بروتوكول الطبقات الأمنية

SSL

(Secure Sockets Layer)

مقدمة:

الحمد لله الذي هدانا وما كنا لنهتدي لولا أن هدانا الله والصلاة والسلام على أشرف خلق الله أجمعين محمد بن عبد الله خاتم الرسل والنبيين (صلى الله عليه وسلم):

يا رب صلي على النبي المصطفى ما غردت في الأيك ساجعة الربا
يا رب صـــلي على النـــبي وآله ما أمـــت الزوار مســـجد بثربا
صلوا على من تدخلـــون بهديه دار الســـلامة تبتغون المـــطلبا
صلـــوا على من ظللته غمامـــة والجزع حن له وناصر في الصبا

****

يا أيها الراجـــون خير شفاعـــة من أحـــمد صلوا عليه وسلموا
وعلى قرابته المقـــرر فضلـــهم وعلى صحابته الذين هموا هموا
جادوا علوا سادوا هدوا فهموا على الســـت الجـــهات الأنجـــم
والتابعين لهم بإحســـــــان فهم نقلوا لمـــا حفظـــــوه منهم عنهم

لقد زال بالشك اليقين، وتناثرت من خلفه حقب السنين، وما كان صعباً قد صار سهلاً ، فمن شاء أن يعلم فإني خلفه ومن عاف ذلك فهذا شأنه ولا يعنين. وأسأل الله أن يرفعنا وإياكم الى قمم المعارف وينصرنا على من عادانا من المتكبرين الهـــائمين الضائعين وأن يجعلنا من عباده المخلصين .... آآآآمييين.....

تمهيد:

قد يكون هناك من يتلصص عند نقل البيانات من خلال قنوات الاتصال.

يمكن أن تكون هذه البيانات لها وضع خاص بالنسبة للمستخدم مثل بطاقات الائتمان أو ذات سرية خاصة مثل طريقة عمل منتج خاص،

عندما تريد منع الغرباء من قراءة البيانات الخاصة بك فلابد من استخدام تشفير البيانات.

برنامج تشفير البيانات يقوم بتغيير شكل البيانات بطريقة معينة خلال قنوات الاتصال ثم يطلب من المستقبل بعض البيانات مثل (كلمة المرور) حتى يقوم بفك الشفرة ووضع الملف إلى شكله الأصلي.

ما هو التشفير:

إذاً التشفير هو تغيير صيغة الملف حتى لا يمكن الاستفادة منه أو معرفة محتواه اذا وقع في يد أي مجهول ولكن بالامكان ذلك بالنسبة للشخص الذي يعرف مفتاح الشيفرة التي تم بها تغيير الملف. ولمزيد من التعريف علينا أن نتحدث عن البروتوكول المختص بمثل هذه الأشياء (بروتوكول الطبقات الأمنية).

طوَّرت شركة نتسكيب بروتوكول الطبقات الأمنية لتأمين نقل آمن للمعلومات بين خادم الويب ومستعرِضات الويب. ويعتمد هذا البروتوكول على خوارزمية المفتاح العام (**public key**) والمفتاح الخاص (**private key**)، إذ يزوِّد الخادمُ المستفيدَ بالمفاتيحَ العامة، وتُستَخدَم هذه المفاتيح العامة في تشفير الرسائل المتَّجِهة إلى الخادم، ولا يمكن استخدام المفتاح العام لِفك شيفرة الرسالة التي شَفَّرها، إذ يتفرَّد المفتاح الخاص (لدى الخادم) بالقدرة على فك شيفرة الرسالة التي شفَّرَها المفتاح العام.

ويستطيع المستفيد (**client**) بالطريقة ذاتِها إنشاء زوج من المفاتيح العامة| الخاصة لإرسال المعلومات إلى الخادم. وتمنع هذه الطريقة ظهور مشاكل الاتصال مثل التجسُّس أو التنصُّت (**eavesdropping**) عند كشف المعلومات الحسّاسة (مثل: البيانات الشخصية، وأرقام بطاقات الائتمان (**credit card**)) ضمن أحد مواقع الويب.

ويُساعِد بروتوكول الطبقات الأمنية (**SSL**) في التحقُّق من المفتاح العام الذي أصدره الخادم، ويتأكَّد من عدم تغيُّر المعلومات أثناء النقل، وذلك باستخدام الشهادات الرقمية (**digital certificates**) التي سنتحدَّث عنها في الفقرات التالية.

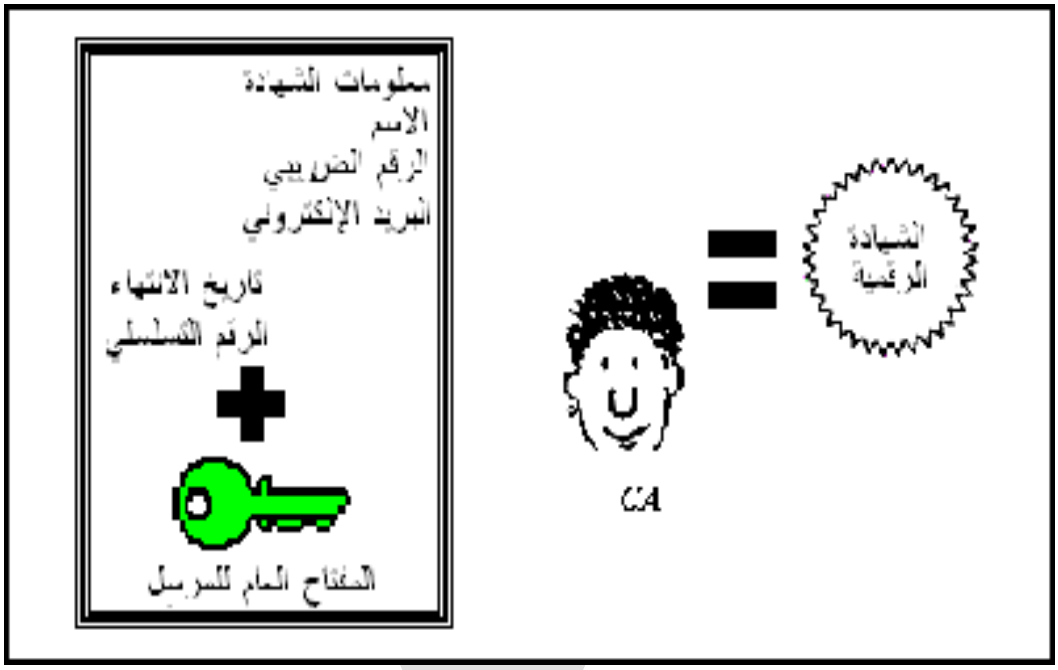
الشهادات الرقمية ﴿Digital Certificates﴾

تصدُرُ الشهادات الرقمية عن الجِهات المانحة (**certificate authorities- CA**) الموثوق بها التي توقِّع عليها، وتُستَخدَم هذه الشهادات للتحقُّق من موثوقية المفاتيح العامة التي أُصدِرَت.

وفي البداية، يقوم شخص (أو شركة) بتوليد زوج من المفاتيح العامة|الخاصة، ثم يُرسَل المفتاح العام إلى جهة مانحة للشهادة (**CA**). وتُضيف الجهة المانحة (**CA**) بعضَ المعلومات المتعلِّقة بالشهادة (مثل: الاسم، ورقم التعريف (**ID No.**)، وعنوان البريد الإلكتروني (**Email address**)، وتاريخ الانتهاء (**expiration date**)، والرقم التسلسُلي (**serial no.**))، وتُوقِّع عليها بالمفتاح العام لطالب الشهادة، وبالمفتاح الخاص للجهة المانحة للشهادة (**CA**). ويصادِق توقيع الجهة المانحة للشهادة (**CA**) على المعلومات المُضافة إلى الشهادة وعلى المفتاح العام الموجود ضمن الشهادة. ويمكن أن ترسِل الجهةُ المانحةُ الشهادةَ إلى طالبها، أو تنشرَها للعموم، أو تحتفظَ بها في خادم الشهادات (**certificate server**) (قاعدة بيانات تسمح بتسليم واسترجاع الشهادات الرقمية).

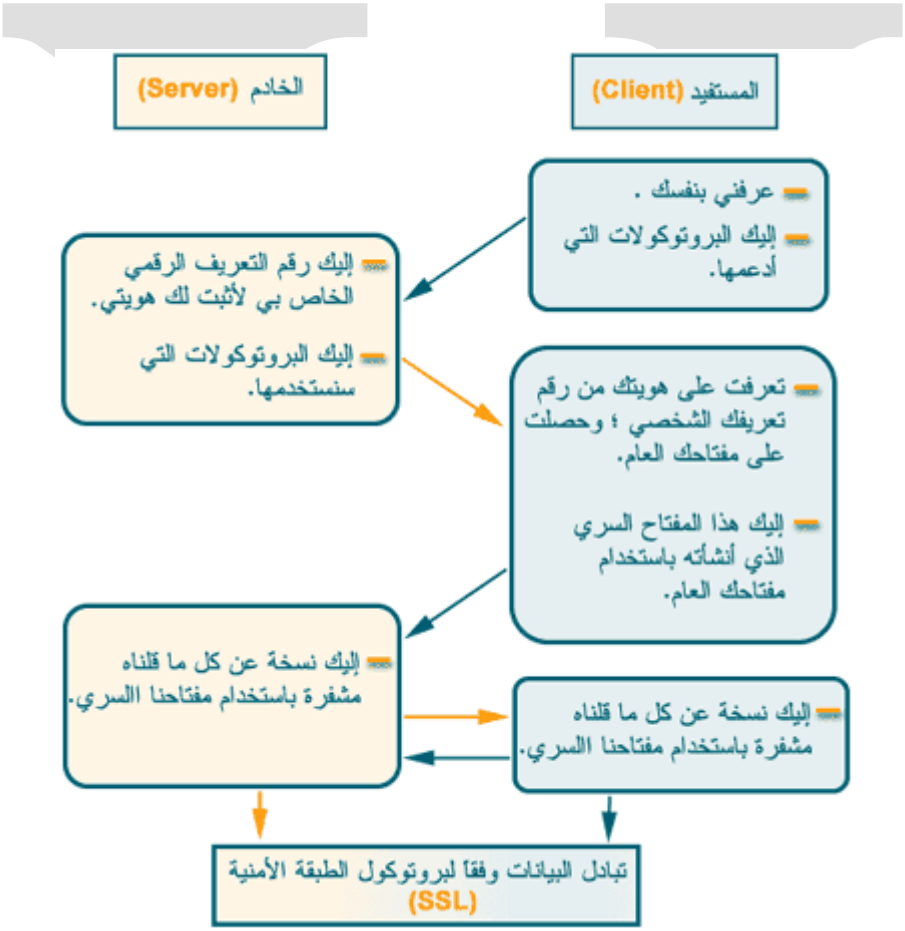
ولِفكّ شيفرة الوثيقة المصدَّقة رقمياً (**digitally certified document**)، تستخدِم البرمجياتُ في الطرف المستقبِل المفتاحَ العام للجهة المانحة للشهادة (**CA**)، فإن نجحت عملية فك شيفرة الشهادة، فإن ذلك يعني أن الجهة المانحة التي وقَّعت الوثيقة هي التي أنشأتها بالفعل. وتستطيع البرمجياتُ في الطرف المستقبِل أيضاً فحصَ جميع معلومات الشهادة المتعلِّقة بمالكها، مما يُمكِّن المستقبِل من الحصول على المفتاح العام للمالك (من الشهادة) للتحقّق من توقيع المرسِل، فإن تمكَّن هذا المفتاح العام المُصدَّق من

فـك شـيفرة توقيـع المرسِـل، يـصبح المـستقبِل علـى ثِقـةٍ بـأن التوقيـع أُنـشِئ باستخدام المفتاح الخاص للمالك.



ينُـشئ المـستفيد اتـصالاً بخـادم آمـن (**secure server**). ويُميَّـز الخادم الآمن بإلحاق حـرف "**s**" بنهايـة اسـم البروتوكـول ضـمن عنـوان محـدِّد المـصدر (**URL**) (مـثلاً: **https://server.com**)، وبعـد إنـشاء الاتـصال، يبـدأ المـستفيد جلـسةَ المـصافحة (**SSL handshake session**)، وذلك بإرسال رسالة أو عبـارة ترحيـب (**client hello**) إلى الخادم تستفسر عن هوية الخادم وتخبره بقدرات التشفير لـدى المستفيد. ويـرُدُّ الخادم برسالة أو عبارة ترحيب (**server hello**)، وإرسال شهادته الرقمية وبعض قوائم خوارزميات التشفير. ويقـوم المـستفيد بفحـص الـشهادة الرقميـة للخادم، وذلك للتحقّق من أنها قد صدرت عن جهـة مانحـة (**CA**) معتَمَـدة. ويقـوم المـستفيد أيـضاً بِفحـص معلومـات الـشهادات الرقميـة واسـم الخـادم والمفتاح العام. وبعد تحقُّق كل طرف من الطرف الآخر، يتَّفِق الخادم والمستفيد

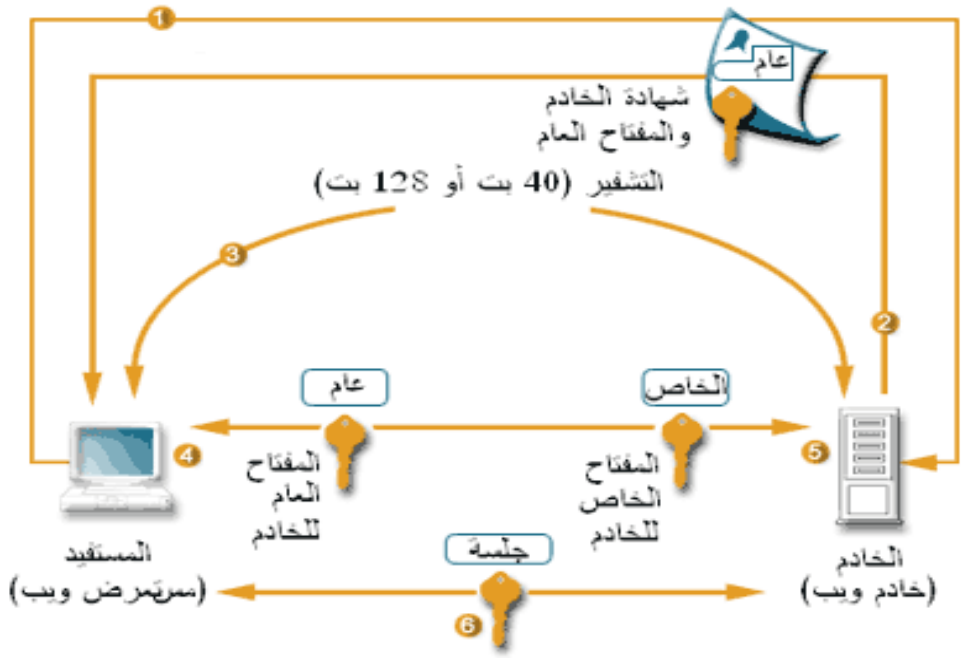
على معيار التشفير الذي سيُستَخدَم في جلسة تبادُل البيانات وفقاً لبروتوكول الطبقات الأمنية (**session SSL data exchange**).



المصافحة في جلسة بروتوكول الطبقات الأمنية Handshaking protocol

كيف يعمل بروتوكول الطبقات الأمنية «SSL»؟

وبعد الانتهاء من جلسة المصافحة في بروتوكول الطبقات الأمنية (SSL)، يولِّد المستفيد مفتاحاً سرياً للجلسة، ويشفِّره باستخدام المفتاح العام للخادم، ثم يفكّ الخادمُ شيفرةَ مفتاح الجلسة باستخدام مفتاحه الخاص. ويستخدِم كل من الخادم والمستفيد هذا المفتاح الفريد لتبادُل المعلومات الحساسة في جلسة بروتوكول الطبقات الأمنيّة. ولا يصلح هذا المفتاح الفريد إلا لجلسة واحدة فقط.



.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

راسلوني على بريدي التالي

Yahia2mee@yahoo.com

من خالص فجاني

يحيى