل طرف ثالث موثوق، وذلك من أجل فض النزاعات في حال نشوئها.
ويجب أن يتضمن التوقيع الرقمي تابع مصادقة (Authentication Function).

متطلبات التوقيع الرقمي:

يجب أن يحقق التوقيع الرقمي المتطلبات الآتية:

1- يجب أن يكون التوقيع الرقمي عبارة عن سلسلة بتات لأصل الرسالة.
2- يجب أن يستخدم التوقيع الرقمي بعض المعلومات الفريدة عن المرسل لمنع التزوير والإنكار.
3- يجب أن يكون إنشاء التوقيع سهلاً نسبياً.
4- يجب أن يكون التحقُّق من التوقيع سهلاً نسبياً.
5- يجب أن يكون تزوير التوقيع غير قابل للتطبيق حسابيا سواء بإنشاء رسالة جديدة من أي توقيع رقمي موجود أو باحتيال توقيع رقمي لأي رسالة معطاة.

إن استخدام تابع تهشير (Hash Function) آمن كجزء لا يتجزأ من طريقة التوقيع يحقق هذه المتطلبات.

أنواع التوقيع الرقمي:

1- التوقيع الرقمي المباشر: يشمل التوقيع الرقمي المباشر (Direct Digital Signature) طرفي الاتصال فقط أي المصدر والوجهة حيث إنه يفترض بأن الطرف الوجهة يعلم بالمفتاح العام (Public Key) للطرف المصدر ويتم إنشاؤه إما بتشفير كامل الرسالة باستخدام المفتاح الخاص (Private Key) للمرسل أو بتشفير ترميز التهشير (Hash Code) للرسالة باستخدام المفتاح الخاص للمرسل.

إن تحقيق السرية في طرائق التوقيع المباشر يتم بتشفير إضافي آخر للرسالة مع التوقيع، وذلك إما باستخدام المفتاح العام للمستلم أو باستخدام المفتاح السري المشترك حيث يتم إنجاز تابع التوقيع أولاً ومن ثم تابع السرية ذلك لأن الطرف الثالث الذي نحتاج إليه في حال نشوء نزاعات والذي يقوم بفحص الرسالة والتوقيع سيحتاج إلى الوصول إلى مفتاح فك التشفير لقراءة الرسالة الأصلية في حال حساب التوقيع بعد تشفير الرسالة.

إن جميع طرائق التوقيع المباشر تتشارك بنقطة ضعف واحدة وهي أن شرعية التوقيع تعتمد على أمان المفتاح الخاص للمرسل الأمر الذي يسمح للمرسل بإنكار توقيعه مدّعيا ضياع مفتاحه الخاص وقيام أحد الأشخاص بتزوير التوقيع علماً أنّ الرقابة الحكومية المتعلقة بأمان المفاتيح الخاصة يمكن توظيفها للحؤول دون حصول ذلك عن طريق تضمين التوقيع طابعاً زمنياً (Timestamp) يبين الزمن والتاريخ.

2- التوقيع الرقمي المحكَّم: يقوم التوقيع الرقمي المحكَّم (Arbitrated Digital Signature) بحل المشاكل المتعلقة بالتوقيع المباشر حيث تذهب فيه كل رسالة موقعة إلى محكِّم موثوق أولاً الذي يقوم بإخضاعها إلى عدد من الاختبارات لفحص أصلها ومحتواها ثم يؤرخها ويرسلها إلى وجهتها بدلالة معينة الأمر الذي يمنع المرسل من إنكار توقيعه.

وهنا نميز حالتين:

1- الطرائق التي تقوم على التشفير التقليدي بالمفتاح المتناظر (Symmetric Key):

في هذه الحالة يتشارك المحكِّم A والمرسل X بالمفتاح السري K_{AX} ويتشارك المحكِّم A والمستلم Y بالمفتاح السري K_{AY}.

يُنشئ المرسل X الرسالة M ويحسب قيمة تهشيرها $H(M)$ ويرسلها إلى المحكِّم A مع التوقيع المؤلف من قيمة التهشير (Hash Value) ومعرِّف (Identifier) المرسل ID_X بعد أن يشفرها (الرسالة مع التوقيع) باستخدام المفتاح K_{AX}.

يقوم المحكِّم A بفك تشفير التوقيع وفحص قيمة التهشير ليعلن شرعية الرسالة.

ثم يقوم المحكِّم A بإرسال الرسالة إلى Y مشفرة باستخدام المفتاح K_{AY} حيث تتضمن الرسالة ما يلي: معرف المرسل ID_X – الرسالة الأصل المرسلة من X – التوقيع – والطابع الزمني.

يقوم المستلم Y بفك تشفير الرسالة لاستعادة الرسالة الأصل والتوقيع مع الطابع الزمني الذي يُخبر المستلم بأن هذه الرسالة جديدة وغير مكررة.

من عيوب هذا السيناريو أن المحكِّم A يستطيع قراءة الرسائل التي تمر عبره وبالتالي يجب على طرفي الاتصال أن يمتلكان ثقة عالية به.

يوجد سيناريو آخر يستخدم التشفير التقليدي وهو يفترض بأن X و Y يتشاركان بالمفتاح السري K_{XY}.

في هذه الحالة يرسل X نسخة عن الرسالة مشفرة باستخدام المفتاح K_{XY} مع التوقيع المؤلف من المعرِّف ومن قيمة التهشير للرسالة وذلك بعد تشفيرها باستخدام المفتاح K_{AX} حيث يقوم المحكِّم كما ذكرنا سابقا بفك تشفير التوقيع

وفحص قيمة التهشير ليعلن شرعية الرسالة وعندئذ يرسل كل ما استلمه من X بالإضافة إلى الطابع الزمني إلى Y مشفرا باستخدام المفتاح K_{AY}.

إن المحكِّم هنا يعمل مع نسخة مشفرة عن الرسالة فهو لا يستطيع قراءتها الأمر الذي يمنعه من الاحتيال على أي من الطرفين على خلاف السيناريو الأول الذي يستطيع فيه المحكِّم الاتفاق مع المرسل لإنكار الرسالة الموقعة أو مع المستلم لتزوير توقيع المرسل.

2- الطرائق التي تقوم على التشفير بالمفتاح العام (Public-key Encryption):

تستطيع طرائق التواقيع بالمفتاح العام حل مشاكل التشفير التقليدي.

في هذه الحالة يقوم المرسل X بتشفير مضاعف للرسالة M الأول باستخدام المفتاح الخاص للمرسل KR_X والثاني باستخدام المفتاح العام للمستلم KU_Y.

تُرسل الرسالة الموقعة مع معرِّف المرسل إلى المحكِّم A بعد تشفيرها ثانية بالمفتاح الخاص للمرسل KR_X.

يجعل التشفير الداخلي المضاعف الرسالة آمنة من احتيال المحكِّم.

يقوم المحكِّم A بفك التشفير الخارجي للتأكد من أن الرسالة قادمة بالفعل من المرسل X من خلال أن المرسل X هو الوحيد الذي يملك KR_X وبعد إجراء الفحوصات اللازمة وإضافة الطابع الزمني يرسلها إلى Y مشفرة باستخدام مفتاحه الخاص KR_A.

إن هذه الطريقة تمتلك عددا من المحاسن عن الطريقتين السابقتين وهي أن عدم وجود معلومات يتشارك بها الطرفان X و Y قبل الاتصال يمنع الروابط من الاحتيال كما أنه لا يمكن إرسال أي رسالة مؤرخة بشكل غير صحيح بالإضافة إلى أن محتوى الرسالة يبقى آمنا من احتيال المحكِّم A ومن احتيال الآخرين.

إن معظم خوارزميات المفتاح العام تقوم على واحدة من ثلاث مسائل صعبة [1] هي:

1- مسألة الجعبة أي إيجاد مجموعة جزئية مجموعها N من مجموعة من الأعداد الفريدة.

2- مسألة اللوغاريتم المقطَّع أي المسألة العكسية للرفع إلى قوة بالمقاس p: فإذا كان p عددا أوليا وكان g و M عددين صحيحين يُطلب إيجاد x التي تحقق العلاقة: $g^x = M \pmod p$

3- مسألة تحليل الأعداد الكبيرة جدا إلى عواملها الأولية: فإذا كان N جداء عددين أوليين يُطلب إما:

أ- تحليل N إلى عامليه الأوليَّين.

ب- بوجود M و C إيجاد d التي تحقق العلاقة: $M^d = C \pmod N$

ت- بوجود e و C إيجاد M التي تحقق العلاقة: $M^e = C \pmod N$

ث- بوجود عدد x الإقرار فيما إذا يوجد عدد y يحقق العلاقة $x = y^2 \pmod N$

ما هي طرائق التواقيع الرقمية ؟

إن أول تعريف غير رسمي لطرائق التواقيع الرقمية من قبل Diffie و Hellman يرى أنّ طرائق التواقيع الرقمية هي شكل من أشكال طرائق التشفير بحيث يتم استخدامه بطريقة معكوسة غير أن هذا التعريف ولو كان صحيحا بالنسبة لبعض طرائق التواقيع الرقمية (طريقة RSA مثلا) فهو غير صحيح لمعظم طرائق التواقيع الرقمية الحالية (طريقة DSS مثلا).

تتألف طريقة التوقيع الرقمي وفقاً للتعريف الذي يبدو نهائياً ويشمل جميع طرائق التواقيع الرقمية من خوارزميتين على الأقل الأولى خوارزمية التوقيع (sig) ويجب أن تكون سرية والثانية خوارزمية التحقُّق من صحة التوقيع (ver) ويجب أن تكون علنية وهي متوافقة مع خوارزمية التوقيع.

تعني طريقة التوقيع الرقمي خمس مترابطات بيانية (P, A, K, S, V) تحقق الشروط الآتية:

1- P هي مجموعة محددة من الرسائل الممكنة.

2- A هي مجموعة محددة من التواقيع الممكنة.

3- K هي مجموعة محددة من المفاتيح الممكنة (فضاء المفاتيح).

4- من أجل كل $k \in K$ توجد خوارزمية توقيع $sig_k \in S$ وخوارزمية تحقُّق متوافقة $ver_k \in V$.

إن كل $sig_k : P \to A$ وإن كل $ver_k : P \times A \to \{true, false\}$ هي توابع تحقق المعادلات الآتية من أجل كل رسالة $x \in P$ وكل توقيع $y \in A$:

$$ver(x, y) = \begin{cases} true & if \quad y = sig(x) \\ false & if \quad y \neq sig(x) \end{cases}$$

ومن أجل كل $k \in K$ يجب أن يكون كل من التابعين sig_k و ver_k من توابع الزمن الحدودي Polynomial-time Functions (أي من فئة التوابع ذات التعقيد الزمني الحدودي [1] و [6]).

كما يجب أن يكون التابع ver_k تابعاً علنياً وأن يكون التابع sig_k تابعاً سرياً.

ما الأمان المقصود في البحث ؟

سيتم التمييز في هذا البحث بين ثلاثة مصطلحات للأمان هي:

1- **الأمان الحسابي (Computationally):** وهو يعني عدم إمكانية كسر الطريقة بالإمكانات المتاحة الحالية والمستقبلية كما يطلق أحيانا على الطريقة الآمنة حسابيا الطريقة القوية.

2- **الأمان دون شروط (Unconditionally):** وهو يعني عدم وجود معلومات كافية لاستعادة التوقيع ولا يمكن لطريقة توقيع أن تكون آمنة دون شروط ما دام يمكن تجريب كل التواقيع الممكنة y للرسالة x باستخدام خوارزمية التحقق العلنية ver حتى إيجاد التوقيع الصحيح.

3- **الأمان المطلق (Full):** وهو يشمل الأمان دون شروط والأمان الحسابي معا كما يطلق عليه أحياناً الأمان المنيع على الإخفاق (Fail–stop Security).

طريقة توقيع لامبورت (Lamport Signature Scheme):

وهي طريقة بسيطة لإنشاء توقيع المرة الواحدة من أي تابع وحيد الاتجاه حيث يعني مصطلح المرة الواحدة بأن هذه الطريقة يمكن أن تستخدم لتوقيع رسالة واحدة فقط (بينما التحقُّق من التوقيع يمكن أن يتم في أي وقت) حيث إنّه بوجود توقيعين مفترضين لرسالتين مختلفتين يمكن إنشاء تواقيع أخرى لرسائل أخرى مختلفة عن الرسالتين الأولى والثانية.

إن الرسالة التي يمكن توقيعها هي مترابطة بيانية مزدوجة $binary\ k-tuple$ حيث يتم توقيع كل بت بشكل مستقل: إن القيمة $Z_{i,j}$ توافق البت ذو الدلالة i من الرسالة الذي يملك القيمة j حيث $(j = 0,1)$.

إن كل $Z_{i,j}$ هي صورة طبق الأصل عن $y_{i,j}$ في التابع f الوحيد الاتجاه ويتم توقيع البت ذي الدلالة i من الرسالة باستخدام الصورة الأولية $y_{i,j}$ لـ $Z_{i,j}$ المتوافقة مع البت ذي الدلالة i من الرسالة.

يكون التحقق من التوقيع ببساطة هو اختبار أن كل عنصر في التوقيع هو صورة أولية لعنصر مناسب من المفتاح العام. يبين الشكل (1) وصفا لهذه الطريقة.

ليكن k عددا صحيحا موجباً وليكن $p=\{0,1\}^k$ ولنفترض أن $f: Y \to Z$ تابع وحيد الاتجاه. كما نفترض أن $A=Y^k$ وأن $y_{i,j} \in Y$ يتم اختيارها بشكل عشوائي حيث $1 \le i \le k, j=0,1$

ولنفترض أن: $z_{i,j}=f\left(y_{i,j}\right)$ حيث $1 \le i \le k, j=0,1$

يتألف المفتاح K من $2k-y's$ ومن $2k-z's$ حيث إنّ قيم y هي قيم سرية وأن قيم z هي قيم معلنة.

من أجل: $K=\left(y_{i,j}, z_{i,j}: 1 \le i \le k, j=o,1\right)$

نحدد: $sig_K\left(x_1,\cdots,x_k\right)=\left(y_{1,x_1},\cdots,y_{k,x_k}\right)$

كما نحدد: $ver_K\left(x_1,\cdots,x_k,a_1,\cdots,a_k\right)=true \leftrightarrow f\left(a_i\right)=z_{i,x_i} \quad , \quad 1 \le i \le k$

الشكل (1): طريقة توقيع لامبورت

نلاحظ بأنه لا يمكن تزوير التوقيع لأنه من المستحيل عكس التابع f (الوحيد الاتجاه) للحصول على قيم y السرية. كما أنه لا يمكن في هذه الطريقة تزوير توقيع على رسالة ثانية بمعرفة توقيع على رسالة معينة ذلك لأن قيم y الموافقة للرسالة الأولى هي ليست مجموعة جزئية من قيم y الموافقة للرسالة الثانية.

إن هذه الطريقة ليست عملية بسبب الحجم الكبير للتواقيع التي تنتجها فعلى سبيل المثال عند استخدام التابع الأسي $f(x)=\alpha^x \bmod p$ يتطلب التنفيذ الآمن أن يكون المقاس p بطول 512 بت على الأقل، وهذا يعني أن كل بت من الرسالة يُوقع باستخدام 512 بت وسيكون التوقيع أطول من الرسالة بـ 512 مرة.

لقد تم إجراء تعديل مناسب على هذه الطريقة من قبل بوس وتشاوم بحيث يسمح بإجراء توقيع أقصر مع المحافظة على نفس الأمان.

طريقة توقيع بوس – تشاوم (Bos - Chaum Signature Scheme):

يبين الشكل (2) وصفا كاملا لهذه الطريقة.

ليكن k عدداً صحيحاً موجباً وليكن $p=\{0,1\}^k$ و ليكن n عدداً صحيحاً بحيث إنَّ $2^k \le \binom{2n}{n}$

وليكن B مجموعة من أصل $2n$ ولنفترض أن: $\phi: \{0,1\}^k \to B$ تطبيقا متباينا (كل عنصر من مجاله مختلف الصورة) حيث B هي مجموعة من كل المجموعات الجزئية n من B.

لنفترض أن $f: Y \to Z$ تابع وحيد الاتجاه ولنفترض أن $A=Y^n$ ولنفترض أن $y_i \in Y$ يتم اختيارها بشكل عشوائي حيث $1 \le i \le 2n$ ولنفترض أن: $z_i=f\left(y_i\right)$ حيث أن $1 \le i \le 2n$

يتألف المفتاح K من $2n-y's$ ومن $2n-z's$ حيث إنّ قيم y هي قيم سرية و قيم z هي قيم معلنة.

من أجل: $K=\left(y_i, z_i: 1 \le i \le 2n\right)$ نحدد: $sig_K\left(x_1,\cdots,x_k\right)=\left\{y_j : j \in \phi\left(x_1,\cdots,x_k\right)\right\}$

كما نحدد: $ver_K\left(x_1,\cdots,x_k,a_1,\cdots,a_k\right)=true \leftrightarrow \left\{f\left(a_i\right): 1 \le i \le n\right\}=\left\{z_j : j \in \phi\left(x_1,\cdots,x_k\right)\right\}$.

الشكل (2): طريقة توقيع بوس– تشاوم

تتطلب هذه الطريقة وجود تابع تطبيق متباين ϕ يربط مجموعة جزئية n من مجموعة $2n$ مع كل مترابطة بيانية ثنائية محتملة $x=\left(x_1,\cdots,x_k\right)$.

لقد تم البرهان على أن اختصارا في حجم التوقيع بواسطة استخدام طريقة بوس – تشاوم يصل إلى 50% من حجم التوقيع باستخدام طريقة لامبورت مع المحافظة على الأمان نفسه في الطريقتين.

طريقة توقيع تشاوم – فان انتويربن غير القابل للإنكار

(Chaum-Van Antwerpen Undeniable Signature Scheme):

لقد تم تقديم هذه الطريقة من قبل تشاوم وفان انتويربن في عام 1989 م وفيها لا يمكن التحقق من التوقيع من دون موافقة وتعاون الموقِّع وتُسمى التواقيع الناتجة بالتواقيع غير القابلة للإنكار.

يبين الشكل (3) توضيحا لخوارزمية التوقيع وبروتوكول التحقق لهذه الطريقة.

ليكن $p = 2q + 1$ عددا أوليا حيث أن q عدد أولي أيضاً وأن مسألة اللوغاريتم المقطع في Z_P عصية لا يمكن حلها في زمن حدودي وليكن $\alpha \in Z_p^*$ عنصر ترتيب q وليكن $1 \le a \le q-1$

ونحدد: $\beta = \alpha^a \bmod p$

ولتكن G تشير إلى المجموعة الجزئية المضاعفة من Z_P^* ترتيب q

(تتألف G من الراسب التربيعي بالمقاس p).

وليكن $P = A = G$ نحدد: $K = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$.

حيث إنّ القيم p, α, β هي قيم معلنة والقيمة a هي قيمة سرية.

من أجل: $K = (P, \alpha, A, \beta)$ و $x \in G$ نحدد: $y = sig_K(x) = x^a \bmod p$

ومن أجل $x, y \in G$ يتم التحقق بواسطة تنفيذ البروتوكول الآتي:

1- يختار المرسل e_1, e_2 بشكل عشوائي بحيث $e_1, e_2 \in Z_q^*$.

2- يحسب المرسل $c = y^{e_1} \beta^{e_2} \bmod p$ ويرسلها إلى وجهتها (المستلم).

3- يحسب المستلم $d = c^{a^{-1} \bmod q} \bmod p$ ويرسلها إلى المرسل.

4- يقر المرسل بأن y هو توقيع صحيح إذا وفقط إذا كانت: $d \equiv x^{e_1} \alpha^{e_2} \pmod p$

الشكل (3): طريقة توقيع تشاوم – فان انتربين غير القابلة للإنكار

تتألف طريقة توقيع تشاوم – فان انتويربن غير القابلة للإنكار من: خوارزمية التوقيع – برتوكول التحقُّق من التوقيع – وبروتوكول الإنكار (Disavowal Protocol).

لقد تم إدخال بروتوكول الإنكار في هذه الطريقة لمنع الموقِّع من إنكار التوقيع الذي قام به ولمنع ادعائه بأن التوقيع الصحيح هو توقيع مزور حيث يستطيع الموقِّع بواسطة هذا البروتوكول اختبار تزوير التوقيع.

كما تم البرهان على أن احتمال أن يستطيع أحد أن يخدع الموقِّع بأن يقبل بالتوقيع المزور كتوقيع صحيح هو $\left(1/q\right)$ ولما كانت هذه النتيجة لا تعتمد على فرضيات حسابية يكون الأمان دون شروط.

كما تم البرهان أيضاً على أن احتمال أن يتمكن الموقِّع من محاولة إنكار توقيع صحيح هو $\left(1/q\right)$ أيضاً.

طريقة توقيع فان هيست وبيدرسن المنيع على الإخفاق

(Van Heyst and Pedersen Fail-stop Signature Scheme):

لقد تم إنشاء هذه الطريقة من قبل فان هيست وبيدرسن في عام 1992م، وهي تؤمن تعزيزا للأمان ضد احتمال تزوير توقيع مهما كانت قوة العدو حيث يستطيع الموقِّع البرهان على حصول التزوير باحتمال كبير جداً.

تسمى التواقيع الناتجة باستخدام هذه الطريقة التواقيع المنيعة على الإخفاق.

إن المبدأ الأساسي لهذه الطريقة هو وجود عدد كبير من المفاتيح الخاصة الممكنة التي تعمل مع مفتاح عام معين وكل من هذه المفاتيح الخاصة ينتج توقيعاً مختلفاً حيث يبين الشكل (4) شرحاً لخوارزميتي التوقيع والتحقق لهذه الطريقة.

ليكن $p = 2q + 1$ عددا أوليا حيث إنّ q عدد أولي أيضاً وأن مسألة اللوغاريتم المقطع في Z_P عصية لا يمكن حلها في زمن حدودي وليكن $\alpha \in Z_p^*$ عنصر ترتيب q وليكن $1 \le a_o \le q-1$

ونحدد: $\beta = \alpha^{a_0} \bmod p$

حيث إنّ القيم $p, q, \alpha, \beta,$ و a_0 يتم اختيارها بواسطة سلطة مركزية (موثوقة).

وحيث إنّ القيم $p, q, \alpha,$ و β هي قيم معلنة وينظر إليها على أنها ثابتة وأن القيمة a_0 هي قيمة سرية

ليكن $P = Z_q$ و $A = Z_q \times Z_q$ والمفتاح يأخذ الشكل: $K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2)$

حيث: $a_1, a_2, b_1, b_2 \in Z_q$ و $\gamma_1 = \alpha^{a_1}\beta^{a_2} \bmod p$ و $\gamma_2 = \alpha^{b_1}\beta^{b_2} \bmod p$

من أجل: $K = (\gamma_1, \gamma_2, a_1, a_2, b_1, b_2)$ و $x \in Z_q$ نحدد: $sig_K(x) = (y_1, y_2)$

حيث: $y_1 = a_1 + xb_1 \bmod q$ و $y_2 = a_2 + xb_2 \bmod q$

و من أجل: $y = (y_1, y_2) \in Z_q \times Z_q$

يكون: $ver_K(x, y) = true \leftrightarrow \gamma_1 \gamma_2^x \equiv \alpha^{y_1}\beta^{y_2} (\bmod p).$

الشكل (4): طريقة التوقيع فان هيست وبيدرسين المنيع على الإخفاق

يتألف نظام طريقة توقيع فان هيست وبيدرسين المنيع على الإخفاق من: خوارزمية التوقيع – خوارزمية التحقُّق – وخوارزمية برهان التزوير (Proof of Forgery).

يمكن حساب مفتاح الموقِّع K بسهولة إذا وُقعت رسالتان مختلفتان باستخدام المفتاح نفسه ولذا تعتبر هذه الطريقة طريقة المرة الواحدة.

إذا كانت y هي توقيع صحيح على الرسالة x عندها توجد q مفاتيح محتملة التي من خلالها تكون لدينا x موقعة بـ y ولكن من أجل أي رسالة أخرى x' حيث $x' \neq x$، فإن هذه المفاتيح q ستنتج q توقيعًا مختلفاً على x'.

كما تم البرهان على أنه إذا كان لدينا $sig_K(x) = y$ وكان لدينا x' حيث $x' \neq x$ فإننا نستطيع حساب $sig_K(x')$ باحتمال $\left(1/q\right)$.

إن النتيجة السابقة لا تعتمد على القوة الحسابية ويتم الحصول على مستوى الأمان من عدم إمكانية إحصاء المفاتيح المحتملة q التي يمكن أن يستخدمها الموقِّع وبالتالي فإن الأمان دون شروط.

كما أن استخدام هذه الطريقة كطريقة توقيع المرة الواحدة يجعل من أمانها أماناً مطلقاً.

إذا أُعطي الموقِّع توقيعاً مزوراً فهو يستطيع البرهان على حدوث التزوير باحتمال $\left(1 - 1/q\right)$ مع الإشارة إلى أن برهان التزوير يعني إيجاد القيمة $a_0 = \log_\alpha \beta$ المعروفة فقط من قبل السلطة المركزية.

طريقة توقيع الجمال (El-Gamal Signature Scheme):

إن طريقة توقيع الجمال تعتمد في قوتها على صعوبة حل مسألة اللوغاريتم المقطَّع وهي ليست مصممة كنظام الجمال للتشفير بالمفتاح العام بل هي مصممة بشكل خاص بهدف التوقيع الرقمي حيث يبين الشكل (5) شرحاً مفصلا لهذه الطريقة.

ليكن p عدداً أولياً حيث إنّ مسألة اللوغاريتم المقطع في Z_P عصية (صعبة) لا يمكن حلها في زمن حدودي.

وليكن $\alpha \in Z_P^*$ عنصراً أولياً وليكن $A = Z_P^* \times Z_{P-1}$, $P = Z_P^*$

ونحدد: $K = \{(P, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$

إن قيم p , α و β هي قيم معلنة وإن قيمة a هي قيمة سرية.

نحدد من أجل $K = (p, \alpha, a, \beta)$ ومن أجل العدد العشوائي السري $k \in Z_{P-1}^*$ ما يأتي:

$sig_K(x,k) = (\gamma, \delta)$ حيث: $\gamma = \alpha^k \bmod p$ و $\delta = (x - a\gamma)k^{-1} \bmod (p-1)$

ومن أجل $x, \gamma \in Z_P^*$ و $\delta \in Z_{P-1}$ نحدد:

$ver_K(x, \gamma, \delta) = true \leftrightarrow \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p$

الشكل (5) طريقة توقيع الجمال

نلاحظ من الشكل بأن التوقيع يتم باستخدام القيمة السرية a التي هي جزء من المفتاح K وباستخدام العدد العشوائي السري k المستخدم لتوقيع رسالة واحدة فقط x.

يُمكن كسر طريقة توقيع الجمال في حالة معرفة قيمة a التي يسهل حسابها بمعرفة قيمة k أو إذا تم استخدام قيمة k نفسها في توقيع رسالتين مختلفتين.

يقل احتمال التزوير إلى درجة كبيرة جداً وذلك بسبب ضرورة حساب اللوغاريتم المقطع عند أي محاولة تزوير.

معيار التوقيع الرقمي DSS (Digital Signature Standard):

وهي طريقة تعتمد في قوتها على صعوبة حل مسألة اللوغاريتم المقطَّع أيضاً كما أنها شكل معدَّل من طريقة توقيع الجمال وهي تقوم على خوارزمية التوقيع الرقمي DSA وقد تم تبنيها كمعيار في عام 1994 م.

يبين الشكل (6) وصفا كاملاً لهذه الطريقة.

ليكن p عدداً أولياً عدداً أولياً حيث إنّ مسألة اللوغاريتم المقطع في Z_P عصية لا يمكن حلها في زمن حدودي

وليكن q عددا أوليا بطول 160 بت ويقسم $p-1$.

وليكن $\alpha \in Z_P^*$ تحقق العلاقة: $\alpha = h^{(p-1)/q} \bmod p$ حيث إنّ h هو أي عدد أصغر من $p-1$ ويحقق العلاقة: $h^{(p-1)/q} \bmod p > 1$ ويمكن أم يشترك فيه مجموعة من المستخدمين.

وليكن $A = Z_q Z_q$, $P = Z_q^*$ ونحدد: $K = \{(p, q, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$

إن القيم p, q, α, β هي قيم عامة معلنة والقيمة a هي قيمة سرية.

نحدد من أجل $K = (p, q, \alpha, a, \beta)$ ومن أجل العدد العشوائي السري k حيث $1 \le k \le q-1$ ما يلي:

$sig_K(x,k) = (\gamma, \delta)$ حيث: $\gamma = (\alpha^k \bmod p) \bmod q$ و $\delta = (x + a\gamma)k^{-1} \bmod q$

ومن أجل $x \in Z_q^*$ و $\gamma, \delta \in Z_q$ يتم التحقُّق بإنجاز الحسابات الآتية:

$$e_1 = x\delta^{-1} \bmod q \quad \text{و} \quad e_2 = \gamma\delta^{-1} \bmod q$$

$$ver_K(x, \gamma, \delta) = true \leftrightarrow \left(\alpha^{e_1} \beta^{e_2} \bmod p\right) \bmod q = \gamma$$

الشكل (6) معيار التوقيع الرقمي DSS

لقد تم توجيه العديد من الانتقادات إلى الـ DSA نوجزها بما يلي:

1- لا يمكن استخدام الـ DSA للتعمية أو لتوزيع المفاتيح.

2- إن وكالة الأمن القومي NSA هي من طوَّر الـ DSA ويمكن أن يكون ثمة باب خلفي في الخوارزمية.

3- إن الـ DSA أبطأ من الـ RSA علماً أنّ توليد التوقيع متماثل في الخوارزميتين أمّا تحقُّق التوقيع بالـ DSA فهو أبطأ بـ 10 إلى 40 مرة.

4- إن طريقة التوقيع RSA هي معيار بالأمر الواقع.

5- لم يُتح الوقت الكافي لتحليل الـ DSA لأن عملية اختيارها لم تكن علنية.

6- قد تكون الـ DSA منتهكة لبراءات اختراع أخرى.

7- طول المفتاح صغير جداً وهذا هو الانتقاد الوحيد المشروع للـ DSA حيث حدد التنفيذ الأصلي للخوارزمية طول المقاس بـ 512 بتا ونظرا لأن الخوارزمية تستمد أمانها من صعوبة حساب اللوغاريتم المقطَّع بوجود هذا المقاس فقد أقلق ذلك معظم المهتمين واستجابة لهذا الانتقاد جعلت NIST طول المفتاح متغيرا من 512 حتى 1024 بتا على أن يكون من مضاعفات العدد (64) الأمر الذي جعلها أكثر أمناً.

8-

طريقة التوقيع RSA (RSA Signature Scheme):

تعتمد هذه الطريقة في قوتها على صعوبة تحليل الأعداد الكبيرة جداً إلى عواملها الأولية وسُميت بهذا الاسم تبعاً لأسماء مطوريها وهم R. Rivest و A. Shamir و L. Adleman وهي أول خوارزمية مفتاح عام تامة النضج.

يبين الشكل (7) وصفا لهذه الطريقة.

ليكن $n = pq$ حيث p و q عددان أوليان.

وليكن $P = A = Z_n$ ونحدد: $K = \{(n, p, q, a, b) : n = pq, p, q - prime, ab \equiv 1 (\bmod \phi(n))\}$

إن القيمتين n و b هما قيمتان معلنتان والقيم p, q, a هي قيم سرية.

نحدد من أجل $K = (n, p, q, a, b)$ ما يلي:

$$sig_K(x) = x^a \bmod n \quad \text{و} \quad ver_K(x, y) = true \leftrightarrow x \equiv y^b (\bmod n)$$

حيث: $(x, y \in Z_n)$

الشكل (7): طريقة التوقيع RSA

تُستخدم RSA كطريقة للتوقيع الرقمي بالإضافة إلى كونها نظام تشفير بالمفتاح العام.

من أجل توقيع رسالة ما x يقوم الموقِّع 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 حيث 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 توابع التهشير الوحيدة الاتجاه (One-way Hash Function) مع هذه الطريقة يُبعد هذا النوع من التزوير.

تمر عملية التوقيع وفقا لطريقة RSA بالخطوات التالية:

1- تستخدم برمجية المرسل خوارزمية تهشير (hashing) لإنشاء ملخص الرسالة (message digest) (أو ما يسمى بصمة إصبع fingerprint) [2] و [3].

2- يتم بعد ذلك تشفير ملخص الرسالة والمعلومات الشخصية المتعلقة بالمرسل والطابع الزمني أحياناً (timestamp) باستخدام المفتاح الخاص للمرسل ليتم إنشاء التوقيع DS.

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

وبذلك يكون قد تم التوقيع على الرسالة وتشفيرها وإرسالها إلى وجهتها.

4- 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.

5- يتم فك تشفير DS المستخلص من الرسالة باستخدام المفتاح العام للمرسل مما يكشف عن ملخص الرسالة الأصلية.

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

خوارزمية التهشير الآمنة SHA (Secure Hash Algorithm):

الخوارزمية SHA هي تابع تهشير وحيد الاتجاه (One-Way Hash Function) يطبق على سلسلة محرفية متغيرة الطول تسمى الصورة الأولية (pre-image) ويحولها إلى سلسلة محرفية ذات طول ثابت تسمى بصمة إصبع(fingerprint) أو ما يدعى ملخص الرسالة(Message Digest).

تم تصميم خوارزمية البصمة الآمنة SHA من قبل المعهد القومي للمعايير و التكنولوجيا NIST بالتعاون مع وكالة الأمن القومي NSA بهدف استخدامها في معيار التوقيع الرقمي DSS، وهي تقوم على الخوارزمية MD4 ومشابهة لها في التصميم.

لقد تم نشر هذه الخوارزمية في عام 1993 ولكن النسخ المعدَّلة منها قادت في عام 1995 إلى إصدار الخوارزمية SHA-1 والتي تمثل النسخة المستخدمة في هذه الأيام حيث فرضت الحكومة الأمريكية استخدام الخوارزمية SHA-1 مع DSA.

الخوارزمية SHA-1 :

تقوم الخوارزمية SHA-1 بإنشاء ملخص رسالة (بصمة) بطول 160 بت على خمس مراحل من المعالجة وتُستخدم في الخوارزمية عملية تدعى توسيع أو حشو الرسالة (Message Padding) لتجعل من حجم السلسلة المحرفية المزمع تهشيرها من مضاعفات العدد 512 حيث تُلحق بنهاية الرسالة مجموعة بتات لجعل طولها من مضاعفات 512 بتاً بشكل يماثل البتات الملحقة التي تضاف للخوارزمية MD5 ويكون ذلك ببت واحد قيمته 1 يُضاف إلى نهاية الرسالة تتبعه متتالية أصفار عددها يساوي العدد الضروري لاستكمال عملية الحشو.

ثم يضاف إلى نهاية الناتج 64 بتا تمثل طول الرسالة (قبل الحشو). ثم تُعطى قيم ابتدائية لخمسة متغيرات حيث أن القيم الأربع الأولى هي نفس القيم المستخدمة في MD5 نفسها ويرمز لها A و B و C و D و E وبعدها تبدأ الحلقة الرئيسة للخوارزمية التي تستمر حتى الانتهاء من كتل الرسالة كلها التي يتكون كل منها من 512 بتا.

ثم توضع نسخة من المتغيرات الخمسة في خمسة متغيرات أخرى a , b , c , d , e:

$$A \to a, B \to b, C \to c, D \to d, E \to e$$

تتألف الحلقة الرئيسة من أربع مراحل وتتألف كل مرحلة من 20 خطوة (يوجد في MD5 أربع مراحل يتألف كل منها من 16 خطوة) ويطبق في كل خطوة تابع لا خطي على ثلاثة من المتغيرات a و b و c و d و e ثم تُجرى عمليات إزاحة وجمع مشابهة لتلك التي تُجرى في MD5.

تُعطى التوابع الأربع اللاخطية بالعلاقات المنطقية الآتية:

$$f_t(X,Y,Z) = (X \wedge Y) \vee (\overline{X} \wedge Z), \qquad for\ t = o\ to\ 19.$$
$$f_t(X,Y,Z) = X \oplus Y \oplus Z, \qquad for\ t = 20\ to\ 39.$$
$$f_t(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z), \qquad for\ t = 40\ to\ 59.$$
$$f_t(X,Y,Z) = X \oplus Y \oplus Z, \qquad for\ t = 60\ to\ 79.$$

حيث إنّ الرموز $\oplus$ و $\wedge$ و $\vee$ و– تمثل العمليات المنطقية XOR وAND وOR وNOT على الترتيب.

تُحوَّل كتلة الرسالة من 16 كلمة طول كل منها 32 بتا (M_0 حتى M_{15}) إلى 80 كلمة طول كل منها 32 بتا (W_0 حتى W_{79}) وذلك باستخدام الخوارزمية التالية:

$$W_t = M_t, \qquad for\ t = 0\ to\ 15$$
$$W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< s^1, \qquad for\ t = 16\ to\ 79$$

حيث إنّ: t هي رقم العملية (الخطوة من 0 حتى 79).

W_t هي الكتلة الجزئية رقم t من الرسالة الموسعة.

$<<< s$ إزاحة دورانية إلى اليسار بمقدار s بتا.

بعدئذ تُجمع المتغيرات a و b و c و d و e إلى A و B و C و D و E على الترتيب ثم تتابع الخوارزمية معالجة كتلة المعطيات الآتية ويكون المُخرَج النهائي هو ضم A و B و C و D و E مع بعضها بعضاً بشكل تسلسلي.

النتائج والمناقشة:

إن أمان كل من طريقة توقيع بوس – تشاوم باستخدام تطبيق متباين وطريقة توقيع لامبورت باستخدام تابع وحيد الاتجاه هو أمان مطلق وهما طريقتان لإنشاء تواقيع المرة الواحدة غير أنه بسبب الحجم الكبير للتواقيع الناتجة فهما لا

يمكن أن يكونا ملائمتين للرسائل الطويلة بالإضافة إلى أنهما لا يوفران إمكانية المصادقة وهما ملائمتان للرسائل القصيرة البالغة الأهمية والمعروفة المصدر مسبقاً.

إن الأمان في طريقة توقيع تشاوم – فان انتويربن غير القابلة للإنكار هو دون شروط ذلك أنها لا تعتمد على فرضيات حسابية غير أن التحقق من التوقيع بهذه الطريقة يتم إنجازه بواسطة بروتوكول الطلب والاستجابة Challenge-and-Response Protcol الأمر الذي يحتاج إلى مصافحة handshake قبل البدء بعملية التحقق مما يجعل هذه الطريقة غير مناسبة للتطبيقات التي تقوم على الإرسال مع عدم ارتباط Connectionless Transmission أي أنها مناسبة فقط للتطبيقات التي لا تحتاج إلى اتصال آمن.

إن الأمان في طريقة توقيع فان هيست وبيدرسن المنيع على الإخفاق هو دون شروط أيضاً حيث إنّها لا تعتمد على القوة الحسابية ولا يمكن إحصاء المفاتيح المحتملة q التي يمكن أن يستخدمها الموقِّع كما أن استخدام هذه الطريقة كطريقة توقيع المرة الواحدة يجعل من أمانها أماناً مطلقاً.

يتطلب كل توقيع بطريقة الجمال قيمة جديدة لـ k يتم اختيارها عشوائيا ويمكن كسر الطريقة في حالة معرفة قيمة a التي يسهل حسابها بمعرفة قيمة k أو إذا تم استخدام قيمة k نفسها في توقيع رسالتين حتى من دون معرفة قيمة k.

تعتمد في أمانها كل من طريقة الجمال – طريقة الـ DSS – طريقة توقيع تشاوم – فان أنتويربن غير القابل للإنكار وطريقة توقيع فان هيست وبيدرسون المنيع على الإخفاق على صعوبة حل مسألة اللوغاريتم المقطّع.

إن طريقة الـ DSA لم تكن آمنة باستخدام مقاس طوله 512 بتا أمانا طويل الأجل وأصبحت آمنة باستخدام مقاس طوله 1024 بتاً كما يتطلب كل توقيع بهذه الطريقة قيمة جديدة لـ k يتم اختيارها عشوائياً ويمكن كسر هذه الطريقة في حالة معرفة قيمة a التي يسهل حسابها بمعرفة قيمة k أو إذا تم استخدام قيمة k نفسها في توقيع رسالتين حتى بدون معرفة قيمة k.

إن الحسابات المسبقة تسرع التنفيذ العملي للـ DSA حيث نجد بأن γ لا تعتمد على الرسالة لذا يمكن توليد سلسلة من الأعداد العشوائية لتمثل قيم k ثم تحسب قيم γ الموافقة لها سلفاً كما يمكن حساب قيم k^{-1} الموافقة لتلك القيم وعندما تأتي الرسالة للتوقيع يتم حساب δ باستخدام γ و k^{-1} معينتين.

إن وجود القناة غير المحسوسة في الـ DSA التي اكتشفها Gus Simmons يسمح بإدراج رسالة سرية في التوقيع لا يستطيع قراءتها إلا من يعرف المفتاح الخاص الذي يمكن تسريب جزء منه مع كل توقيع لذا لا بد من توفر الثقة بالموقِّع عند استخدام تطبيقات الـ DSS.

تعتمد طريقة الـ RSA في قوتها على صعوبة تحليل الأعداد الكبيرة جداً إلى عواملها الأولية وإن استخدامها للمفاتيح الطويلة التي تصل إلى 1024 بت و 2048 بت بالإضافة إلى استخدام توابع تهشير وحيدة الاتجاه كجزء لا يتجزأ من هذه الطريقة جعل منها الطريقة الأقوى والأكثر شهرة.

الاستنتاجات والتوصيات:

لقد تم التوصل في هذا البحث إلى الاستنتاجات التالية:

1- لا توجد أية طريقة من الطرائق التي تقوم على مسألة اللوغاريتم المقطَّع بفعالية طريقة RSA التي تقوم على صعوبة تحليل الأعداد الكبيرة جداً إلى عواملها الأولية.

2- إن صعوبة إيجاد اللوغاريتم المقطَّع ليست أقل صعوبة من صعوبة كسر التابع الوحيد الاتجاه في الـ RSA التي تستخدم عدداً أولياً قوياص واحداً P باعتباره مقاساً.

3- عند استخدام خوارزميات المفتاح العام للتوقيع الرقمي (RSA و DSS مثلا) يكون من غير الضروري وجود المحكِّم من أجل التوقيع أو التحقُّق من التوقيع بل توجد حاجة إلى المحكِّم من أجل الشهادة على صحة المفتاح العام حتى إنّ الطرفين لا يحتاجان إلى فض النزاعات التي يمكن أن تنشأ بينهما لأنه بمجرد تعذر التحقُّق من التوقيع يعني أن التوقيع غير صالح.

4- إن وجود التوابع الوحيدة الاتجاه يكافئ وجود الطرائق الآمنة للتوقيع، فإن طرائق التواقيع الرقمية الآمنة يمكن إنشاؤها من أي تابع وحيد الاتجاه.

5- يمكن للقيم العشوائية المستخدمة في بعض طرائق التوقيع أن تكون مخارج لتابع تهشير وحيد الاتجاه.

6- يوجد العديد من خوارزميات التهشير أهمها: MD-5 و SHA-1 اللتان تملكان التصميم نفسه لاشتقاقهما من الخوارزمية نفسها (MD-4) وتختلفان فيما بينها في طول البصمة وعدد مراحل المعالجة (128 بتا للخوارزمية MD-5 على أربع مراحل من المعالجة مقابل 160 بتا للخوارزمية SHA-1 على خمس مراحل من المعالجة) كما تختلفان في أسلوب المعالجة واستخدام المتغيرات و الثوابت الجمعية والمعادلات المنطقية اللاخطية غير أن كلتيهما بسيتطان للفهم والتطبيق ولا تتطلبان برامج ضخمة.

7- تستخدم الخوارزمية SHA-1 البناء الطرفي الكبير (Big-endian Architecture) بينما تستخدم MD-5 طريقة البناء الطرفي الصغير (Little-endian Architecture – الذي يقوم على وضع البايت الأول في المواقع الأقل دلالة عند ترتيب البايتات في الذاكرة) علما أنّ هذه الميزة ليست من المزايا التفضيلية.

8- إن استخدام طريقة التوقيع *RSA* بمقاس طويل يصل حتى 2048 بتا مع خوارزمية التهشير الآمنة *SHA*−1 ذات البصمة 160 بتا يجعل منها الطريقة الأفضل والأكثر قوة.

كما تم بهدف تحسين الأمان اقتراح التوصيات التالية:

1- استخدام توابع قوية وحيدة الاتجاه كجزء لا يتجزأ من الطريقة.

2- استخدام توابع أسية في الطريقة تكون فيها قيمة الأس كبيرة.

3- استخدام الخوارزميات القوية في الطريقة ذات المفاتيح الطويلة (التي قد تصل إلى 2048 بت) بالإضافة إلى عدد كبير نسبيا من دورات المعالجة التي تجريها هذه الخوارزميات وإلى تعقيد حسابي معين للمسائل التي تستند إليها.

المراجع:

1- بروس شناير، د. حاتم النجدي، د. أميمة الدكاك. *التعمية التطبيقية – موافيق وخوارزميات ورماز مصدري باللغة C* ، الطبعة الثانية – الجمعية العلمية السورية للمعلوماتية، سورية، 2006 ، ص 317-237.

2- م. عمار عريان، م. محمد شيخو معمو. *دليلك إلى النجاح في امتحان Security+* ، الطبعة الأولى – شعاع للنشر والعلوم، سورية – حلب، 2004، ص 200-153.

3- طوم توماس، مركز التعريب والبرمجة. *الخطوة الأولى نحو أمان الشبكات*، الطبعة الأولى – الدار العربية للعلوم، لبنان – بيروت، 2004، *ص* 225-224.

4- CHARLES, P. P. , SHARI, L. P. Security in Computing, Third Edition, PH PTR, New Jersey, 2003, PP. 79-89.

5- STALLINGS,W. *Cryptography and Network Security - Principles and Practice* Second Edition, Prentice Hall, New Jersey, 1999, pp.1 – 537.

6-DOUGLAS, R.S. *Cryptography – Theory and Practice* , Second Edition, CRC Press , New Jersey , 2000 , pp. 1- 408.

7-HEYST,E.V. , PEDERSEN,T.P.: *How to make efficient fail-stop signatures* , Eurocrypt "92" Springer-Verlag , Berlin 1993, pp. 366-377.

8-CHAUM,H., ANTWERPEN,H.V. *Undeniable Signature*, Crypto"89" Springer Verlag, Heidelberg 1990, pp. 212-216 .

9-CHAUM,H, ROIJAKKERS,S.: *Unconditionally Secure Digital Signatures* , Crypto"90" Springer-Verlag , Berlin 1991, pp. 206-214 .

10-POINTCHEVAL, D., STERN, J. *Security proofs for signature scheme,* proc. 0f Eurocrypt"96", 1996, pp. 387-398.

11-ROMPEL, J. *One-way functions are necessary and sufficient for secure signature* Proc. of STOC"90", 1990, PP. 387-394 .