جامعة دمشق
كلية الاقتصاد
مجموعة كلية الاقتصاد في جامعة دمشق :
https://m.facebook.com/groups/faculty.economic/
قناة التلغرام : https://t.me/ecodamas

نظم المعلومات المصرفية

السنة الرابعة– قسم المصارف والتأمين

د. ليدا بركات

المحاضرة الرابعة

التجارة الإلكترونية وتشفير البيانات

(الفصل الرابع من نوطة المقرر (ص٩٣-٩٧)+ من خارج النوطة)

خطة العرض

- التجارة الإلكترونية
- بعض القضايا الرقابية المرتبطة بالتجارة الإلكترونية
- التشفير

التجارة الإلكترونية
Electronic Commerce

- استخدام الشبكات في بيع وشراء الخدمات والمنتجات المختلفة والقيام بمختلف أنواع التعاملات المالية بين الأفراد والمنظمات والمنظمات فيما بينها

- مزاياها :

– بناء المواقع الإلكترونية للتعريف بمنتجات وخدمات الشركات والتواصل بينهم وبين عملاهم
– تلقي طلبات العملاء ومقترحاتهم بشكل سريع والاستجابة لها
– تخفيض التكاليف
– الوصول السريع إلى المعلومات
– التكامل بين مختلف أقسام المنظمات البعيدة جغرافياً

بعض القضايا الرقابية المرتبطة بالتجارة الإلكترونية

- **التحقق من صحة العمليات**: التأكد من هوية الأطراف المتعاملة وسلامة المعلومات أثناء انتقالها عبر الشبكات الداخلية أو الخارجية
- **التفويض الصحيح للعمليات**: التأكد من أن العملية تم اعتمادها بشكل نظامي من الطرف الآخر لحماية كل طرف من فسخ العملية من قبل الطرف الآخر
- المحافظة على **سرية البيانات** أثناء تخزينها أو انتقالها عبر الشبكات
- الحماية من **الوصول غير المصرح به إلى البيانات** المخزنة من قبل الموظفين أو الأطراف الخارجية
- الحماية من **مسح وضياع البيانات**

التشفير
Encryption

- **مفهوم التشفير** : ترميز المعلومات بحيث تظهر كسلسلة غير مفهومة من الأحرف والرموز

- تساعد عملية التشفير في حل المشاكل الأمنية المتعلقة بسرية وسلامة المعلومات أثناء تخزينها أو انتقالها عبر الشبكات الداخلية أو الخارجية، إضافة إلى أهمية التشفير في توليد التواقيع الرقمية المستخدمة للتأكد من الهوية وعدم الإنكار للصفقات الإلكترونية (سنتحدث عن التواقيع الرقمية في المحاضرة الخامسة)

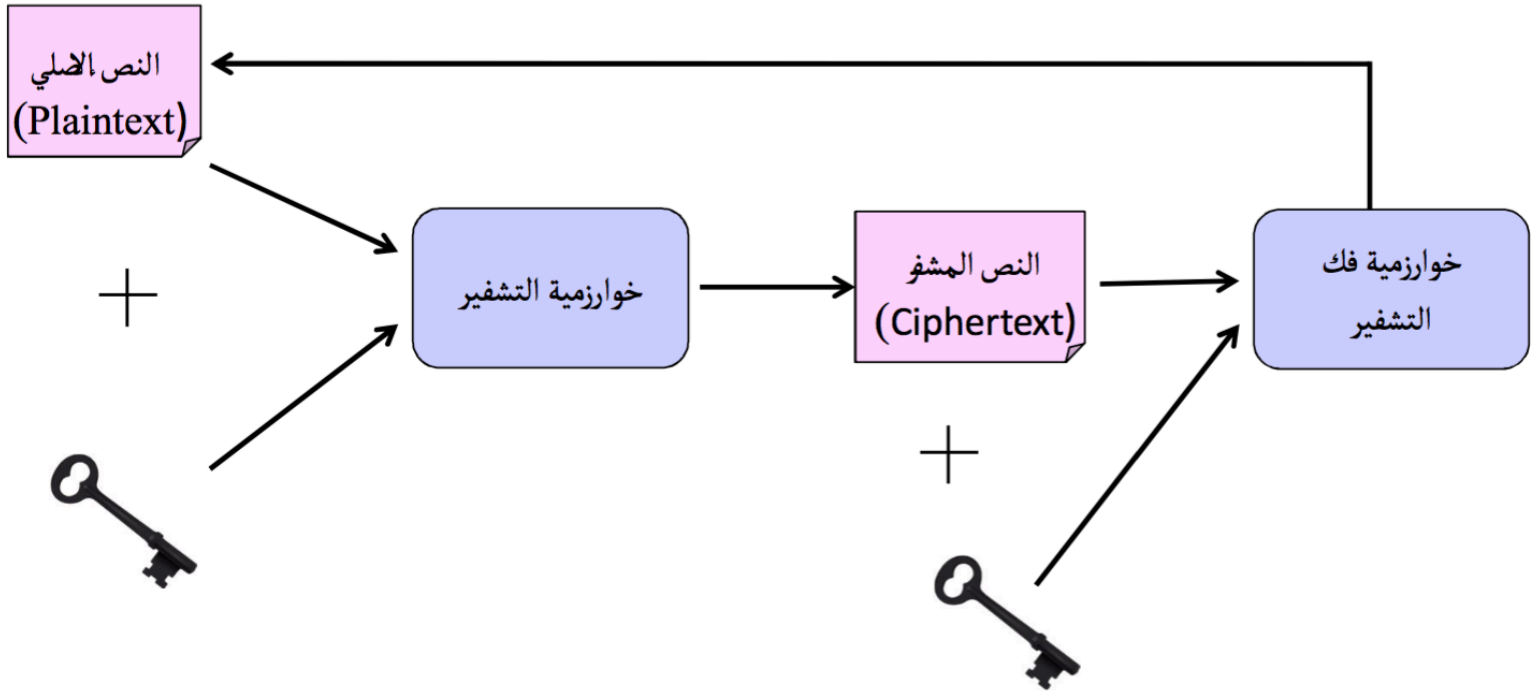
متطلبات عملية التشفير

- **مفتاح التشفير** : معادلة حياكة لغز تشفير البيانات
- **خوارزمية التشفير** : إجراءات عملية التشفير وتسلسلها
- **مفتاح فك التشفير** : معادلة فك لغز التشفير
- **خوارزمية فك التشفير** : إجراءات فك التشفير وتسلسله

بما أنّ التشفير يحول المعلومات إلى مجموعة غير منظمة من الأحرف والرموز، فإنّ المعلومات تبقى سرية سواء أثناء تخزينها أو انتقالها داخل النظام وبالتالي حتى لو تمكنت الأطراف غير المشروع لها من الوصول إلى تلك المعلومات فهي لن تتمكن من قراءتها

عملية التشفير وفك التشفير

- عملية التشفير :تحويل النص الأصلي الذي يسمى Plaintext إلى كتابات غير مفهومة تسمى Ciphertext
- عملية فك التشفير (Decryption) : تحويل النص المشفر إلى النص الأصلي



قوة التشفير

تتحدد قوة أي نظام تشفير من خلال ثلاثة عوامل أساسية:

- طول المفتاح
- سياسات إدارة المفتاح
- طبيعة خوارزمية التشفير

قوة التشفير

- **طول المفتاح**: توفر المفاتيح الطويلة عادة تشفيراً أقوى وذلك من خلال تقليل عدد المجموعات المتكررة للنص المشفّر، وهذا يجعل من الصعب أن يتم اكتشاف نماذج في النص المشفر لتعكس نماذج في النص غير المشفر الأصلي

مثال: (The) هي من أكثر الكلمات ذات الثلاثة أحرف شيوعاً في اللغة الإنكليزية، وبما أنّ كل محرف في اللغة الإنكليزية يُمثَّل بشيفرة طولها ٨ بت فإن مفتاح تشفير طوله ٢٤ بت سيولد نص مشفر في مجموعات تُمثل كل منها ثلاثة محارف متتابعة. يُعتبر مثل هذا المفتاح القصير ضعيفاً لأنه يوفر فرصة لتحديد المجموعات المتكررة عادة للنص المشفر التي من المرجح أن تُمثِّل كلمات شائعة وبالتالي تمكّن المحلل من فك رمز التشفير

قوة التشفير

- **سياسات إدارة المفتاح**: تعتبر الإجراءات المستخدمة في تخزين وإدارة مفاتيح التشفير على درجة كبيرة من الأهمية، فمهما كانت خوارزمية التشفير قوية فإنه بمجرد الوصول إلى المفاتيح فإن التشفير يمكن أن يتم فكه بسهولة
  - مفاتيح التشفير يجب أن لا تخزن على الحواسيب التي تستخدمها
  - الاحتفاظ بنسخ من المفاتيح في مواقع آمنة
- **طبيعة خوارزمية التشفير**: الخوارزمية القوية من الصعب –إن لم يكن من المستحيل– اكتشافها باستخدام تقنيات تجريب كل الاحتمالات (Brute-Force Guessing)، والسرية ليست ضرورية للقوة، فالإجراءات المستخدمة من قبل خوارزميات التشفير الشائعة الاستخدام والأكثر قبولاً متاحة للجميع، لأنّ قبولها ليس ناتجاً عن كون هذه الإجراءات سرية وإنما لكون أنّ هذه الإجراءات تمّ اختبارها بشكل دقيق

أنواع نظم التشفير

- **نظم التشفير المتناظرة**: تستخدم **نفس المفتاح** في عملية التشفير وفك التشفير
- **نظم التشفير غير المتناظرة**: تستخدم نوعين من المفاتيح هما **المفتاح العام** (Public Key) المتاح للجميع **والمفتاح الخاص** (Private Key) الذي يبقى سرياً ومعروفاً فقط لمالك زوج المفاتيح
- يمكن أن يتم استخدام المفتاح العام أو الخاص في عملية التشفير غير المتناظر ولكن المفتاح المقابل وحده يمكنه أن يفك تشفير النص المشفّر وبالتالي فإنّ المعلومات التي تم تشفيرها بواسطة المفتاح الخاص يمكن أن يتم فك تشفيرها فقط بواسطة المفتاح العام المقابل، وبشكل مماثل فإنّ المعلومات التي تم تشفيرها بواسطة المفتاح العام يمكن أن يتم فك تشفيرها فقط بواسطة المفتاح الخاص المقابل

التشفير المتناظر

يعتبر التشفير المتناظر أسرع من التشفير غير المتناظر ولكنه يمتلك مشاكل عديدة :

- المفتاح السري المشترك يجب أن يكون معروفاً لكل من المرسل والمرسل له (كلا الطرفين يحتاج لطريقة آمنة لتبادل المفتاح)
- الحاجة إلى ابتكار مفاتيح سرية منفصلة مع كل طرف مختلف سيتم استخدام التشفير معه، وإلا فإنّ أي شخص يمتلك المفتاح السري العام سيتمكن من فك تشفير أي وثائق مشفرة تمكن من الوصول إليها (بشكل مقصود أو غير مقصود) . إلى جانب أنّ النمو في عدد المفاتيح السرية المطلوبة سيخلق صعوبة في إدارتها وخاصة إذا كان التشفير مطلوباً مع الآلاف من الأطراف الأخرى
- لا يوفر إمكانية إنشاء اتفاقيات ملزمة قانونياً : عند استخدام التشفير المتناظر فإنه يتوجب على كلا الطرفين معرفة المفتاح السري نفسه، وبالتالي ليس هناك من طريقة لإثبات من قام بتوليد مستند معين، فكل طرف يمكن أن يدّعي أنّ الطرف الآخر استخدم المفتاح السري المشترك

التشفير غير المتناظر

تحل نظم التشفير غير المتناظرة المشاكل الثلاثة السابقة:

- معرفة المفتاح العام لا تشكل أهمية كبيرة لأن أي نص مشفّر عن طريقه يمكن أن يتم فك تشفيره عن طريق استخدام المفتاح الخاص المقابل فقط، ولهذا السبب يمكن أن يتم توزيع المفتاح العام عن طريق البريد الإلكتروني أو حتى يمكن أن يتم تقديمه على موقع الويب، وبالتالي بإمكان أي شخص أن يُرسل معلومات مشفرة إلى مالك المفتاح الخاص
- يمكن لعدد كبير من الأطراف أن يستخدموا المفتاح العام نفسه لإرسال الرسائل المشفرة لأنّ مالك المفتاح الخاص المقابل فقط يمكنه أن يفك تشفير تلك الرسائل
- إمكانية خلق اتفاقيات إلكترونية ملزمة قانونياً: بما أن المفتاح الخاص معروف من قبل طرف واحد فقط، بالتالي فإنّ مرسل الرسالة يمكن أن يتم توثيقه كمالك المفتاح الخاص من قِبل أي شخص يفك تشفير الرسالة بالمفتاح العام

التشفير غير المتناظر

- العيب الرئيسي في نظم التشفير غير المتناظرة هي السرعة، فهي أبطأ بآلاف المرات من التشفير المتناظر وبالتالي من الصعب استخدامها في تبادل كميات كبيرة من البيانات

- تعتمد الأعمال التجارية الإلكترونية عادةً على كلا النوعين من أنظمة التشفير: تستخدم التشفير المتناظر لمعظم البيانات المتبادلة والتشفير غير المتناظر لعملية إرسال مفتاح التشفير المتناظر للمرسل له ليستخدمه في فك تشفير النص المشفّر

جامعة دمشق
كلية الاقتصاد
مجموعة كلية الاقتصاد في جامعة دمشق :
https://m.facebook.com/groups/faculty.economic/
قناة التلغرام : https://t.me/ecodamas

نظم المعلومات المصرفية

السنة الرابعة– قسم المصارف والتأمين

د. ليدا بركات

المحاضرة الخامسة

التوقيع الإلكتروني

(محاضرة من خارج النوطة)

خطة العرض

- التقطيع
- التوقيع الإلكتروني
- الشهادة الرقمية

التقطيع
Hashing

- العملية التي يتم من خلالها تحويل النص الأصلي (Plaintext) إلى رمز قصير ذات طول ثابت يدعى Hash

- خوارزميات التقطيع الأكثر استخداماً: MD5 و SHA_1
  - خوارزمية MD5 تنتج مقطعاً (Hash) طوله ١٢٨ بت من الرسالة الأصلية
  - خوارزمية SHA_1 تنتج مقطعاً طوله ١٦٠ بت

التقطيع

- تختلف عملية التقطيع عن التشفير في جانبين أساسيين:

عملية التشفير	عملية التقطيع
ينتج عن عملية التشفير نص مشفر مساوي في الطول للنص الأصلي	ينتج عن عملية التقطيع Hash قصير ذات طول ثابت بغض النظر عن طول النص الأصلي
قابلة للعكس	غير قابلة للعكس

التوقيع الإلكتروني
Digtial Signature

- يُستخدم التوقيع الإلكتروني للتأكد من سلامة البيانات المرسلة في المعاملات الإلكترونية وللتأكد من هوية الأطراف المتعاملة

- يتم توليد التوقيع الإلكتروني باستخدام التشفير غير المتناظر وخوارزمية التقطيع

- توليد التوقيع الإلكتروني لا يعتمد عادةً على تشفير الوثيقة بكاملها بواسطة المفتاح الخاص (نظراً لبطء التشفير غير المتناظر)، عوضاً عن ذلك يتم إخضاع الوثيقة أولاً لخوارزمية التقطيع والمقطع (Hash) الناتج يتم تشفيره باستخدام مفتاح المرسل الخاص لتوليد التوقيع الإلكتروني

التوقيع الإلكتروني

- **تعريف التوقيع الإلكتروني**: معلومات تم إخضاعها لخوارزمية التقطيع ومن ثم تشفيرها بواسطة المفتاح الخاص بحيث يمكن أن يتم فك تشفيرها فقط باستخدام المفتاح العام المقابل

- فك التشفير الناجح للرسالة بواسطة المفتاح العام يُثبت أنّ الرسالة قد تم إنشاؤها باستخدام المفتاح الخاص المرافق، وبما أنّ المفتاح الخاص معروف فقط من قِبل مالكه فإن الكيان المالك لزوج المفاتيح الخاصة والعامة هو وحده استطاع أن يخلق تلك الرسالة

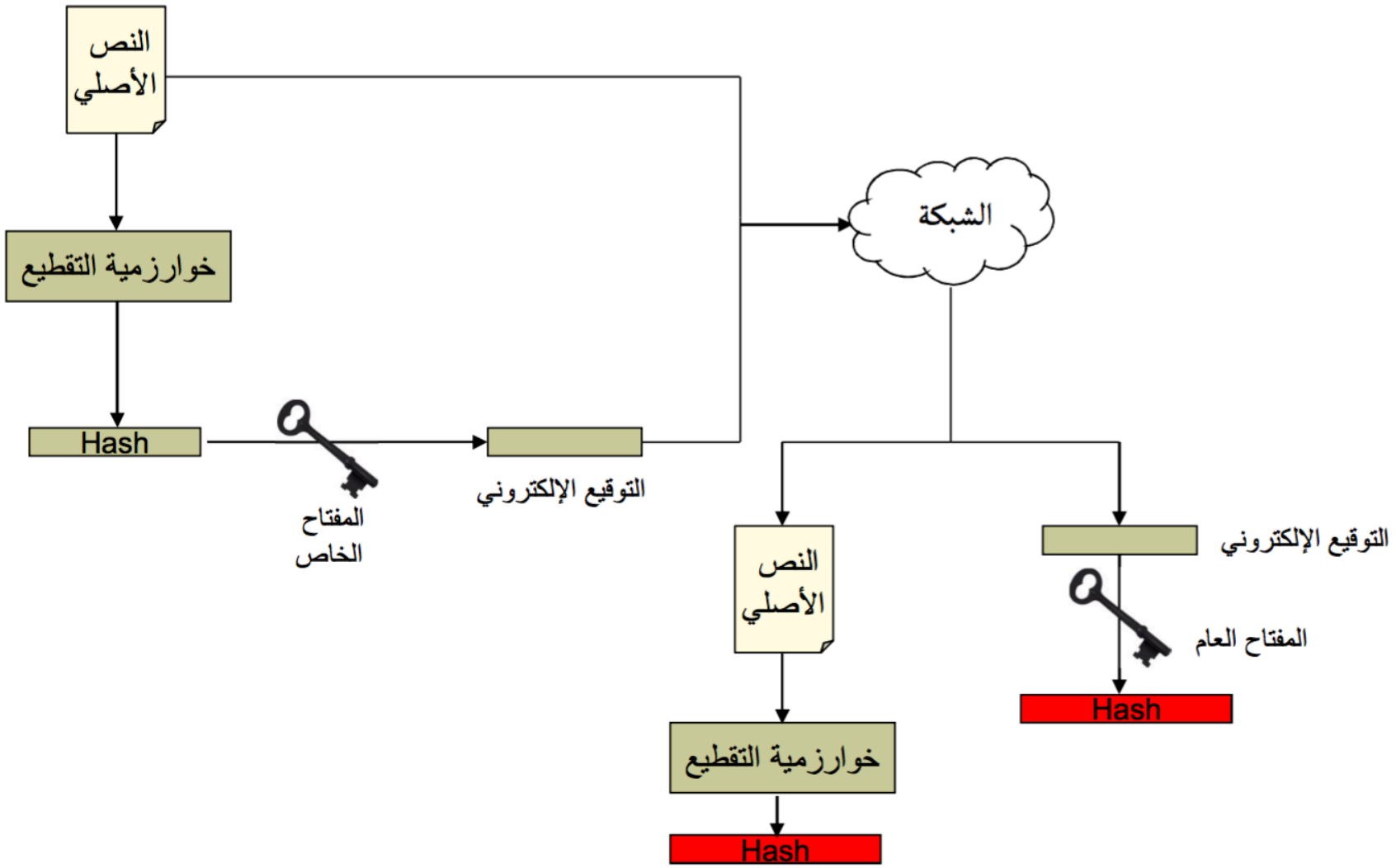
خطوات توليد التوقيع الإلكتروني

- يتم إخضاع الرسالة الأصلية غير المشفرة لخوارزمية التقطيع والتي ينتج عنها ما يسمى بملخص الرسالة (تمثيل محرفي مميز للبيانات) يُطلق على هذا الملخص بـ Hash

- يتم تشفير ملخص الرسالة بواسطة المفتاح الخاص للحصول على التوقيع الإلكتروني الذي يُرسل مع الرسالة، بحيث يحصل المرسل له على كل من الرسالة وملخص الرسالة المشفّر

- يقوم المرسل له بفك تشفير ملخص الرسالة، حيث يُساعد الاستخدام الناجح للمفتاح العام في فك تشفير ملخص الرسالة في إثبات أنّ الرسالة قد تمّ خلقها من قبل الكيان المالك للمفتاح الخاص المقابل، وبالتالي فإنّ هوية المرسل يمكن أن تُعرف وتُربط برسالة معينة

استخدام التوقيع الإلكتروني للتأكد من سلامة البيانات



استخدام التوقيع الإلكتروني للتأكد من سلامة البيانات

- تساعد عملية التقطيع المستخدمة في توليد التوقيع الإلكتروني في إثبات أنّ الرسالة التي قام المرسل له بفك تشفيرها هي تماماً نفس الرسالة المنشأة من قبل المرسل، لأنّ خوارزمية التقطيع تستخدم كل بت في النص الكامل الأصلي لحساب قيمة المقطع، وبالتالي فإنّ تغيير أي محرف في المستند الذي تم إخضاعه لعملية التقطيع (مثلاً استبدال ١ بـ ٧) سينتج عنه قيمة مختلفة للمقطع، وهذه الخاصية المميزة لخوارزميات التقطيع توفر إمكانية التحقق من أنّ محتويات الرسالة لم يتم تغييرها

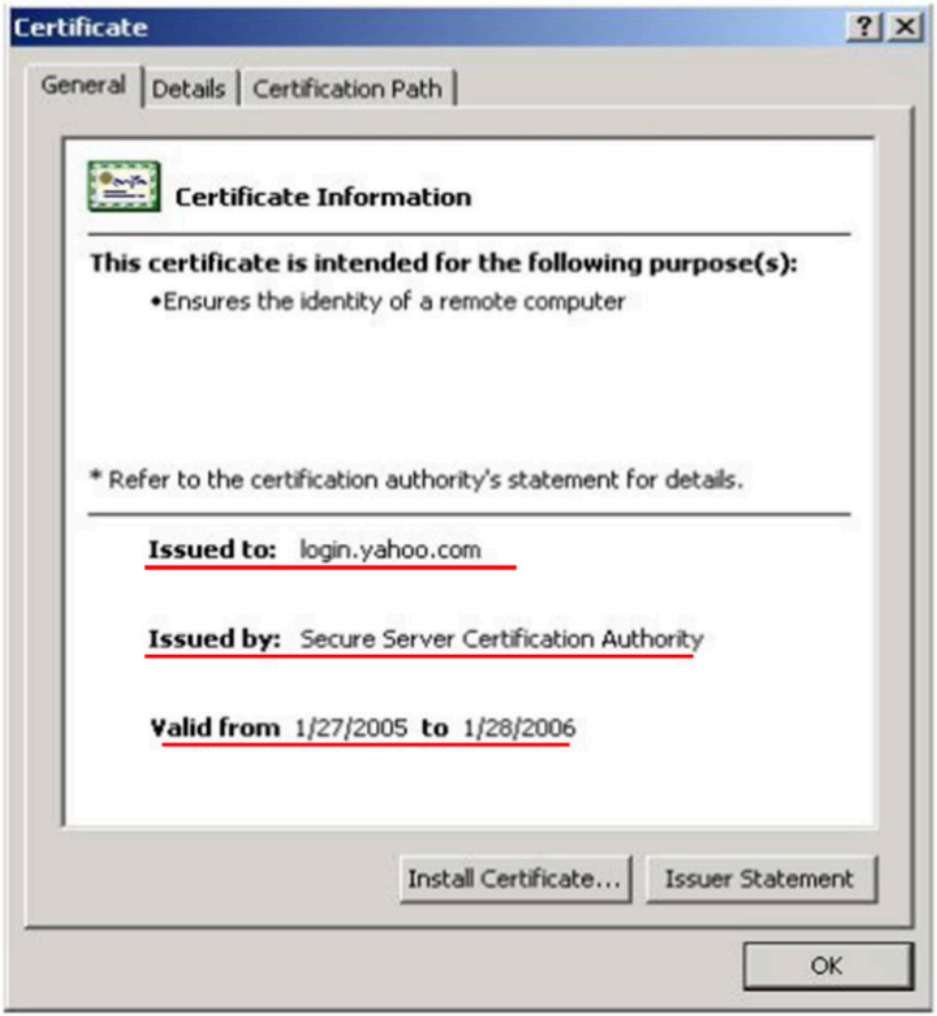
- للتحقق من سلامة البيانات، يقوم المرسل له بفك تشفير ملخص الرسالة، ويُخضع الرسالة لخوارزمية التقطيع مرة أخرى، وفي حال تطابق ملخص الرسالة الناتج مع الملخص المرسل مع الرسالة، فإنّ ذلك يُثبت أنّ الرسالة لم يتم تعديلها وبالتالي ضمان كمال وسلامة المعلومات (يمكن تحقيق سرية المعلومات عبر تشفير الرسالة نفسها)

الشهادة الرقمية
Digtial Certificate

- كيف يمكن للمستلم أن يتأكد من هوية الكيان المالك للمفتاح الخاص المقابل؟ على سبيل المثال، كيف يمكن للعميل أن يتأكد من أنّ الملف المدّعى بكونه مرسلاً من قبل المصرف قد تمّ فعلاً إنشاؤه من قِبل ذلك المصرف وليس من قبل شخص آخر استطاع أن ينسخ زوج المفاتيح (الخاصة والعامة)؟ وكيف يحصل المرسَل له على المفتاح العام للمرسِل؟

الإجابة على هذه الأسئلة تتضمن استخدام الشهادات الرقمية (Digital Certificates)

الشهادة الرقمية



- مستند رقمي مُنشأ وموقع إلكترونياً من قِبل طرف ثالث موثوق هو عادةً الوكالة المسؤولة عن الشهادات وذلك بواسطة المفتاح الخاص لتلك الوكالة، حيث يُصادق هذا المستند على هوية الطرف الذي تمثله الوكالة، ويحوي المفتاح العام للطرف الممثَّل

الشهادة الرقمية

- يمكن أن يتم تخزين الشهادات الرقمية على مواقع الويب حيث يتم تصميم المتصفحات (Browsers) للحصول أوتوماتيكياً على نسخة من تلك الشهادة الرقمية واستخدام المفتاح العام المحتوى فيها للتواصل مع موقع الويب (توفرّ الشهادات الرقمية أسلوباً آلياً للحصول على المفتاح العام للمنظمة أو لشخص معين)

- تقوم الوكالة المسؤولة عن الشهادات بتقطيع المعلومات المخزنة على الشهادة الرقمية ثمّ تقوم بتشفير ذلك المقطع الناتج بواسطة مفتاحها الخاص وتُلحق التوقيع الإلكتروني الناتج بالشهادة الرقمية بما يوفر وسيلة للمصادقة على موثوقية الشهادة