محاضرة رقم 5: أمن المعاملات الالكترونية

مقدمة:

حملت لنا الانترنيت فوائد كثيرة وأصبحت وسيلة سهلة وممتعة تتيح للملايين الولوج إلى كم هائل من المعلومات إضافة إلى التواصل وتبادل المعلومات و الرسائل فيما بينهم ولكن صاحب هذه الفوائد الجمة انتشار العديد من الجرائم و الاختلافات عبر الشبكة مما أدى إلى ضعف الثقة لدى الأفراد ومن الممارسة التجارية عبر الانترنيت . والجرائم التي ترتكب في عالم الانترنيت و التجارة الإلكترونية لا تختلف كثيرا عن الجرائم التقليدية من حيث الهدف النهائي وهو الاستيلاء على المال بطريقة غير قانونية سواء بالغش أو السرقة.

أمن المعاملات الإلكترونية:

وهي مجموعة من المعايير والأنظمة والتي توفر السرية والأمن والخصوصية لتعاملات التجارة الالكترونية، والمتمثلة فيما يلي:

1/التشفير: وهو من وسائل حفظ سرية المعلومات لاسيما في التجارة الإلكترونية. و يعد ا من وسائل حفظ وسرية المعلومات في نطاق الأنظمة الإلكترونية حيث يهدف إلى منع الغير من التقاط الرسائل أو المعلومات ومن ثم منع وصولها أو وصولها مشوهة إلى الطرف الآخر في المعاملة التجارية. حيث يعرَّف التشفير بأنه : **عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة.**

- **طرق التشفير**: يتم تقسيم طرق التشفير بناء على معيار المفتاح المستخدم إلى:

- ✓ **الطريقة الأولى (طريقة المفتاح المتماثل):** في التشفير المتماثِل، يستخدم كل من المرسِل والمستقبِل **المفتاحَ السري ذاته** في تشفير الرسالة وفك تشفيرها، كما يتفق الطرفان في البداية على عبارة المرور التي سيتم استخدامها. ويمكن أن تحوي عبارة المرور حروفاً كبيرة أو صغيرة أو رموزا أخرى. وبعد ذلك، تحوِّل برمجيات التشفير عبارةَ المرور إلى عدد ثنائي، ويتم إضافة رموز أخرى لزيادة طولها. ويشكِّل العدد الثنائي الناتج مفتاح تشفير الرسالة. وبعد استقبال الرسالة المُشفَّرة، يستخدم المستقبِل عبارةَ المرور نفسها من أجل فك شيفرة النص المُشفَّر إذ تترجِم البرمجيات مرة أخرى عبارةَ المرور لتشكيل المفتاح الثنائي (binary key) الذي يتولى إعادة تحويل النص المُشفَّر إلى شكله الأصلي المفهوم.
- ✓ **الطريقة الثانية (طريقة المفتاح اللامتماثل):** ظهر نظام المفتاح اللامتماثل بغرض معالجة نقائص نظام التشفير بالمفتاح المتماثل والمتمثلة في تعرض المفتاح إلى أخطار أمنية أثناء تبادله، فبفضل نظام المفتاح اللامتماثل أصبح من الممكن تجنب هذه الأخطار عن طريق تشفير البيانات باستخدام المفتاحين هما:
  - **المفتاح العام:** ويكون معروفا لدى شريحة كبيرة من الأشخاص الراغبين في مراسلة المستقبل والتعامل معه.
  - **المفتاح الخاص:** هو مفتاح شخصي جدا خاص بالمرسل إليه وغير معروف لدى أي شخص آخر، ويحتكر صاحبه حق استخدام هذا المفتاح في فك شفرة الرسائل التي يستقبلها.

2/البصمة الإلكترونية: وهي بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تدعى دوال إذ تطبق هذه الخوارزميات حسابات رياضية على الرسائل لتوليد بصمة " سلسلة صغيرة " تمثل ملفا كاملا أو رسالة "سلسلة كبيرة" أو تدعى البيانات الناتجة عن البصمة الإلكترونية للرسالة .

3/التوقيع الالكتروني: هو وسيلة مأمونة لتحديد هوية الشخص الذي قام بالتوقيع و ذلك بعد إتباع إجراءات معينة ، يمكن التأكد بواسطة الحاسوب من أن من قام بالتوقيع هو صاحب بطاقة السحب مثلا. فهو علامة شخصية يمكن عن طريقها تمييز هوية الموقع أو شخصيته ،والعلة في الحاجة إلى التوقيع الإلكتروني ،سببها اعتبارات الأمن والخصوصية على شبكة الانترنيت ،لاسيما في مجال التجارة الإلكترونية والذي من خلاله كذلك يمكن التحقيق من أن صاحب الرسالة أو المعاملة هو الشخص الذي قام فعلا بإرسالها أو تنفيذها.

❖ **صور التوقيع الالكتروني:** التوقيع الإلكتروني هو عبارة عن وحدة قصيرة من البيانات تحمل علامة رياضية مع تلك البيانات الموجودة في الوثيقة ، و له صورتان :

- **التوقيع الرقمي الكودي:** و يستخدم هذا النظام في التعاملات البنكية والمعاملات المالية، وأوضح مثال على ذلك بطاقة الإئتمان التي تحتوي على –رقم سري– لا يعرفه سوى صاحب البطاقة الذي يدخل بطاقته في مكنة السحب، حين يطلب الاستعلام عن عن حسابه أو صرف جزء من رصيده.
- **التوقيع بالقلم الإلكتروني:** ويتم ذلك التوقيع عن طريق استخدام قلم إلكتروني حسابي يمكن عن طريقه الكتابة على شاشة الكمبيوتر، وذلك عن طريق استخدام برنامج خاص، ويقوم هذا البرنامج بوظيفتين الأولى وهي خدمة التقاط التوقيع والثانية خدمة التحقق من صحة هذا التوقيع. وهذا النوع من التشفير يطلق عليه **التشفير البيومتري**، وهو طريقة من طرق التحقق من الشخصية، عن طريق الاعتماد على الخواص الفيزيائية والطبيعية والسلوكية للأفراد.

4/الشهادات الرقمية digital certificats: وتصدر هذه الشهادات من طرف الجهات المانحة الموثوق بها التي توقع عليها وتستخدم التحقق من موثوقية المفاتيح العامة التي أصدرت. ومن المعلومات الواجب توافرها في الشهادة :الاسم ،رقم التعريف ،عنوان البريد الإلكتروني ،تاريخ انتهائها ،الرقم التسلسلي ، وتوقع عليها بالمفتاح العام لطالب الشهادة وبالمفتاح الخاص للجهة المانحة للشهادة ويمكن أن ترسل الجهة المانحة الشهادة إلى طالبها أو تنشرها على العموم أو تحتفظ بها في خادم الشهادات "قاعدة بيانات تسمح بتسليم واسترجاعه الشهادات الرقمية".

بروتوكولات الأمن و الحماية

❖ **بروتوكول الطبقات الأمنية SSL (Secure Sockets Layer):** هو برنامج به بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الإنترنت بطريقة آمنة بحيث لا يمكن لأيّ شخص قراءتها غير المرسل والمستقبل وفي نفس الوقت تكون قوة التشفير فيها قوية ويصعب فكها، ويقوم هذا البرنامج بربط المتصفح الموجود بحاسوب المستخدم بالحاسوب المزود (الخادم) الخاص بالموقع المراد الشراء منه، وهذا طبعاً إذا كان الحاسوب الخادم مزود بهذه التقنية، ويقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح وصولاً إلى الحاسوب الخادم الخاص بالموقع بإستخدام بروتوكول التحكم بالإرسال وبروتوكول الإنترنت TCP/IP.

❖ **بروتوكولات الحركات المالية الآمنة :** إن هذه تقنية تعتبر احد بروتوكولات تطبيقات الانترنت و التي تم تطبيقها من طرف الشركتين فيزا و ماستر كارد كطريقة أمنة لإجراء المعاملات و التحويلات المالية عبر الانترنت .