الفصل السابع

إجراءات معيارية في أمن المعلومات

1.7 بعض إجراءات أمن المعلومات على الشبكات

تزداد أهمية إجراءات الأمن السايبري للمعلومات على الشبكات الحاسوبية بشكل سريع، فقد قُدِّر حجم هذا السوق بأكثر من 75 بليون دولار عام 2015م، وحجمه عام 2020 بـ 170 بليون دولار[1] وتوجد من أجل كل نوع من أنواع المهددات إجراءات معاكسة لحماية المبادلات الإلكترونية.

1. فللحماية من الدخول أو النفاذ غير المشروع إلى المعلومات المخزونة والاطلاع عليها، تستعمل وسائط مختلفة تمنع هذا الدخول غير المشروع، مثل: كلمات السر Passwords، والبطاقات المغناطيسية الشخصية Magnetic Cards، والبطاقات الذكية Smart Cards، والخصائص البيولوجية للأفراد (بصمات الأصابع، شبكية العين، تعرف الصوت،...).

(1) http://cybersecurityventures.com/cybersecurity_market_report/.

2. أما الدخول إلى الشبكات فيمكن التحكم فيه عن طريق استعمال تجهيزات أو برمجيات منع الدخول غير المشروع إلى الشبكات، ومنها: جدران النار Firewalls، والمرشحات Routing Filters، والمُخدِّم الوكيل أو البروكسي Proxy ، والفصل الفيزيائي للشبكة المحمية عن شبكة الإنترنت.
3. وللحماية من التنصت ومن تحليل الاتصالات، وبهدف تحقيق السرية والخصوصية Confidentiality or Privacy يُستخدم التشفير (التعمية)، حيث تخزن هذه المعلومات في الذواكر وفي الأقراص والأشرطة المغناطيسية بشكل معمى لا يمكن الاطلاع عليه إلا لمن يملك مفتاح التعمية، وعند التراسل بين جهتين باستعمال الشبكات الحاسوبية، تُعمى المعلومات المرسلة أيضًا، وتستعمل أيضًا تقانات الحشو بالأغفالTraffic Padding والتحكم بالتوجيه Routing Control من أجل الحماية من تحليل الاتصالات.
4. أما حماية المعلومات من التغيير أو التعديل بهدف ضمان صحتها Integrity فيتم باستعمال التعمية أيضًا وباستعمال التوقيع الإلكتروني Digital Signature، وسنأتي فيما بعد على شرح لتكنولوجيا التشفير والتوقيع الإلكتروني المستعملة في المبادلات الاقتصادية.
5. والقضية الرابعة المهمة في المبادلات الإلكترونية على الشبكات الحاسوبية هي التحقق من هوية المتراسلين Authentication، منعًا من حدوث تقمص للشخصيات الحقيقية أو الاعتبارية. والتكنولوجيا المستعملة في ذلك هي التوقيع الإلكتروني، ويمكن استعمال بعض التكنولوجيات الخاصة بالتحكم في الدخول إلى النظم، مثل كلمة السر، والبطاقات المغناطيسية أو الذكية، أو عبر تعرف الخصائص البيولوجية التي أتينا على ذكرها فيما سبق.
6. وللحماية من إنكار حدوث الاتصال Non-Repudiation أي أن ينكر المرسل أنه قام بالمبادلة الإلكترونية أو أن ينكر المستقبل أنه تسلّم هذه المبادلة، فتستعمل أيضًا تكنولوجيا التوقيع الإلكتروني، ويستفاد في هذا المجال

مـن طـرف ثالث على الشـبكة يقـوم مقام كاتـب العدل فـي المبـادلات الورقية Notarization، وتوجد الآن كثير من الشركات على الإنترنت تقوم بهذه الوساطة بين الجهات التي تجري مبادلات اقتصادية فيما بينها، وذلك بتوثيق الطرفين وتوثيق مبادلاتهما.

7. أخيـرًا، لا بـد مـن مراقبـة مـا يجـري وتسـجيله ضمـن النظـم المعلوماتية من إجـراءات واتصـالات بهـدف العودة لهذا السـجل عنـد حدوث أي طـارئ أو أي خرق أمني للنظام Auditing، ويتم ذلك عادة عبر برمجيات خاصة تقوم بشكل آلـي بعمليـات، مثل سـجلات المراقبـة Audit Trails، ومتابعة الحـوادث الأمنية Security Events Tracking.

ويلخص الجدول الآتي آليات تأمين الخدمات الأمنية المطلوبة للتبادلات الإلكترونية للمعلومات:

جدول آليات توفير الخدمات الأمنية المطلوبة لحماية الاتصالات الحاسوبية

	Mechanisms الآليات							
	Encryption تعمية	Digital Signature التوقيع الإلكتروني	Access Control التحكم بالنفاذ	Data Integrity صحة البيانات وتكاملها	Authenti_cation التحقق من الهوية	Traffic Padding رصد انسياب المعلومات	Routing Control التحكم في مسار المعلومات	Notarization التسجيل الرسمي
Confidentiality السرية	√	*	*	*	*	√	√	*
Integrity الصحة والتكامل		√	*	√	*	*	*	*
Authentication صحة الهوية	√	√	*	*	√	*	*	*
Access Control التحكم في النفاذ	*	*	√	*	*	*	*	*
Non_repudiation عدم نكران التعامل	*	√		√	*	*	*	√

2.7 أنظمة الحماية المعيارية

إن الهدف المبتغى من مختلف الأجهزة والبرامج المعلوماتية، كالمخدم الوكيل proxy servers وجدران النار Firewalls، على سبيل الذكر لا الحصر، هو إيقاف الفيروسات المعلوماتية، وتثبيط عزيمة المخربين والقراصنة، وتقليص النفاذ للمواقع غير المرغوب فيها، ولهذا الغرض هناك إجراءات أساسية عدة متمثلة في إدراج كلمة السر المعماة (Encrypted Password) على مستويات مختلفة، واستعمال الشهادات المصادق عليها (Certificates) والإمضاء أو التوقيع الرقمي أو الإلكتروني (Digital signature) أو تثبيت مضاد فيروس (Antivirus).

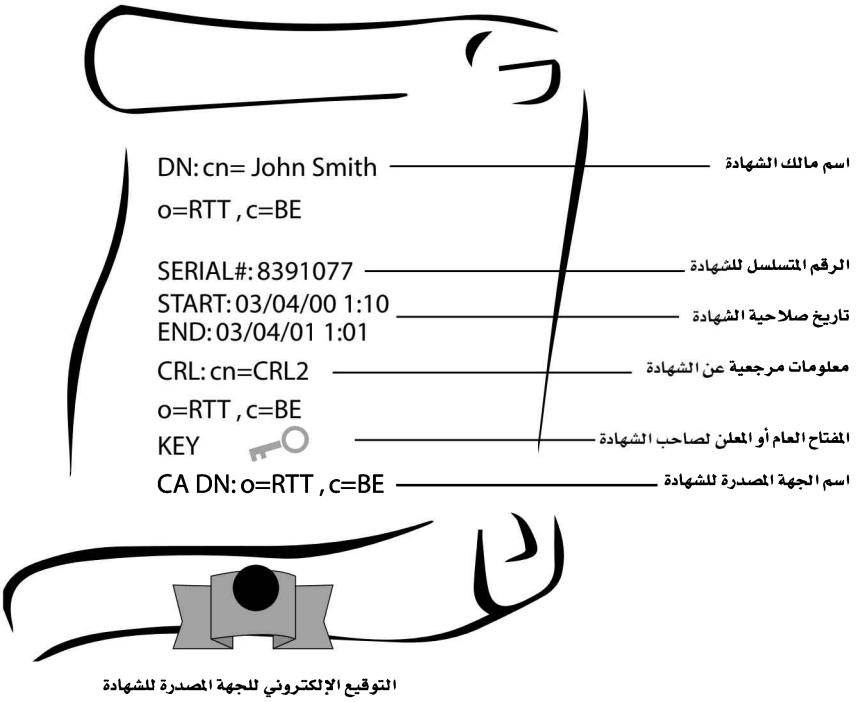
3.7 إجراءات التعمية أهم آليات الحماية.

تستخدم التعمية في إجراءات عدة في أمن المعلومات، بل في معظم هذه الإجراءات، ومن هذه الإجراءات ما ذكرنا سابقًا من آليات السرية، والحفاظ على صحة المعلومات وتكاملها، وإثبات هوية المتراسلين، وستبيّن الفقرات الآتية أهمية التعمية في إجراءات أمن المعلومات وأمانها بشكل مبسط:

4.7 إجراء استعمال الشهادات المعتمدة.

إن التحقق من الهوية داخل شبكة الإنترنت أمر في غاية التعقيد؛ ذلك أن الأطراف المتصلة لا يمكنها أن تلتقي ماديًّا كما هو الحال في أثناء المقابلة المادية، وهذا ما يمكّن الكثير من الأشخاص من استراق الرسالة أو القيام بتشخيص نفسه على شخص أو كيان آخر؛ أي انتحال شخصية غير شخصيته.

الشهادة الرقمية CA



إن شهادة الاعتماد، سواء للأشخاص أو لمواقع الإنترنت، يجب أن تشترك في الهوية بواسطة (**المفتاح العام**) ولا يَعرِفُ (**المفتاحَ الخاص**) الموافق إلا من يملك شهادة الاعتماد، ويسمح (**المفتاح الخاص**) للمالك باستعمال (**الإمضاء الرقمي**) أو فك شفرة المعلومات المشفرة باستعمال (**المفتاح العام**) الموافق، فعندما ترسل شهادة الاعتماد الشخصية لأشخاص آخرين، فإنك تمنح لهم المفتاح العام الشخصي، ومن ثم يمكن لهم أن يرسلوا لك المعلومة المعماة التي لا يمكن لأحد سواك أن يفك تعميتها أو قراءتها، وذلك باستعمال مفتاحك الخاص.

5.7 إجراء التحقق من هوية المخدم

تمنع عملية التحقق من هوية المخدم انتحال الشخصية، حيث يطلب الزبون الشهادة الرقمية للمخدم، فعند إرسال المخدم لشهادته الرقمية يسأل الزبون نفسه الأسئلة الآتية التي يجب أن يكون جواب كل منها (نعم) حتى يتم نجاح التحقق من هوية المخدم، السؤال الرابع من الأسئلة الآتية ليس جزءًا من تقنية الـ SSL وإنما أضيف لمنع نوع من الاختراق للأمن يدعى (رجل في الوسطMan in The Middle) وهذه الأسئلة هي:

عملية إقامة اتصال آمن باستعمال المنتج SSL/TLS

- **هل تاريخ اليوم ضمن مدة صلاحية الشهادة؟**

في حال كان الجواب لا، تُنهى عملية التحقق عند هذا الحد وإعادة رسالة خطأ.

- **هل مصدر الشهادة الرقمية هو CA موثوق أي مصدر شهادات موثوق بالنسبة إلى الزبون؟**

يملك كل زبون SSL قائمة لمصدري الشهادات الموثوقين بالنسبة إليه، تحتوي هذه القائمة على حقل (Distinguished Name (DN يحوي الاسم المميز لمصدر الشهادة، يفحص هذا الشرط بالبحث عن مصدر شهادات موثوق في القائمة المخزنة لدى الزبون يتطابق حقل DN لديه مع حقل DN الموجود في الشهادة، في حال تجاوز هذا الشرط ينتقل إلى السؤال الثالث.

- **هل المفتاح العام العائد لمصدر الشهادة يفك تشفير التوقيع الرقمي، وهل المعلومات المرسلة في الشهادة تتناقض مع التوقيع؟**

للتحقق من التوقيع الرقمي يقوم الزبون بالخطوات الآتية:

1. يفك الزبون شيفرة التوقيع الرقمي للجهة المصدرة CA بواسطة المفتاح العام الذي من المفترض وجوده في قائمة مصدري الشهادات الموثوقين.
2. يطبق الزبون تابع الاتجاه الواحد المستخدم من قِبل الـ CA المصدرة للشهادة على البيانات المرسلة من المخدم، ويتم بعد ذلك المطابقة بين التوقيع الرقمي المرسل مع الشهادة وقيمة التابع الناتجة :

- نستنتج في حال التطابق أن المعلومات المرسلة في الشهادة صحيحة، ويُنتقَل إلى السؤال الرابع.
- ينتج عدم التطابق إما بسبب تغيير في الشهادة، أو أن المفتاح العام المستخدم في فك التشفير لا يتوافق مع المفتاح الخاص المستخدم في تشفير المعلومات، وفي هذه الحالة تُرفَض الشهادة.

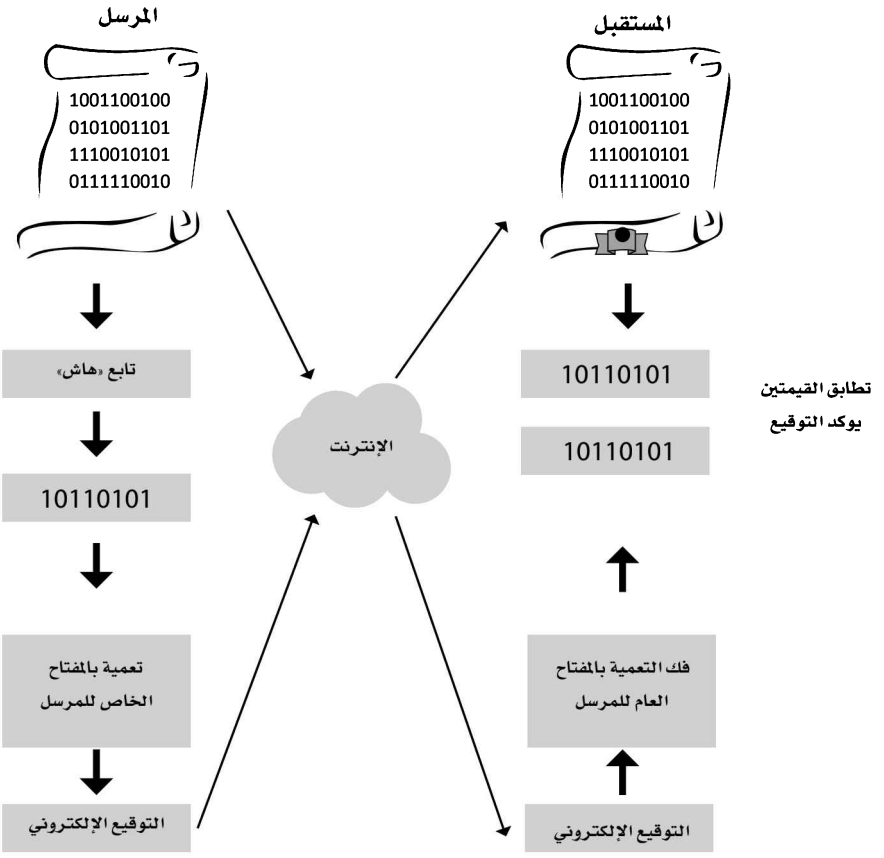
- **هل اسم النطاق في الشهادة الرقمية يطابق اسم نطاق المخدم؟**

ذكرنا سابقًا أن هذا السؤال ليس من تقنية SSL وإنما أضيف لمنع نوع من الاختراق يدعى (رجل في الوسط Man in The Middle)، حيث يتحقق الزبون من أن اسم النطاق المسجل في الشهادة الرقمية يطابق اسم النطاق الذي يتصل معه حاليًّا، وهو الحل الوحيد المطروح لمنع هذا النوع من الاختراق.

6.7 إجراء الإمضاء الرقمي أو التوقيع الإلكتروني

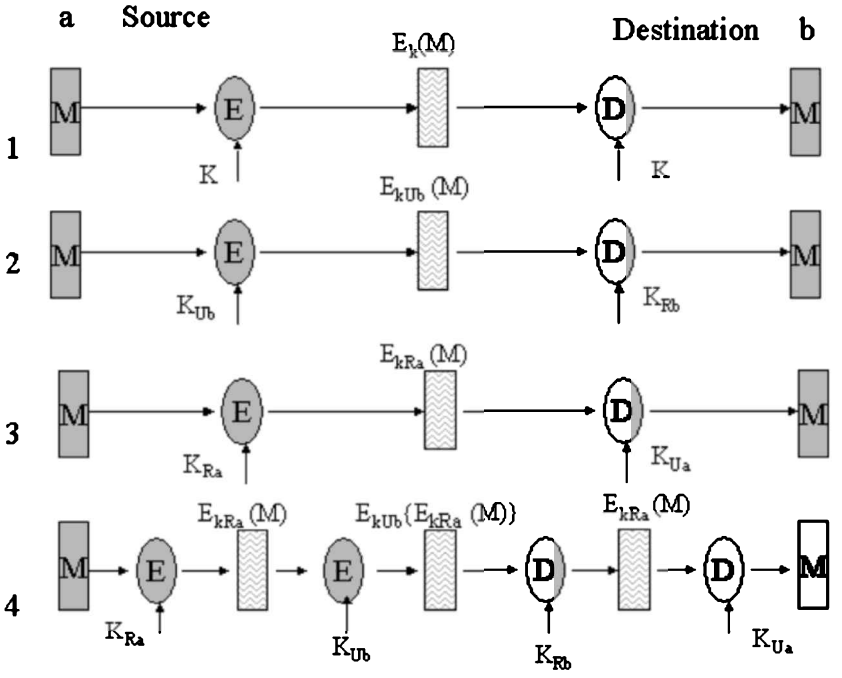
تحتوي الرسائل المرسلة عبر شبكات الاتصال أحيانًا على أوامر خاصة ومهمة، مثل طلب صرف مستحقات مالية من المصارف، وفي هذه الحالة يجب إثبات صحة الرسالة المستقبلة والوثوق بها، وطريقة التوثيق في حالة تسلم الرسائل باليد هي إمضاء المُرْسِل على الوثيقة، أما في حالة الانتقال عبر شبكات الاتصالات، فإن التوثيق في هذه الحالة يتم بالإمضاء الرقمي digital signature، وهو عبارة عن رسالة معماة بالمفتاح المعلن تستعمل من أجل التوقيع الإلكتروني طريقة التشفير بالمفتاح المعلن، ويقوم المرسل ولنسمِّه (سامر) باختصار الرسالة مستعملًا تابع اختصار أو (بصمة) وهو تابع رياضياتي محدد Hash Function، ثم يشفر المختصر الناتج مستعملًا مفتاحه الخاص السري، وبعدها يرسل الرسالة الأصلية مع تشفير مختصرها إلى المستقبل ولنسمِّه (سليم)، ويقوم المستقبل (سليم) بإجراء عملية اختصار الرسالة نفسها مستعملًا تابع الاختصار نفسه، ويقارن النتيجة مع ناتج فك تشفير المختصر المرسل له الذي حصل عليه باستعمال المفتاح المعلن للمرسل (سامر)، فإذا كانت نتيجة المقارنة التطابق يكون هذا إثباتًا على أن الرسالة مرسلة من (سامر)، وأنه لم يُجرِ عليها أي تعديل.

إرسال وثيقة موقعة توقيعًا اللكترونيًا



هناك أربعة ترتيبات أساسية تستخدم فيها طريقتا التشفير المتناظرة وغير المتناظرة لتأدية الوظائف الأمنية المطلوبة للتبادلات الإلكترونية، ولتحقيق الاتصال بين المرسل a والمستقبل b وهي المذكورة أدناه، والمبينة في الشكل الآتي:

1. الطريقة التقليدية التي تشفر فيها على سبيل المثال النصوص المخزونة أو الرسائل المتبادلة على الشبكات.
2. طريقة التشفير بالمفتاح المعلن التي تستعمل لتبادل معلومات قصيرة مشفرة، كالمفاتيح السرية.



3. طريقة التشفير بالمفتاح المعلن في حالة التوقيع الإلكتروني لتحديد هوية المرسل.
4. طريقة التشفير بالمفتاح المعلن في حالة سرية المعلومات (أي تشفيرها) + توقيع إلكتروني + هوية المرسل.

ومما لا شك فيه، يمكن دمج الطريقة 1 مع أيٍّ من الطرق الثلاث الأخر 2 و3 و4.

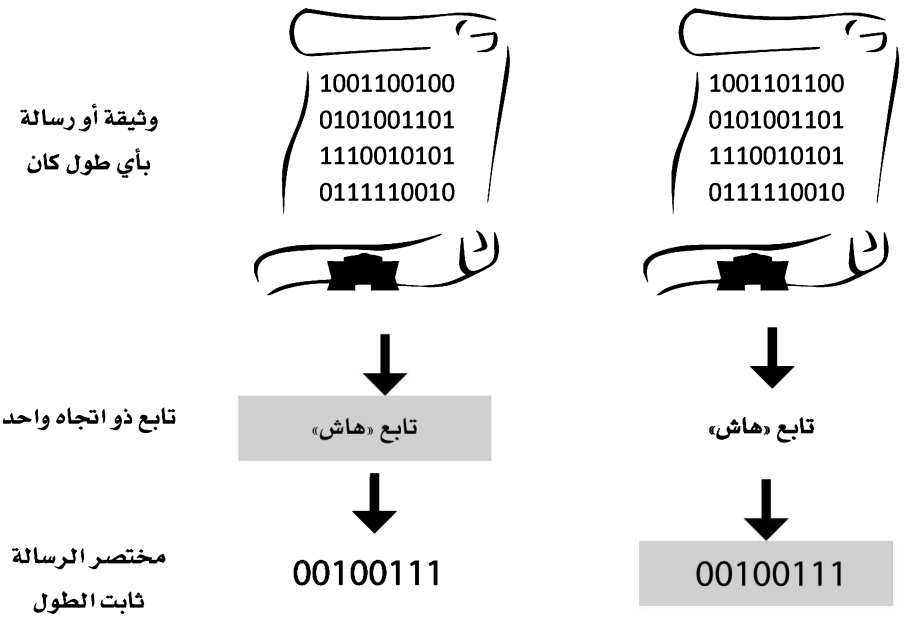
والأشكال السابقة تشرح الطريقة المستعملة لإجراء التوقيع الإلكتروني، حيث ينطلق المرسل (سامر) من نص الرسالة الواضح، ويستخرج ملخصًا لهdigest ، ثم يُشفِّر هذا الملخص باستعمال مفتاحه السري، وبعد ذلك يرسل الرسالة الواضحة وناتج تشفير ملخصها إلى (سليم)، ويفكّ (سليم) تشفير ملخص الرسالة باستعمال مفتاح

(سامر) المعلن، ويقوم بحساب ملخص الرسالة، ويقارن نتيجة الحسابين، فإذا تطابقتا يكون (سامر) هو مرسل الرسالة، وتكون الرسالة غير معدلة.

7.7 توابع البصمة (هاش)

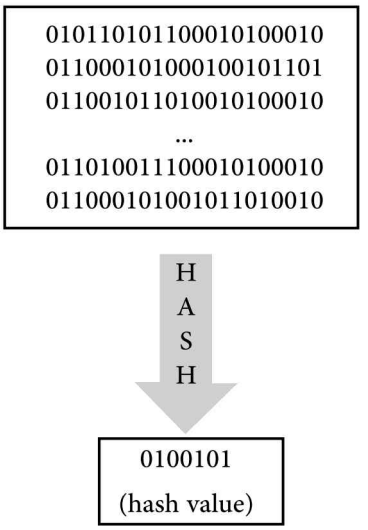
مثلما تُؤمِّن التعمية المتماثلة أو المتناظرة والتعمية غير المتماثلة (أي التعمية بالمفتاح السرِّي والتعمية بالمفتاح العلني) خدمة السرِّية Confidentiality، تؤمِّن توابع البصمة بنوعيها خدمتَي سلامة البيانات Data Integrity واستيقان الرسالة Message Authentication (أو استيقان منشأ البيانات Data Origin Authentication).

تابع «هاش» المستعمل لفحص عدم حصول تغير في الرسالة



إن تغيرت خانة «بت» واحد في الوثيقة يغير مختزلها أو بصمتها كليًا

يأخُذ **تابع البصمة** Hash Function (ويُدعَى أيضًا **تابع الضغط** Compression Function و**تابع التقليص** Contraction Function)[1] كدخل إمّا وسيطًا واحدًا (رسالة طولها يساوي m بت) أو وسيطين (رسالة طولها يساوي m بت ومفتاح سري طوله يساوي k بت)، ويعطي كخرج قيمة طولها يساوي n بت، حيث n < m، تُدعَى **ترميز البصمة** Hash Code أو **نتيجة البصمة** Hash Result أو **قيمة البصمة** Hash Value أو **الدمغة** Imprint أو **البصمة الرقمية** Digital Fingerprint أو **خلاصة الرسالة** Message Digest أو ببساطة **بصمة** Hash.



أبسَط مثال على تابع البصمة هو تابع يقوم بالجمع الاثناني لبايتات سلسلة دخل (ولتكن رسالة) وتحويلها إلى بايت واحد طوله يساوي 8 بتات (وهو قيمة البصمة)، ويمكننا تمثيل هذا المثال وفق الإجراء الرياضي الآتي:

$$Message = X_1 || X_2 || X_3 || \ldots || X_{t-1} || X_t$$

(1) في الحقيقة، إنَّ تابع الضغط (أو كما يُسمَّى تابع التقليص) هو الجزء الأساسي والمكوِّن لتابع البصمة، وليس هو تابع البصمة نفسه، ولكن سُمِّي تابع البصمة بهذين الاسمين انطلاقًا من المبدأ العام لعمل تابع البصمة الذي يقوم بعملية الضغط، وهي تحويل سلسلة كبيرة ومتغيِّرة إلى سلسلة صغيرة وثابتة.

HashValue = 0

For i = 1 to t

HashValue = HashValue $\oplus X_i$

Next i

حيث Message: رسالة طولها يساوي t بايت، وX_1، X_2، X_3، ...، X_t: البايتات التي تُشكِّل الرسالة، وHashValue: كلمة غير مؤشَّرة طولها يساوي 8 بتات، وهي قيمة البصمة المطلوبة، و⊕: عملية الجمع الاثناني.

نمطَا توابع البصمة.

في البداية تنقسم توابع البصمة إلى نوعين رئيسين، هما: **توابع البصمة غير المزوَّدة بمفتاح** Unkeyed Hash Functions و**توابع البصمة المزوَّدة بمفتاح** Keyed Hash Functions. تأخذ توابع البصمة غير المزوَّدة بمفتاح دخلًا واحدًا فقط هو الرسالة، بينما تأخذ توابع البصمة المزوَّدة بمفتاح دخلين، هما: الرسالة والمفتاح السرِّي.

يَتميَّز تابع البصمة H (بنوعيه غير المزوَّد بمفتاح والمزوَّد بمفتاح) بخاصتين أساسيتين:

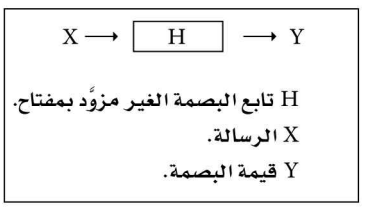
1. **الضغط** Compression: يقوم تابع البصمة H بضغط سلسلة بتية x ذات طول متغيِّر ومنتهٍ طولها يساوي m بت إلى سلسلة بتية y صغيرة وثابتة طولها يساوي n بت، حيث $n < m$.
2. **سهولة البصم** Ease of Computation: في حال H غير مزوَّد بمفتاح، وبتوافر تابع البصمة H وسلسلة بتية x، من السهولة حساب البصمة $H(x)$. وفي حال H مزوَّد بمفتاح، وبتوافر تابع البصمة H وسلسلة بتية x ومفتاح سري k، من السهولة حساب البصمة $Hk(x)$.

ثمة نمطان رئيسان من توابع البصمة: النمط الأول هو **ترميز اكتشاف التعديل** Modification Detection Code ، واختصارًا MDC (ويُعرَف هذا النمط أيضًا **بترميز اكتشاف التلاعب** Manipulation Detection Code ، **وترميز سلامة الرسالة** Message Integrity Code ، واختصارًا MIC). والنمط الثاني هو **ترميز استيقان الرسالة** Message Authentication Code، واختصارًا MAC (ويُعرَف هذا النمط أيضًا **بترميز استيقان البيانات** Data Authentication Code، واختصارًا (DAC)، وسوف نتحدَّث عن كل نمط من هذين النمطين بالتفصيل[1].

ترميز اكتشاف التعديل MDC.

الـ MDCs هي توابع بصمة غير مزوَّدة بمفتاح، ويستطيع نمط الـ MDC تأمين خدمة سلامة البيانات data integrity فقط، ويأخذ هذا النمط دخلًا واحدًا فقط هو الرسالة، وتُسمَّى **الصورة الأمامية** Preimage، ويُعيد كخرج قيمة هي قيمة البصمة. انظر الشكل (5-1)، وانطلاقًا من ذلك، يمكننا تمثيل تابع البصمة غير المزوَّد بمفتاح H على النحو الآتي:

$$H: M \rightarrow R$$



حيث M: فضاء الرسالة، وهو المجموعة التي تضم قيَم الدخل (قيمة الدخل هي أي رسالة طولها يساوي m بت)، وR: فضاء البصمة، وهو المجموعة التي تضم قيَم الخرج

(1) يمكن أن يأتي المصطلح MDC (ومرادفاته) بمعنى (تابع حساب ترميز اكتشاف التعديل) و(ترميز اكتشاف التعديل) في الوقت نفسه. كذلك، يمكن أن يأتي المصطلح MAC (ومرادفاته أيضًا) بمعنى (تابع حساب ترميز استيقان الرسالة) و(ترميز استيقان الرسالة)، ويتم تمييز ذلك بحسب سياق النص.

(قيمة الخرج هي أي قيمة بصمة طولها يساوي n بت)، و n < m. يُلاحَظ هنا أنَّ طول قيمة الدخل الذي يساوي m بت كبير ومتغيِّر، ولكنه منتهٍ، أمّا طول قيمة الخرج الذي يساوي n بت فهو صغير وثابت لجميع قيَم الدخل.

الشكل: تابع البصمة غير المزوَّد بمفتاح (MDC).

يُقسّم نمط الـ MDC إلى نوعين:

8.7 بعض المنتجات التقليدية المتوافرة للتبادل الآمن للمعلومات على الشبكات

توجد حاليًّا منتجات ومعايير عدة لتوفير الوظائف اللازمة لضمان أمن الاتصالات على الإنترنت، ومنها أمن المبادلات الإلكترونية والتجارة الإلكترونية.

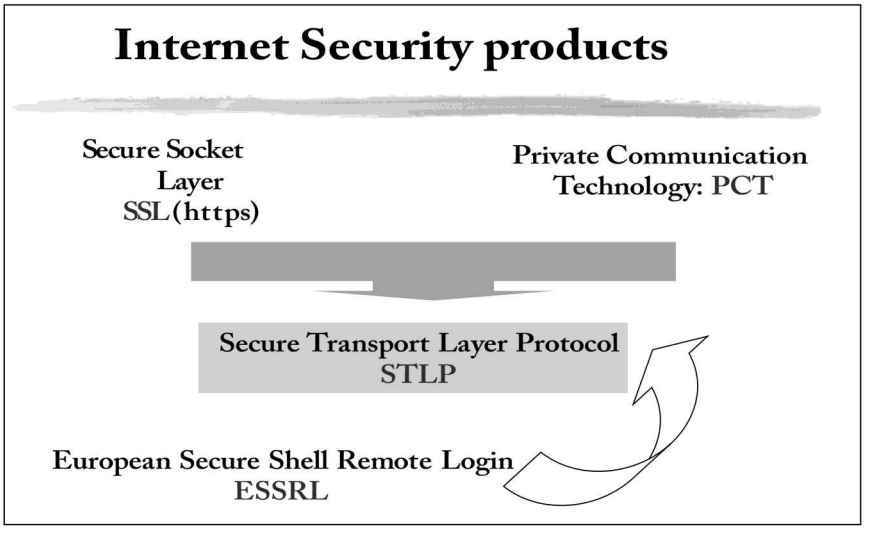
تُصمّم هذه المنتجات من جمع خوارزميات عدة في منتج واحد، فمثلًا المنتج:

Pretty Good Privacy (PGP)

يتألف من جمعٍ لخوارزمية التشفير المتناظرة IDEA مع خوارزمية المفتاح المعلن RSA إضافة لخوارزمية تابع الاختصار (أو البصمة أو هاش) The MD5 Hash function ، ويبين الشكل المرفق بعض هذه المنتجات والخوارزميات الداخلة في تصميمها.

وتتوافر على الإنترنت بعض المعايير الأمنية المتداولة، مثلSecure Socket Layer (https SSL) ومثل Private Communication Technology PCT ، علمًا أنه يجري أخيرًا دمج هذين المعيارين مع المعيار الأوروبيEuropean Secure Shell Remote Login ESSRL في معيار واحد هو Secure Transport Layer Protocol STLP كما هو مبين في الشكل الآتي:

مثال يبيّن بعض منتجات أمن التواصل عبر الإنترنت


Internet Security products
Secure Socket Layer SSL(https)
Private Communication Technology: PCT
Secure Transport Layer Protocol STLP
European Secure Shell Remote Login ESSRL