1.5 مقدمة :

في هذا الفصل يتم تناول التقنيات المستخدمة في بناء النظام وإستخراج الشهادات الرقمية وإستخدامها في التحقق من تكاملية وسرية بيانات المعاملات المصرفية.

2.5 ASP.NET (Active Server Pages):

هي عبارة عن آخر تطوير لإصدارات تكنلوجيا مايكروسوفت في برمجة صفحات الخادم النشطة .Active Server Pages - ASP. هي النسخة الجديدة من ASP المعروفة التي تشابه ال PHP، وقد جاءت لتحل مشكل وعيوب ال ASP ، ASP.NET تقدم دعماً برمجياً قوياً جداً، فمثلاً أصبح بمقدورك استخدام أي لغة برمجة تقريباً لتطوير هذا النوع من الصفحات [12].

1.2.5 الاختلافات بين ASP.net والASP:

1. ال ASP.NET هي الجيل الجديد من تقنية ال ASP كما ذكرنا؛ لكنها ليست تطويرا على ال ASP Classic بل هي تقنية جديدة بحد ذاتها حيث انها تعتمد على New Platform ألا و هي ال .NET Framework
2. ASP.NET هي نموذج جديد من ال.Server Side Scripting .
3. تعمل على visual studio [12].

2.2.5 مميزا ت الASP.NET :

1. دعم أقوى للغات البرمجة بكل تطبيقاتها ودعمها لل Object Oriented Programming.
2. دعم ال (XML(Extensible Markup Language .
3. برمجة الأحداث من خلال ال OOP .
4. كل مايتعلق بال User Authentication وال Roles .
5. Code Compile مما يزيد من كفاءة الأداء.
6. لا تدعم الASP بشكل كامل [12].

3.5 Visual Studio 2010 :

Visual Studioهي مجموعة كاملة من أدوات التطوير الصالحة لبناء تطبيقات الASP.NET وتطبيقات سطح المكتب "خدمات الويب لxml" وتطبيقات المحمول Visual C#،Visual C++، visual Basic يتسخدمون نفس بيئة التطوير المتكاملة (IDE) ، والتي تقوم بتمكين مشاركة الأداة وتسهل إنشاء حلول لغة مختلطة. بالإضافة إلى ذلك ، تستخدم هذه اللغات الوظيفية (NET Framework) ، والتي توفر الوصول إلى مفاتيح التقنيات التي تقوم بتبسيط تطوير تطبيقات ويب ASP وخدمات الويب لxml .

هي بيئة التطوير المتكاملة الرئيسية من مايكروسوفت. وهي تتيح برمجة واجهة المستخدم الرسومية والبرامج النصية إلى جانب (Windows form) وتطبيقات الويب وخدمات الويب مدعومة بمايكروسوفت ويندوز ووندوز موبايل (Windows Mobile) وإطار عمل الدوت نت (NET framework) ومايكروسوفت سيلفرلايت (Microsoft Silver light.) [14]. وهي مدعومة بتقنيات Entity Framework، ونظام Framework 4.0 NET [13].

1.3.5 تقنية الNET framework :

الNET Framework هو مكون تكاملي ل Windows يدعم إنشاء وتشغيل الجيل القادم من التطبيقات وخدمات XML للويب .تم تصميم ال NET Framework. لتلبية الأهداف التالية :

- توفير بيئة برمجية متناسقة كائنية التوجيه بغض النظر عن ما إذا كانت التعليمات البرمجية للكائن مخزنة وتنفذ محلياً، أو تنفذ محلياً ولكن موزعة على الإنترنت أو تنفذ عن بعد.
- توفير بيئة تنفيذ لتعليمات برمجية تقلل لأقصى حد تعارضات نشر وتعيين إصدارات البرامج.
- توفير بيئة تنفيذ للتعليمات البرمجية ترتقي بالتنفيذ الآمن للتعليمات البرمجية ، ما في ذلك التعليمات البرمجية التي تم إنشاؤها من قبل جهة خرجية غير معروفة أو شبه موثوق بها.
- توفير بيئة تنفيذ للتعليمات البرمجية تزيل مشاكل أداء البيئات النصية أو المفسرة.
- لجعل تجربة المطور متناسقة عبر أنواع من التطبيقات المختلفة على نطاق واسع، مثل التطبيقات المستندة إلى Windows والتطبيقات المستندة إلى الويب.
- إنشاء كل الإتصالات بمواصفات الصناعية القياسية للتأكد من أنه يمكن أن تتكامل التعليمات البرمجية التي تعتمد على الNET Framework. مع أي تعليمة برمجية أخرى.

2.3.5 مكونات الNET Framework. :

له مكونين رئيسيين :

1.2.3.5 وقت تشغيل اللغة العامة :

هو أساس ال NET Framework. أي أنه يمكن اعتبار وقت التشغيل كعامل يقوم بإدارة التعليمات البرمجية في وقت التنفيذ، ويوفر الخدمات الأساسية مثل: (إدارة الذاكرة ،الإتصال عن بُعد) ، بينما يفرض الأمان أيضاً وأشكال أخرى من دقة التعليمات البرمجية التي ترتقي بالأمان والمتانة .

2.2.3.5 مكتبة فئات NET Framework. :

يحتوي الفيجوال ستوديو على محرر أكواد يدعم تقنية (Intelligence) وإعادة كتابة الكود ، ويحتوي أيضاً على مترجم يكشف أخطاء وقت التشتغيل ومفسر يكشف الأخطاء الإملائية في الأكواد، كما يحتوي أيضاً على مصمم نماذج لبناء واجهة مستخدم رسومية ومصمم ويب ومصمم فئات ومصمم مخطط قواعد بيانات ومصمم لتقارير الكريستال.

يدعم الفيجوال ستوديو العديد من لغات البرمجة مثل : C++،C#، Visual basic ، Java script والعديد من لغات الترميز أيضاً مثل :xml ، html .

يحتوي فيجوال ستوديو على متعقب أخطاء تدعمه جميع اللغات المدعومة، يكشف أخطاء وقت التشغيل والأخطاء الاملائية ويسمح بوضع نقاط توقف عند سطور الكود والتي يتوقف البرنامج عن العمل عندما يصل لهذا السطر. يوجد أيضا في فيجوال ستوديو نافذة immediate window والتي تسمح بتجريب الدوال أثناء كتابتها [13].

4.5 لغة C# :

سي شارب (C#) أحد لغات بيئة الدوت نت لتطوير البرامج من إنتاج شركة مايكروسوفت يرمز إليها بالرمز c# وتنطق "سي شارب"، وهي إحدى اللغات التي أنتجتها شركة مايكروسوفت وذلك خروجاً من ورطة الجافا والقضية الشهيرة التي رفعتها عليها شركة صن ، تم الإعلان عنها في أواسط العام 2000 تزامنا مع الإعلان عن بيئة الدوت نت . تتميز سي شارب بأنها أحد لغات البرمجة الكائنية وتجمع صفات بالسي والبيزك المرئي حيث أنها تستخدم القواعد الخاصة بالسي وسرعة التطوير كما في البيزك المرئي ، لغة السي شارب موجهة إلى مبرمجي الفيجول سي ومبرمجي السي على أنها امتداد لهذه اللغات.

1.4.5 مميزات C# :

استفادت لغة السي شارب إلى حد كبير من جهود مطوري الجافا وتشاركها في كل مزاياها ومبادئ التصميم وتفوقها في بعض الأجزاء . لغة السي شارب كباقي لغات الدوت نت والجافا تنتج برامج لاتعتمد على بيئة معينة مثل برامج موجهة للينكس Linux أو ويندوز أو موبايل . هي لغة كائنية بالمعني الحقيقي للكلمة حيث كل شيء في تركيب اللغة هو عبارة عن كائن تم تعريفة مسبقاً ، لذلك لا تسمح هذة اللغة بالكتابة الحرة أي أن أبسط التراكيب البرمجية يجيب أن تكون داخل إحدي الكائنات. منذ الوهلة الأولي لظهور السي شارب كان من الواضح أنها أتت لتعزز موقف شركة مايكروسوفت في منتجها الدوت نت، وذلك لأنها أفضل لغة تتعامل مع الدوت نت و تستفيد من قدراتها كاملة. و قد أصدر في أواخر العام 2005 الإصدار الثاني من اللغة(C#2) تتنوع التطبيقات التي يمكن إنتاجها بلغة السي شارب للعمل على منصات متعددة ، ثم تلاه فى أواخر عام 2007 للإصدار الثالث فى فيجوال ستوديو 2008.

2.4.5 مجالات استخدام C# :

- تطبيقات منصة التشغيل و يندوز.
- تطبيقات الانترنت (الويب) و ذلك باستخدام منصة ال ASP.NE .
- تطبيقات الموبايل وتعتمد على منصة التشغيل وينوز سي إي WINDOWS CE .
- تطبيقات تعامل مع قواعد البيانات باستخدام مكتبة ADO.NET .
- تطبيقات الجرافيكس والوسائط المتعددة .
- تطبيقات إدارة المحتوي.
- الألعاب Games والترفية.

مما سبق يتضح أن لغة السى شارب لغة قوية ومتميزة فى الكثير من المجالات ويتم تطويرها بشكل مستمر ، وتعتبر ضمن عائلة لغات السى ، ولكنها تتميز عن السى بأنها أسهل فى التعلم كالفيجوال بيسيك [22].

5.5 SQL Server R2 2008 :

هي نظام إدارة قاعدة بيانات علائقية يستخدم فيها أسلوب العلاقة بين الجداول، كما أنها لغة غير إجرائية وهي بذلك تختلف عن لغات البرمجة مثل (الجافا و السي) حيث أن اللغات الغير إجرائية هي لغات متخصصة،

وهي لغة للتعامل والتحكم مع قواعد البيانات المترابطة من خلال التعامل مع تراكيب البيانات وإجراء عملية إدخال البيانات والحذف والفرز والبحث وخلافه، بالاضافة إلى أنها متاحة تحت ترخيص مفتوح، كما أنها صممت حول ثلاث مفاهيم رئيسية السرعة والثبات وسهولة التعلم . SQL Server تعتبر بمثابة أساس يمكن الاعتماد عليه والثقة به لانه يمهد الطريق لتطبيقات فعالة وقابلة للتطوير. (تقريبا مطور لجميع التطبيقات)، سواءً على مستوى صغير أو المؤسسات، ويتطلب على الأرجح تخزين واسترجاع البيانات من قاعدة بيانات النهاية الخلفية.

1.5.5 مميزات ال SQL Server :

- إدارة البيانات
- الربط
- سهولة الإستخدام
- التدقيق
- استخبارات الأعمال

6.5 تعريف IIS :

هو خادم ويب من شركة مايكروسوفت ، وهو مايعرف بخدمة معلومات الإنترنت. وهو اختصار لـ (Internet Information services)

وقد تم تطويره من قِبل شركة مايكروسوفت لخدمة وإستضافة مواقع الإنترنت وصفحات الويب (Web) ، ويعتبر واجهة تخطيطية لتشكيل مجموعات التطبيقات أو المواقع (Websites) باستخدام بروتوكول NNTP،SMTP،FTP. وهو عبارة عن ملف خادم التطبيقات (File Application Server) و يمكن استخدامه في الشبكات المحلية (LAN) والشبكات الواسعة النطاق (WAN)، وينتمي إلى طبقة التطبيقات في الشبكات [7].

1.6.5 محتويات خدمة معلومات الإنترنت (IIS):

تحتوي خدمة معلومات الإنترنت على تطبيقات وبروتوكولات مهمة وهي :

- خدمة إضافة اللغات (BITS Server Extensions).
- خدمة بروتوكول نقل الملفات (FTP).
- بروتوكول نقل الأخبار في الشبكة (NNTP).
- مدير خدمة معلومات الإنترنت (IIS Manager).
- بروتوكول نقل البريد (SMTP).
- الملفات العامة (Common Files).
- خدمة النشر للشبكة العنكبوتية (WWWPS). [7]

2.6.5 بعض البروتوكولات الداعمة لبروتوكولات IIS هي:

- Secure Sockets Layer (SSL) :

يستخدم لتشفير عملية التحقق ونقل البيانات في بروتوكول HTTP ، nntp باستخدام تشفير المفتاح العمومي.

- Transport Layer Security (TLS) :

يستخدم لتشفير عمليات نقل الـ (SMTP) فقط ، وهو مختلف عن الـ (SSL).

- Light weight Directory Access Protocol (LDAP) :

يستخدم من قبل خدمة (SMTP) للوصول إلى المعلومات في خدمة الدليل.

- Multipurpose Internet Mail Extension (MIME) :

يستخدم من قبل خدمة الـ(http) لإيصال تنسيق الملفات المقبولة إلى زبائن (http) [21].

3.6.5 فوائد ومميزات (IIS) :

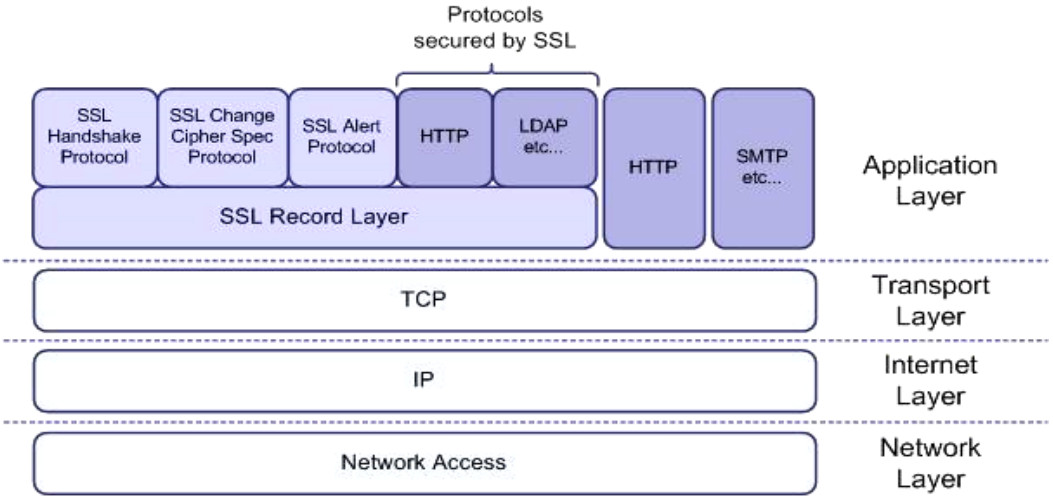
- مع مدير IIS يمكنك أن توفر الأمان والأداء وميزات الثقة. وتعتبر خاصية الـ IIS كبرنامج خادم إفتراصي لنظام التشغيل Windows من شركة مايكروسوفت.
- IIS يأتي بشكل مجاني ومرفق مع نظام التشغيل Windows ولا يعمل على أي نظام تشغيل آخر غير نظام Windows.

- تستطيع أن تضيف أو تحذف المواقع و تشغيل المواقع و إيقافها مؤقتاً أو إيقافها تماماً.
- يدعم ويعيد ترتيب الخادم ، وينشئ أدلة افتراضية لإدارة أفضل ، وهذا ما يعرف بمدير خدمة الإنترنت.
- يتميز بسهولة الإستخدام.
- يساعد مدير الـ (IIS) في عملية إدارة وتنظيم كامل بالموقع الإلكتروني والحماية والأمان.
- قبل البدء بتثبيت خادم معلومات الإنترنت (IIS) ولكي يكون العمل بصورة سليمة يجب أولاً تثبيت بروتوكول Windows TCP/IP وأدوات الربط النفعية (Connectivity Utilities) ، كما ينبغي التأكد من أنه تم تثبيت جميع ملفات التصحيح الأمنية (Security Patches) .
- يجب مراعاة تحميل مدير (IIS) باستخدام حساب مستخدم له صلاحيات مناسبة لذلك كحساب المشرفين (Administrator) [7].

7.5 بروتوكول أمن الإتصال :

هو بروتوكول للتحقق من هوية طرفيّ الإتصال وتشفير المعلومات المتبادلة بينهما، صمم البروتوكول في الأساس من قبل شركة Netscape وأصدر مجلس IETF (Internet Engineering task Force) معياراً جديداً هو TLS (Transport Layer Security) والمبني بالإعتماد على بروتوكول الـ SSL.

يقدم بروتوكول TCP/IP خِدمة النقل والتوجيه للبيانات على الإنترنت، وتقوم بروتوكولات التطبيقات باستخدام TCP/IP لأداء مهامها، ولكن يفتقر بروتوكول TCP/IP إلى الأمن والسرية في نقله للمعلومات مما أظهر الحاجة إلى وجود طبقة وسيطة بين بروتوكول النقل وبروتوكولات التطبيقات [7].



الشكل (1.5) : طبقات برتوكول SSL

1.7.5 يستطيع بروتوكول SSLالقيام بالمهام التالية :

- التحقق من هوية المخدم :

يستطيع المُستخدم بواسطة هذا البروتوكول التحقق من هوية المُخدم الذي يتعامل معه وذلك بإستخدام تقنيات معيارية للتشفير بالمُفتاح العام، حيث يتم التحقق من الشهادة الرقمية للمُخدم فيما إذا كانت صالحة وصادرة من جهة موثوقة بالنسبة للزبون ويتم التحقق أيضاً من المُفتاح العام لشخصية البنك ويقوم بالتقاط رقم بطاقة إعتماده مثلاً عندما يرسلها على الشبكة.

- التحقق من هوية الزبون :

يتم في هذه المهمة عمل نفس الخطوات في الوظيفة السابقة ولكن هذه المرة يحتاج المُخدم إلى التحقق من شرعية الزبون ويقوم بذلك بنفس التقنيات أيضاً، على سبيل المثال تظهر الحاجة إلى هذه الوظيفة عندما يريد البنك إرسال معلومات مالية مهمة إلى زبون دون غيره.

- الإتصال المشفر :

تهتم الوظيفتان السابقتان بالتحقق لكل طرف من هوية الطرف السابق ولكن قد يحتاج الطرفان إلى عدم إطلاع طرف ثالث على المعلومات المُرسلة أيضاً، لذلك يؤمن (SSL) بناء إتصال مشفر بين الطرفين مما يمنح سرعة عالية للإتصال، ولكن حتى الآن بقيت لدينا مشكلة وحيدة وهي العبث بالمعلومات، يقوم (SSL) بحل هذه المشكلة حيث يقوم بشكل تلقائي من أن المعلومات لم تتغير منذ إرسالها.

2.7.5 بنية بروتوكول SSL :

يتألف بروتوكول (SSL) من بروتوكولين جزئيين :

1- بروتوكول سجل SSL :

حيث يعرف البنية المُستخدمة لإرسال المعلومات.

2- بروتوكول المصافحة في SSL :

يغلف بواسطة البروتوكول الجزئي الأول حيث يقوم بتبادل سلسة من الرسائل بين (SSL) المُخدم و(SSL) الزبون وذلك عند بدء تأسيس إتصال (SSL)، يتم في هذه السلسلة من الرسائل تحقيق الوظائف التالية:

- التحقق من هوية المُخدم لصالح الزبون .
- إختيار المشفر أو خوارزمية التشفير التي يستطيع كلا الطرفين دعمها.
- التحقق من هوية الزبون وذلك في حال طَلب المُخدم ذلك.
- إستخدام تقنية التشفير بالمفتاح العام لتوليد سرية مشتركة لكليهما.
- تأسيس إتصال (SSL) المشفر.
- خوارزميات التشفير المُستخدمة في SSL .

يدعم (SSL) عدداً من خوارزميات التشفير التي يستخدمها في العمليات المختلفة مثل إرسال الشهادة الرقمية وتوليد مفاتيح الجلسة وما إلى ذلك، قد يدعم كل من الزبون والمُخدم مجموعة مختلفة من خوارزميات التشفير وذلك عائد إلى عدة عوامل منها إختلاف نسخة (SSL) التي يعمل عليها كل منهما أو إختلاف درجة الحماية المطلوبة من عملية لأخرى أو القوانين التي تمنع إستخدام خوارزميات تشفير محددة.

توجد مجموعو معينة من خوارزميات التشفير والمدعومة من قبل SSL 2.0 و SSL 3.0، ولذلك يستطيع المسؤول عن الأمن في الشبكة أن يقوم بإلغاء تمكين بعض الخوارزميات وذلك حسب القوة المطلوبة للتشفير والتي تعتمد بشكل أساسي على نوع المعلومات المراد نقلها ومدى سريتها والسرعة المطلوبة، حيث يقوم الطرفان بالتفاوض على إستخدام الخوارزمية ذات القوة الأعلى والمطلوبة من أحدهما.

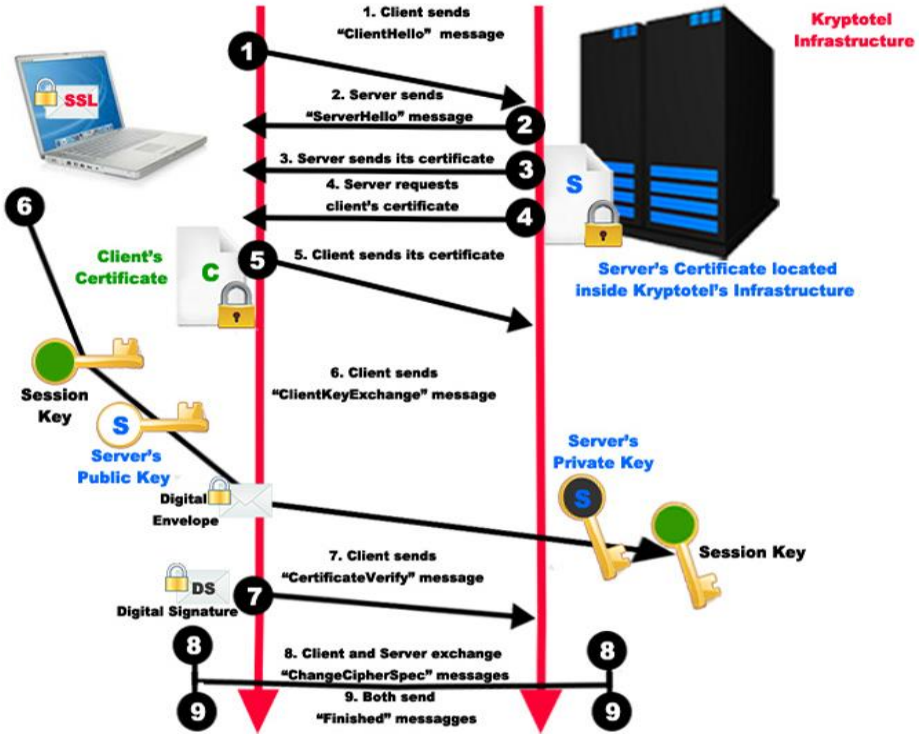
- ### المصافحة في SSL

تعد الخوارزميات التي تستخدم المفتاح المتناظر أسرع من خوارزميات المفتاح غير المتناظر - المفتاح العام – ولكن خوارزميات المفتاح العام أفضل من حيث التحقق من الهوية، ولذلك تستخدم (SSL) مزيج من هذه التقنيتين، حيث تقوم في بداية فتح إتصال (SSL) بتبادل عدد من الرسائل تدعى بالمصافحة، تستخدم في المصافحة تقنية المفتاح العام للتحقق من هوية المُخدم من قبل الزبون، وبعد إتمام هذه العملية بنجاح يتعاون

الطرفان في إنشاء المفاتيح المتناظرة التي ستستخدم في الجلسة للتشفير وفك التشفير وكشف محاولات العبث بالمعلومات، يتم ذلك وبشكل اختياري التحقق من هوية الزبون.

يمكن تلخيص خطوات المصافحة كالتالي :

- يرسل الزبون إلى المُخدم نسخة (SSL) التي يدعمها وإعدادات المشفرات وبعض البيانات المولدة عشوائياً بالإضافة إلى معلومات أُخرى يستخدمها المُخدم في الإتصال مع الزبون.
- يرسل المُخدم إلى الزبون نسخة (SSL) التي يدعمها وإعدادات المشفرات وبعض البيانات المولدة عشوائياً بالإضافة إلى شهادة المُخدم الرقمية، وفي حال كان المُخدم يحتاج إلى التحقق من هوية الزبون يرسل أيضاً طلب تحقق من هوية الزبون.
- يقوم الزبون بواسطة المعلومات المُقدمة من المُخدم بالتحقق من المُخدم، وفي حال عدم نجاح العملية يتم قطع الإتصال، أما في حالة نجاحها ينتقل الزبون إلى الخطوة التالية.
- يستخدم الزبون كافة المعلومات المتوفرة في المصافحة في توليد المفتاح الأساسي الأولي لهذه الجلسة ويقوم بإرساله إلى المُخدم مشفراً بواسطة المفتاح العام للمُخدم.
- في حال طلب المُخدم التحقق من هوية الزبون يقوم الزبو ن بوضع توقيعه الرقمي على البيانات المولدة عشوائياً من المُخدم ويرسلها مع الشهادة الرقمية في نفس الرسالة التي يرسل فيها المفتاح الأساسي الأولي.
- إذا كان المخدم قد طلب التحقق من هوية الزبون، فإنه يقوم بالتحقق من المعلومات المُرسلة من الزبون وفي حال نجاح ذلك يقوم المُخدم بفك تشفير المفتاح الأساسي الأولي بواسطة مفتاحه الخاص ومن ثم ينفذ المُخدم والزبون عدد من العمليات كل على حده بإستخدام نفس المفتاح الأساسي الأولي وذلك لتوليد المفتاح السري الأساسي.
- بعد توليد المفتاح السري الأساسي لدى كل من المُخدم والزبون، يقوم الطرفان بإستخدامه في توليد مفاتيح الجلسة والتي سوف تستخدم لاحقاً في تشفير وفك تشفير الرسائل بالإضافة إلى كشف محاولات العبث بها.
- يرسل الزبون رسالة إلى المُخدم يخبره فيها بأنه سوف يستخدم مفاتيح الجلسة في تشفير الرسائل القادمة ومن ثم يرسل رسالة تدل على إنتهاء عملية المصافحة من جانبه، ولكنه يستمر في إستقبال رسائل المُخدم.
- يُرسل المُخدم رسالة إلى الزبون يخبره فيها بإستخدامه لمفاتيح الجلسة في تشفير الرسائل القادمة، ومن ثم يُرسل رسالة تدل على إنتهاء عملية المصافحة.



الشكل (2.5) : خطوات المصافحة

Open SSL 8.5:

هو تطبيق مفتوح المصدر يعتمد على بروتوكولات (SSL) و (TLS)، ويحتوي على مكتبة مكتوبة بلغة (C) توفر دوال تقوم بتنفيذ المهام الأساسية في عمليات التشفير وفك التشفير [7].

1.8.5 مزايا ال Open SSL :

- إنشاء وإدارة المفاتيح الخاصة والعامة ومعاملات المفاتيح.
- عمليات التشفير بالمفتاح العام.
- إنشاء الشهادات الرقمية معيار X.509 وشهادات الـ CSR وشهادات CRL.
- حساب خلاصة الرسالة (Message Digests).
- إختبارات كل من المُخدم والعميل لبروتوكول SSL/TLS .
- التعامل مع S/MIME الموقعة أو البريد المشفر [7].

9.5 التشفير:

تقنية التشفير(cryptography) هي فن حماية المعلومات عن طريق تحويلها إلى رموز معينة غير مقروءة تدعى النصوص المشفرة (cipher text) لا يمكن حلها إلا من خلال مفتاح سري يقوم بفك ذلك التشفير وتحويله إلى نص عادي مقروء، ونظراً للانتشار الكبير الذي حققته الاتصالات الإلكترونية وخصوصاً الإنترنت، فقد غدا الأمن الإلكتروني من أهم القضايا التي يركز عليها العالم بأجمعه، وتستخدم تقنية التشفير في هذا المجال لحماية الرسائل الإلكترونية والمعلومات المهمة المنقولة إلكترونياً كالبيانات المتعلقة ببطاقات الائتمان والبيانات الخاصة بالشركات [2].

1.9.5 أنواع التشفير:

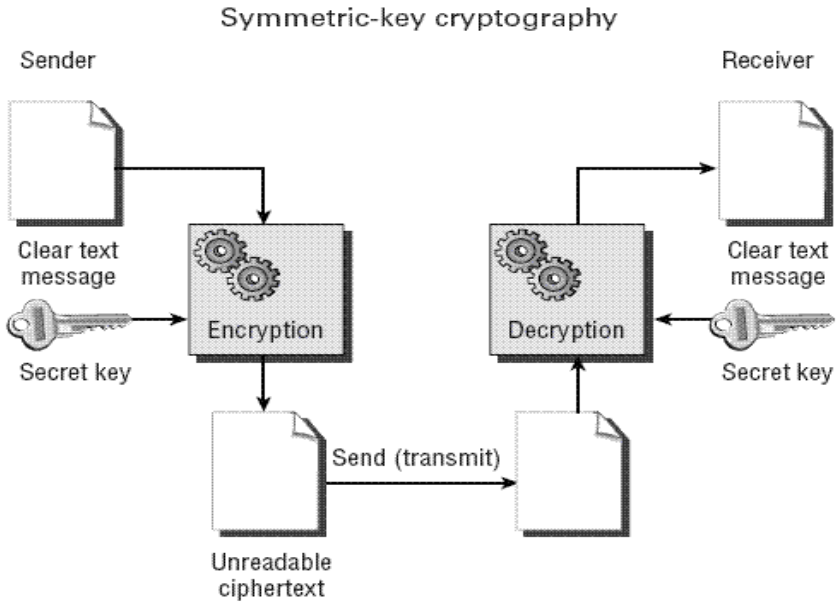
ينقسم التشفير عادة إلى نوعين أساسيين :

1- التشفير المتماثل (symmetric systems) :

حيث يستخدم هنا مفتاح شفرة واحد لعمليتي التشفير وفك التشفير.

من مزايا التشفير المتماثل انه سهل الاستعمال وسريع ولكن لديه عيب مهم)خصوصا حين يستخدم في الشبكات الكبيرة) وهو كيفية توزيع المفاتيح بين طرفي عملية التواصل على الشبكة الذان يستخدمان عملية التشفير.

من الأمثلة على الخوارزميات التي تستخدم المفتاح المتناظر DES AES, وغيرها [14].



الشكل (3.5) : التشفير بإستخدام التشفير المُتماثل

2- التشفير غير المتماثل (المفتاح العام)(asymmetric systems):

يتم فيه إستخدام مفتاحان للتشفير إحداهما يخصص للتشفير كمرحلة أولية ، في حين يستخدم المفتاح الثاني لفك الشفرة وإعادة البيانات إلى شكلها المقروء والمفهوم.

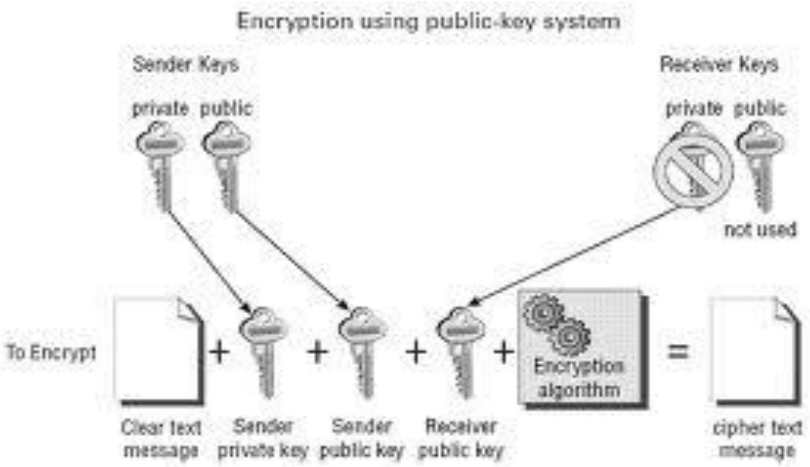
فهو يقوم بتوليد مفاتيح مختلفة ثم استخدامها في تشفير وفك تشفير زوجين من مفاتيح الحماية. وباستخدام هذين الزوجين من المفاتيح، أحدهما عام (public) والآخر خاص (private)، يستطيع مفتاح واحد منهما فقط أن يقوم بفك الشفرة التي ينشئها الآخر.

في هذا النوع من التشفير كل كيان entity (مستخدم، حاسب ، ..) يملك مفتاحين مترافقين مع بعض ، مفتاح عام public key ومفتاح خاص private key. كما يوحي الإسم أن المفتاح العام يكون متوفراً للجميع بينما المفتاح الخاص يكون محمياً بعناية ولا يُنقل إطلاقاً عبر الشبكة.

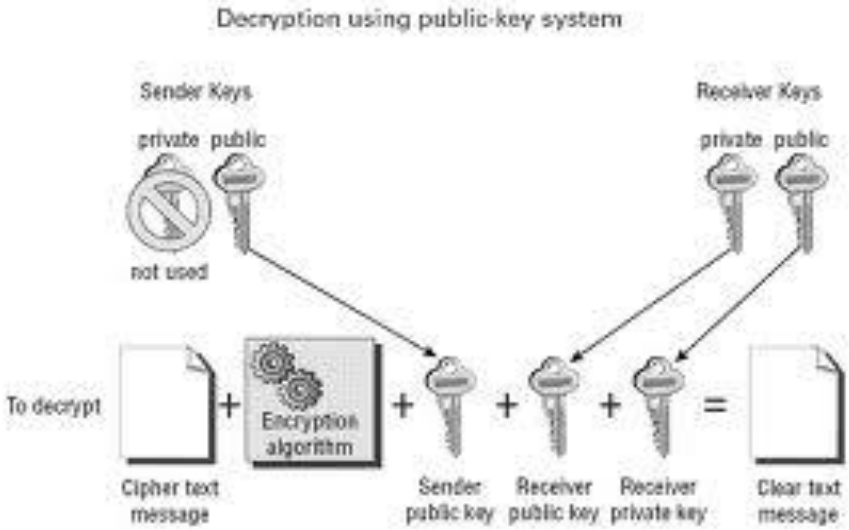
الطريقة التي تتعامل فيها الأنظمة مع هذه التقنية كالتالي: إن المعلومات المشفرة بواسطة المفتاح العام يمكن فقط فك تشفيرها بواسطة المفتاح الخاص. والعكس صحيح : المعلومات المشفرة بواسطة المفتاح الخاص يمكن فقط فك تشفيرها بواسطة المفتاح العام.

ومن غيرالمرجح أن تؤدي معرفة مفتاح واحد فقط إلى تحديد المفتاح الآخر، ولهذا يتم استخدام نظام التعمية غير المتماثل في إنشاء التوقيعات الرقمية ونقل المفاتيح المتماثلة.

من الأمثلة على الخوارزميات التي تستخدم المفتاح غير المتناظر خوارزمية RSA. [14]



الشكل (4.5) : عملية التشفير بإستخدام التشفير غير المُتماثل



الشكل (5.5) : عملية فك التشفير بإستخدام التشفير غير المُتماثل

2.9.5 أهمية التشفير:

يستخدم التشفير للتغلب على الأخطار التالية :

1- الاطلاع على المعلومات المحظورة.
2- محاولات تعديل البيانات المنقولة بالشبكة.
3- إعادة توجيه البيانات إلى وجهة أخرى .
4- تأخير إيصال بعض الرسائل.
5- تغيير محتويات الرسائل المتبادلة .
6- إقحام رسائل زائفة ضمن الرسائل المنقولة عبر الخط .
7- تغيير كلمات السر الخاصة بالمستفيدين .
8- انتحال شخصية المستخدم الحقيقي .
9- تعديل البيانات المخزنة على الحاسبات نفسها [14].

10.5 خوارزمية RSA :

هي خوارزمية للتشفير بواسطة مفتاح عام. ولعلها الأولى المعروفةً على هذا الصعيد ، وهي مناسبة للتّوقيع بالإضافة إلى التشفير، وكانت أحد التقدّمات العظيمة الأولى في التشفير بواسطة مفتاح عامّ. آر إس إيه مستخدم في بروتوكولات التّجارة الإلكترونيّة على نطاق واسع، وهي آمنة طالما كان طول المفتاح طويل جدا مثل: 1024 بت ، وهي تعتمد بشكل كبير على أنَّه لا يوجد خوارزمية لتحليل عدد لعوامل بسرعة عالية.

خوارزمية (RSA) تَتضمّنُ مفتاحا عامّا ومفتاحا خاصّا. المفتاح العامّ هو مفتاح التشفير فقط ويجب ان يكون معلوما لكل من يحاول الاتصال بمالك المفتاح . الرسائل المشفّرة بالمفتاح العامّ يمكن أن تُفَكّ فقط باستخدام المفتاح الخاصّ. وذلك بتنفيذ الخوارزمية التالية :

- اختيار عددين أوليّين عشوائيّين كبيرين مختلفين p وq.
- حساب (n=p . q) . يستخدم n كالمعامل لكل المفاتيح الخاصة والعامة.

- حساب $\emptyset(n) = (p-1)(q-1)$.حيث أن الدالة $\emptyset(n)$ تعطي عدد الأعداد التي بين (2 وn) والتي هي أعداد أولية مع n. أي أنه $GCD(n, i) = 1$ حيث أن $(2 \leq i \leq n)$.
- اختيار عدد صحيح بشكل عشوائي e بحيث أن $1,2 \leq e \leq \emptyset(n)$ $GCD(\emptyset(n), e) = 1$.هذا العدد e سوف يكون الأُس العمومي.
- إيجاد قيمة d أو المفتاح الخاص، بحيث أنه يحقق التالي :

$$d.\ e = 1 (\text{mod}\ \emptyset(n)) \text{ and } 0 \leq d \leq n$$

- يكون المفتاح العام مكوناً من الصيغة $KU=\{e, n\}$ حيث KU ترمز للمفتاح العام، الذي سوف يتم توزيه بعد ذلك.
- يتم الإحتفاظ بشكل سري بالمفتاح الخاص، والذي يفك شفرة المفتاح العام، والمكون من الصيغة .

$KR=\{d, p, q\}$ حيث KR ترمز للمفتاح الخاص [15].

11.5 دالة الهاش Hash :

- تنشئ دالة الهاش مايشبه بصمة Hash، للملفات أو الرسائل أو البيانات:

$$h = H(M)$$

- تختزل الأحجام المختلفة للرسائل M إلى بصمة ثابتة الحجم.
- يفترض أن تكون عامة، متاحة للجميع.

متطلبات تنفيذ دالة الهاش :

1. تكون قابلة للتطبيق على أي رسالة بأي حجم.
2. مخرجاتها ثابتة من حيث عدد ال Bits .
3. سهلة الحساب بالنسبة لأي رسالة M والشكل العام $h = H(M)$.
4. الحصول على h لايساعد للحصول على M حسب الدالة أعلاه (خاصية الإتجاه الواحد).
5. إذا كان $H(y) = H(x)$ حسب شكل دالة الهاش، فإن الحصول على x لا يعني مطلقاً القدرة على إيجاد y.
6. إذا كان $H(y) = H(x)$ فإنه غير المجدي الحصول على x ولا y [25].

12.5 جهاز توثيق الرقم السري (Token) :

هو جهاز يمنح لكل شركة أو مؤسسة تشترك بهذه الخدمة، وذلك لإضفاء المزيد من السرية و الأمان، و يتمتع الجهاز بمواصفات أمان عالية حيث تتغير كلمة السر تلقائياً كل دقيقة، ويستخدم عند تنفيذ أي إجراء إداري أو مالي خاص بمستخدم واحد (صلاحية موافقة) مع إمكانية طلب أجهزة إضافية حسب الطلب.

13.5 بروتوكول التحقق من حالات الشهادة على الإنترنت :

يعرف برمز (OCSP) اختصاراً لـ (Online Certificate Status Protocol). هو بروتوكول على شبكة الإنترنت يستخدم للتحقق من حالة الشهادة الرقمية. تم إنشاء هذا البروتوكول كبديل لقوائم الشهادات الملغية

((Certificate revocation lists (CRLs وتحديداً لمعالجة مشاكل معينة مرتبطة باستخدام البنية الأساسية للمفتاح العام.

الرسائل التي يتم إرسالها باستخدام الـ OCSP يتم ترميزها في الـ ASP.1 ويتم غالباً إرسالها باستعمال بروتوكول الـ HTTP .طبيعة الرسائل تكون (طلب / إستجابة)، هذه الطبيعة تقود إلى مايسمى بخوادم بروتوكول أوضاع الشهادات على الإنترنت [7].

1.13.5 مزاياه :

يفضل استخدام (OCSP) بدلاً عن (CRLs) وذلك للأسباب التالية :

- يوفر المعلومات في الوقت المناسب، بشأن إلغاء /تعليق حالة شهادة معينة.
- باستخدام الـ OCSP لا يحتاج العملاء للقيام بتحويل قوائم الـ CRLs بأنفسهم.
- يمكن النظر لقوائم الـ CRLs على أنها مماثلة لشركات بطاقات الإئتمان (قوائم العملاء السيئين)، ولا داعي لعرض هذه القوائم للجمهور [7].

2.13.5 تفاصيل بروتوكول (OCSP) :

- من الممكن أن يُعيد مُجاوب الـ OCSP رد مُوقع يدل على أن حالة الشهادة المحددة في الطلب هي "جيدة"، "مُلغاة" أو "غير معروف"، إذا كان الطلب لا يمكن معالجته أو الاستجابة له فإنه يتم إعادة ما يدل على وجود خطأ.
- بروتوكول الـ OCSP له مقاومة عالية ضد هجوم إعادة الإرسال، حيث أن رد موقع بأن الشهادة "جيدة" يتم الحصول عليه من قِبَل وسيط غير مرغوب به (Malicious) وتتم إعادة إرساله للعميل في موعد لاحق بعد أن تكون الشهادة المعنية قد تم إلغائها، OCSP يتغلب على ذلك بإدراج رقم خاص بالطلب، وهذا الطلب يجب إدراجه مع الاستجابة (الرد) المناسبة له.
- هجوم إعادة الإرسال مُحتمل لكنه لا يُشكل تهديداً أساسياً للأنظمة التي تم تصديقها، يعود ذلك للخطوات المتبعة لمقاومة هذا الهجوم، يجب أن يكون المهاجم في موقع يسمح له بالقيام بالتالي:

1. السيطرة على حركة الشبكة (Network traffic).
2. الحصول على وضع الشهادة التي على وشك أن تتغير.
3. إجراء معاملة معينة تتطلب الحصول على وضع تلك الشهادة ضمن الإطار الزمني لصلاحية الإستجابة.

[17]