أمن الحاسبات والمعلومات
الفصل الرابع: التوقيع الرقمي والشهادات الرقمية

إعداد الدكتور / أسامة حسام الدين

كلية علوم وهندسة الحاسبات بينبع
جامعة طيبة

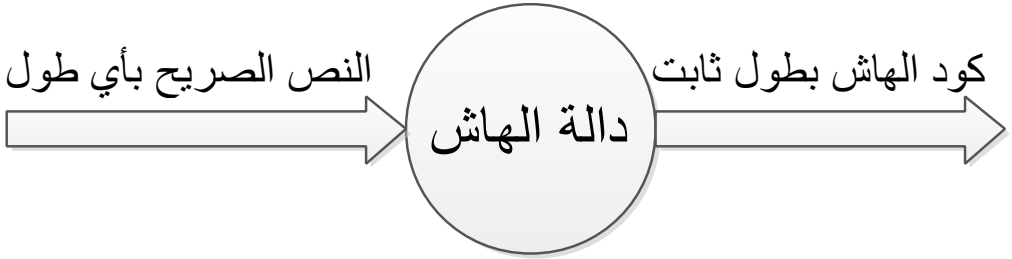
محتوى الفصل الربع

- نقدم في هذا الفصل طرق عمل التوقيع الرقمي والشهادات الرقمية

1. الهاش
2. دوال الهاش
3. التوقيع الرقمي
4. الشهادات الرقمية

ما هو الهاش

- **الهاش** هي أداة لتحقيق تماسك البيانات بأخذ البيانات الثنائية (الرسالة) ثم إنتاج قيمة للرسالة بطول ثابت،
- هذه القيمة تسمى (**الهاش كود**) أو ملخص الرسالة.
- إذا تم تطبيق الهاش على كلمة المرور **بدالة هاش** معينة أكثر من مرة فإن الناتج دائما يكون نفس ملخص الرسالة.
- ودوال الهاش لها اتجاه واحد لسببين، **الأول** أنه لا يمكن استرجاع النص الصريح من قيمة الهاش. **والثاني** أنه من المستحيل أن تكون قيمة الهاش هي نفسها لمجموعتين مختلفتين من البيانات.



خصائص الهاش

طحن القهوة هو مثال جيد لدوال الاتجاه الواحد. حيث أنه من السهل طحن بذور القهوة إلى قطع صغيرة، ولكن من المستحيل وضع كل هذه القطع الصغيرة بجوار بعضها لاسترجاع البذور الأصلية

ولدوال تشفير الهاش الخواص التالية

- يمكن أن تكون المدخلات بأي طول
- المخرجات لها طول ثابت **(خاصية التشتيت)**
- لها اتجاه واحد ليس لها اتجاه عكسي
- للمدخلات المختلفة تكون دائما قيمة الهاش مختلفة تماما حتى لو الاختلاف طفيف. **(خاصية الانتشار)**

دوال الهاش البسيطة – باقي القسمة mod

دال الهاش mod تم تسميتها h للتبسيط تقوم بتحويل الأرقام الطويلة مثل الرقم الجامعي للطالب أو أي رقم آخر (طويل او قصير) إلى هاش كود ثابت في مدى الرقم m. يتم كتابة دالة الهاش بالشكل التالي

$$h(k) = k \bmod m$$

حيث ان k هو الرقم الجامعي للطالب . و m يعبر عن الطول الثابت المطلوب في دالة الهاش. ودالة mod هي دالة باقي القسمة. لحساب كود الهاش يتم فقط حساب باقي القسمة .

يجب أن تكون دالة الهاش (فوقية Onto) بمعنى انه لا يوجد رقمان جامعيان ينتجان نفس الهاش الكود . وحدوث ذلك يعني وجود تصادم collision

دوال الهاش البسيطة – باقي القسمة mod

مثال 1: أوجد الهاش كود للأرقام الجامعية التالية 064212848 و 037149212. بحيث يكون كود الهاش في المدى 111. مستخدما دالة الهاش الخاصة بباقي القسمة

الحل: نستخدم الدالة الخاصة بباقي القسمة التالية

$h(k) = k \bmod m$

$h(064212848) = 064212848 \bmod 111 = 14.$

$h(037149212) = 037149212 \bmod 111 = 65,$

الهاش كود للرقم 064212848 هو 14

والهاش كود للرقم 037149212 هو 65

دوال الهاش البسيطة – باقي القسمة mod

مثال 2: أوجد الهاش كود للأرقام الجامعية التالية 064212848 و 107405723. بحيث يكون كود الهاش في المدى 111.

الحل: نستخدم الدالة الخاصة بباقي القسمة التالية

$h(064212848) = 064212848 \bmod 111 = 14.$

$h(107405723) = 107405723 \bmod 111 = 14,$

الهاش كود للرقم 064212848 هو 14

والهاش كود للرقم 107405723 هو 14 أيضا. (**تصادم !!**) والحل للتصادم هو البحث عن كود الهاش التالي والذي لم يتم تعيينه. في هذه الحالة الرقم 15 لم يتم تعيينه فيكون هو الحل. لكن 16 لا يصلح إذ تم تعيينه من قبل (انظر المثال 1)

دوال الهاش المتقدمة

خوارزمية مد5 MD5 : قام رون ريفست بابتكار خوارزمية مد5 بالإضافة إلى العديد من تطبيقات الإنترنت المستخدمة في هذه الأيام. تنتج خوارزمية مد5 كود هاش بطول 128 بت.

خوارزمية شا SHA : قام المعهد الوطني للمعايير والتكنولوجيا، نست (NIST) ببناء خوارزمية شا. وتم تضمين الخوارزمية ضمن معيار الهاش السري (SHS). قامت نست بنشر خوارزمية شا1 سنة 1994. ثم استبدلت شا1 بشا2 مع أربعة دوال هاش إضافية ضمن عائلة شا والدوال هي ، شا 224 (224 بت) و شا 256 (256 بت) و شا 384 (384 بت) و شا 512 (512 بت)

يوجد أيضا خوارزمية HMAC **اتشماك** وتختلف اتشماك عن مد5 وشا في أن البيانات في اتشماك يتم عمل هاش لها مع توقيعها من المرسل.

خواص دوال الهاش

- **خاصية الانتشار :**تعني انقطاع العلاقة بين شكل البيانات وشكل الهاش، فتغيير بسيط في البيانات يعطي هاش كود مختلف تماما.
- **خاصية التشتيت** :تعني انقطاع العلاقة بين طول البيانات وطول الهاش . فكلمة من أربعة أحرف فقط تعطي هاش بطول 32حرف وملف 10جيجا أيضا يعطي هاش بطول 32حرف .

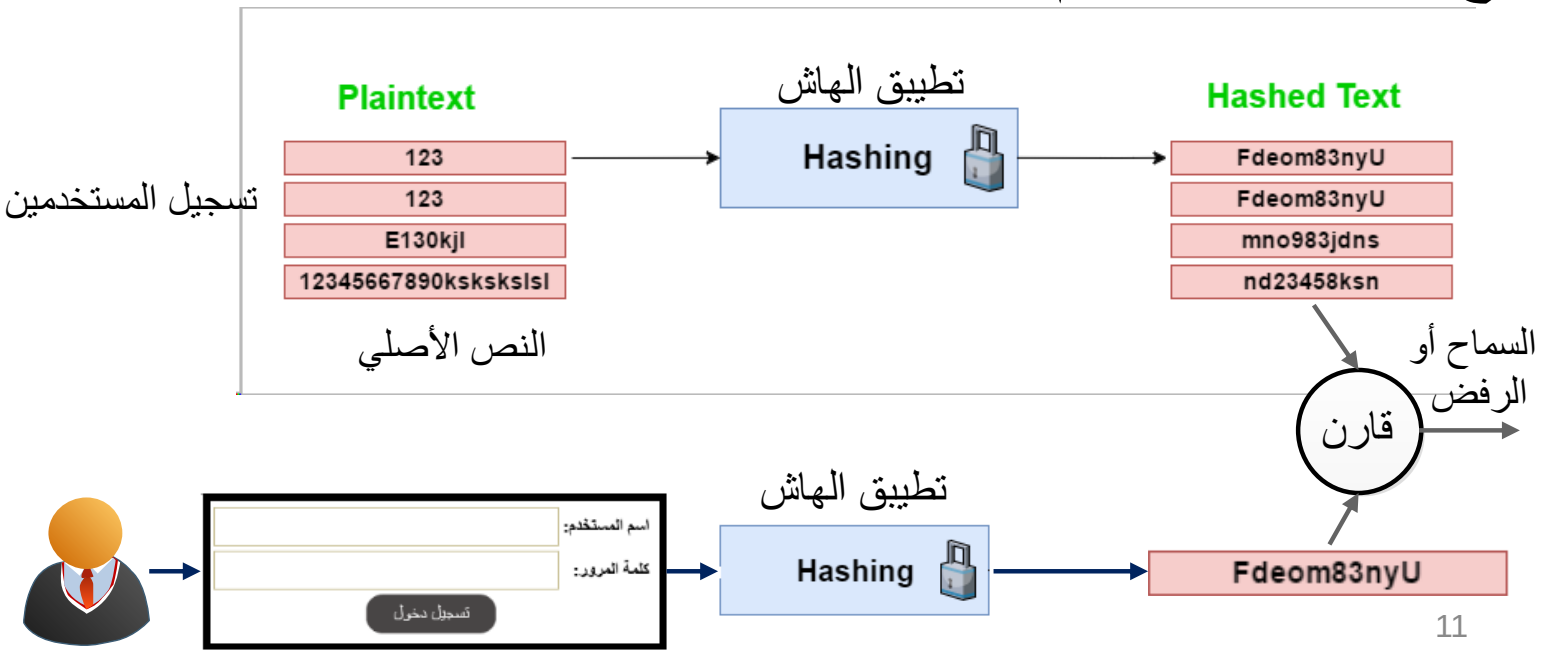
Ahmed	f1e43d880f09c64ac6378af6de47702
Ahmad	44bc2be4245c022748235a46dedf15
ملف كامل 100ميجا	c248c6b98c56ff0362bc4013eb33c8f

تمرين عملي – دول الهاش لفحص التماسك

- قم بتنزيل برنامج HashCalc
- قم بحساب الهاش لنصوص طويلة وقصيرة
- قم بحساب الهاش لملف (وورد) وقم بالتعديل فيه ثم قم بحساب الهاش مرة أخرى. (لاحظ الفرق)
- قم باستخدام الهاش في فحص تماسك البرنامج Snort
- يمكن استخدام أدوات مساعدة اونلاين:
  https://www.fileformat.info/tool/md5sum.htm
- أكد على وجود خاصيتي التشتيت والانتشار.

تطبيقات الهاش – استخدام الهاش بدلا من كلمة المرور

- عند تسجيل المستخدم في النظام لا يتم حفظ كلمة السر الخاصة به ولكن تحفظ الهاش الخاص بكلمة السر. وعند ولوج المستخدم ، يأخذ النظام كلمة السر المدخلة ويقوم بأجراء هاش عليها ثم يقارنها بالهاشات المخزنة ، وان وجد تطابق، يدخل المستخدم للنظام، والا لن يسمح بدخول المستخدم.



الهجوم على كلمات المرور

لكسر الهاش الخاص بكلمات المرور يجب على المهاجم أن يخمن كلمة المرور. وأشهر هجومين لتخمين كلمات المرور هما هجمة القاموس والبحث الغاشم.

- **هجمة القاموس** وأحيانا تسمى هجمة جدول قوس قزح rainbow table تتم باستخدام ملف يحتوى على الكلمات الشائعة والعبارات وكلمات المرور. ويحتوى الملف على قيم محسوبة للهاش. وتتم الهجمة بمقارنة قيم الهاش الموجودة في الملف مع قيمة الهاش الخاص بكلمة السر. فإذا وجد تطابق، سيقوم المهاجم بمعرفة مجموعة من كلمات السر المتوقعة والجيدة. https://crackstation.net
- أما **هجمة البحث الغاشم** فتتم بمحاولة كل التباديل الممكنة لعدد معين من الحروف، مناظر لعدد حروف كلمة السر المطلوبة. على سبيل المثال لو علمنا أن رقم المرور مكون من أربعة أرقام، لذا يمكن تجربة 9999 تبديلة للأرقام حتى نصل إلى الرقم السري.

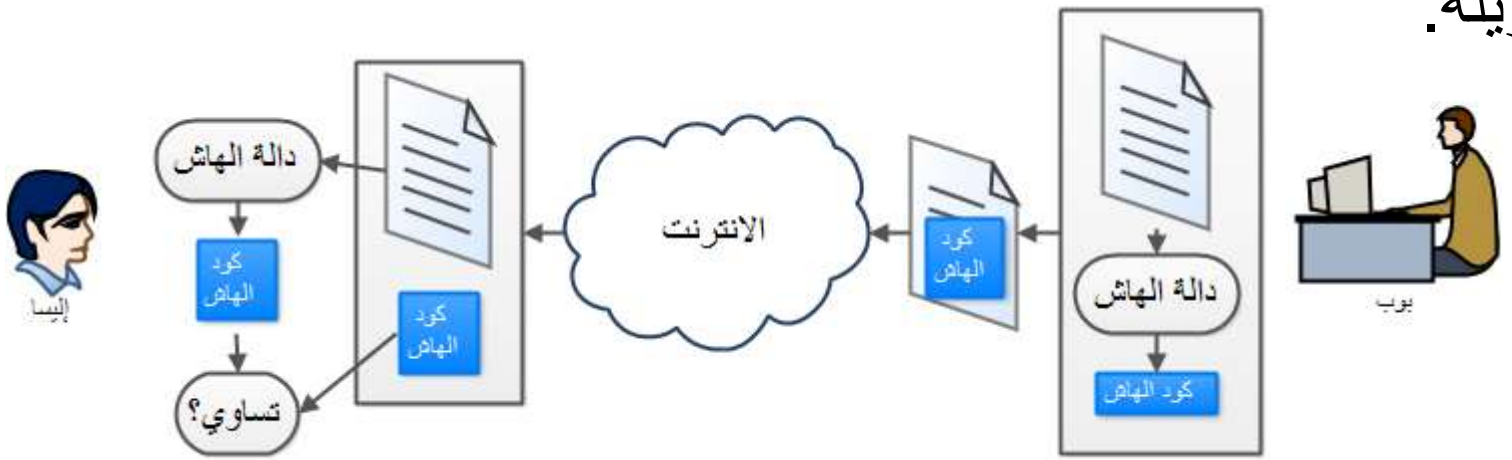
صد الهجوم على كلمات المرور

يجب أن تكون كلمات السر طويلة بما فيه الكفاية لإطالة الوقت الذي تمكثه عملية التخمين الغاشم حتى يكون الهجوم غير مجدي. يتم ذلك عن طريق استخدام طريقة **التمليح** salting.

كلما زاد الملح كلما صعب الأكل. أما هنا فيعني جعل عملية الهاش لكلمات السر أكثر سرية. فكلما زاد طول قيمة الملح كلما صعب على المهاجم تخمين كلمات المرور.

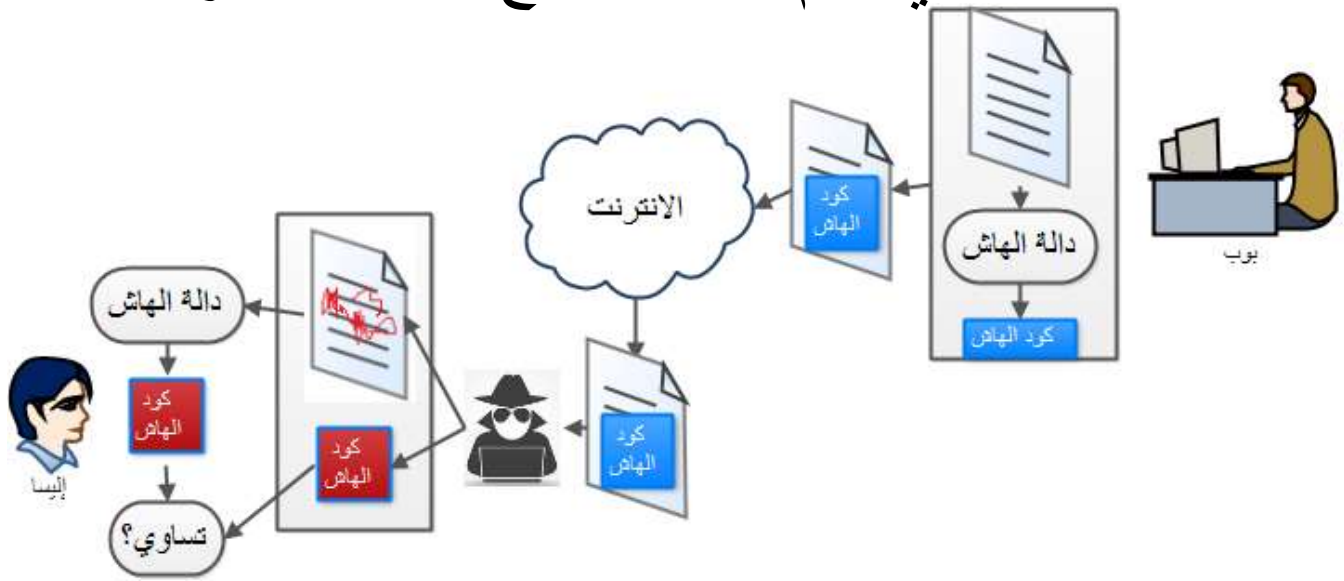
تطبيقات الهاش: التأكد من سلامة البيانات المرسلة

- عند إرسال بيانات من طرف إلى طرف، يتم إرسال كود الهاش الخاص بالبيانات أيضا، ثم يقوم المستقبل بفحص التماسك باستخدام كود الهاش.
- تقوم معظم شركات انتاج البرامج بوضع كود الهاش الخاص ببرامجها. يستطيع المستخدم التأكد من سلامة البرنامج عند الرغبة في تنزيله.



الهجوم على البيانات المرسلة

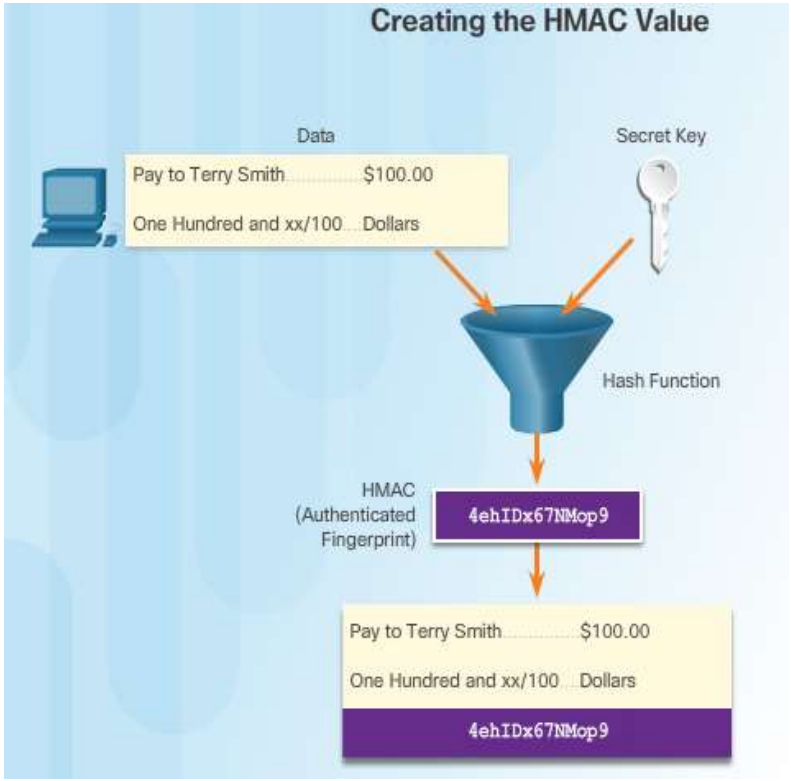
- عند إرسال بيانات من طرف إلى طرف، يقوم المهاجم بقطع الطريق بين المرسل والمستقبل.
- ومع معرفته بدالة الهاش المستخدمة، يقوم المهاجم بالتعديل على البيانات الأصلية ثم يقوم بحساب الهاش الجديد ويرسله مع الرسالة المعدلة للمستقبل.
- يقارن المستقبل بالهاش الذي قام بحسابه مع الهاش المرسل فيجد تطابق



صد الهجوم عن البيانات المرسلة

- لمنع القراصنة من عمل هجوم على البيانات المرسلة هو إضافة مفتاح سري للهاش. الشخص الذي يعرف المفتاح فقط هو من يستطيع التحقق من الهاش.
- من الطرق المشهورة لتحقيق ذلك هو تضمين مفتاح سري في الهاش باستخدام خوارزمية **(HMAC) إتشماك**.

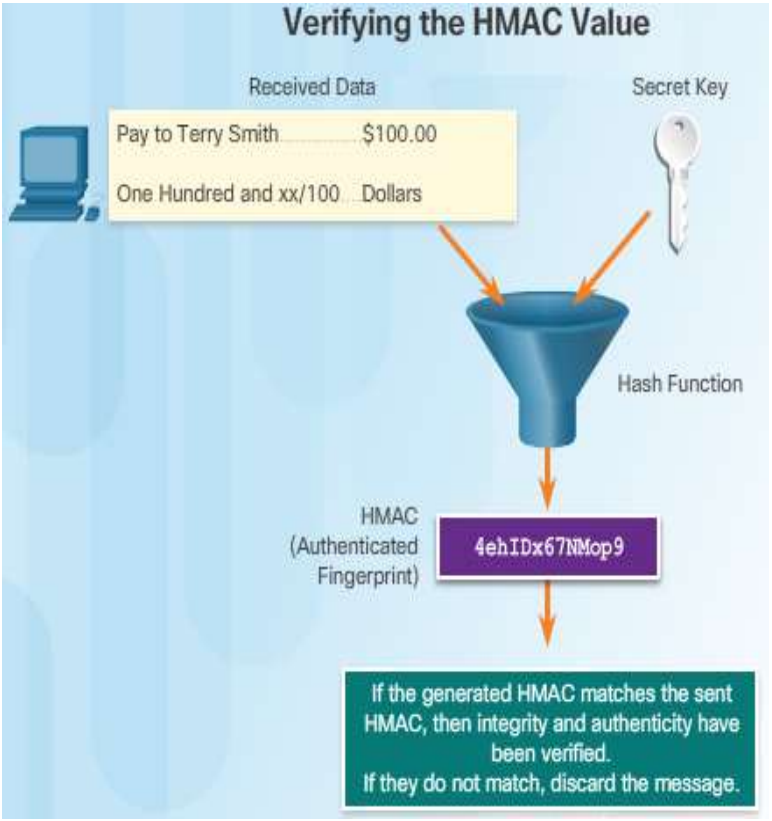
صد الهجوم عن البيانات المرسلة



كيف يعمل إتشماك: افترض أن المرسل يريد التحقق من سلامة الرسالة ومن هوية مرسلها.

- يقوم الجهاز المرسل بإدخال البيانات الآتية (مثل ادفع لجون سميث مبلغ 100 دولار، المفتاح السري) إلى خوارزمية الهاش ثم يحسب الملخص التشفيري الثابت الطول اتشماك لتلك البيانات، والملخص التشفيري يكون بمثابة البصمة الرقمية.

صد الهجوم عن البيانات المرسلة



- يقوم المستقبل باستقبال البصمة الرقمية المصدقة والمرفقة بالرسالة.
- يقوم الجهاز المستقبل بإزالة البصمة الرقمية من الرسالة ويستخدم نص الرسالة الصريح مع المفتاح السري كمدخلات لنفس دالة الهاش.
- إذا كانت البصمة المحسوبة عند الجهاز المستقبل تساوي البصمة المرسلة فإن الرسالة سليمة. بالإضافة إلى ذلك، سيتأكد المستقبل من مصدر الرسالة لأن المرسل هو الوحيد الذي يمتلك نسخة من المفتاح المشترك. ولذا فإن دالة إتشماك تثبت هوية صاحب الرسالة.

التوقيع الرقمي

تثبت التوقيعات اليدوية والأختام ملكية المحتوى لمستند ما. والتوقيعات الرقمية كذلك. وخصائص التوقيع الرقمي هي كالتالي:

- مصادَق: لا يمكن تزوير التوقيع، و يجب توفير إثبات بأن الموقع وليس أحد غيره هو الذي وقع المستند.
- متماسك: فبعد توقيع المستند لا يمكن تعديل المستند أو التوقيع.
- لا يعاد استخدامه: فالتوقيع جزء من المستند ولا يمكن نقله لمستند آخر.
- لا يمكن إنكاره: لأغراض قانونية، التوقيع والمستند يعتبران أشياء حسية. ولا يمكن للموقعين بعدها ادعاء انهم لم يقعوا على المستند.

التوقيعات الرقمية هي بديلة لإتشماك.(يتم استخدام الهاش والتشفير معا)

في اتشماك يتم التشفير بمفتاح خاص وفي التوقيع الرقمي يستخدم المفتاح العام

كيف يعمل التوقيع الرقمي

تأتي الفكرة الأساسية للتوقيع الرقمي من استخدام التشفير الغير متماثل مع الهاش. فخوارزمية ذات مفتاح عام مثل خوارزمية ريشاد (RSA) تنتج مفتاحين، واحد خاص وواحد عام.

- تريد إليسا إرسال بريد إلكتروني لبوب يحتوى على معلومات هامة عن طرح منتج جديد.
- وتريد إليسا أن تتأكد أن بوب يعرف أن الرسالة هي التي أرسلتها وليست فتاه أخرى،
- وتريد أيضا أن تتأكد بأن الرسالة وصلت لبوب دون تعديل في الطريق

الخطوات التالية نوضح كيف تقوم اليسا بعمل ذلك.

كيف يعمل التوقيع الرقمي

مرحلة التوقيع: لعمل ذلك تقوم إليسا بتجهيز الرسالة وتجهيز هاش الرسالة. ثم تقوم بتشفير الهاش مستخدمة مفتاحها الخاص،

كيف يعمل التوقيع الرقمي

مرحلة ارسال المستند الموقع: تقوم إليسا بتجميع كل من الرسالة و الهاش المشفر ومفتاحها العام لتقوم بتركيب المستند النهائي الموقع. وترسل ذلك المستند لبوب.

كيف يعمل التوقيع الرقمي

مرحلة استقبال المستند الموقع: يستقبل بوب الرسالة. وليتأكد من أن الرسالة أتت من إليسا، يقوم بحساب هاش الرسالة (هاش1). ثم يقوم بأخذ هاش الرسالة المشفر والمرسل مع رسالة إليسا ويقوم بفك تشفيره مستخدما المفتاح العام لإليسا (هاش2). ثم يقارن الهاش الذي استقبله من إليسا (هاش2) مع الهاش الذي حسبه هو (هاش1). إذا وجد تطابق يعرف بعدها أن تلك رسالة إليسا وأنها لم يتم التلاعب بالرسالة في الطريق.

استخدامات التوقيع الرقمي

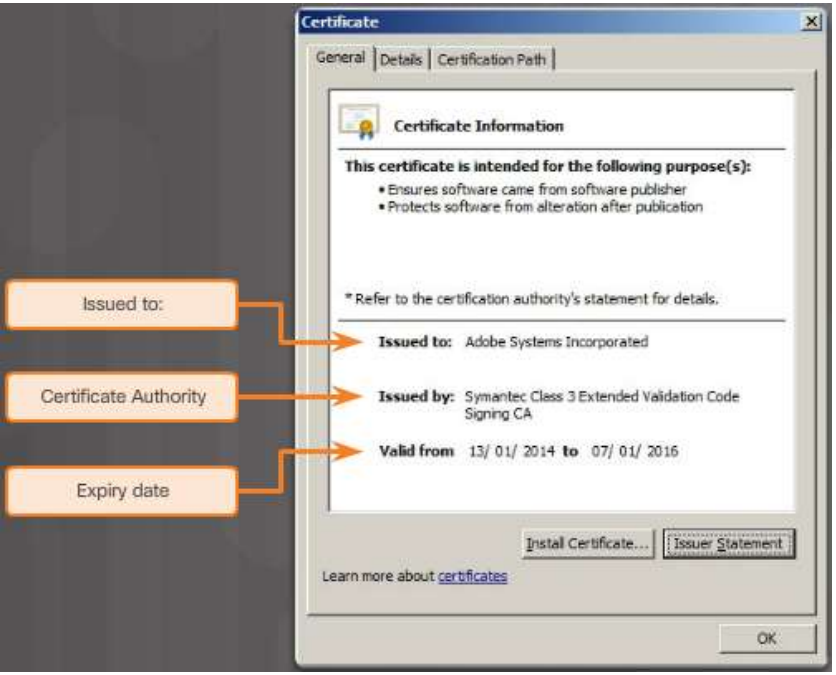
توقيع الهاش بدلا من كامل المستند يعطي كفاءة وتوافق وتماسك لعملية التوقيع التي تتماشي مع كل المتطلبات القانونية والإدارية.

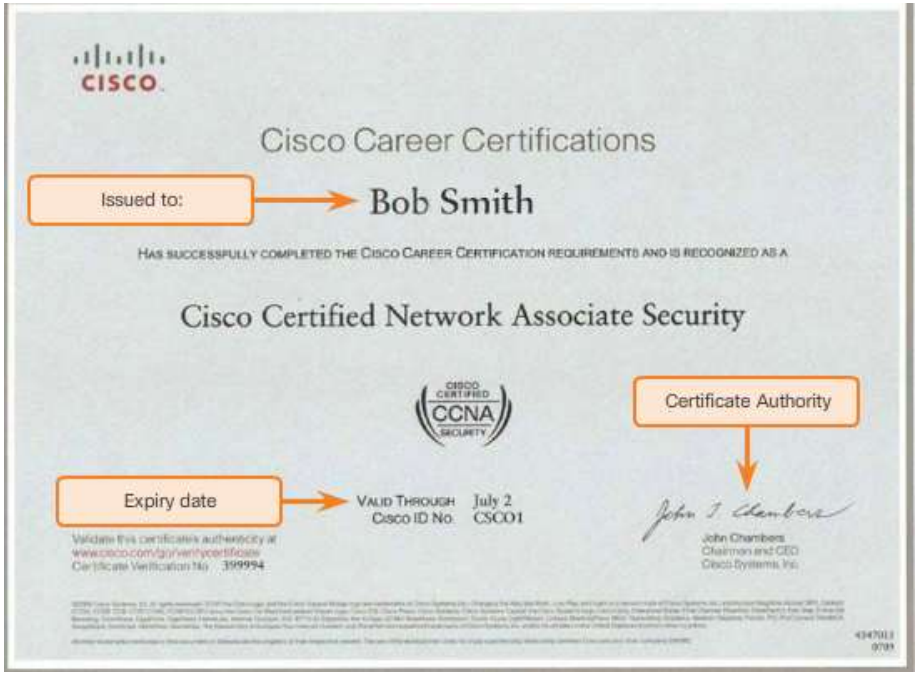
وفيما يلي حالتين لاستخدام التوقيعات الرقمية:

- **توقيع البرامج** – ويستخدم في إثبات تماسك الملفات التنفيذية التي يتم تحميلها من موقع بيع تلك الملفات. ويستخدم توقيع البرامج شهادات رقمية موقعة لمصادقة وإثبات هوية الموقع.
- **الشهادات الرقمية** – وتستخدم في تحديد هوية المؤسسة أو الفرد لمصادقة موقع البيع وإقامة قناة اتصال لتبادل المعلومات المصنفة والسرية.

الشهادات الرقمية

الشهادة الرقمية تمثل جواز السفر الإلكتروني. فهي تمكن المستخدم والأجهزة المضيفة والمؤسسات من تبادل المعلومات بطريقة سرية عبر الإنترنت. والمطبوعة كما بالشكل تعرف الفرد باسمه وتعرف سلطة الاعتماد (من اعتمد الشهادة) وتعرف أيضا فترة صلاحية الشهادة.





استخدام الشهادات الرقمية

يريد بوب تأكيد طلب شراء مع إليسا. يستخدم خادم الويب الخاص بإليسا الشهادات الرقمية لتأكيد التراسل الآمن. يتم عمل تأكيد طلب الشراء بالخطوات التالية:

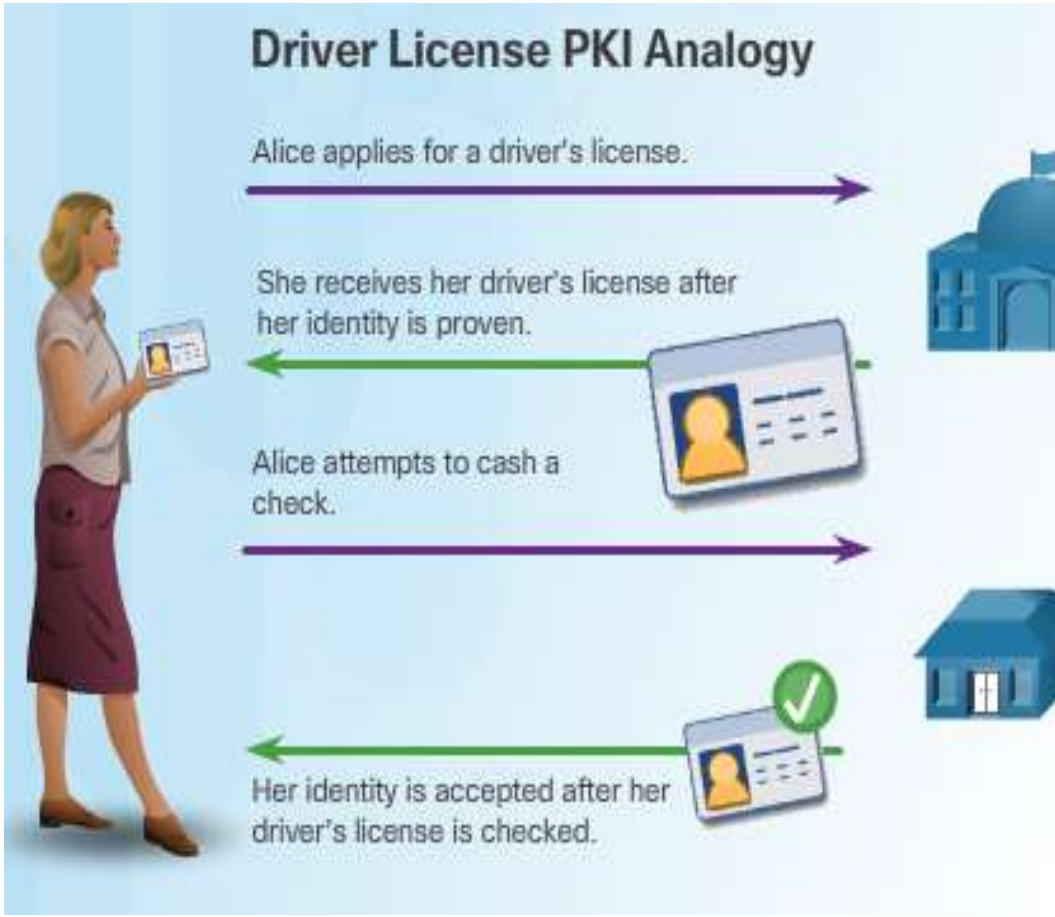
استخدام الشهادات الرقمية

1. يقوم بوب بتصفح الموقع الإلكتروني لإليسا. والمتصفح عند بوب يخبر بوب بأن الاتصال آمن عن طريق عرض رمز قفل في شريط الحالة الأمنية.
2. يرسل خادم ويب إليسا شهادة رقمية لمتصفح بوب.
3. يقوم متصفح بوب بفحص الشهادة المخزنة في إعدادات المتصفح. والشهادات الموثوق فيها فقط هي التي تسمح لعملية الاتصال أن تكتمل.

استخدام الشهادات الرقمية

4. لا يزال بوب محتاجا للمصادقة فيعطي كلمة مرور. وفي هذه الحالة يتم عمل جلسة سرية في الخلفية بين حاسب بوب وخادم ويب إليسا.
5. يقوم متصفح بوب بخلق مفتاح جلسة فريد لمرة-واحدة.
6. يستخدم متصفح بوب المفتاح العام الخاص بخادم الويب والموجود على شهادة الخادم الرقمية لتشفير الجلسة.
ونتيجة لذلك نجد أن خادم إليسا هو الوحيد الذي يستطيع قراءة المعاملة التي أرسلها متصفح بوب.

سلطة إصدار الشهادات الرقمية CA



سلطة إصدار الشهادة (CA) تعمل بنفس المبدأ الذي تعمل به إدارة المرور. حيث تقوم السلطة بإصدار شهادات رقمية والتي تصادق هوية الشركات والمستخدمين.

وهذه الشهادات تقوم بتوقيع الرسائل للتأكد من أنه لا أحد قد عبث بمحتوى الرسالة أثناء نقلها.

سلطة إصدار الشهادات الرقمية CA

يحصل الفرد على الشهادة والمفتاح العام من سلطة إصدار تجارية.

والشهادة تنتمي لسلسة من الشهادات تسمى سلسلة الثقة.

عدد الشهادات في سلسلة الثقة يعتمد على التركيب الهرمي لسلطة الإصدار (CA). يعطي الشكل التالي معلومات عن سلسلة الشهادات في مستويين فقط

يوجد في العادة جهازين لسلطة الإصدار جهاز جذعي متصل وجهاز تابع منفصل. والسبب في اتخاذ التركيب يسهل عملية التعافي في حالة الاختراق

تمرين عملي: الشهادات الرقمية وسلطة الإصدار

Part 1: Certificates Trusted by Your Browser, Display the Root Certificates in Chrome

- Click Settings and then click Show advanced Settings.
- Scroll down the page and click the Manage certificates… button, under the HTTPS/SSL section.

Part 2: Checking for Man-In-Middle

Bad scenario can happen like the following:

- IT department in the company add falsified info for CA related to https proxy, in addition to currently installed trusted CA's on the user's machine.
- Https proxy is controlled by the IT department.
- User's machine wants to login to website H, it must go through the https proxy, https proxy say that "I'm H", https proxy impersonates website H, and make man-in-middle attack.

Step 1: Gathering the correct and unmodified certificate fingerprint.(linkedin website)

- Login to https://www.grc.com/fingerprints.htm and keep the linkedin fingerprint,
- Open your browser and enter www.linkedin.com to surf linkedin website.
- Click the small "lock" icon beside the website url, then click certificate-> details then scroll down to thumbprint,
- Compare the thumbprint with the one obtained from the above first step (grc website). If they match, then you are on the real website and there is no man-in-middle attack.

الأسئلة