Information System Security

أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الأربعاء 14/6/2023

جَامعة المَنارة
MANARA UNIVERSITY

عناوين المحاضرة الثامنة

- مقدمة
- التوقيع الرقمي (Digital Signature)
  - ✓ 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
- فكرة هيكلية المفتاح العام (PKI)
- الشهادة الرقمية (Digital Certificate)

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

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

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

3. تستقبل أليس الرسالة والتوقيع

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

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

2- 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

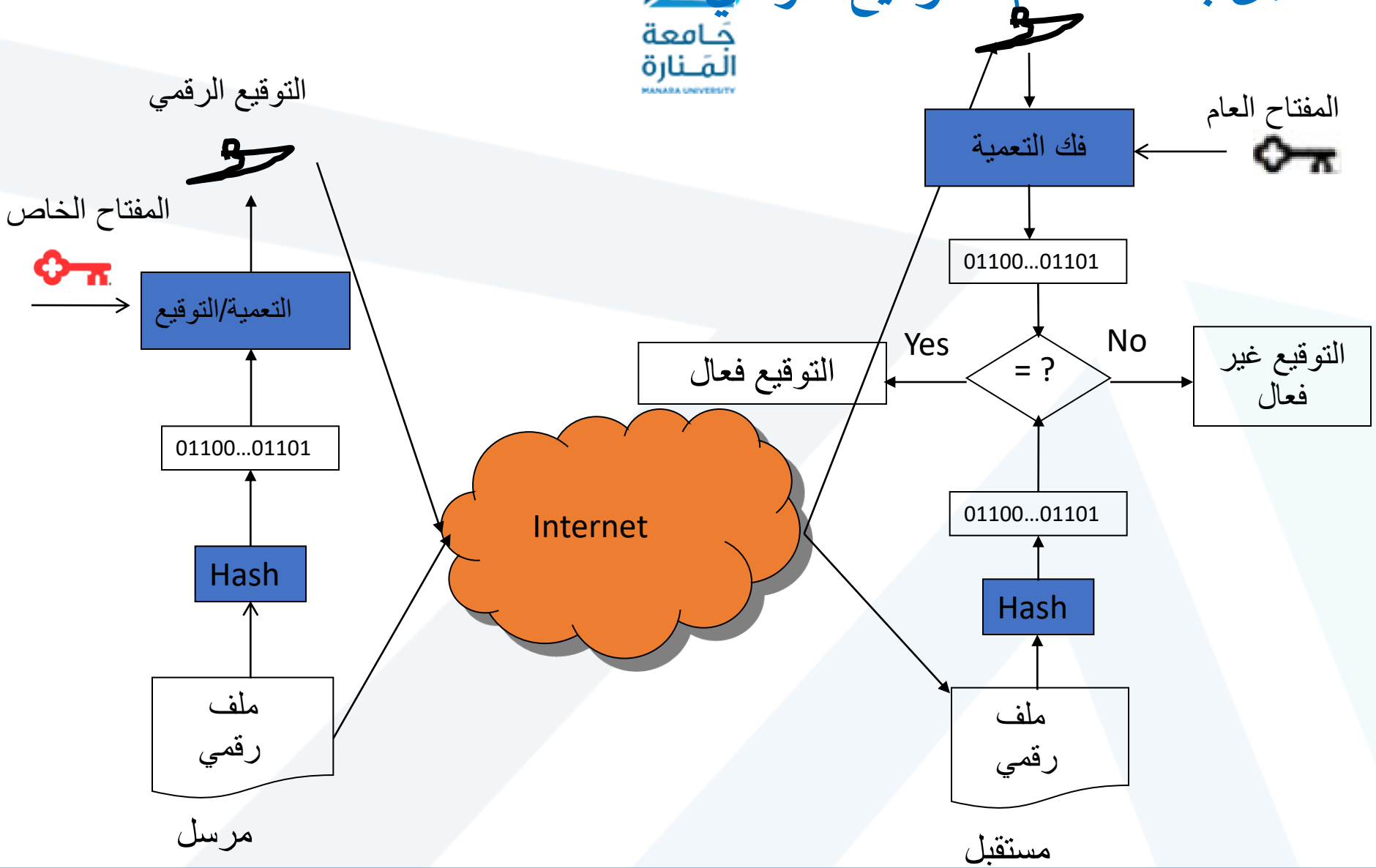
التوقيع الرقمي مع تابع البعثرة (Hash)

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: $K_{pri} = \{d, n\}$

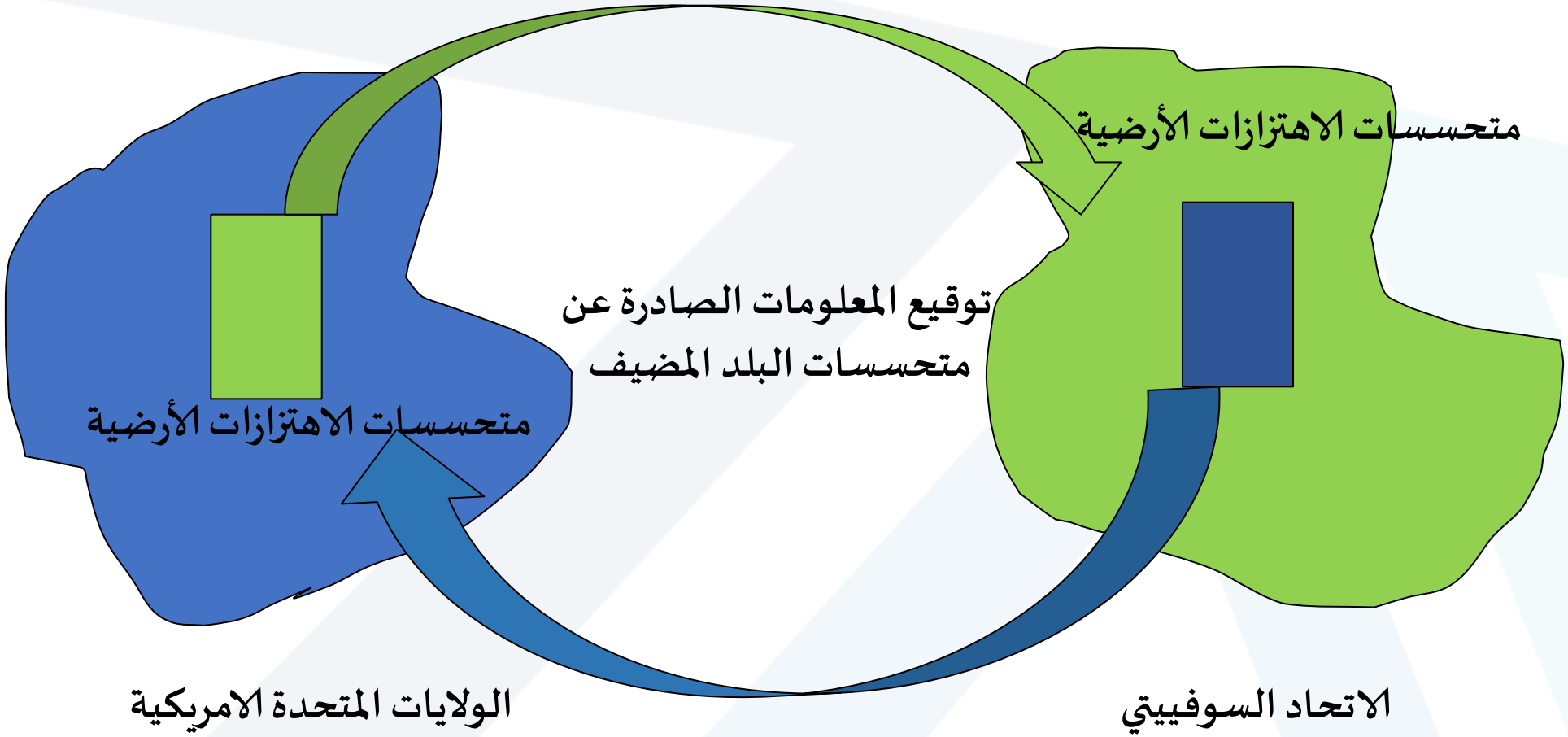
✓ يستقبل المستقبل الرسالة M و التوقيع الرقمي (S) و يتحقق من الرسالة M باستخدام المفتاح العام للمرسل :

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

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

من تطبيقات التوقيع الرقمي:

التحقق من معاهدات حظر التجارب النووية



جَامعة المَنارة
MANARA UNIVERSITY

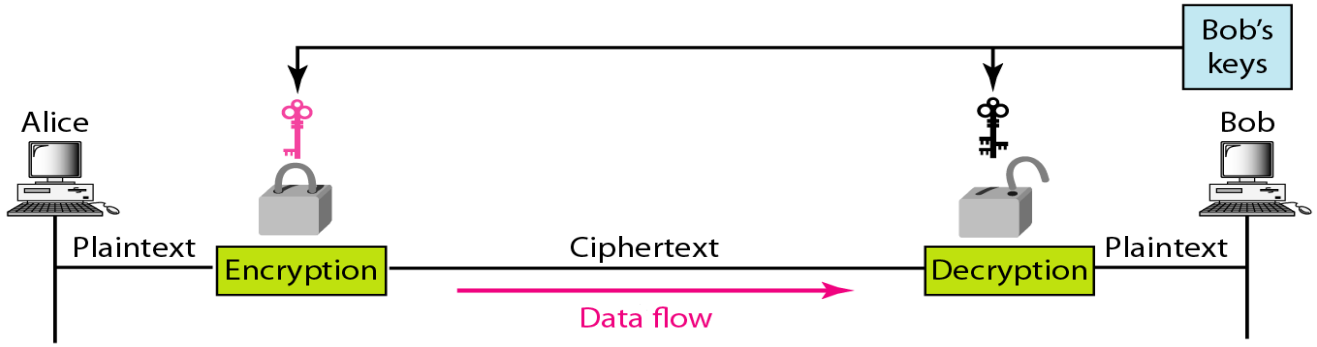
البطاقة المصرفية

- 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:

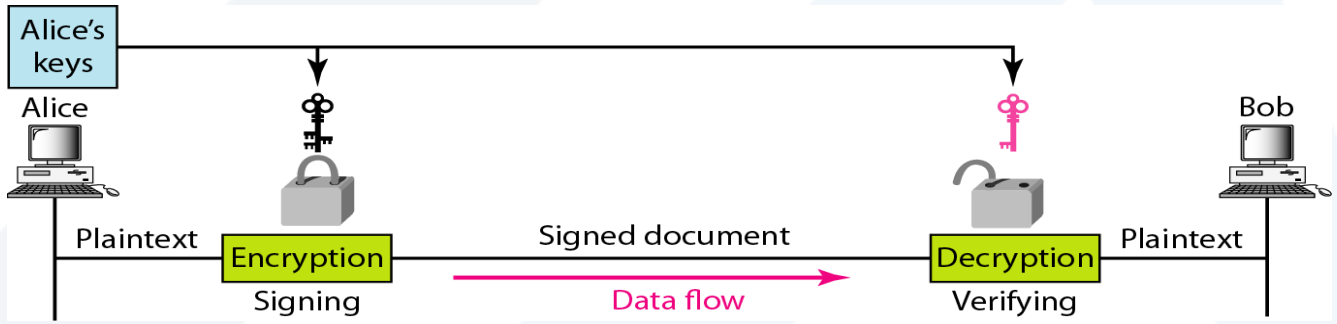
    مثل (حامل البطاقة, عدد, تاريخ الفعالية, الشعار)
  - ✓قيمة المصادقة (VA): و هي قيمة VI المشفرة باستخدام الخوارزمية RSA باستخدام المفتاح الخاص للموزع (GIE)
- عند وضع البطاقة في الطرفية، يتم التحقق من أن القيمة الناتجة من فك تشفير VA باستخدام المفتاح العام للموزع مطابقة لقيمة VI المخزنة ضمن البطاقة

الفرق بين نظام التشفير و التوقيع الرقمي من حيث المفاتيح

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



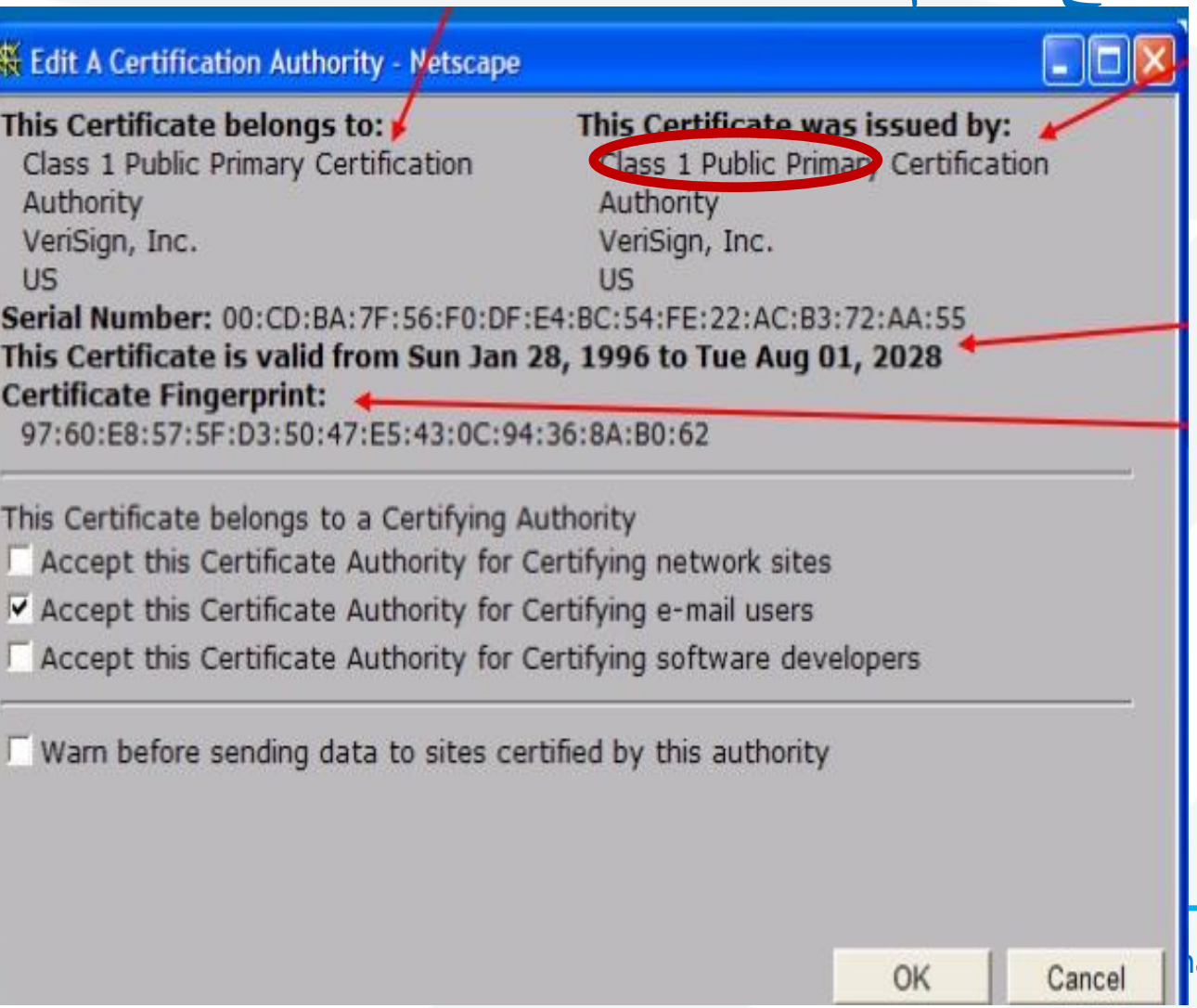
✓ في التوقيع الرقمي: يستخدم المفتاح الخاص و المفتاح العام للمرسل.



مقدمة إلى هيكلية المفتاح العام
(Public Key Infrastructure(PKI))

- إن أعداد كبيرة من الناس يبيعون و يشترون عبر الانترنت ، وهذا يجعل من الصعب إدارة و ضمان أمن هذه التعاملات باستخدام مفتاح سري (تشفير متناظر)
- ظهرت أهمية البحث عن هيكيلية للمفتاح العام عندما أصدرت الحكومة الأمريكية القانون الذي نص على إلغاء الحكومة الورقية و التوجه إلى الحكومة الالكترونية منذ عام 2003
- الهدف من هذه الهيكلية هو :حماية وتوزيع المعلومات المطلوبة في بيئة موزعة على نطاق واسع، حيث يمكن للمستخدمين والموارد وأصحاب المصلحة أن يكونوا في أماكن مختلفة في أوقات مختلفة.
- تزود هذه الهيكلية المتطلبات الأمنية الأساسية الآتية : التكاملية والموثوقية والمصادقة
- تتضمن هذه الهيكلية:
  - ✓ الشهادات الرقمية
  - ✓ التعمية باستخدام المفتاح العام
  - ✓ كيانات مانحة للشهادة من أجل هيكلية أمنية لشبكة واسعة أو شركة

مكونات الأساسية لهيكلية المفتاح العام PKI (1/2)



- هيئة إصدار الشهادات CA (Certification Authority)

تمثل حجر الأساس في هذه الهيكلية ، وهي مسؤولة عن كل ما يتعلق بتوليد الشهادات و توقيعها ، وتحتفظ بالمعلومات الدالة على حالة الشهادة (فعالة أو ملغاة)

عملياً هي شركات عالمية موثوقة ومرخص لها بمنح الشهادات الرقمية نذكر منها: **VeriSign** Thawte, Geotrust, Comodo, Entrust, DigiCert, SwissSign, TurkTrust

مكونات الأساسية لهيكلية المفتاح العام PKI (2/2)

- **هيئة التسجيل RA (Registration Authority)**

تسجل و تتحقق من طلبات الشهادة المقدمة من قبل المستخدمين و يكون موثوقاً بها من قبل CA إذ تُعلِمْه ليقوم بإصدارها

- **المستودع Repository/ Directory**

يتضمن قاعدة بيانات الشهادات الرقمية الفعالة لـ CA ، كما يوفر البيانات التي تسمح للمستخدمين بتأكد من حالة الشهادات الرقمية للأفراد والشركات التي تتلقى رسائل موقعة رقمياً

- **الأرشيف Archive:**

لتخزين وحماية معلومات تكون كافية لتحديد فيما إذا كان ينبغي الوثوق بالتوقيع الرقمي الموجود على وثيقة "قديمة" أو لا

- **الشهادات Certifications:**

تتضمن المفتاح العام، ومعلومات عن هوية الكيان الذي يحمل المفتاح الخاص المقابل، و زمن حياة الشهادة، والتوقيع الرقمي الخاص بالـCA.
قد تحتوي على معلومات أخرى عن الطرف أو المعلومات الموقعة حول الاستخدامات الموصى بها للمفتاح العام.

وظائف هيكلية المفتاح العام PKI

- تتمثل وظائف PKI الأكثر شيوعاً في:
  - ✓ إصدار الشهادات
  - ✓ إلغاء الشهادات
  - ✓ إنشاء قوائم الشهادات الملغاة CRL(Certificate Revocation Lists) ونشرها وتخزينها واسترجاعها
  - ✓ إدارة حياة المفتاح
  - ✓ تطوير وتحسين وظائف للتحقق من الختم الزمني
  - ✓ التحقق من صحة الشهادة

آلية عمل الـ PKI (1/6)

1. تقوم هيئة التسجيل (RA) بتسجيل طلبات الحصول على الشهادات و التحقق من هذه الطلبات
2. تقوم هيئة إصدار الشهادات (CA) بإنشاء و توزيع الشهادات
3. تقوم هيئة التحقق من الفعالية الـ (Authority of validation) AV بالتحقق من فعالية الشهادات
4. في كل لحظة, يقوم مخزن قائمة الشهادات الملغاة CRL بإدارة حالة الشهادات و ذلك للأخذ بالحسبان الشهادات التي أصبحت ملغاة
5. تنشر الشهادات و تخزن ضمن مستودع الشهادات (directory)

آلية عمل الـ PKI (2/6)

Directory

Certificate Authority (CA)

User (Bob)

Registration Authority (RA)

آلية عمل الـ PKI (3/6)

Directory

Certificate Authority (CA)

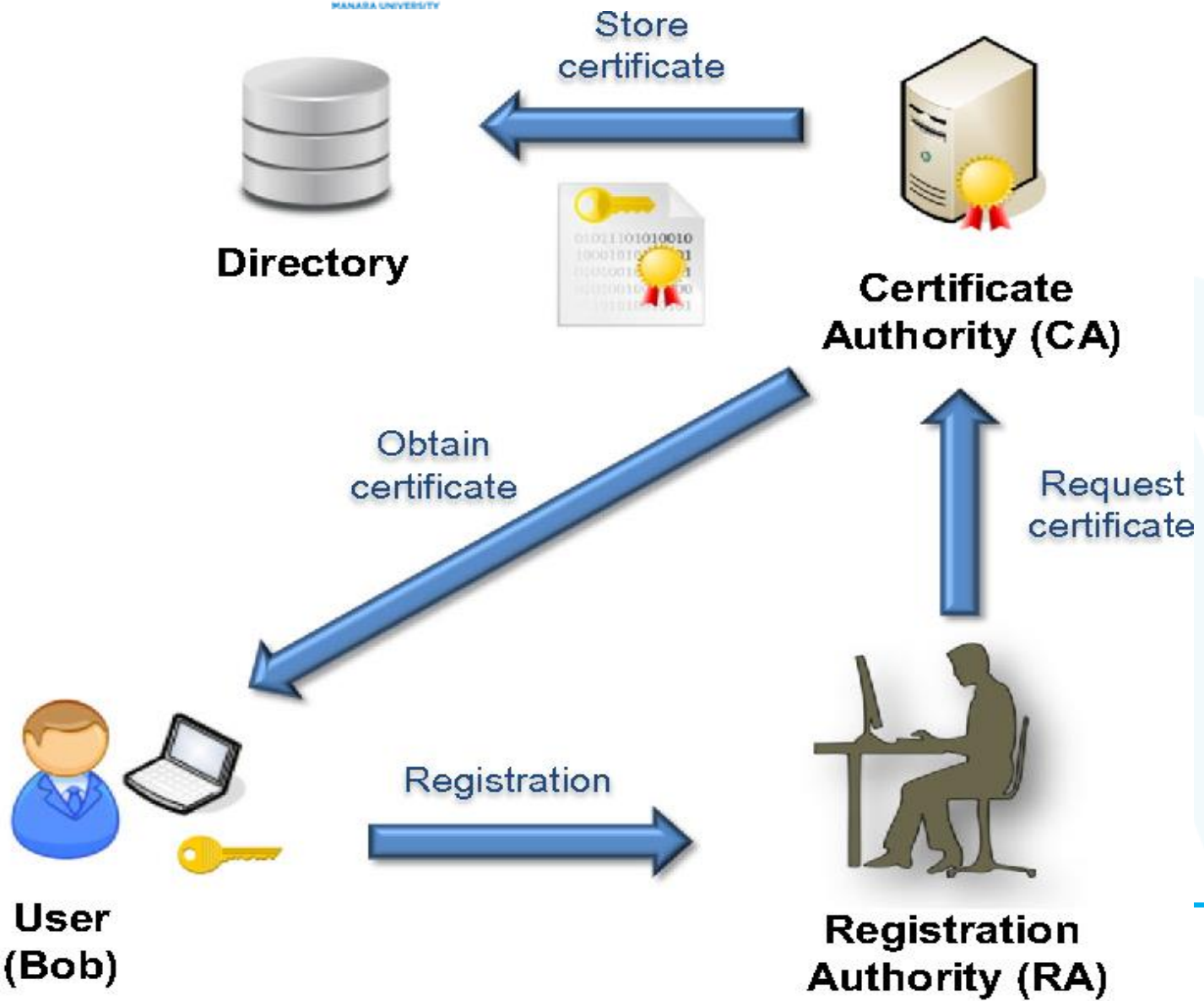
User (Bob)

Registration

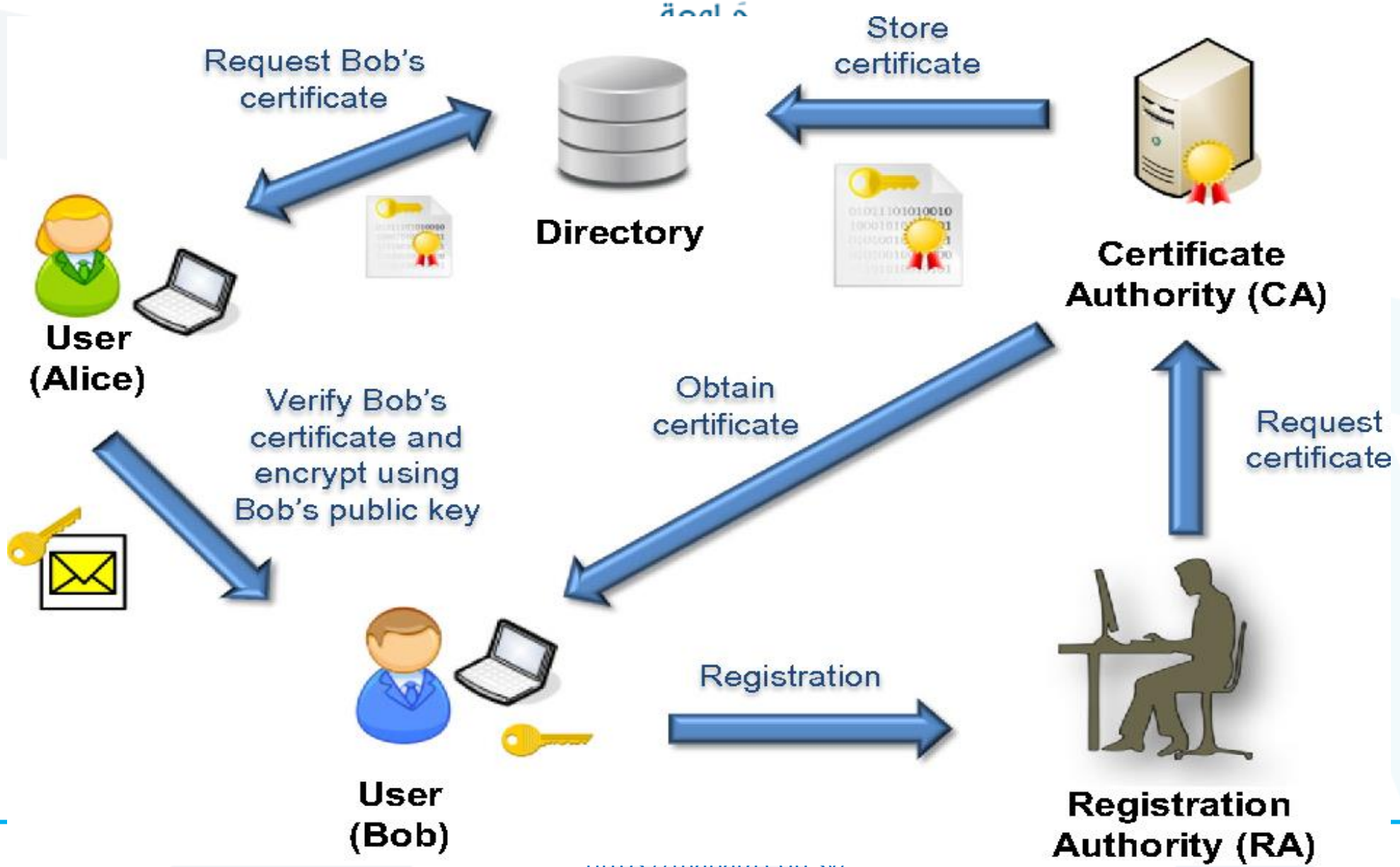
Registration Authority (RA)

آلية عمل الـ PKI (4/6)

آلية عمل الـ PKI (5/6)

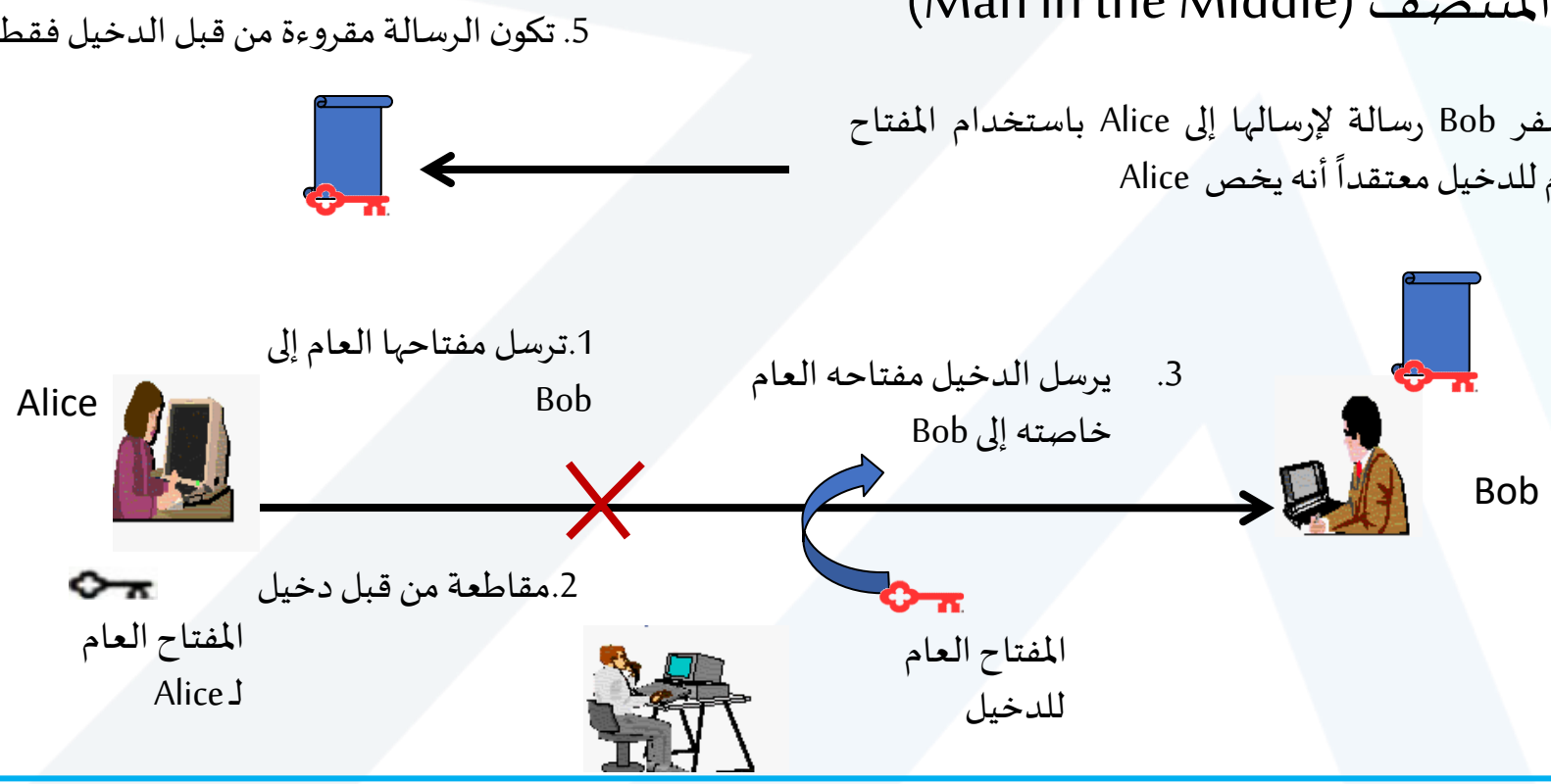


آلية عمل الـ PKI (6/6)



الشهادة الرقمية (Digital Certificate) (1/ 3)

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



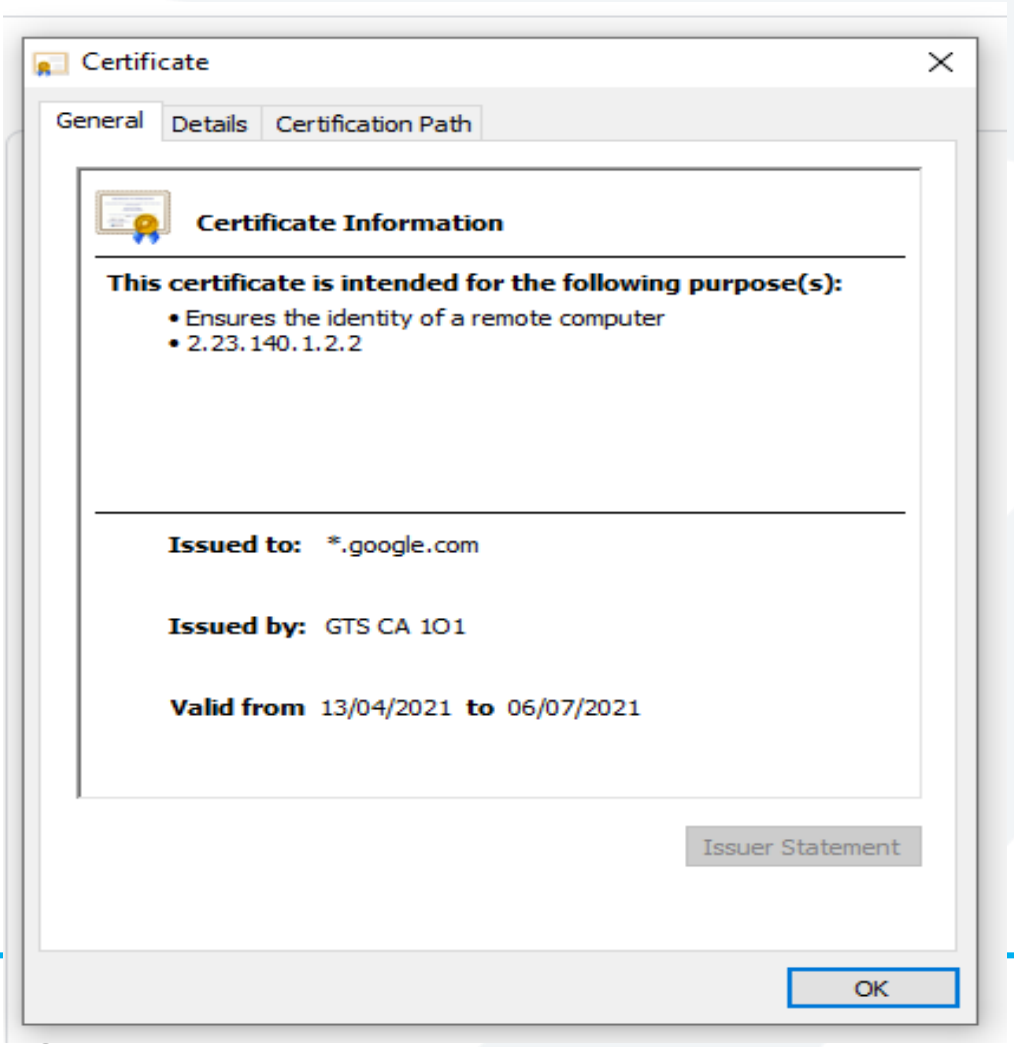
الشهادة الرقمية (Digital Certificate) (2/ 3)

- 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)

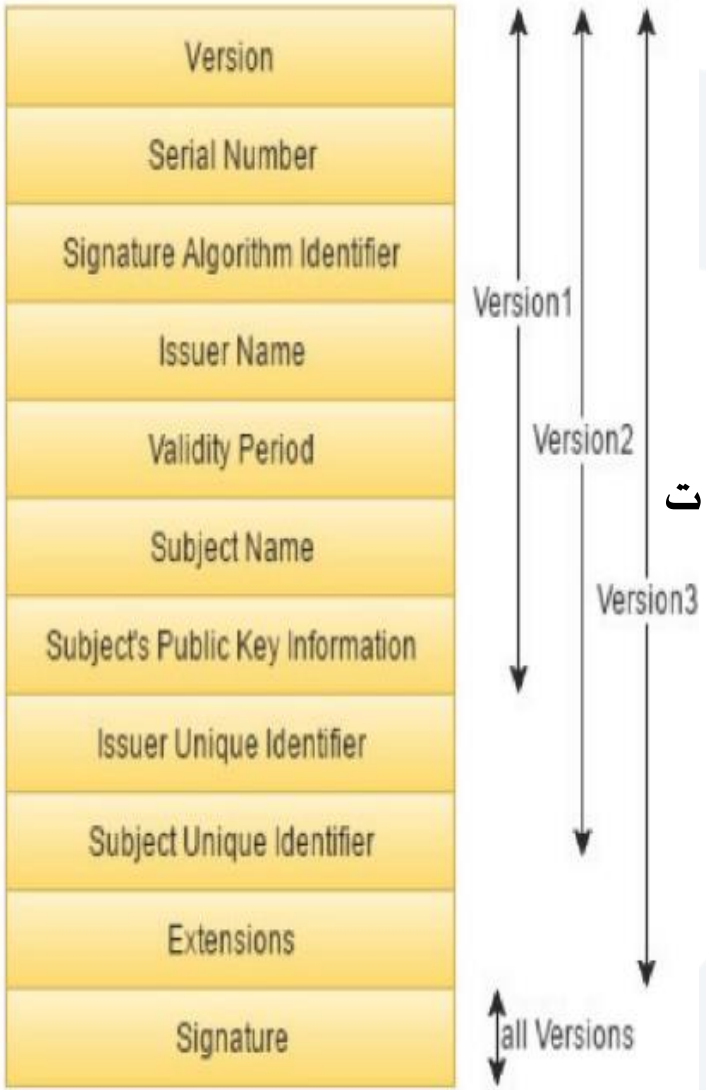
كيف أعرف أن الموقع آمن:



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

مثال عن نموذج الشهادة الرقمية (1/2)

نموذج الشهادة الرقمية X.509



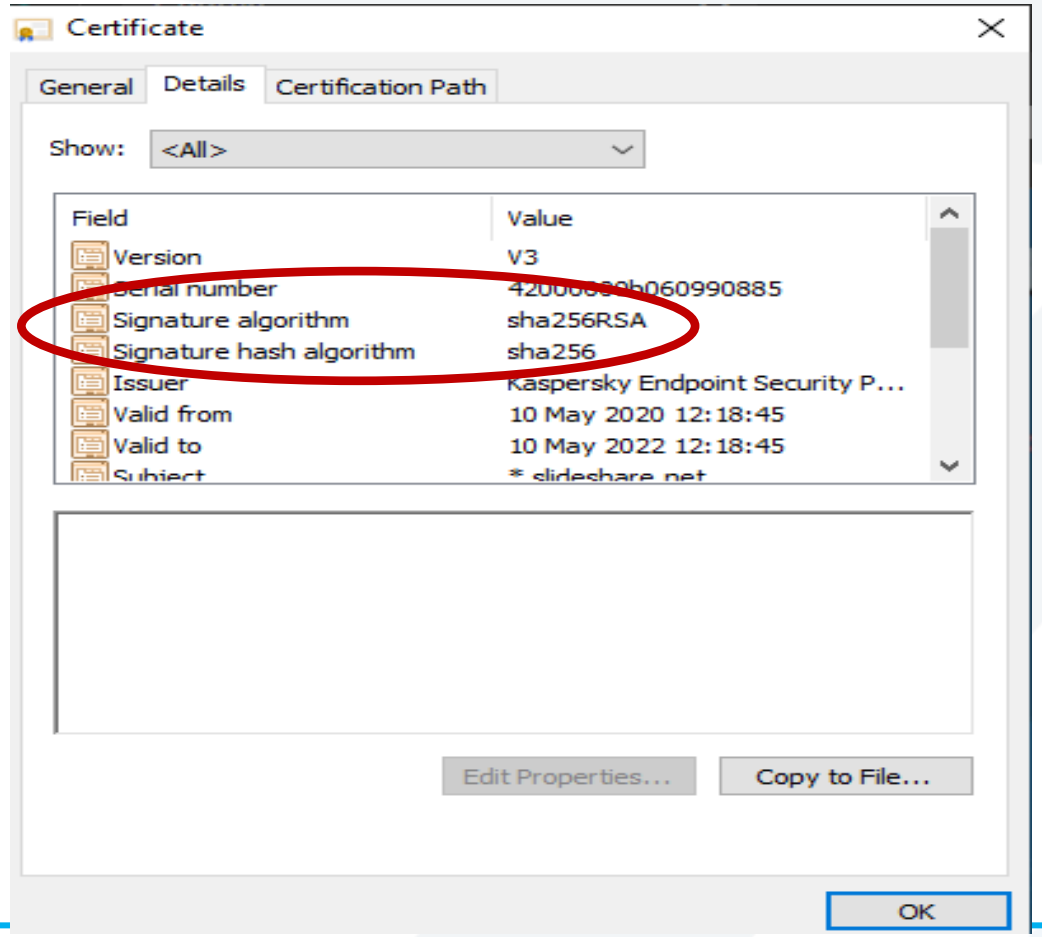
- الإصدار(VERSION):يحدد نسخة الشهادة الرقمية و بالتالي المعلومات التي يجب أن تكتب.
- الرقم التسلسلي (Serial Number): رقم فريد معطى من مخصص من قبل هيئة إصدار الشهادات
- محدد خوارزمية التوقيع(Signature Algorithm Identifier): يحدد الخوارزمية المستخدمة من قبل CA لتوقيع الشهادة
- اسم المانح (Issuer Name): يعطي اسماً مميزاً لـCA الذي وقع و أصدر الشهادة
- الصلاحية (Validity): يحدد المجال الزمني لصلاحية الشهادة
- اسم الكيان (Subject Name) : يصف اسم الكيان الذي أصدرت من أجله الشهادة

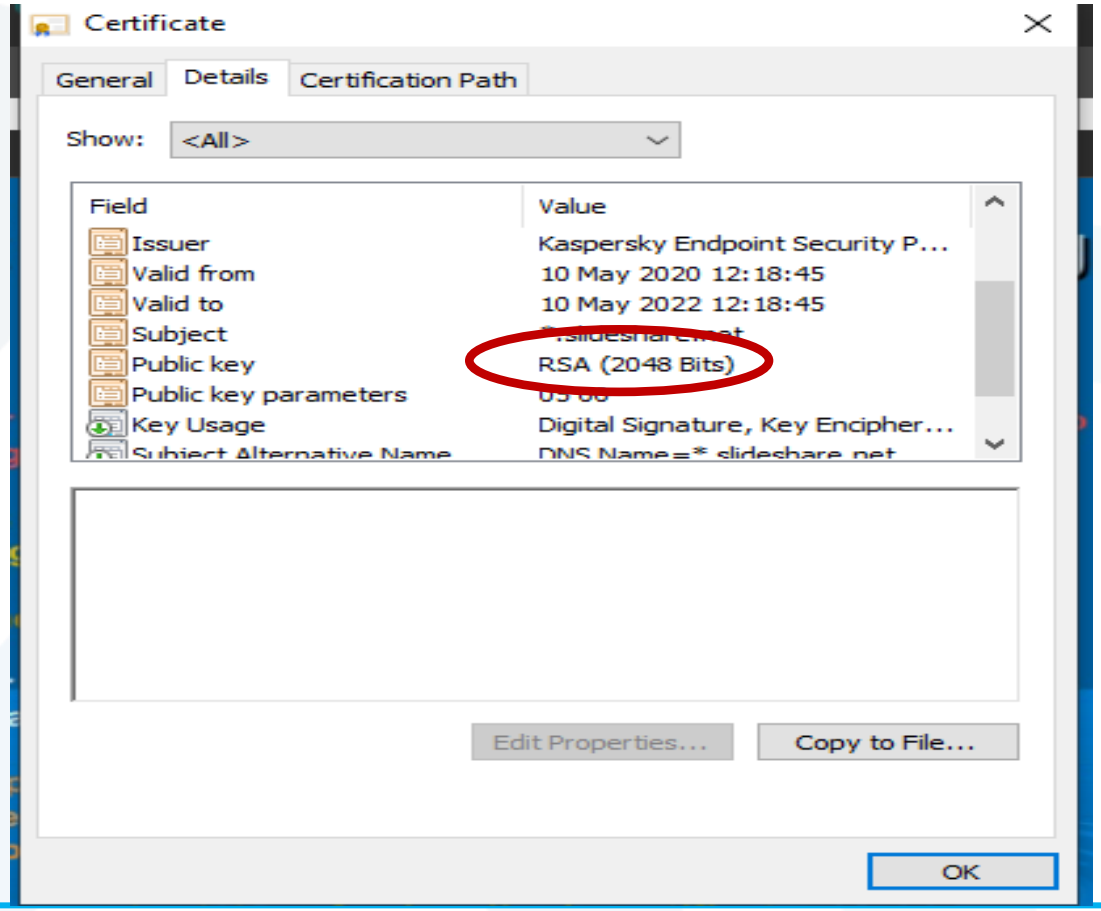
مثال عن نموذج الشهادة الرقمية (2/2)

نموذج الشهادة الرقمية X.509

- معلومات المفتاح العام للكيان (Subject Public Key Information): يحدد خوارزمية المفتاح العام و النوع و الطول المرتبط بالشهادة
- معرف فريد للمانح / الكيان الإصدار (Subject/Issuer Unique Identifier): إنه حقل إفتراضي.يستخدم ليتيح إمكانية إعادة استخدام اسم الكيان/ المانح لاحقاً
- ملحقات (Extensions): هذا الحقل متاح فقط في النسخة 3 . يتيح إضافات بما يخص هيكلية المفتاح العام.

مثال فعلي للشهادة الرقمية (Digital Certificate)





جَامعة
المَنارة
MANARA UNIVERSITY

نهاية المحاضرة الثامنة