جامعة المنارة
كلية الهندسة
قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

عناوين المحاضرة السابعة

- التوقيع الرقمي (Digital Signature)

- ✓ مقدمة
- ✓ تعريف بالتوقيع الرقمي
- ✓ تمثيل التوقيع الرقمي رياضياً
- ✓ التوقيع الرقمي مع الختم الزمني
- ✓ التوقيع الرقمي مع تابع البعثرة (Hash)
- ✓ عدم التنصل للأصل باستخدام التوقيع الرقمي
- ✓ استخدام التوقيع الرقمي مع التشفير
- ✓ تطبيقات التوقيع الرقمي

تعريف التوقيع الرقمي Digital Signature

- يضمن التوقيع الرقمي عدم التنصل للأصل (Non-repudiation to origin) أي أن المرسل لن يكون مستقبلاً قادراً على أن يتنصل من أنه هو من أرسل الرسالة.
- هو آلية تقوم على نظام تشفير غير متناظر
- يحسب التوقيع الرقمي باستخدام المفتاح الخاص للمرسل و يتم التحقق منه بواسطة المفتاح العام للمرسل.

تمثيل التوقيع الرقمي رياضياً

١. يوقع بوب الرسالة باستخدام مفتاحه الخاص اعتماداً على خوارزمية التوقيع المستخدمة: $S = E_{K_{priB}}(M)$

٢. يرسل بوب الرسالة و التوقيع الرقمي معاً: $S \| M$

٣. تستقبل أليس الرسالة والتوقيع

٤. تقوم بالتحقق من التوقيع كالآتي: $V_{K_{pub_A}}[S(M)]$

١-تحسب الرسالة اعتماداً على التوقيع المستقبل: $M_{cal.} = D_{pub_B}(S) = D_{pub_B}\left(E_{K_{pri_B}}(M)\right)$

٢- تقارن الرسالة المحسوبة مع المستقبلة: $M_{cal.} ? = M$

يكون التوقيع فعال وصحيح في حال التساوي $M_{cal.} = M$

التوقيع الرقمي مع الختم الزمني

إرسال الرسالة مع التوقيع

↓

إمكانية إعادة استخدامهما أكثر من مرة من قبل المستقبل

↓

الخطورة تكمن في حال الشيكات الرقمية

↓

يمكن للمستقبل الاستفادة من الشيك وسحب المبلغ أكثر من مرة

لذا يتضمن التوقيع الرقمي ختماً زمنياً **Timestamp** :

- تاريخ التوقيع
- زمن فعاليته

توقع هذه المعلومات مع الرسالة

التوقيع الرقمي مع تابع البعثرة (Hash)

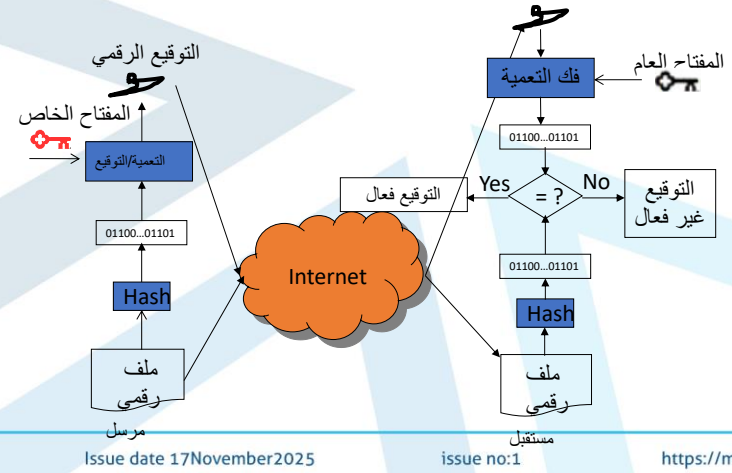
يستغرق التوقيع الرقمي وقتاً طويلاً للحساب في حال الرسائل الطويلة

لذلك

↓

استخدام التوقيع الرقمي على خرج تابع الـ Hash

عدم التنصل للأصل باستخدام التوقيع الرقمي



استخدام التوقيع الرقمي مع التشفير

Alice

$$S = E_{K\,pri_A}(M)$$

$$E_{K\,pub_B}[S(M)]$$

Bob

$$D_{K\,pri_B}\left[E_{K\,pub_B}[S(M)]\right] = S(M)$$

$$V_{K\,pub_A}[S(M)] = M$$

استخدام خوارزمية RSA من أجل التوقيع الرقمي

✓ يولد المرسل التوقيع الرقمي (S) انطلاقاً من الرسالة M باستخدام مفتاحه الخاص :

$$S = M^{d} \bmod(n)$$

حيث أن المفتاح الخاص هو: $K_{pri} = \{d, n\}$

✓ يستقبل المستقبل الرسالة M و التوقيع الرقمي (S) و يتحقق من الرسالة M باستخدام المفتاح العام للمرسل :

$$M = S^{e} \bmod(n)$$

حيث أن المفتاح العام هو : $K_{pub} = \{e, n\}$

من تطبيقات التوقيع الرقمي

البطاقة المصرفية

❖ إن شريحة البطاقة المصرفية هي عبارة عن كومبيوتر صغير، يحتوي على CPU,RAM,ROM ....إلخ.

❖ من أجل مصادقة البطاقة يخزن في البطاقة:

✓ قيمة معرِّف (محدد)(VI): تكوَّن هذه القيمة من معلومات تخص البطاقة:

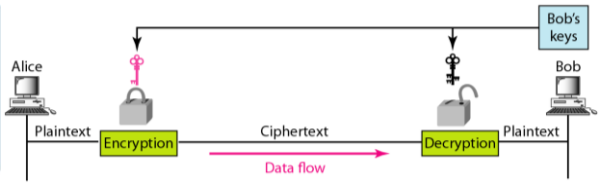
مثل (حامل البطاقة، عدد، تاريخ الفعالية، الشعار)

✓ قيمة المصادقة (VA): و هي قيمة VI المشفرة باستخدام الخوارزمية RSA باستخدام المفتاح الخاص للموزع (GIE)

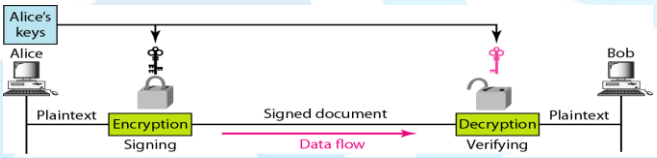
❖ عند وضع البطاقة في الطرفية، يتم التحقق من أن القيمة الناتجة من فك تشفير VA باستخدام المفتاح العام للموزع مطابقة لقيمة VI المخزنة ضمن البطاقة

الفرق بين نظام التشفير و التوقيع الرقمي من حيث المفاتيح

✓في نظام التعمية : يستخدم المفتاح العام و المفتاح الخاص للمستقبل .

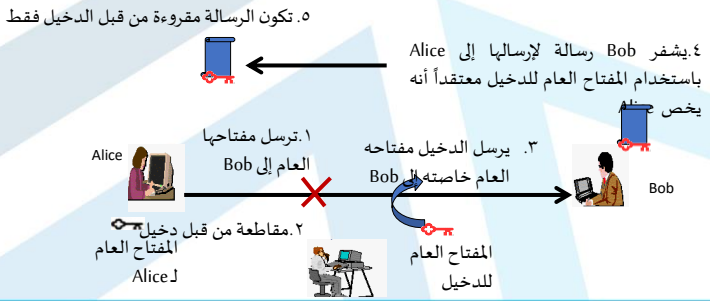


✓في التوقيع الرقمي: يستخدم المفتاح الخاص و المفتاح العام للمرسل.



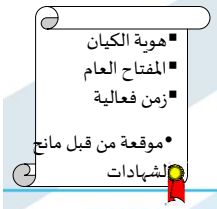
الشهادة الرقمية (Digital Certificate) (1/ 3)

❖رغم الفوائد التي يقدمها استخدام التوقيع الرقمي، تبقى لدينا مشكلة متعلقة بالهوية الحقيقية للموَقِّع. إذ يظهر لدينا ما يسمى هجوم رجل المنتصف (Man in the Middle)



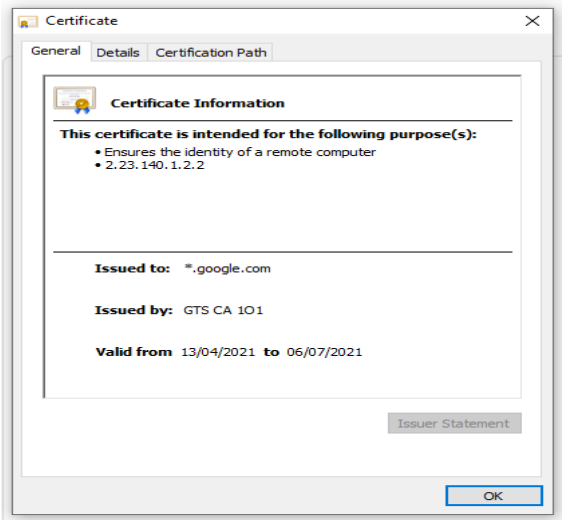
الشهادة الرقمية (Digital Certificate) (2/ 3)

- الحل لمشكلة ((رجل في المنتصف)) هو استخدام الشهادة الرقمية .
- تضمن الشهادة الرقمية الارتباط ما بين هوية الكيان و المفتاح العام لذلك الكيان في ملف رقمي موقع من قبل طرف ثالث موثوق (Trusted Third Party) أو مايسمى مانح الشهادات ((Certification Authority (CA))



- تثبت الشهادة :
  - ✓ من أنت
  - ✓ ما هو مفتاحك العام
  - ✓ من هو مانح الشهادة

الشهادة الرقمية (Digital Certificate) (3/ 3)



- كيف أعرف أن الموقع آمن:

عند ظهور رمز قفل في زاوية شريط العنوان في مستعرض الانترنت، نعلم أن الموقع يستخدم SSL لتشفير البيانات، وعند الضغط على هذا الرمز نستطيع معرفة معلومات الشهادة الرقمية المستخدمة

جَامعة المَنارة
MANARA UNIVERSITY

نهاية المحاضرة السابعة