أمن الشبكات

سامي شريف

مارس 2008

المحتويات

مقدمة

ازدادت في الأعوام الأخيرة عمليات الحوسبة في المؤسسات الحكومية وشركات القطاع الخاص وذاك باستخدام نظم المعلومات الإلكترونية والحواسيب وما يرافقهما من شبكات ربط بين المواقع المختلفة لهذه المؤسسات وتبادل للمعلومات بين الإدارات والأقسام المختلفة بها. ونظراً لما توفره نظم المعلومات من سهولة سير الأعمال، أصبح الاعتماد عليها أمراً ضرورياً وحاسما لكي تحقق المؤسسة استراتيجياتها. لكن استخدام نظم المعلومات الإلكترونية يؤدي بدوره إلى ظهور أخطار جديدة ناتجة عن تجميع كميات كبيرة من المعلومات في مكان واحد واستخدام أساليب اتصال غير أمن، مما يجعل تلك المعلومات الهامة عرضةً للفقدان أو السرقة أو العبث بها من قبل أشخاص غير مخولين بالإطلاع عليها أو التعامل معها.

خلصت دراسة أجراها "معهد أمن الحواسيب Computer Security Institute بالتعاون مع مكتب التحقيقات الفدرالية (FBI) في الولايات المتحدة الأمريكية، في العام 2006، حول الأمن وجرائم الحواسيب، أن تكاليف الهجمات عبر الإنترنت باهظة جداً. فقد أعلنت 250 مؤسسة شاركت في هذه الدراسة السنوية التي تجرى للعام الثالث عشر على التوالي، عن خسائر بلغت أكثر من 400 مليون دولار، نتيجة أسباب تراوحت بين التطفل على المعلومات وانتهاك السرية والخصوصية، وهجمات حجب الخدمة (DoS)، والفيروسات، وإساءة استخدام الموظفين داخل الشركة أو المؤسسة لحقوق النفاذ إلى الشبكة.

أمن المعلومات ونظمها يتطلب الكثير من الإعداد والمجهود، بحيث يضمن أمن المعلومات (قواعد البيانات والبيانات المتبادلة بين الأطرف) وأمن نقل المعلومات من المصدر (المنبع) إلى المقصد (المصب). وهذا معناه تنوع نظم الحماية واختلافها تبعاً لطبيعة عمل المؤسسة ونمط النظام التقني الذي تتبعه أو تعتمده. في كل الحالات لا بد أن تسبق الحماية وقاية شاملة كخطوة أولى لابد منها قبل التفكير في الاعتماد على آليات الأمن مثل التشفير والترميز وبرمجيات تحري الفيروسات ومكافحتها أو حجب البريد الطفيلي. إن السباق بين استخدامات نظم المعلومات وبرمجيات الحماية لايزال لمصلحة الأولى إذ أن الثانية تعاني من بطء رغم تسارعها مقارنة مع وتيرة تسارع استخدامات النظم والشبكات. هجمات المتسللين لا تزال محدودة التطوير والكم، ورغم ذلك يحظي تطوير برمجيات ووسائل الحماية الشاملة باهتمام كبير في مجال تقنية المعلومات والشبكات وخاصة مع تزايد استخدامات الأجهزة المحمولة من قبل كثير من الموظفين.

شهدت مطلوبات امن المعلومات في المؤسسات خلال العقود العديدة السابقة تغيرين أساسين. قبل الاستخدام الواسع لعتاد معالجة البيانات الالكتروني كان تامين وحماية المعلومات القيمة بالمؤسسة يتم عبر إجراءات مادية (مثل استخدام نظام ملفات صارم وخزن مغلفة بإحكام) وإجراءات إدارية (مثل إجراءات انتقاء العاملين خلال عمليات التعين). الاستخدام المتنامي للحاسوب في نظم المعلومات تتطلب أدوات ذاتية لحماية الملفات والمعلومات الأخرى المخزنة بالحواسيب. وبالأخص في حالة نظم الشراكة مثل نظم مشاركة الزمن أو شبكات البيانات أو الانترنت. التغيير الأساسي الثاني الذي اثر على امن المعلومات هو استخدام النظم الموزعة والشبكات ومعينات الاتصالات الاخري لنقل البيانات بين المستخدم الطرفي والحاسوب أو بين الحاسوب وحاسوب أخر. مما تطلب آليات لحماية البيانات خلال انتقالها.

تعتمد درجة تامين وحماية الشبكة على مدى حساسية البيانات المتداولة عبرها. حيث تنظم إجراءات الأمن والحماية فقأ لنوع الشبكة والمعلومات. يهتم امن الشبكات بمنع السلوك غير الحميد والممارسات التي قد تهدد امن المعلومات المخزنة والمنقولة.

يهتم أمن المعلومات والشبكات إبقاء معلومات تحت سيطرة المؤسسة المباشرة والكاملة، وتأكيد عدم إمكانية النفاذ إليها من قبل أي شخص غير مصرح له بذلك. يمكن النظر إلى امن المعلومات من وجهات نظر مختلفة. فمن وجهة النظر الأكاديمية، امن المعلومات هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن

أنشطة الاعتداء عليها . ومن وجهة النظر الفنية، هو الوسائل والأدوات والإجراءات الضرورية لحماية المعلومات من الإخطار الداخلية والخارجية . ومن وجهة النظر القانونية ، فان أمن المعلومات يهتم بسن وإجازة التشريعات لحماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الحاسوب والإنترنت)

يهتم هذا الكتاب بوجهة النظر الفنية لأمن الشبكات، حيث سندرس أساليب امن وحماية الشبكات المستخدمة بكثرة في كثير من التطبيقات لتوفير الحماية للبيانات والشبكات. حيث يركز على تدابير وآليات إعاقة ومنع وكشف وتصحيح الثغرات الأمنية المرتبطة بإرسال المعلومات وتخزينها في الشبكات. يناقش الكتاب آليات وبرتوكولات امن مختلفة تعمل على مستوى الطبقات المختلفة لنموذج شبكات الحواسيب المرجعي. أهداف الكتاب تتلخص في بتزويد الدارس بالمعرفة والمهارات في المحاور التالية:

- التهديدات الأمنية في الشبكات وأساليب مكافحتها.
- آليات توفير الأمن والحماية للمستخدم والنظم والشبكات
- نظم وأساليب التشفير المختلفة
- برتوكولات ونظم من الشبكات

وتغطى هذه المواضيع في اثنتا عشر وحدة دراسية. المرجع الأساسي الذي استخدم في إعداد هذا الكتاب هو كتاب وليام استيرلنق "*التشفير وامن الشبكات*". William Starling, Cartography and Network Security, ...

■

الوحدة الأولى: امن المعلومات والشبكات

أهداف الوحدة:
في نهاية هذه الوحدة سيكون بمقدورك:
- تعريف امن الشبكات والمعلومات وشرح أهميتهما.
- تحديد مطلوبات امن نظم الحاسوب والشبكات.
- شرح المخاطر التي قد تتعرض لها شبكات المعلومات.
- شرح الثغرات في الشبكات وأنواع الهجمات التي قد تتعرض لها.
- وصف نماذج حماية الشبكات.

1.1: مقدمة

نحرص جميعاً على حماية ممتلكاتنا الخاصة أو العامة من العبث و السرقة و التخريب. فالمعلومات بأشكالها المختلفة سواء كانت ورقية أو إلكترونية، هي ممتلكات تنفق المؤسسات أموالاً طائلة لتدوينها وحفظها .وبالتالي فالمعلومات الإلكترونية هي ممتلكات ولكي نحافظ عليها يجب علينا الحفاظ على أمن النظم الالكترونية (الحاسوبية) الحاملة لها والشبكات الالكترونية الناقلة لها. فنحن معنيون بالحفاظ على امن Security المعلومات ومنع النفاذ إليها إلا من قبل الأشخاص المخولين بذلك وعلى تكامليتها (سلاماتها) Integrity من حيث الدقة وعدم تغيير أي جزء منها وعلى جاهزيتها Availability لتمكين المخولين من النفاذ إليها عند الحاجة أي توفير استمرارية الحصول عليها في كافة الظروف والأوقات والتحكم في عمليات النفاذ Access Control، وتسجيل الأحداث Auditing. ,من هنا تظهر أهمية أمن المعلومات ونظم المعلومات التي تغطي المتطلبات السابقة.

يهتم أمن المعلومات بالحفاظ على سرية وسلامة المعلومات وإبقائها تحت سيطرة المؤسسة المباشرة والكاملة. وفي هذا السياق يهتم *امن الحاسوب* بالأدوات والآليات الضرورية لحماية البيانات في الحاسوب من الهجوم عليها من قبل المخترقين والمتطفلين والفيروسات وإيقاف الخدمة، أما *أمن الشبكات* فيهتم باتخاذ التدابير والإجراءات الضرورية لحماية المعلومات خلال نقلها بين الحواسيب والأجهزة والشبكات المختلفة. يستخدم التعبير *امن الانترنت* لتعريف الإجراءات والتدابير الأمنية الضرورية لحماية البيانات خلال إرسالها عبر الشبكات المترابطة بينياً.

تشتمل مطلوبات امن وحماية المعلومات والشبكات على ثلاث محاور رئيسة، كما سنوضح لاحقا في هذه الوحدة وهى:
- التهديدات الأمنية والهجمات التي قد تتعرض لها نظم المعلومات الالكترونية والشبكات.
- الخدمات الأمنية وتشتمل على الأساليب والخطط المستخدمة لمواجهة التهديدات.
- واليات الأمن والحماية وتشتمل على الأدوات المستخدمة بواسطة الخدمات الأمنية.

سندرس في هذه الوحدة مطلوبات امن وحماية المعلومات والشبكات المذكورة أعلاه، حيث ندرس طبيعة التهديدات الأمنية التي قد تواجهها نظم المعلومات الالكترونية والشبكات. كما سنتعرف على الخدمات الأمنية الضرورية لتحقيق بيئة معلومات الكترونية آمنة وموثوق فيها وسنحدد مواصفات هذه الخدمات. سنناقش في هذه الوحدة أيضا الآليات التي قد تستخدم في تقديم الخدمات الأمنية.

1.2. أمن المعلومات والشبكات

ظل مجال امن المعلومات والشبكات حتى أواخر سبعينيات القرن الماضي معروفاً باسم أمن الاتصالات Communication Security, COMSEC والذي حددته توصيات أمن نظم المعلومات والاتصالات لوكالة الأمن القومي بالولايات المتحدة بما يلي:

"المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أشخاص غير مخولين عبر الاتصالات وضمان أصالة وصحة هذه الاتصالات."

تضمنت النشاطات المحددة لأمن الاتصالات أربعة محاور هي :
- أمن التشفير Crypto security.
- أمن الإرسال Transmission Security.
- أمن الإشعاع Emission Security.
- الأمن الفيزيائي (المادي) Physical Security.

كما تضمّن تعريف أمن الاتصالات خاصيتين وهما:
- *السرية Confidentiality*: وتعني بالتأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- *التحقق من الهوية (الموثوقية او الشرعية) Authentication*، وهذا إجراء أمني للتأكد من صلاحية الاتصال أو الرسالة أو المصدر أو المستلم أو التحقق من مصدر المعلومات

بدأت في الثمانينات من القرن الماضي ومع النمو المضطرد للحواسيب الشخصية واستخداماتها، حقبة جديدة من الأمن وهى حقبة أمن الحواسيب ,Computer Security COMPUSEC والتي حددتها توصيات أمن نظم المعلومات والاتصالات لوكالة الأمن القومي بالولايات المتحدة بما يلي:

"المعايير والإجراءات التي تضمن سرية، كمال وتوفر مكونات نظم المعلومات بما فيها التجهيزات والبرمجيات والبرمجيات المدمجة firmware والمعلومات التي يتم معالجتها وتخزينها ونقلها."

تضمن أمن الحواسيب خاصيتين إضافيتين وهما:
- *التكاملية وسلامة المحتوى Integrity:* وتعني بالتأكد من أن محتوى الرسائل (المعلومات) صحيح ولم يتم تعديله أو العبث به. وبشكل خاص لم يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع خلال الإرسال .
- *استمرارية توفر المعلومات أو الخدمة Availability:* التأكد من استمرار عمل نظام المعلومات والشبكات واستمرار مقدرتها على التفاعل مع المعلومات والمستخدمين، وعدم توقف أو حجب الخدمة وعدم إمكانية النفاذ كنتيجة للهجوم عليها أو تدميرها وتخريبها.

لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي أمن الاتصالات وأمن الحواسيب لتشكيل ما أصبح يعرف باسم أمن نظم المعلومات– Information Systems Security .INFOSEC. يشتمل مفهوم أمن تظم المعلومات الخصائص الأربعة المذكورة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب، وهي السرية والموثوقية والكمال والتوفر، كما أضيف إليها خاصية جديدة وهي *مكافحة الإنكار*، أو منع إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation، والقصد هنا هو ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها انه هو الذي قام بهذا التصرف، بحيث توفر هذه الخاصية المقدرة على إثبات إن تصرفا ما قد تم من شخص ما في وقت معين.

1.3. الخطر والثغرات والتهديدات:

يعرف الأمن بالحماية من المخاطر والفقدان. بصورة عامة مفهوم الأمن شبيه بمفهوم السلامة. الفارق الدقيق بين المفهومين يتمثل في التركيز الإضافي للأمن على الحماية من المخاطر الخارجية المتمثلة في الإفراد والأنشطة التي تنتهك الحماية وتكون مسئولة مباشرة عن خرق الأمن. يستخدم تعبير الأمن بصورة عامة كمرادف لتعبير السلامة، ولكن من ناحية فنية يعنى تعبير الأمن ليس فقط السلامة بل العمل على توفير السلامة أيضا.

هناك مفاهيم محددة تتكرر في مجالات المن المختلفة منها:

1. *الخطر risk*، وهو مفهوم يشير إلى التأثيرات السالبة والمحتملة على الأصول والممتلكات القيمة والتي قد تنتج من عملية حالية أو حدث مستقبلي. بمعني أخر، الخطر هو احتمال حدوث حدث معين يكون لديه تأثير على إنجاز الأهداف. في مجال العلوم الهندسية، يعرف الخطر كمياً بحاصل ضرب احتمال حدوت الحادثة و الخسارة في الحادثة الواحدة. ويعتبر الخطر مؤشر للتهديدات ويعتمد على التهديدات والثغرات والتأثير على العمليات وعدم التأكد. يوجد العديد من الطرق والأساليب لتقيم وقياس الخطر.

في امن المعلومات والشبكات يحدد الخطر باستخدام ثلاثة متغيرات (عوامل) وهى:
- احتمال أن يكون هناك تهديداً
- احتمال إن تكون هناك ثغرات
- التأثير المحتمل للخطر.

إن أصبحت أي من هذه المتغيرات تساوي صفراً، يقترب الخطر الكلي على النظام أو الشبكة من الصفر أيضا.

إدارة الخطر نشاط إنساني يهدف إلى تكامل تميز الخطر وتقيمه وتطوير الاستراتجيات لإدارته وتخفيفه باستخدام الموارد الإدارية.

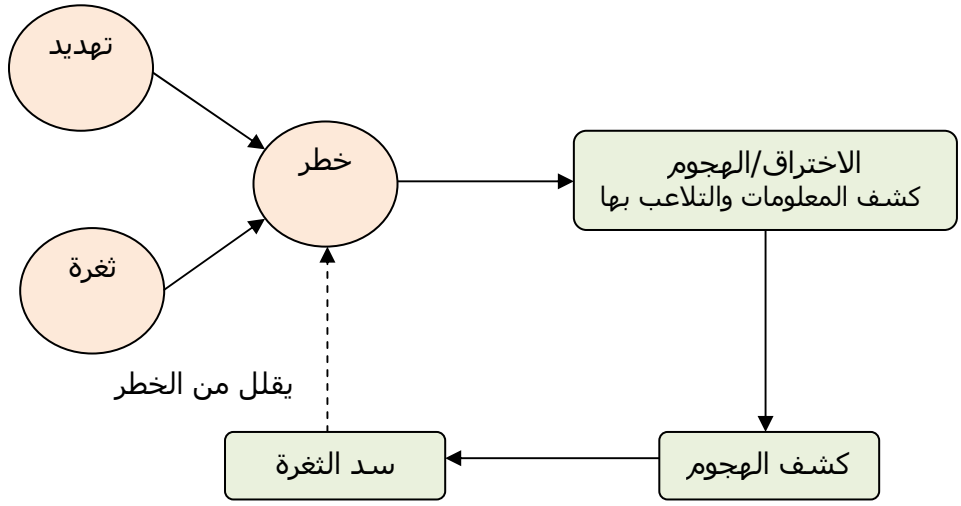
2. *الثغرات Vulnerability* (أو عدم التحصين) وبصورة عامة تعرف بالحساسية اتجاه الأذى أو الهجوم الجسدي أو النفسي. كما تعني أيضا عدم توفر الحماية اللازمة للممتلكات والأصول القيمة. في امن الحاسوب والشبكات يستخدم تعبير الثغرات للإشارة إلى أماكن الضعف في هذه النظم والتي تتيح للمهاجم بالاعتداء على سلامة النظام. وقد يتسبب في الثغرات قصوراً في البرمجيات أو خللاً في التصميم، نتيجة لإهمال المبرمج أو المصمم، أو استخدام المهاجم لبرامج خبيثة مثل برامج الفيروسات.

يمكن تصنيف الثغرات في امن الحاسوب والشبكات إلى فئتين:
- ثغرات فنية، وتكون نتيجة لضعف التحصين الناتج من التقنيات المستخدمة في النظم والشبكات، في هذه الحالة يعرف الهجوم على الشبكة بالهجوم التقني.
- ثغرات إدارية، وتكون نتيجة لأسباب غير فنية ويعرف الهجوم على الشبكة أو الحاسوب في هذه الحالة بهجوم الهندسة الاجتماعية social engineering Attack.

كما يمكن تقسيم الثغرات من حيث الصعوبة والسهولة إلى فئتين:
- ثغرات المستوي الأعلى High-level Vulnerability، وهو ثغرات سهلة الاستغلال, ومثال عليها كتابه شفرة برنامج لاستغلال تلك الثغرة.
- ثغرات المستوى الأدنى Low-level Vulnerability وهذا النوع الثغرات يصعب استغلاله ويتطلب الكثير من الجهد والموارد من قبل المهاجم.

3. *التهديدات Threats*، وهو احتمال التطفل على الأصول والممتلكات (المعلومات) بدون أذن صاحبها وقسراً وعبر ثغرة محتملة في النظام، بهدف سرقتها أو تخريبه، وفى حالة حدوثها تمثل التهديدات خطراً على النظام. هناك ثلاث مكونات أساسيه للتهديد وهي:
- الهدف، ويمثل في امن الحاسوب والشبكات المعلومات المخزنة أو المرسلة عبر الشبكات بغرض انتهاك سريتها أو سلامتها أو تواجدها.
- العميل وهي البرامج والأشياء المكونة والمنشأة للتهديد، ويتطلب استخدامها النفاذ إلى الحاسوب أو الشبكات بالإضافة إلي معلومات عن خصائص تشغيلها وآليات الأمن المستخدمة فيها وذلك للبحث عن ثغرة للنفاذ من خلالها إلى النظام أو الشبكة.
- الحدث، ويمثل نوعية التأثير لوضعية التهديد ويستخدم لذلك بطرق عديدة من أهمها إساءة النفاذ المخول Authorized وغير المخول Unauthorized إلى المعلومات أو النظام.ووضع شفرات خبيثة Malicious مثل شفرات الفيروسان في النظم.

الشكل 1.1 يوضح العلاقة بين مكونات نظام امن المعلومات والشبكات وتأثرها ببعضها البعض.



الشكل 1.1: مكونات نظم امن المعلومات والشبكات

1.4. عناصر أمن المعلومات

تتمحور عناصر أمن المعلومات في عدة مجالات وأهمها :

- *أمن أماكن حفظ البيانات و المعلومات*: ويهتم هذا المجال بالعديد من الآليات العلمية والعملية المرتبطة بأمكن حفظ البيانات والبيئة المحيطة بها، وذلك للتأكد من تواجد المعلومات في أماكن آمنة مثل مراكز البيانات Data Centers، والتي يجب أن تخضع لرقابة دقيقة وإجراءات أمنية مادية عالية في الدخول، بحيث لا يصل إلي الأجهزة إلا من هو مصرح له ومن خلال بوابة آمنة والتي قد تعتمد أحياناً على التقنيات المتقدمة مثل قراءة بصمة الإصبع (Printfinger) وقزحية العين (Printeye) أو تردد الصوت أو من خلال الأرقام المتسلسلة أو البطاقات الممغنطة، وغيرها.
- *أمن طريقة حفظ البيانات*: ويتم ذلك من خلال استخدام التقنيات المتقدمة لتشفير المعلومات المحفوظة (Encryption) بمختلف أنواع التشفير المتناظر أو غير المتناظر، وسواء كان معتمداً دولياً أو اسلوب تشفير مطوراً محلياً.
- *أمن وسائط حفظ البيانات*: ويتحقق هذا المحور من خلال الحفظ على الأنسب من الأقراص الصلبة (HDD) أو كروت الذاكرة (CASH) أو الأقراص المدمجة (CD) وغيرها من وسائط الحفظ المناسبة.
- *أمن حماية المعلومة*: ويتم بعدة آليات مثل استخدام برامج الحماية أو الجدران النارية Firewalls للحماية من اختراق الأجهزة المرتبطة بالشبكات ، واستخدام المرشحات Filters لضمان عدم نقل المعلومات غير المسموح بنقلها، واستخدام برامج مكافحة الفيروسات (Anti-Virus) للحماية من الفيروسات المختلفة والنسخ الاحتياطي Backup) لمعالجة مشكلة فقدان البيانات الرقمية غير المكتوبة والتي تكون أكثر عرضة من غيرها للتلف أو العطب أو الفقدان ويتم ذلك بعدد من الآليات.
- *أمن نقل المعلومات والبيانات*: قديماً كانت تستخدم آليات النقل المادي المباشر للبيانات وتحاط بسرية وحماية هذه الآليات ببطيئة نسبيا، والمتأمل حالياً يرى أن تلك الطريقة كانت أكثر أمناً من الطرق الحديثة المعتمدة علي التواصل الإلكتروني. وبعد التقدم التقني أصبحت آليات النقل الحديثة بما تميزت به من سرعة النقل والدقة هي الأنسب عند أخذ الاحتياطات الأمنية اللازمة في عمليات نقل البيانات ولذا نرى بأن هذا المجال يهتم بالبيئات الآمنة لنقل البيانات والمعلومات عبر الشبكات والنفاذ إليها.
- *أمن نظم الاتصالات وبيئات النقل* المستخدمة: وذلك عندما يكون الاتصال مباشراً بواسطة خطوط الهاتف أو بالاتصال المباشر بالأقمار الاصطناعية، وعندما يكون حجم البيانات متوسطاً نسبياً. وتكمن الخطورة هنا عند وجود متطفلين يقومون بعمليات

بالتطفل Sniffing على خطوط الاتصال وتبرز هنا أهمية تشفير البيانات بقوة وكفاءة عالية والمحافظة على سلامة خط الاتصال من وجود المعترضين أو المتجسسين.

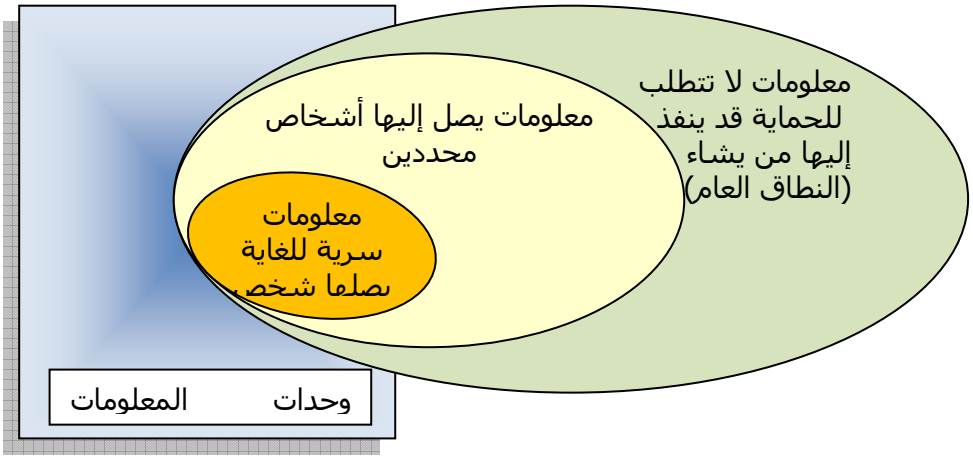
- *أمن التطبيقات المستخدمة والبروتوكولات*: عندما يكون الاتصال غير مباشر وعبر وسيط مثل الإنترنت أو يكون نقل البيانات لموقع خدمات عالي الأهمية الأمنية مثل المصاريف أو للشراء المباشر ببطاقات الائتمان الإلكترونية، يمثل التجسس والاختراق أبرز المشاكل الأمنية والتي لا يمكن القضاء عليها بشكل كامل بل يمكن الحد منها بشكل كبير عن طريق استخدام البروتوكولات الآمنة على مستوي طبقة التطبيقات أو طبقة الشبكة، وهنا تظهر أهمية التوقيعات الرقمية والشهادات الإلكترونية للمواقع الآمنة وغيرها من وسائل الحماية.
- *البحث عن مصادر الخطر المتوقعة على المعلومة لمكافحتها*: تعتبر مصادر الخطر وتهديدات أمن البيانات والشبكات كثيرة جداً و لعل من أهمها خطورة النفاذ إلى البيانات من قبل أشخاص غير مسموح لهم بذلك وبالتالي يتم تسريب المعلومات أو إتلافها أو تغييرها ويمكن أن يستعين أولئك المهاجمون بالعديد من الوسائل التي توصلهم للبيانات أو تمكنهم من إتلافها أو تغييرها بعدة طرق، كما سنرى لاحقا في هذه الوحدة.

1.5. منطلقات خطة حماية المعلومات

تعتمد خطط حماية المعلومات والشبكات بصورة كاملة على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها. فليس كل المعلومات تتطلب السرية وضمان عدم الإفشاء ، وليس كل المعلومات في منشأة واحدة بذات الأهمية من حيث النفاذ إليها أو ضمان عدم العبث بها، لهذا تنطلق خطط أمن المعلومات من الإجابة على التساؤلات التالية :-

- ما الذي نريد أن نحميه ؟
- ما هي المخاطر التي تتطلب هكذا حماية؟
- كيف يتم توفير الحماية لما نرغب بحمايته من المخاطر والتهديدات التي تم تحديدها (وسائل الحماية)؟
- ما العمل إن تحقق أي من المخاطر رغم وسائل الحماية المستخدمة؟

الشكل 1.2 يوضح تصنيف المعلومات ويوضح هذا التصنيف إن المعلومات تتدرج من معلومات لا تتطلب الحماية إلى معلومات تتطلب حماية قصوى.



الشكل 1.2: تصنيف المعلومات

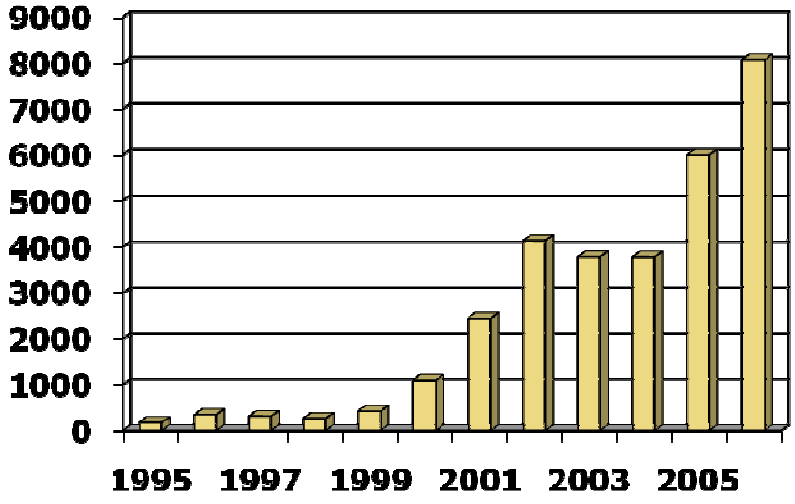
تحدد المخاطر والتهديدات باعتبار كل العوامل التي قد تؤثر على امن وسلامة الشبكات والمعلومات مثل انقطاع مصدر الطاقة والتخريب واختراق الشبكات ونظم المعلومات وإساءة استخدام كلمات المرور وغيره, تصنف هذه العوامل كمخاطر من حيث مصدرها ووسائل تنفيذها، وغرض المتسببين فيها وأثرها على نظام الحماية وعلى المعلومات. تحدد كل مؤسسة

طريقتها الخاصة في توفير الأمن من المخاطر والتهديدات والاختراقات، ويجب أن لا تكون هذه الإجراءات رخوة وضعيفة بحيث لا تكفل الحماية اللازمة وبالمقابل يجب أن لا يكون مبالغا فيها إلى الدرجة التي تؤثر سلبا على أداء المؤسسة. على المؤسسة وضع خطة لمواجهة الأخطار عند حصولها ، وتتضمن هذه الخطة مراحل متتالية، تبدأ من مرحلة الإجراءات الفنية والإدارية والإعلامية والقانونية اللازمة عند حصول ذلك، ومرحلة تحليل طبيعية المخاطر التي حدثت وسبب حدوثها وكيفية تفاديها لاحقا . وأخيرا مرحلة العودة إلى الوضع الطبيعي قبل حدوث الخطر مع مراعاة تنفيذ ما أظهره التحليل عن كيفية حدوث المخاطر وضمان عدم تكرارها مستقبلا.

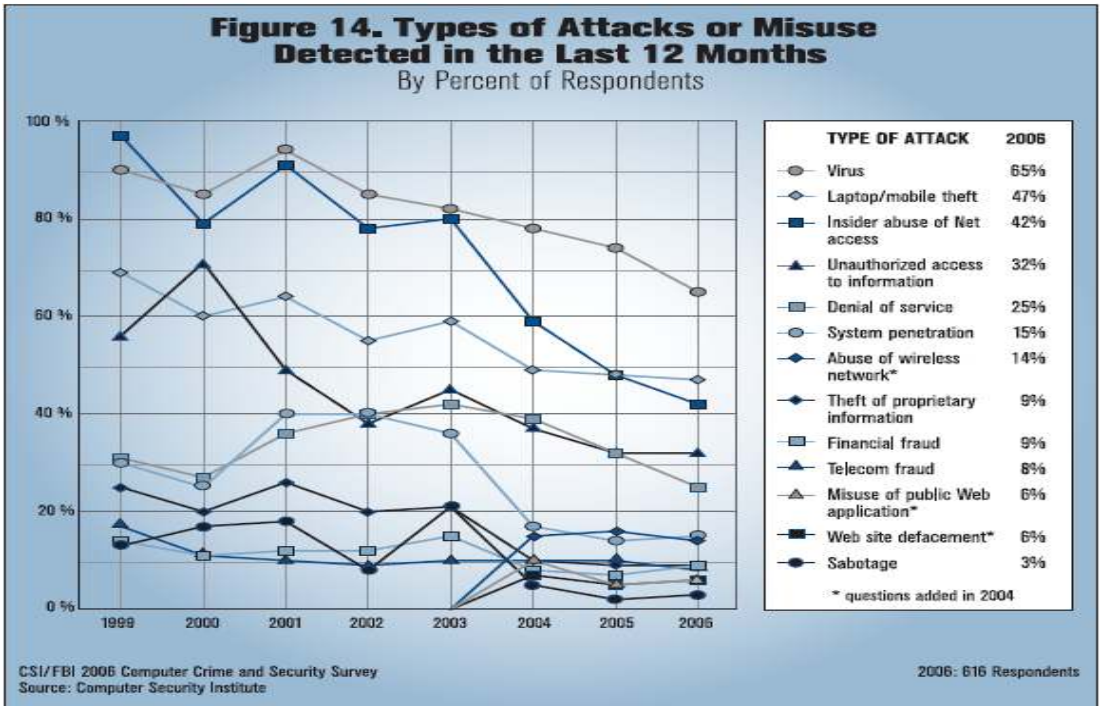
تطال المخاطر والاعتداءات في بيئة المعلومات أربعة عناصر من المكونات التقنية (الفنية) لنظم وشبكات المعلومات وهى :-

- *العتاد*: هو كافة المعدات والأدوات المادية التي تتكون منها شبكة المعلومات، كالحواسيب والشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها.
- *البرامـج*: هي الأوامر المرتبة في نسق معين لانجاز الأعمال، وقد تكون مستقلة عن الحاسوب أو مخزنة فيه.
- *البيانات*: تمثل العنصر الحيوي للنظم، ومما يجعلها أكثر عرضة لجرائم الحاسوب والشبكات، وتشمل على كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها ، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم . والبيانات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات ، وقد تخزن داخل النظم أو على وسائط التخزين خارجه .
- *الاتصالات*: تشمل شبكات الاتصال التي تربط الحواسيب ونظم المعلومات الالكترونية الأخرى بعضها بعض محليا وإقليميا ودوليا، وتتيح فرصة لاختراق (مهاجمة) النظم عبرها كما أنها بذاتها محل للاعتداء وتمثل احد مكامن الخطر الحقيقي.

الشكل 1.3 والشكل 1.4 يوضح عدد والمؤسسات والشركات التي تعرضت لخسائر في بياناتها أو برمجياتها نتيجة إصابتها بالأخطار والمهددات. هذه المعلومات خلاصة دراسة أجراها معهد أمن الحواسيب Computer Security Institute بالتعاون مع مكتب التحقيقات الفدرالية FBI في الولايات المتحدة الأمريكية، على عدد من المؤسسات في العام 2006، حول جرائم الحواسيب و المهددات الأمنية والاختراقات المسجلة، ويلاحظ من هذه النتائج أن أنواع المهددات الأمنية لنظم معلومات تتنوع مصادرها حسب الأغراض التي تقوم بها تلك النظم. فمثلاً تكون النظم المرتبطة مع شبكة الإنترنت أكثر عرضة للفيروسات من النظم غير المرتبطة مع الشبكة. ويلاحظ من هذه الدراسة أن حوالي 85% من المؤسسات فقدت بيانات وبرمجيات نتيجة لهجوم الفيروسات بينما حوالي 55% من المؤسسات فقدت بياناتها أو برمجياتها نتيجة تعطل تجهيزات الربط والشبكات (هجوم حجب الخدمة) و50 %منها فقدت بيانات نتيجة للاختراقات الداخلية من قبل العاملين في المؤسسة.



الشكل 1.3: الاختراقات المسجلة المصدر /http://www.cert.org/stats



الشكل 1.4: أنواع الهجمات المصدر http://www.cert.org/stats/

1.6. مطلوبات أمن وحماية نظم المعلومات والشبكات:

تعتبر مسألة أمن نظم المعلومات من المسائل الحساسة والحاسمة في مؤسسات القطاع العام وشركات القطاع الخاص التي تقوم بحوسبة نظم معلوماتها. وكما ذكر أعلاه تختلف المطلوبات الأمنية لنظم المعلومات الالكترونية تبعاً لاختلاف تطبيقات وأعمال كل مؤسسة. ويمكن حصر أهم هذه المطلوبات بما يلي:

- يجب وضع سياسة امن وحماية عامة المعلومات ونظم المعلومات والشبكات وفق طبيعة عمل وتطبيقات المؤسسة. ومن الضروري أن تدعم الإدارة العليا في المؤسسة سياسة أمن المعلومات لديها.
- تحديد مسئولين عن أمن المعلومات والشبكات في المؤسسة.
- تحديد الحماية اللازم توفرها في نظم التشغيل والتطبيقات المختلفة.
- تحديد آليات المراقبة والتفتيش في نظم المعلومات والشبكات الحاسوبية والرصد الدوري للأخطار الناتجة عن اختراق نظم المعلومات .
- حفظ وسائط التخزين العادية والاحتياطية بشكل آمن.
- تعمية أو تشفير المعلومات عند الحفظ والتخزين والنقل على مختلف الوسائط.
- تأمين استمرارية عمل وجاهزية نظم المعلومات، للعمل في حالة الأزمات والكوارث من خلال استخدام تجهيزات منيعة ومرتبة بحيث تكون متسامحة مع الأخطاء ومن خلال تكرارية التجهيزات في مواقع أخرى.

يمكن حصر إجراءات الحماية الواجب توفرها في نظم المعلومات الالكترونية لمجابهة المهددات التي تتعرض لها ولتحقيق المطلوبات الأمنية ضمن ثلاثة محاور رئيسية هي الحماية الفيزيائية (المادية) وحماية البرامج والبيانات وحماية شبكات نقل المعلومات. ويتفرع عن هذه المحاور عدد من الإجراءات الرئيسية التي يمكن تلخيصها بما يلي:

- إجراءات الحماية الفيزيائية (المادية) لنظم المعلومات.
- انتقاء العاملين في نظم المعلومات وتوعيتهم أمنياً.
- إجراءات الحماية الخاصة بنظم التشغيل والبرامج التطبيقية وضبط الصلاحيات.
- إجراءات الحماية الخاصة بشبكات المعلومات.

- تعمية وتشفير المعلومات المنقولة والمخزنة.
- إجرائية حفظ البيانات بصورة عامة وحفظ نسخ عنها في مواقع آمنة.
- إجراءات لضمان استمرارية عمل وجاهزية النظم المعلوماتية في كافة الظروف بما فيها حالات الكوارث الطبيعية.

1.7. السياسات الأمنية

لتحقق بيئة معلومات أمنة ليس من المجدي اقتصادياً وعملياً تحقيق امن مطلق للحواسيب والشبكات يمنع تسريب المعلومات أو تخريبها أو التطفل عليها، فلابد من تحقق نوعاً من التوازن بين الترتيبات الأمنية من ناحية وكلفة هذه الترتيبات من ناحية أخري. يجب أن تركز الخطوة الأولى لتحقيق هذا التوازن بين الإجراءات والتكلفة علي استنباط سياسة أمنية شاملة للمؤسسة أو علي تطوير السياسة الأمنية المتعبة بحيث تأخذ في الاعتبار التغييرات الحديثة في بيئة المعلومات, ويجب أن تحدد هذه السياسة بالتفصيل صلاحيات الموظفين وحقوقهم في النفاذ إلي الخدمات الالكترونية التي تقدمها المؤسسة، كما يجب أن يثقف الموظفين في مجال مسئولياتهم تجاه حماية معلومات بالمؤسسة مثل مسؤولياتهم تجاه حماية كلمات المرور التي يستخدمونها. بالإضافة إلى تحديد الإجراءات التي ستقوم المؤسسة بها في حال حدوث خرق لمثل هذه الخطة الأمنية.

تعتبر السياسة الامنية بالمؤسسة أداة هامة جدا في تحديد المجالات التي ستنفق فيها أموال المؤسسة للحفاظ علي أمن معلوماتها ، ويقدم كتاب دليل امن المواقع Site Security handbookالذي أصدره مجموعة عمل الشبكة Network Working Group التابعة للفريق الهندسي للانترنت Internet Engineering task Force أو IETF فكرة جيدة عن الموضوعات التي يجب أخذها بعين الاعتبار عند وضع السياسات الأمنية
.
تتطلب السياسة الأمنية كجزء من ترتيباتها تقدير الكلفة التي ستتحملها المؤسسة، في حال خرق الترتيبات الأمنية. ويجب أن ينخرط الموظفون في اعلي المستويات في هذه العملية وقد يكون من المفيد أن تقوم المؤسسة بتوظيف مستشار لأمن المعلومات والشبكات، لضمان أمن معلوماتها. تقدم الكثير من الشركات المزودة لخدمة الانترنت Internet Services Providers ISP، الاستشارة والنصح في هذا المجال، وتبدأ بعد تحديد السياسة المتبعة، عملية تقويم استخدام برامج الجدران النارية firewall، والتشفيرencryption والتثبت من المستخدم (الموثوقية) Authentication.

بعض الأمثلة على السياسات الأمنية:

- مسح كلمة السر الخاصة بالموظف المنتهي عقدة فورا (مثلا كإجراء خلال سحب أوراقة من المؤسسة).
- وضع مجسات مياه أو حرائق قرب أجهزة تخزين البيانات
- استخدام الجهاز الخاص بالمؤسسة فقط للربط بالانترنت, ويمنع استخدام أي جهاز غيره.
- لا يسمح بتبادل الرسائل التي تحتوي على رسائل خاصة أو برامج خبيثة داخل المؤسسة.
- تحديد بصورة صارمة صلاحيات كل مستخدم على البيانات المحفوظة على قاعدة البيانات.
- الدخول مراكز المعلومات عن طريق البطاقة الخاصة وعبر أجهزة التحقق من البصمة.

وهناك بعض الإجراءات التي قد تساعد في المحافظة على أمن المعلومات والشبكة وتنفيذ السياسة الأمنية بكفاءة مثل:

- التدريب المتقن للمستخدمين على التعامل مع إجراءات الأمن.
- التأكد من أمن المعدات وصعوبة الوصول إليها من قبل المتطفلين.
- حماية الأسلاك النحاسية وإخفاؤها عن الأعين لأنها قد تكون عرضة للتجسس.
- تشفير البيانات عند الحاجة.

- تزويد المستخدمين بأجهزة لا تحتوي على محركات أقراص مرنة أو مضغوطة أو حتى أقراص صلبة،
- استخدام برامج لتسجيل جميع العمليات التي يتم إجراؤها على الشبكة لمراجعتها عند الضرورة.
- إعطاء تصاريح Permissions للمستخدمين للنفاذ للبيانات والمعدات كلٍ حسب طبيعة عمله.
- تزويد المستخدمين بحقوق Rights تحدد الأنشطة والعمليات المسموح لهم إجراؤها على النظام.

تحدد السياسة الأمنية أيضاً الآليات المستخدمة لحماية البيانات والشبكات من الاختراق والهجمات، أدناه بعض الأمثلة لآليات الأمن والحماية

- الحماية بكلمات المرور.
- التشفير ,
- جدران النار
- بروتوكولات الحماية.

1.8. الاختراق:

بشكل عام الاختراق Hacking هو القدرة على الوصول لهدف معين بطريقة غير مشروعة، وذلك عبر الثغرات في نظام الحماية الخاص بالهدف. وبطبيعة الحال هذه سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين عنوه ودون رغبة منهم وحتى دون علمهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية او بنفسياتهم عند سحبة ملفات وصور تخصهم وحدهم . يمكن تقسيم المخترقين إلى مجموعتي:

- *المجموعة الأول*: وهم الهواة وعامة المخترقين الذين يستخدمون برامج سهلة وبسيطة للاختراق وغالبية هذه البرامج تعمل تحت بيئة نظام التشغيل Windows، وهؤلاء المخترقين عادة لا يتمكنون من النفاذ إلى بيانات إي جهاز إلا إذا كان متصل بشبكة الإنترنت ومصاب بفيروسات من نوع "حصان طروادة" Trajan التي تدعم برامج المخترقين حيث يقوم حصان طروادة بفتح منفذ في الجهاز المصاب يمكن للمخترق من خلاله التحكم في جهاز الضحية والوصول لبياناته.
- *المجموعة الثانية*: وهم القلة والأخطر وهم المخترقين المحترفون وعادة ما يكونوا مبرمجين أو متخصصين في مجال البرمجيات والشبكات، ويشكلون تحالفات في عالم الإنترنت الافتراضي. وهؤلاء المخترقون لا يعتمدون فقط على برامج الاختراق بل يقومون باستغلال الثغرات الأمنية في نظم التشغيل والشبكات، حيث يعترضون البيانات والحصول على نسخة منها في نقاط الاتصال سواء كانت أجهزة ربط شبكات مثل الموجهات Routers أو المبدلات القابلة للإدارة Manageable Switches أو يقومون بالتواصل مع الموجهات Routers وبالتالي يعطلون نطاقات كاملة عن العمل أو قد يتمكنوا من ضرب أجهزة الربط والإضرار بقطاع كبير من مستخدمي الشبكة الإنترنت.

تتلخص دوافع الاختراق في التالي:

- *الدافع السياسي والعسكري:* مما لاشك فيه أن التطور العلمي والتقني أديا إلي الاعتماد بشكل شبة كامل على الحاسوب والشبكات في أغلب الاحتياجات الفنية والمعلوماتية. فمنذ الحرب الباردة والصراع ألمعلوماتي و ألتجسسي بين الدولتين العظميين آنذاك على أشده. ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية في المؤسسات والدول، حيث أصبح الاعتماد كليا على الحاسوب وعن طريقه أصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.
- *الدافع التجاري:* من المعروف أن الشركات التجارية الكبرى في حالة حرب مستعرة وقد بينت الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجرى عليها أكثر من خمسين محاولة اختراق لشبكاتها كل يوم.

- *الدافع الفردي:* بدأت أولى محاولات الاختراق الفردية بين طلاب الجامعات بالولايات المتحدة الأمريكية كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم و ما لبثت أن تحولت تلك الظاهرة إلي تحدي فيما بينهم في اختراق النظم بالشركات ثم بمواقع الانترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية.

يمكن تقسيم الاختراق من حيث الطريقة المستخدمة إلي ثلاثة مجموعات:
- اختراق المزودات أو الأجهزة الرئيسية للشركات والمؤسسات أو الجهات الحكومية وذلك باختراق الجدران النارية التي عادة توضع لحمايتها وغالبا ما يتم ذلك باستخدام المحاكاة (الاحتيال) Spoofing وهو مصطلح يطلق على عملية انتحال شخصية للدخول إلي النظام.
- اختراق الأجهزة الشخصية والعبث بما تحويه من معلومات
- التعرض للبيانات أثناء انتقالها والتعرف على شفرتها إن كانت مشفرة وهذه الطريقة تستخدم في كشف أرقام بطاقات الائتمان وكشف الأرقام السرية للبطاقات المصرفية ATM.

1.8.1. طرق الاختراق

يعتمد الاختراق على السيطرة علي جهاز الحاسوب عن بعد من خلال عاملين مهمين:
- البرنامج المسيطر ويعرف بالعميل (الزبون) Client.
- ووحدة الخدمة Server الذي يقوم بتسهيل عملية الاختراق ذاتها .

وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج وحدة الخدمة وفي جهاز المخترق يوجد برنامج العميل. تختلف طرق اختراق الأجهزة والنظم باختلاف وسائل الاختراق، ولكنها جميعاً تعتمد على فكرة توفر اتصال عن بعد بين جهازي الضحية والذي يزرع به وحدة الخدمة الخاصة بالمخترق، وجهاز المخترق على الطرف الأخر حيث يوجد برنامج المستفيد أو العميل هناك ثلاث طرق شائعة لتنفيذ ذلك:

- عن طريق ملفات أحصنة طروادة Trojan: ولتحقيق الاختراق لابد من توفر برامج تجسس يتم إرسالها وزرعها من قبل المستفيد في جهاز الضحية ويعرف بالملف اللاصق أو الصامت وهو ملف عادة ما يكون صغير الحجم مهمته الأساسية المبيت بجهاز الضحية (وحدة الخدمة) ويمثل حلقة الوصل بينه وبين المخترق (المستفيد).
- منافذ الاتصال Ports**:** يتم الاتصال بين العمليات في أي جهازين عبر منفذ اتصال والذي يكون جزء من الذاكرة له عنوان معين يتعرف عليه الجهاز بأنه منطقة اتصال يتم عبره إرسال واستقبال البيانات مع برتوكولات طبقة التطبيقات ويمكن استخدام عدد كبير من المنافذ للاتصال وعددها يزيد عن 65000.
- استخدام عنوان برتوكول الانترنت IP Address: عند اتصال جهاز الحاسوب بالإنترنت يكون معرضاً لكشف الكثير من المعلومات الخاصة به، مثل عنوان الجهاز وموقعه ومزود الخدمة الخاص به، كما يمكن تسجيل كثير من تحركاته على الشبكة. حينما يتمكن المحترف من معرفة رقم عنوان برتوكول الانترنت الخاص بالضحية قد يتمكن من خلاله من الدخول إلي الجهاز والسيطرة عليه خلال الفترة التي يكون فيها الضحية متصلاً بالشبكة فقط،
- عن طريق كعكات الإنترنت Internet Cookies**.** يمكن أيضاً تحقيق التواصل للاختراق عن طريق كعكات الإنترنت وهي عبارة عن ملف صغير تضعه بعض المواقع التي يزورها المستخدم على قرصه الصلب. هذا الملف به آليات تمكن الموقع التابع له من خلال جمع وتخزين بعض البيانات عن الجهاز وعدد المرات التي زار المستخدم فيها الموقع كما أنها تسرع عمليات نقل البيانات بين جهاز المستخدم والموقع فالهدف الأساسي منها هو تجاري ولكنه قد يساء استخدامه من قبل بعض المبرمجين المتمرسين . يتم الاختراق بوضع برنامج وحدة الخدمة بجهاز الضحية ويتم الاتصال به عبر المنفذ الذي فتحه للمستفيد (المخترق) في الطرف الأخر ولكن حلقة الوصل هذه تنقصها المعابر وهي البرامج المخصصة للاختراق.

1.9. معمارية امن نموذج الربط السني للنظم المفتوحة:

من الواضح من كل النقاش أعلاه إن تقيم وتحديد احتياجات امن المعلومات والشبكات ليست بالمهمة السهلة. ويحتاج مسئول أمن المعلومات بالمؤسسة إلى أسلوب نِظاميّ للتقييم الفعال لحاجات المؤسسة الأمنية وتقدير واختيار معدات وأجهزة الأمن والسياسات وتوصيف أساليب واليات الأمن والحماية. هذه المهمة صعبة بدرجة كبيرة في بيئة معالجة البيانات المركزية، ومع استخدام شبكات المناطق المحلية والمناطق الواسعة تصبح هذه المشكلة أكثر تعقيداً. حددت التوصية X.800، الصادرة من قطاع الاتصالات بالتحاد الدولي للاتصالات ITU-T،معمارية امن لنموذج الربط البيني للنظم المفتوحة Open Systems Interface OSI. تعطي هذه التوصية أسلوب نِظاميّ لتنظيم مهام توفير امن المعلومات والشبكات بالمؤسسة.

تهتم معمارية امن نموذج الربط البيني للنظم المفتوحة بثلاثة محاور أساسية هي الهجمات الأمنية والية الأمن وخدمة الأمن، والتي يمكن تعريفها كالأتي:

- *الهجمات الأمنية*: إي حدث أو فعل يخل بأمن نظام معلومات المؤسسة
- *إلية الأمن*: العمليات أو المعدات المصممة لاكتشاف ومنع الهجمات الأمنية والاسترجاع منها.
- *خدمة الأمن*: العمليات أو خدمات الاتصال التي تعزز امن نظم معالجة البيانات ونقل المعلومات في المؤسسة. تهدف الخدمات لمكافحة الهجمات الأمنية وتستخدم آلية أمن واحدة أو أكثر من إلية لتوفير الخدمة

تعرف التوصية X.800 الخدمات الأمنية بالأتي: " *الخدمة التي يوفرها برتوكول الطبقة في نموذج اتصال النظم المفتوحة والتي تضمن امن نظم أو إرسال بيانات ملائم* ". تعرف مجموعة الانترنت في التوصية RF 2828 الخدمات الأمنية على النحو التالي: "*خدمات المعالجة أو الاتصالات التي يوفرها النظام للحصول على نوع محدد من حماية لموارده*". وتحقق الخدمات الأمنية أهداف السياسة الأمنية، وتنفذ باستخدام الآليات الأمنية. تحدد التوصية X.800 الخدمات الأمنية التالية:

- الموثوقية أو الشرعية
- ضبط النفاذ
- سلامة (تكامل) البيانات
- عدم الإنكار

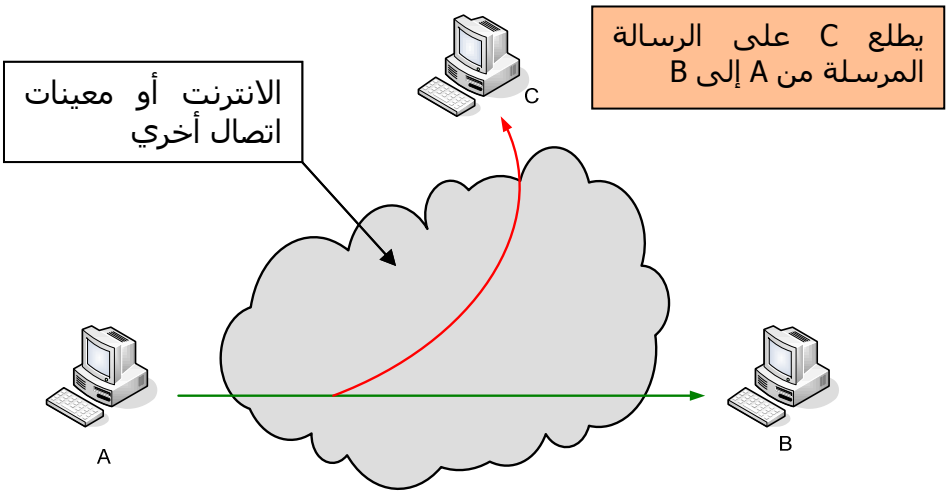
كما ذكر أعلاه، هذه الخدمات تعزز امن نظم معالجة البيانات ونقلها في المؤسسة، وتهدف إلى مكافحة الهجمات باستخدام آليات الأمن.

آليات الأمن هي أساليب محددة تستخدم لتحقيق الخدمات الأمنية. توجد آليات متعددة ومختلفة. وتصنف الآليات إلى آليات امن محددة واليات امن احترازية. وعادة وترتبط إي آلية بطبقة محددة في نموذج اتصالات النظم المفتوحة. اشتملت توصية X.800 على الآليات التالية (بالإضافة إلى آليات أخري): التشفير والتوقيع الرقمي وضبط النفاذ وسلامة البيانات وموثوقية التبادل وحشو الحركة وضبط التوجيه. أما الآليات الاحترازية غير المرتبطة ببرتوكولات الطبقات قد تشتمل على وظائف التوثيق والتصنيفات الأمنية وكشف الأحداث ومراجعة محاولات الاختراق.

1.10. أنواع الهجمات

يهدف الهجوم على نظم المعلومات الالكترونية وشبكات المعلومات إلى تدمير (تخريب) المعلومات أو سرقتها أو منع الوصول إليها أو تنصيب برامج خبيثة malicious software. يقسم الهجوم إلى قسمين رئيسين وهما الهجوم النشط Active Attack والهجوم الخامل Passive Attacks.

في الهجوم الخامل، الشكل 1.4، يتم باعتراض الرسائل من اجل التعرف على محتوياتها واستخدامها داخليا دون تغير محتوياتها أو تحليل الحركة. من الصعب اكتشاف هذا النوع من الهجوم ولابد من اخذ التدابير الاحترازية للحماية منه.



الشكل 1.4: الهجوم الخامل

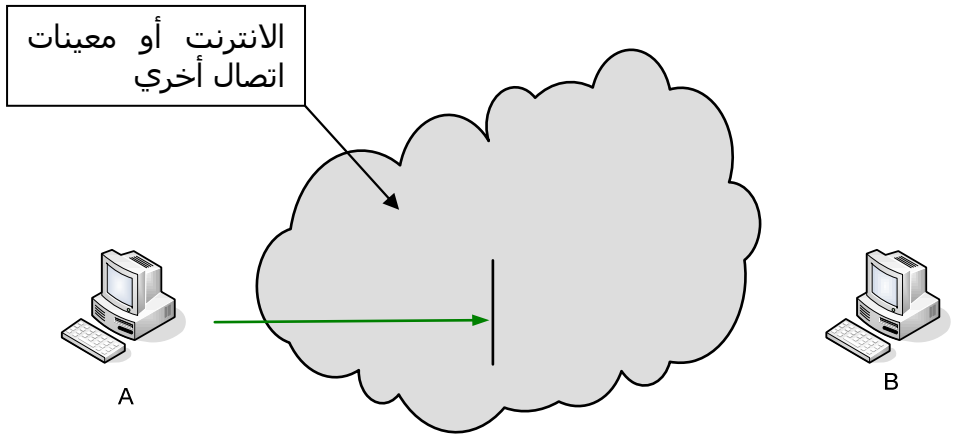
يعرف هذا الهجوم أيضا بهجوم التصنت على الرسائل Interception Attacks، حيث يراقب المهاجم الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الاتصال Eavesdropping

في الهجوم النشط قد يعالج المخترق الرسالة ببراعة ويغير محتواها. يهدف الهجوم النشط إلى تغيير إمكانيات النظام والتأثير على عملياته وذلك بتعديل تتدفق البيانات من اجل:

- انتحال هوية احد أطراف الاتصال.
- إعادة إرسال رسائل السابقة.
- تعديل محتويات الرسالة التي في الانتظار.
- منع أو حجب الخدمة

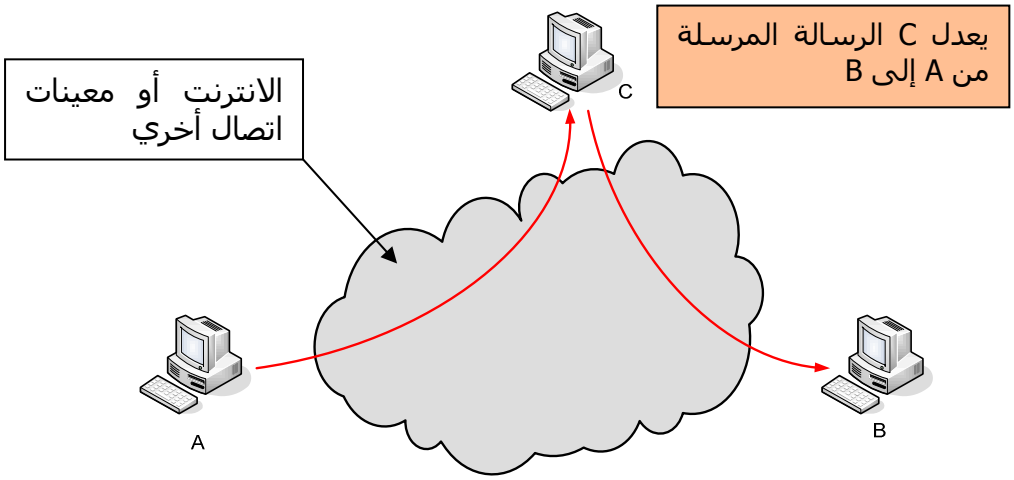
من الصعب منع الهجمات النشطة كليا نتيجة للثغرات المحتملة في العتاد والبرمجيات والشبكات. وذلك عكس الهجمات الخاملة والتي من الصعب اكتشافها ولكن يمكن منعها كليا. وتهدف أساليب مكافحة الهجمات النشطة إلى اكتشاف الهجمات والاسترجاع من أثارها, يقسم الهجوم النشط إلى أربعة أقسام رئيسة وهي:

- هجوم الإيقاف Interruption Attacks ، الشكل 1.5، هذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض أو حجب الخدمة.(Denial of service)

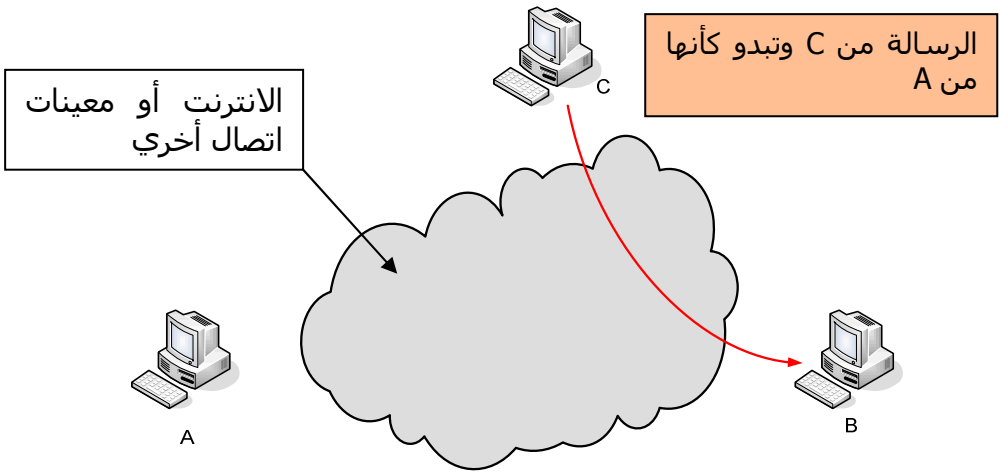


الشكل 1.5: الهجوم حجب الخدمة

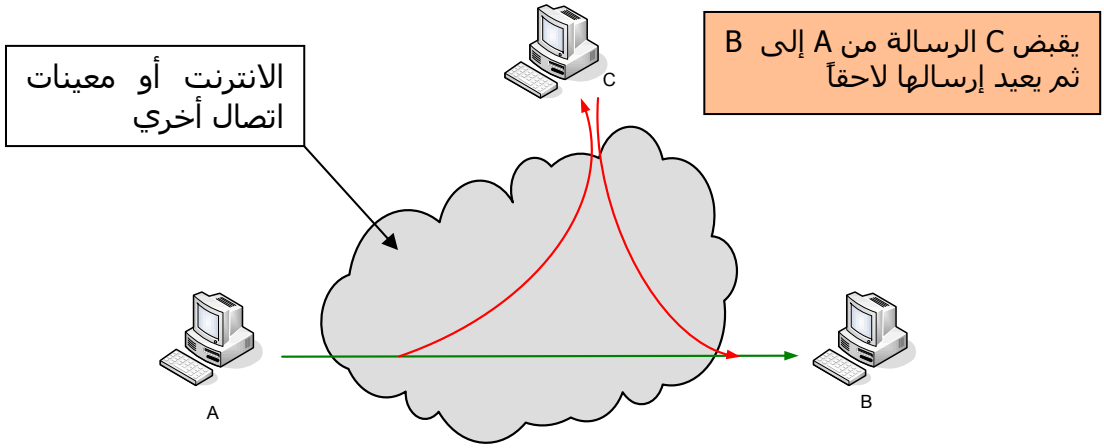
- هجوم تعديل محتوى الرسالة Modification Attacks، الشكل 1.6، هنا يتدخل المهاجم بين المرسل والمستقبل (يعتبر وسيط بين المرسل والمستقبل) وعندما تصل الرسالة إلى المهاجم يقوم بتغيير محتوى الرسالة ومن ثم إعادة إرسالها إلى المستقبل, و قد لا يعلم المستقبل بتعديل الرسالة من قبل المهاجم
- هجوم التزوير أو الفبركة Fabrication Attack، الشكل 1.7، هنا يرسل المهاجم رسالة الي احد اطراف الاتصال مفادها إن جهة موثوق فيها تطلب منه معلومات أو كلمات سرية خاصة به مثلا.
- هجوم إعادة الإرسال Replay attack، هنا يستلم المهاجم نسخة من الرسالة المرسلة من A إلى B ثم يعيد إرسالها لاحقا للتأثير على العمليات في الطرف B أو قد يستخلص منها على معلومات تساعده علي مهاجمة النظام مستقبلا، الشكل 1.8.



الشكل 1.6: هجوم تعديل الرسالة



الشكل 1.7: هجوم التزوير



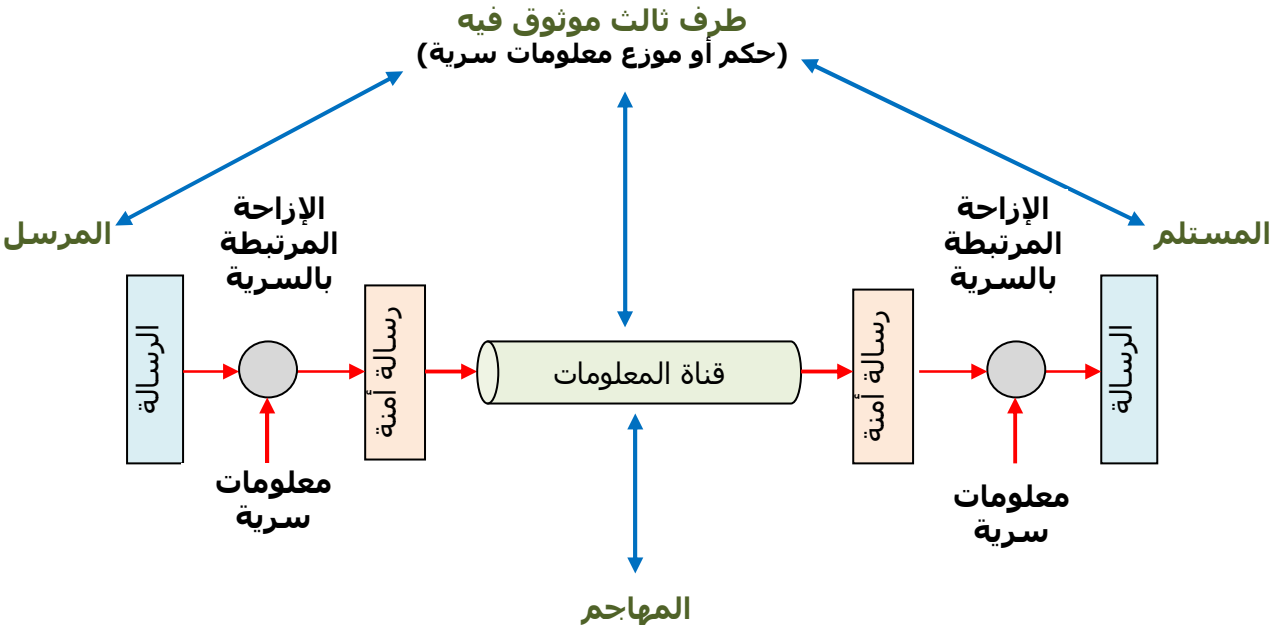
الشكل 1.7: هجوم إعادة الإرسال

1.12. نموذج امن الشبكات

الشكل 1.8 يوضح نماذج انسياب المعلومات على قنوات الاتصال ألآمنة، في حالة تواجد مهاجم (خصم) محتمل. يعتمد نموذج الاتصال الأمن هذا على آليات نقل أمنة (استخدام خوارزميات تشفير) مع مفتاح مناسب يمكن أن يتفاوض عليه مع طرف ثالث موثوقاً فيه. بدراسة هذه النموذج العام تتضح ضرورة القيام بأربعة مهام أساسية لتصميم خدمة اتصال أمنة وهي:

- تصميم خوارزمية مناسبة للنقل الآمن (خوارزمية تشفير)
- توليد معلومات سرية (مفاتيح) لاستخدامها مع الخوارزميات
- تطوير أساليب للمشاركة في المعلومات السرية وتوزيعها
- تحديد برتوكول يمكن من أطراف الاتصال من استخدام النقل والمعلومات السرية لخدمة الأمن.

هذه المطلوبات سندرسها بالتفصيل في الوحدات القادمة.

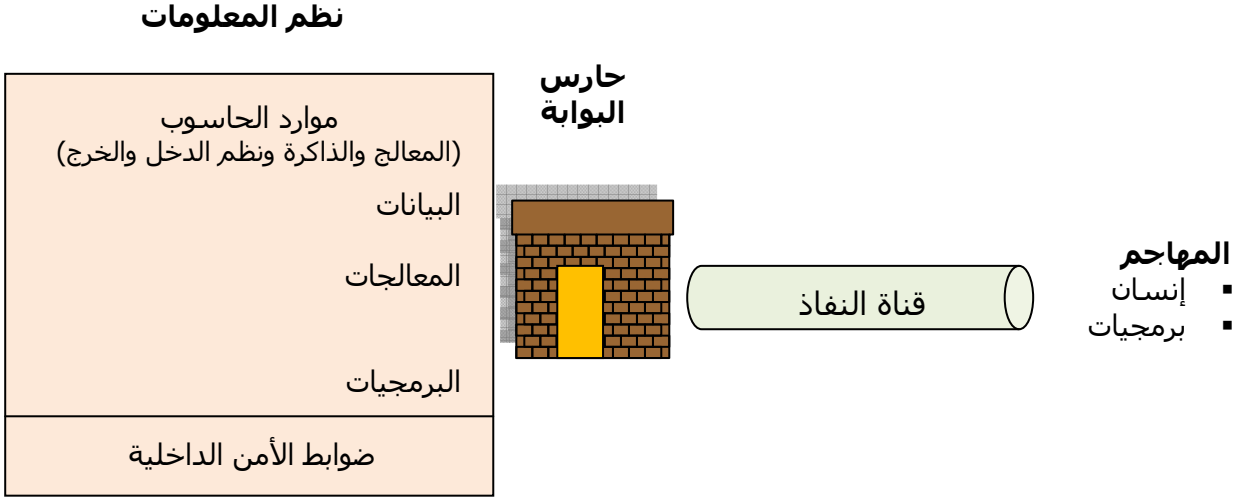


الشكل 1.8: نموذج الاتصال الأمن

الشكل 1.9، يوضح نموذج نفاذ امن إلى الشبكة، حيث يضبط النفاذ إلى المعلومات والموارد في نظم الحاسوب والشبكة وفي حالة تواجد مهاجم محتمل. هنا نحتاج إلى إجراءات مناسبة ضبط النفاذ إلى النظام لتوفير مستوى امن مناسب، وقد يكون استخدام بعض أساليب التشفير مفيداً هنا. إن استخدام نموذج النفاذ الآمن هذا يتطلب:

- تواجد حارس بوابة (منفذ) لتحقق من المستخدمين
- تنفيذ ضوابط أمنية للتأكد من نفاذ المستخدمين المخول لهم فقط إلى المعلومات والموارد.

إن استخدام نظم حاسوب ذات موثوقية قد يكون مفيداً لتنفيذ هذا النموذج، وهذا ما سندرسه في الوحدات القادمة في هذا المقرر.



الشكل 1.9: نموذج النفاذ الأمن

ملخص:

في هذه الوحدة درسنا الأتي:

- امن الشبكات والمعلومات وشرح أهميتهما
- تحديد مطلوبات امن نظم الحاسوب والشبكات
- تحديد المخاطر التي قد تتعرض لها شبكات المعلومات
- تحديد الثغرات في الشبكات وأنواع الهجمات التي قد تتعرض لها
- نماذج الشبكة والنفاذ الأمن في الشبكات

أسئلة:

1. صنف كل من الحالات التالية على إلى ثغرات سرية أو سلامة أو خليط منهم:
   أ. أستنسخ هيثم حل واجب على.
   ب. غير هيثم قيمة شيك على من 100 جنيه إلى 1000 جنيه
   ج. سجل هيثم أسم النطاق sudanopenuniv.edu.sd ورفض لجامعة السودان المفتوحة بشراء أو استخدام اسم النطاق هذا.
   د. تحصل هيثم على بطاقة ائتمان على، وقامت الجهة المصدرة للبطاقة بإلغائها وتغييرها ببطاقة أخري تحمل رقم حساب مختلف

2. أعطي مثال (مع الشرح) لكل من الحالات التالية:
   أ. أن يكون الاحتراز أكثر أهمية من كشف الاختراق والاسترجاع من الهجوم
   ب. أن يكون كشف الاختراق أكثر أهمية من الاحتراز والاسترجاع من الهجوم

ج. أن يكون الاسترجاع من الهجوم أكثر أهمية من اكتشاف الهجوم والاسترجاع منه.

3. في مجال امن الحاسوب والشبكات يستخدم المهاجمين (المخترقين) وأخصائي الأمن نفس الأدوات لمواجهة بعضهم البعض، في حالة شبيهة بحالة المجرمين والشرطة. تشمم الحزم packet sniffer أداة تسمح للمستخدم بترشيح حزم برتوكول TCP/IP على الشبكات على أساس مجموعة من الخواص تضع من قبل المستخدم. مثلا أن يسمح فقط بمرور الحزم التي يكون مصدرها أو مقصدها عنوان برتوكول انترنت محدد، أو لديها محتويات محددة، الخ.
   أ. أشرح كيف يمكن للمخترق استخدام هذه الأداة. ما هي المعلومات التي يمكن أن يجمعها؟ ماهية الصعوبات التي قد تواجهه؟
   ب. أشرح كيف يمكن مدير الشبكة أو أخصائي الأمن استخدام هذه الأداة لحماية النظام من الهجمات والاختراق. ما هو الالتفاف الذي قد يقوم به المهاجم لتفادي هذه الإجراءات الأمنية؟

4. لنفترض إن احد المخترقين يود النفاذ إلى الانترنت باستخدام حاسوبه المحمول وعبر شبكة مؤسستك. ولكن هذه المهاجم لا يملك تعريف هوية بالشبكة تخوله لاستخدامها وللحصول على عنوان برتوكول انترنت فيها. أشرح كيف يمكن لهذا المخترق بالنفاذ إلى الانترنت عبر شبكة مؤسستك ودن استخدام هوية مسجلة بها.

5. وضح الخطوات الضرورية التي يجب إتباعها لوضع سياسة أمنية مناسبة للمعلومات والشبكات. أضع سياسة امن معلومات وشبكات لمؤسسة من اختيارك.

6. أشرح الثغرات والمخاطر الأمنية المختلفة التي قد يقابلها موقع للتجارة الالكترونية والمستفيدون منه. أذكر الأساليب الاحترازية التي قد تستخدم لكل من هذه المخاطر والثغرات.

أهداف الوحدة:
في نهاية هذه الوحدة سيكون بمقدورك:
- تعريف على أساليب التسفير المتناظر
- استخدام خوارزميات مختلفة للتشفير المتناظر التقليدي
- التعرف على علم الإخفاء (Steganography)

2.1. مقدمة

علم التعمية Cryptography أو التشفير encryption واحد من المجالات المهمة والمعقدة في نفس الوقت في مجال الحاسوب والشبكات، وقد ازداد الطلب على تقنيات التشفير (التعمية) في البرامج التي يستخدمها العامة من الناس مع انتشار الانترنت بسبب الحاجة لنقل المعلومات السرية والخاصة على شبكة عمومية، حيث يسهل اعتراض المعلومات فيها والتجسس على اتصالاتها.

هنالك عدة أساليب أو طرق للتشفير Encryption Schemes، لكل منها نقاط قوتها وضعفها واستخداماتها، وهذه الأساليب هي أفكار عامة وليست تطبيقات عملية للتشفير، أما التطبيقات العملية للتشفير فتسمى خوارزميات التشفير Encryption Algorithms، وسيتضح الفرق بينهما أكثر عندما نأخذ أمثلة عل كل منهما في هذه الوحدة والوحدات اللاحقة.

تتمثل عملية التشفير في إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة أو تحويلها إلى رموز غير ذات معنى، بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهمها واستغلالها. و لهذا تنطوي عملية التشفير بكل بساطة على تحويل النصوص العادية الواضحة إلى نصوص مشفرة غير مفهومة، وهي مبنية على مفهوم أساسي مفاده أن كل معلومة مشفرة تحتاج لفكها و إعادتها إلى وضعها الأصلي .

تستخدم المفاتيح keys (وهى معلومات سرية) في تشفير Encryption النصوص المرسلة و فك تشفيرها Decryption من قبل صاحبها المسموح له بتسلمها. و تستند هذه المفاتيح إلى صيغ رياضية قد تكون معقدة على هيئة خوارزميات. و ترتكز قوة و فعالية التشفير على نوعية الخوارزميات المستخدمة و طول المفتاح الذي يقاس بعدد الثنائيات Bits المستخدمة في بنائه .

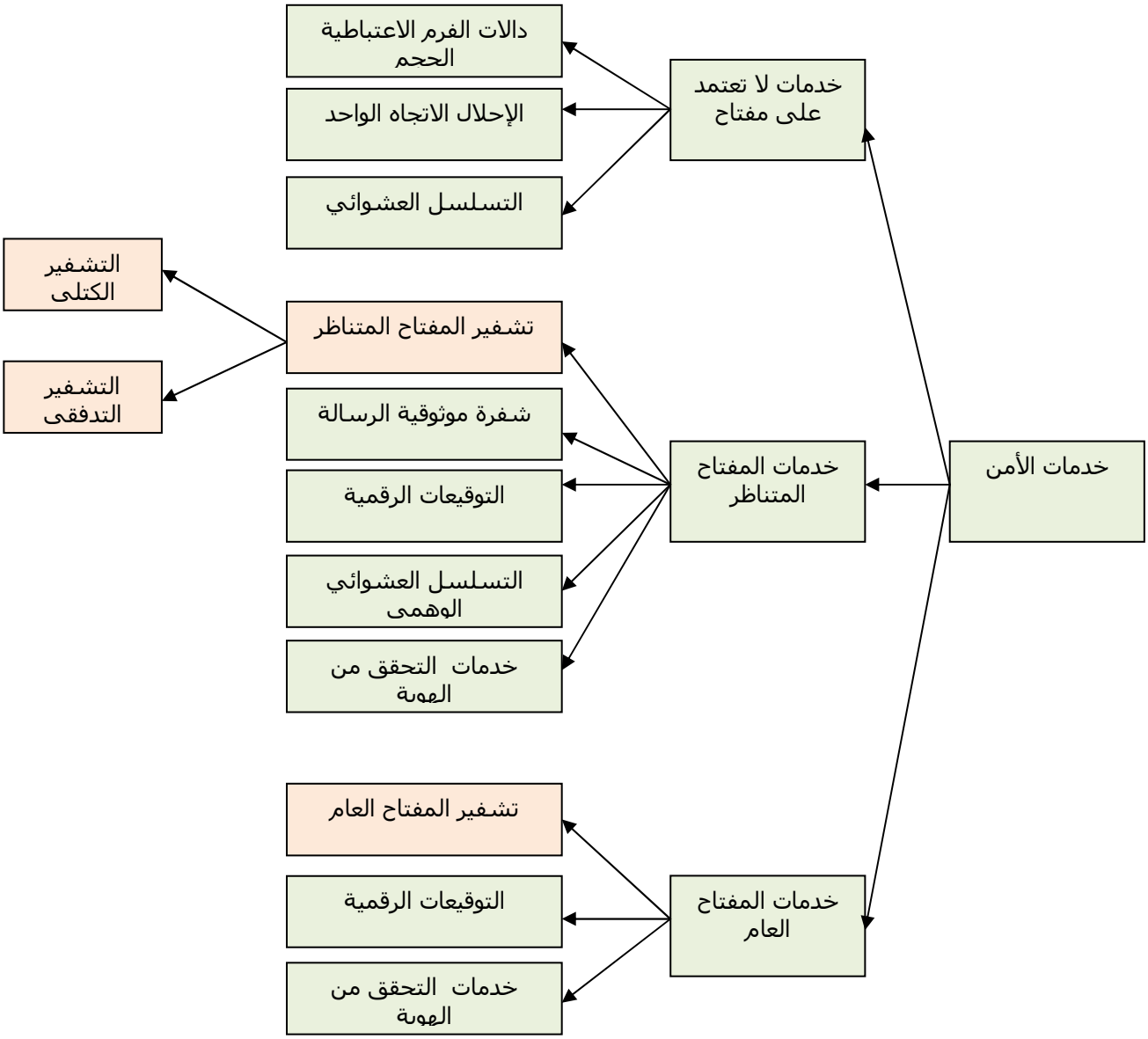
كانت عملية التشفير، و لا زالت في بعض الحالات، تتم بواسطة مفتاح سري يستخدم لتشفير النصوص و في نفس الوقت لفك تشفيرها و ترجمتها إلى وضعها الأصلي، وهو ما نعبر عنه بالتشفير المتناظر Symmetric Encryption، كما يسمى أيضا بالتشفير الأساسي أو التشفير باستخدام المفتاح الواحد. أسلوب التشفير هذا مفيد من حيث قدرته على تحويل محتوى الرسالة الأصلية إلى معلومات غير مفهومة، و لكن تعدد ملكية المفتاح السري لا تجعل المتعاملين معه في مأمن من إمكانية الحصول عليه من قبل جهات غير مخول لها في استخدامه لفك تشفير المعلومات. وسندرس في هذه الوحدة بعض أساليب وخوارزميات خواص التشفير المتناظر التقليدي.

لاحقا استخدم أسلوب التشفير غير المتناظر Asymmetric Encryption كحلا لمشكلة التوزيع غير الآمن للمفاتيح في مجال التشفير المتناظر. فعوضا عن استخدام مفتاح واحد، يستخدم التشفير غير المتناظر مفتاحين اثنين مرتبطين بعلاقة رياضية عند بنائهما. و يدعى هذان المفتاحان بالمفتاح العام Public key ، والمفتاح الخاصPrivate key . فالمفتاح الخاص يكون معروفا لدى شخص واحد أو جهة واحدة فقط، وهو المرسل، يستخدم لتشفير النصوص أو فك شفرتها. و أما المفتاح العام فهو معروف لدى أكثر من جهة أو شخص، يستطيع فك شفرة النصوص التي تم تشفيرها بواسطة المفتاح الخاص. و يمكن استخدامه أيضا لتشفير الرسائل الموجهة لصاحب المفتاح الخاص، و لكن ليس بإمكان أحد استخدام المفتاح العام لفك شفرة رسالة تم تشفيرها بواسطة هذا المفتاح العام إذ أن صاحب المفتاح الخاص هو الوحيد الذي يستطيع فك شفرة الرسائل التي شفرها المفتاح العام .

هنالك عدة خوارزميات تستخدم للتشفير المتناظر، ولعل أشهرها على الإطلاق هي خوارزمية معيار تشفير البيانات Data Encryption Standard, DES التي لا تزال تستخدم على نطاق واسع لتحقيق الاتصال الآمن على شبكات المعلومات وسندرس هذه الخوارزمية في الوحدة الثالثة.

خوارزمية DES بدأت تظهر ضعفا خلال السنوات الأخيرة أمام أساليب تحليل التشفير، واستبدلت في كثير من التطبيقات بنسخ معدلة منها مثل خوارزمية معيار تشفير البيانات الثلاثية Triple DES، كما أن DES استبدلت كليا في كثير من الأحيان بخوارزمية معيار التشفير المتقدم Standard Advanced Encryption AES والتي سندرسها في الوحدة الرابعة.

الشكل 2.1 يوضح تصنيف أساليب التشفير المستخدمة في امن المعلومات والشبكات وارتباطها بخدمات الأمن.



الشكل 2.1: تصنيف خدمات الأمن وأساليب التشفير

2.2. مصطلحات وتعاريف:

خلال دراستنا للتشفير أو التعمية سنستخدم المصطلحات التالية:

- *النص الصريح* plaintext، ويستخدم هذا المصطلح لتعريف الرسالة الأصلية
- *النص المشفر* ciphertext، ويطلق هذا المصطلح على الرسالة المشفرة أو المعماة
- *عملية التشفير* enciphering أو *التعمية* encryption، وتشير إلى عملية تحويل النص الصريح إلى نص مشفر
- *فك التشفير* deciphering أو *فك التعمية* decryption، وتعنى عملية استرجاع النص الصريح من النص المشفر
- *التعمية cryptography* ويستخدم هذا التعبير لتعريف مجموعة المخططات والطرق المستخدمة لإنجاز عملية التعمية ويدعى المخطط الواحد *بنظام التعمية* cryptographic system أو *نظام التشفير* cipher
- *تحليل الشفرة* Cryptanalysis ويطلق هذا المصطلح على التقنيات والأساليب المستخدمة لفك تشفير الرسالة المشفرة دون معرفة تفاصيل نظام التشفير المستخدم، ويستخدم في كثير من الأحيان المصطلح *كسر الشفرة* breaking the code للإشارة إلى هذه العملية.
- علم التعمية Cryptography، ويشير المصطلح إلى طرق وأساليب تشكيل التعمية وتحليلها.

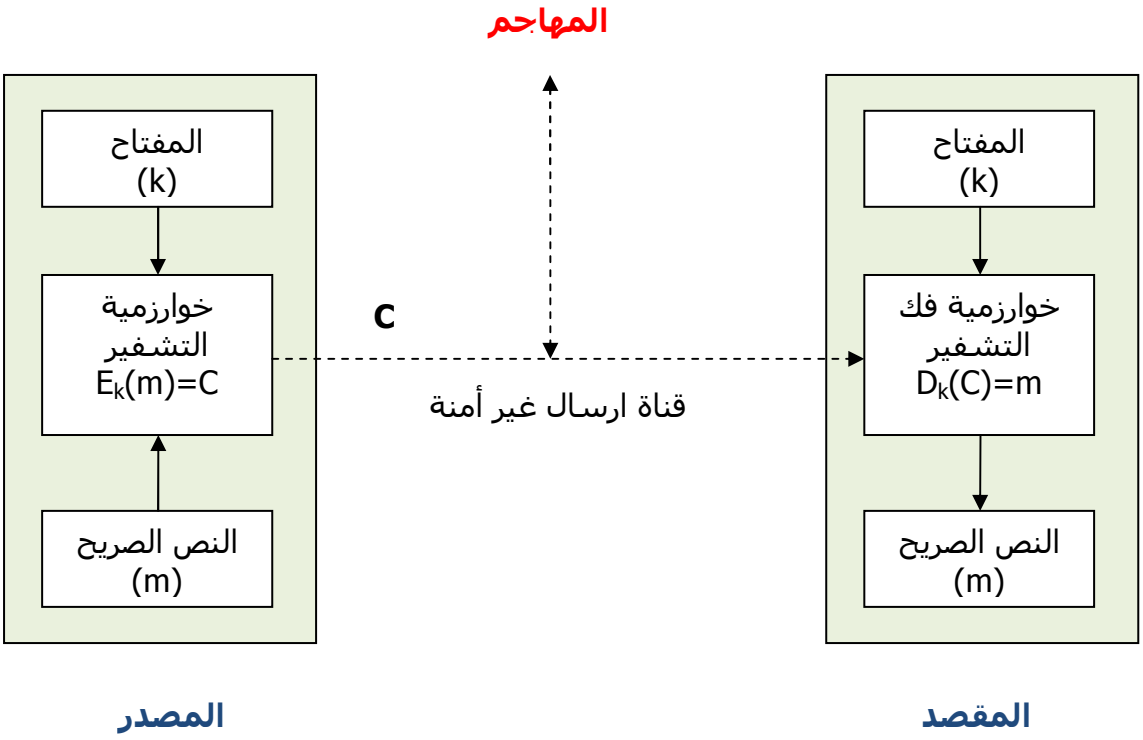
تصنف نظم التشفير على الأسس التالية (انظر الشكل 2.1):

- *أسلوب عملية التشفير*، حيث تعتمد كل عمليات التشفير على الإحلال (الاستبدال) substitution أو النقل transportation. في عمليات الإحلال يتم استبدال إي عنصر في النص الصريح (خانة أو حرف أو مجموعة خانات أو ثنائيات الخ) بعنصر أخر محدد مقابل له. أما في عملية النقل فيتم إعادة ترتيب العناصر في النص الصريح مع ضرورة عدم إضاعة أي عنصر، حتى تكون كل العمليات معكوسة. وقد تتضمن نظم التشفير عدة مراحل من الإحلال والنقل.
- *عدد المفاتيح المستخدمة*، عند استخدام كل من المرسل والمستقبل نفس المفتاح، يطلق على نظام التشفير نظام التشفير المتناظر أو التشفير بمفتاح واحد أو التشفير الأساسي. أما إذا استخدم كل من المرسل والمستقبل مفتاحين مختلفين عن بعضهما البعض يسمى نظام التشفير بنظام التشفير غير المتناظر أو نظام المفتاحين أو التشفير بالمفتاح العمومي.
- *طريقة معالج النص الصريح*، قد يعالج الدخل (النص الصريح) على هيئة كتلة block واحدة من العناصر في كل مرة، مما ينتج في الخرج كتلة تتوافق مع كتلة الدخل ويعرف هذا بالتشفير الكتلي block chipper، كما يمكن أن يتم التعامل مع الدخل وفق تتدفق العناصر وعلى التوالي باعتبار عنصرا واحدا في أي وقت، مما ينتج خرجا على هيئة سلسلة، ويعرف هذا بالتشفير التدفقي stream chipper.

2.3. نظم التشفير المتناظر

الشكل 2.2 يوضح مكونات نظام التشفير المتناظر المستخدم لتوفير اتصال آمن بين طرفين على قناة اتصال غير أمنة. تكون هذا النظام من الأجزاء الخمسة التالية:

- *النص الصريح* m، والذي يمثل الرسالة التي يراد تشفيرها وتمثل الدخل إلى خوارزمية التشفير
- *خوارزمية التشفير* $E_k(m)$، وتطبق على النص الصريح لإنتاج النص المشفر، وتمثل عادة بعلاقات رياضية
- *المفتاح السري k*، وهو عبارة عن قيمة سرية تستخدم بواسطة الخوارزمية لتشفير النص الصريح، حيث تعتمد عملية التشفير على هذا المفتاح الذي قد يتغير من عملية تشفير إلى أخرى
- *النص المشفر C*، هو الرسالة غير الواضحة الناتجة من عملية التشفير، وتعتمد على النص الصريح والمفتاح السري وخوارزمية التشفير.
- *خوارزمية فك التشفير* $D_k(C)$، وعادة تكون نفس خوارزمية التشفير ولكن تعمل بشكل معكوس، حيث يكون دخلها النص المشفر والمفتاح السري وخرجها النص الصريح.



الشكل 2.2: الاتصال الأمن باستخدام التشفير

إذا افترضنا إن

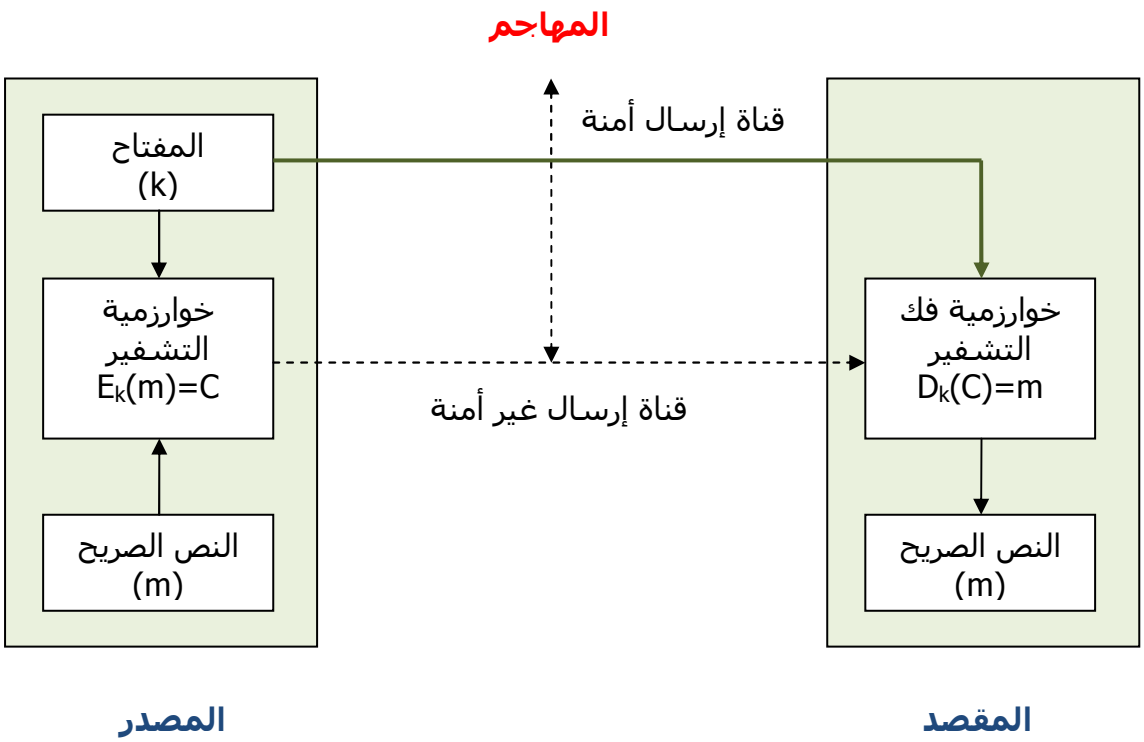
- النص الأصلي = m حيث $m=[m_1m_2 \dots m_M]$ وتمثل المكونات m_1 و m_2 و ... و m_M الحروف او الثنائيات أو الثمانيات المكونة للرسالة
- والنص المشفر = C حيث $C=[C_1C_2 \dots C_N]$ وتمثل المكونات C_1 و C_2 و ... و C_N الحروف او الثنائيات أو الثمانيات المكونة للرسالة
- المفتاح = k، حيث $k=[k_1k_2 \dots k_J]$ وتمثل المكونات k_1 و k_2 و ... و k_J الحروف او الثنائيات أو الثمانيات المكونة للمفتاح

يمكن التعبير عن نظام التشفير هذا رياضيا كالآتي:

$$C=E_k(m) \quad \text{.....2.1}$$
$$m=D_k(C) \quad \text{.....2.2}$$

حيث يمثل E_k خوارزمية التشفير و D_k خوارزمية فك التشفير.

ينتج المفتاح السري بواسطة المرسل فلابد من إيجاد قناة اتصال أمنة لإرسال هذا المفتاح إلى المستقبل لاستخدامه في عملية فك التشفير، كما هو موضح في الشكل 2.3.



الشكل 2.2: الاتصال الآمن باستخدام التشفير قناة إرسال أمنة لتبادل المفتاح

2.4. تحليل التشفير

هناك أسلوبان يمكن استخدامهما لمعرفة النص الصريح ولفك تشفير الرسالة المشفرة دون معرفة تفاصيل نظام التشفير المستخدم أو المفتاح مسبقاً، وهما:

- *تحليل التشفير*: ويعتمد هذا الأسلوب على تحليل التشفير بناء خوارزمية معينة والاعتماد على بعض معطيات النص الصريح المعروفة للمحلل (المهاجم) لاستنتاج النص الصريح أو استنتاج المفتاح المستخدم. يتطلب هذا الأسلوب أن تكون خوارزمية التشفير معروفة بالنسبة للمحلل. قد يستخدم المحلل بعض الطرق الإحصائية للحصول على النص الصريح أو المفتاح.

- *هجوم الكسر الأعمى أو البحث الشامل*، في هذا الأسلوب يحاول المهاجم تجريب كل المفاتيح المحتملة على مقطع من النص المشفر ويستمر في هذه المحاولات حتى يتحصل على نص صريح مفهوم وواضح. في هذا الأسلوب كلما زاد طول المفتاح أصبح كسر الشفرة أكثر صعوبة. إن الزمن المطلوب لتحليل الشفرة بهذا الأسلوب يعتمد بدرجة كبيرة على مقدرات الحاسوب المستخدم.

يعتبر أسلوب التشفير "أمنا بشكل مطلق" unconditionally secure إن لم يحتوى النص المشفر على معلومات كافية لاستنتاج النص الصريح المقابل له مهما بلغ عدد النصوص المشرفة المتوفرة لدى المحلل. ومن المفروض في هذه الحالة أن لا يتمكن المحلل فك تشفير الرسالة مهما توفر له من الوقت والقدرة الحاسوبية، حيث لا تتوفر المعلومات اللازمة لذلك. لا توجد خوارزمية تشفير أمنة بشكل مطلق، إلا في حالة أساليب التشفير المعروفة باسم "الطبعة التي تستخدم مرة واحدة" (one-time pad). لذلك تصمم خوارزميات التشفير بناءَ على الأتي:

- أن تكون تكلفة تحليل الشفرة تفوق قيمة المعلومات المشفرة
- أن يكون الزمن اللازم لتحليل الشفرة يفوق الفترة الزمنية المفيدة للمعلومات المشفرة.

إن توفرت هذه الشروط في أسلوب التشفير يعتبر الأسلوب "أمنا نسبياً" computationally secure. وتكمن الصعوبة هنا في تقدير حجم المجهود اللازم لتحليل النص المشفر بنجاح.

2.5. التشفير بالإحلال

تعتمد نظم أساليب تشفير الإحلال substitution chipper على خوارزميات التشفير المتناظر والمفتاح الواحد والخاص, حيث يستخدم مفتاح واحد وخاص لتشفير وفك تشفير الرسالة من قبل كل من المرسل والمستقبل. وتعتبر هذه التقنيات أساس لجميع تقنيات التشفير وتساعد دراستها على توضيح نظم التشفير المستخدمة حاليا. بصورة عامة يحتاج نظام التشفير إلى خوارزمية قوية ومفتاح سرى معروف للمرسل والمستقبل فقط. وكمثال بسيط على ذلك نأخذ على سبيل المثال كلمة "sudan" ونفترض أن الخطوات أو الخوارزمية لتشفير هذه الكلمة هي إحلال أي حرف بالحرف الذي تليه أي:

s→T, u →W, d→E, a→B, n→ M

في هذا الكتاب سنستخدم الحرف الصغيرة لتمثيل النص الأصلي والحروف الكبيرة لتمثل النص المشفر والحروف المائلة لتمثيل المفتاح. وفي هذا المثال النص الصريح "sudan" والنص المشفر هو "TWEBM" وبذلك نكون قد أخفينا النص الصريح وعندما تصل الرسالة إلى الطرف الثاني (المستقبل) فإنه يقوم بعكس التشفير بجعل كل حرف يساوي الحرف السابق , وبذلك قد يتحصل على النص الصريح.

مستوى الحماية في هذا المثال غير مشروط حيث وبغض النظر عن مقدرات الحاسوب المستخدم لا يمكن التعرف على الشفرة المستخدمة حيث النص المشفر لا يقدم معلومات كافية عن المفتاح المستخدم أو الخوارزمية لتحديد النص الصريح.

يمكن التعبير عن تشفير الإحلال رياضيا على النحو التالي:

افترض A مجموعة حروف أبجدية مكونة من q رمز و M مجموعة الحروف (الرموز) طولها t علي A. افترض أن K مجموعة استبدالات كل رموز المجموعة A. عرف لكل مفتاح e تحويل تشفير E_e على النحو الأتي:

$$E_e = [e(m_1)e(m_2)\dots e(m_t)] = C_1C_2\dots C_t \qquad \dots.2.3$$

حيث $m = (m_1m_2\dots m_t) \in M$.

لفك تشفير $C = C_1C_2\dots C_t$ ، احسب معكوس الاستبدال $e^{-1} = d$، ثم

$$D_d = [d(C_1)d(C_2)\dots d(C_t)] = (m_1m_2\dots m_t) \qquad \dots\dots\dots 2.4$$

E_c يسمي تشفير الإحلال البسيط.

5.1. طريقة قيصر:

يعتمد تشفير الإحلال كما وضح أعلاه على استبدال العنصر في النص الصريح بعنصر مقابل له. استخدم قدماء الإغريق أساليب مختلفة لتشفير الإحلال وخاصة في المجالات العسكرية، وأشهرها ما يعرف بأسلوب قيصر (جيليوس قيصر Julius Casear) وهي من أبسط طرق التشفير وكما تعتبر من أقدم طرق التشفير. وفكرة هذه الطريقة هي استبدال أي حرف بثالث حرف بعده مثلا A→D, B→E, ... وهكذا, الجدول 2.1 يوضع الحروف المقابلة جميع الحروف اللاتينية :

الجدول 2.1: أحلال أسلوب تشفير قيصر

حروف النص الصريح	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
حروف النص المشفر (المفتاح)	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
الرقم المكافئ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

لنأخذ على سبيل المثال النص الصريح "meet me after the lecture", لتشفير هذا النص باستخدام طريقة قيصر نقوم باستبدال كل حرف بثالث حرف بعده كما هو موضح أدناه:

النص الأصلي meet me after the lecture
النص المشفر PHHW PH DIWHU WKH OHWXUH

يسمى اليوم إي أسلوب تشفير يستخدم تبديل الأحرف بطريقة قيصر.

يمكن استخدام أسلوب الكسر الأعمى ببساطة وسهولة لتحليل الشفرة الناتجة من استخدام تشفير قيصر وذلك بتجريب كل المفاتيح المحتملة والبالغ عددها 25 مفتاحا. وهذه طريقة معروفه لفك التشفير وتسمى أيضاً بأسلوب البحث الشامل Brute force Search. مما يسهل استخدام التحليل هذا الأسباب التالية:

- خوارزميات التشفير وفك التشفير معروفتان
- هناك 25 مفتاحا محتملا فقط
- لغة النص الصريح معروفة ويمكن تمييزها بسهولة.

أسئلة تقويم ذاتي 1:
شفر النص الأصلي التالي باستخدام طريقة قيصر بتبديل كل حرف بالحرف الثاني بعده:
this course is about network security

أسئلة تقويم ذاتي 2:
اوجد النص الأصلي المقابل للنص المشفر التي والذي شفر بطريقة قيصر تبديل كل حرف بالحرف الثاني بعده: GCUA VQ DTGCM

الإجابة: easy to break

باعتبار الرقم المكافئ لكل الحروف الأبجدية p_i الموضح في الجدول 2.1، يمكن التعبير عن هذه الخوارزمية كما يلي:

- لكل حرف m_i من النص الصريح، يوجد حرف استبدال (إحلال) C_i في النص المشفر، بحيث

$$C=E(p_i)=(p_i+3) \ mode(26) \ .....2.5$$

- يمكن بشكل عام يمكن إجراء الإزاحة بأية قيمة n، وبالتالي يكون:

$$C=E(p_i)=(p_i +n) \ mode(26) \ .....2.6$$

- يمكن أن يأخذ المتحول n أية قيمة بين 1 و 25، وعليه يمكن التعبير عن خوارزمية فك التسفير كما يلي:
-

$$C=D(p_i)=(p_i -n) \ mode(26).....2.7$$

2.5.2. أسلوب التشفير بمجموعة حروف واحدة Monoalphabetic

تعتمد هذه الطريقة أن يكون لدينا مفتاح ونقوم باستبدال النص الصريح بذلك المفتاح. هذه الطريقة أفضل من طريقة قيصر لان المفتاح متغير. نختار المفتاح عشوائيا, وليس هناك قاعدة محددة لاختيار المفتاح، ولكننا نحاول أن نوزع الحروف بشكل متباعد، كما هو موضح في المثال المعطي في الجدول 2.2.

الجدول 2.2: مثال لاختيار المفتاح في أسلوب التشفير بمجموعة حروف واحدة

حروف النص الصريح	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	Q	r	s	t	u	v	w	x	y	z
حروف النص المشفر (المفتاح)	D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

لنفترض على سبيل المثال النص الصريح "If we wish to replace letters"، لتشفير هذا النص باستخدام أسلوب التشفير بمجموعة حروف واحدة، نستبدل أي حرف في النص الصريح بالحرف المقابل له في المفتاح الموضح في الجدول 2.2، ولتتحصل على النص المشفر الموضح أدناه. يعرف هذا الأسلوب باسم "تشفير استبدال (إحلال) الحروف باستخدام مجموعة حروف واحدة", وذلك لأنه يتم استخدام مجموعة حروف واحدة لتشفير كل رسالة، إي مجموعة حروف وحيدة تحول النص الصريح إلى نص مشفر.

النص الأصلي	if we wish to replace letters
النص المشفر	WI RF RWAJ UH YFTSDVF SFUUFYA

العدد المحتمل للمفاتيح يساوى 26! أي $4x10^{26}$ مفتاحاً محتملاً. أن هذا العدد الكبير للمفاتيح يزيد من صعوبة تحليل الشفرة ويحد من إمكانية الكسر ألأعمى كأسلوب لتحليل الشفرة. ورغم ذلك، يعاني أسلوب التشفير هذا من ضعف ناتج من خواص اللغة. فإذا عرف المحلل طبيعة النص الصريح، مثلا نصا انجليزيا غير مضغوط، عندها يستطيع استخدام قوانين توزيع اللغة لتحليل الشفرة،

2.5.3. فائض اللغة وتحليل الشفرة

أي اللغة (سواء اللغة العربية أو اللغة الإنجليزية أو غيرهما) تستخدم أحرف زائدة في الكلمات لا تنطق، وتعرف هذه الحروف بحروف العلة، وأيضا إن استخدام الحروف في كلمات اللغة ليست متساوية. في اللغة الانجليزية على سبيل المثال الحرف E هو الأكثر استخداما ثم يأتي من بعده الحروف: T, R, N, I, O, A, S. والحروف التالية نادرة الاستخدام: Z, J, K, Q, X. الشكل 2.3 يوضح التكرار النسبي لاستخدام الحروف الأبجدية في كلمات اللغة الانجليزية، هذه النتائج ملخص دراسة أجريت في أواخر ثمانيات القرن الماضي، وتوجد في المراجع تكرار نسبي لاستخدام الحروف في أكثر من عشرين لغة اغلبها لغات أروبية.

يستخدم هذا الفائض في اللغة لضغط ملفات النص، حيث يمكن للحاسوب من استخدام ترميز مضغوط دون أن يفقد أي معلومات. تحليل الشفرة باستخدام تحليل اللغة تعتمد على تحديد التكرار النسبي لاستخدام الحروف في الرسالة المشفرة ومقارنته بالتكرار النسبي النموذجي، الموضح الشكل 2.3.

.

الشكل 2.3: التكرار النسبي النموذجي لاستخدام الحروف الانجليزية

رغم الاستخدام الشائع لتشفير استبدال الحروف باستخدام مجموعة حروف واحدة منذ القرن الأول من بعد الميلاد، يمكن تحليله وكسر شفرته باستخدام تحليل اللغة. أوضح ابن أبو الكندي طريقة لتحليل الشفرة الناتجة من أسلوب التشفير هذا، في كتابة المنشور في القرن التاسع، والذي تم اكتشافه فقط في العام 1987 في اسطنبول. يعتمد أسلوب ابن الكندي لتحليل الشفرة على الحقيقة إن التشفير لا يغير التكرار النسبي لاستخدام الحروف في النص الصريح، وأيضا كلما ما كان حجم النص المشفر كبيرا كلما زاد احتمال استنتاج النص الصريح أو المفتاح المستخدم في التشفير.

يتلخص أسلوب ابن الكندي لتحليل الشفرة من الخطوات التالية:

1. يحدد التكرار النسبي للحروف في النص المشفر ومقارنته مع التكرار النسبي المعياري للأحرف مثل الذي موضح في الشكل 2.3.
2. في حالة تشفير قيصر نبحث عن أعلى تكرار عند الحروف الثلاثة المشتركة A-E-I، وعدم وجود أجواز حروف مشتركة والحروف الثلاثة المشتركة RST، كما نبحث عن التكرار المنخفض للمجموعات JK و X-Z.
3. في حالة التشفير بمجموعة حروف واحدة نحدد تكرار كل حرف على حده، وقد تساعد جداول الحروف المجوزة و الحروف الثلاثية المشتركة في تحليل الشفرة.

مثال:

ولنأخذ على سبيل المثال النص المشفر التالي :

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETXAIZVUEPHZHMDZS
HZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMD
JUDTMOHMQ

بتحديد التكرار النسبي للحروف تتحصل على التوزيع الأتي:

الحرف	التكرار النسبي	الحرف	التكرار النسبي
P	13.33	Q	2.50
Z	11.67	T	2.50
S	8.33	A	1.67
U	8.33	B	1.67
O	7.50	G	1.67
M	6.67	Y	1.67
H	5.83	I	0.83
D	5.00	J	0.83
E	5.00	C	0.00
V	4.17	K	0.00
X	4.17	L	0.00
F	3.33	N	0.00
W	3.33	R	0.00

- بمقارنة هذا التكرار بالتكرار المعياري الموضح في الشكل 2.3، تتحصل على الأتي:
  - يمكن أن نستنتج أن Z,P → t,e دون التأكد من صحة ترتيبها.
  - يلاحظ أن الأحرف S و U و O و M و H في النص المشرف لديها تكرار نسبي عالي، مما يجعل الاحتمال كبير في مقابلتها لمجموعة الأحرف {a, h, i, n, o, r ,s} في النص الصريح
  - الأحرف ذات التكرار النسبي المنخفض في النص المشفر وهى J و I و Y و G و B و A قد تكون واحتمال كبير مقابلة للأحرف {b, j, q, v, x, z} في النص الصريح
- بالتخمين نفترض أن P → e و Z → t
- وبالتخمين أيضا تتحصل على ZW → th ومن ثم يكون ZWP → the
- بعد العديد من المحاولات قد نحصل على النص التالي :

it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in Moscow.

2.5.4. أسلوب تشفير بلايفير (Playfair)

كما أوضحنا أعلاه، أن أسلوب التشفير بمجموعة حروف واحدة لا يوفر اتصال امن رغم استخدامه عدد كبير من المفاتيح، حيث يمكن تحليل الشفرة بدراسة تكرار الحروف. احد الطرق التي قد تؤدى إلى تشفير أكثر أمنا هي تجميع الحروف ثم تشفيرها. أسلوب تشفير بلايفير مثال لذلك. طور هذا الأسلوب العالم Charles Wheatstone في عام 1854م ولكنها سميت بعد ذلك باسم صديقة ,Baron Playfair وكانت هذه الطريقة تستخدم لعدة سنين بين بريطانيا والولايات المتحدة الأمريكية في الحرب العالمية الأولى. يعتبر أسلوب التشفير هذا أكثر أساليب التشفير استخداما، ويتم معالجة المقاطع الثنائية في النص الصريح كوحدات متكاملة وتحول إلى مقاطع ثنائية في النص المشفر. يعتمد أسلوب تشفير بلايفير على استخدام مصفوفة حروف إبعادها 5×5 تكون باستخدام كلمة سرية (مفتاح). تعبأ المصفوفة من الشمال إلى اليمن ثم من أعلى إلى أسفل. ونبدأ بالمفتاح أولا بعد إزالة التكرار إن وجد، ثم نتبعه ببقية الحروف الأبجدية وفق ترتيبها الأبجدي مع اعتبار الحرفين I و J كحرف واحد (إبعاد المصفوفة تستوعب 25 حرفاً وعدد الحروف الانجليزية 26 حرفاً).

لنفترض المفتاح MONARCHY تعبأ المصفوفة على النحو التالي:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

يشفر كل حرفين في النص الصريح دفعة واحدة وذلك وفق القواعد التالية:

- إذا كان الحرفين حرف مكرر يتم الفصل بينهم بحرف بيني مثل الحرف X، فمثلا يتم التعامل مع كلمة balloonعلى النحو التالي ba lx lo on.
- إن كان الحرفين في نفس الصف يتم استبدال أحرف النص الصريح بالأحرف التي تليها على اليمن في النص المشفر، مع الأخذ في الاعتبار إن الحرف الذي يلي أخر حرف في الصف هو الحرف الأول من نفس الصف، فمثلا تستبدل الثنائية ar بالثنائية RM
- إن كان الحرفين على نفس العمود تستبدل أحرف النص الصريح بالأحرف التي تقع أسفلها مع الأخذ في الاعتبار إن الحرف الذي يلي الحرف الأخير في العمود هو الحرف الأول من نفس العمود، فمثلا تستبدل الثنائية mu بالثنائية CM
- إن لم تتوافق الثنائية مع القواعد أعلاه، يستبدل كل حرف بالحرف الذي يقع في نفس الصف وفى عمود الحرف الثاني، فمثلا تستبدل الثنائية hs بالثنائية BP, والثائية ea بالثنائية MI أو MJ.

ولفك التشفير نقوم بعكس الخطوات السابقة.

التشفير باستخدام أسلوب بلايفير ينتج نص مشفر أكثر أمنا مقارنة مع النص المشفر باستخدام أسلوب مجموعة الحروف الواحدة. فبينما هناك 26 حرفا فقط في أسلوب مجموعة الحروف الواحدة، يحتوى أسلوب بلايفير على 26×26 أي 676 مقطعا ثنائياً، مما يجعل استنتاج المقطع أكثر صعوبة. ومن ناحية أخرى دمج الأحرف يجعل تحليل تكرار الأحرف أكثر صعوبة أيضا. وعلى الرغم من المستوى الحماية العالي الذي تحققه هذه الشفرة، فقد تتعرض للكسر لأنها تترك قسما كبيراً من بنية النص الصريح بدون أي تأثير أو تغيير.

2.5.5. أسلوب تشفير هيل

شفرة هيل شفرة متعددة الحروف تم تطويرها من قبل العالم الرياضي هيل ليستر Lester Hill في العام 1929. يأخذ أسلوب التشفير هذا n حرفاً متتالية من النص الصريح ويستبدلهم بنفس عدد الأحرف في النص المشفر. تتم عملية الاستبدال باستخدام n معادلة خطية حيث يتم الاستعاضة عن كل حرف بقيمة رقمية كما هو موضح في الجدول 2.1.

نعتبر n=3، عندها تكون معادلات الاستبدال الخطية على النحو التالي:

$C_1=(k_{11}p_1+k_{12}p_2+k_{12}p_3) \bmod 26$ 2.8a

$C_2=(k_{21}p_1+k_{22}p_2+k_{22}p_3) \bmod 26$ 2.8b

$C_3=(k_{31}p_1+k_{32}p_2+k_{32}p_3) \bmod 26$ 2.8c

يمكن التعبير عن هذه المعادلات باستخدام المصفوفات كالأتي:

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod 26 \quad \text{.....2.9}$$

أو

$$[C] = [k][p] \bmod 26 \quad \text{.....} \quad 2.10$$

حيث أن كلا من [C] و [p] شعاعان عموديان بطول 3، ويمثلان النص المشفر والنص الصريح على التوالي، أما [K] مصفوفة بأبعاد 3×3 ,تمثل مفتاح التشفير. تتم كل العمليات الحسابية بالمقياس 26.

مثال:
نفترض النص الصريح "pay more money" مفتاح التشفير المستخدم يعطى بالمصفوفة التالية:

$$[\mathbf{K}]=\begin{bmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{bmatrix}$$

يمثل الشعاع (15 0 24) الأحرف الثلاثة الأولى في النص الصريح أي pay وعندها سيكون

$$[K][p]=\begin{bmatrix}17 & 17 & 5\\ 21 & 18 & 21\\ 2 & 2 & 19\end{bmatrix}\begin{bmatrix}15\\ 0\\ 24\end{bmatrix} \ mod\ 26$$

$$=[375 \quad 819 \quad 486]\ mod\ 26$$

$$=[11 \quad 13 \quad 18] \Rightarrow LNS$$

بالمتابعة بنفس الطريقة سيكون النص المشفر الكلى المقابل للنص الصريح أعلاه هو LNSHDLEWMTRW

تتحصل على النص الصريح أي فك الشفرة باستخدام مقلوب المصفوفة [K]، والذي يرمز إليه باستخدام $[K]^{-1}$، $[K][K]^{-1}$ =[K] $[K]^{-1}$[K] = [I] حيث [I] المصفوفة الأحادية، لإيجاد مقلوب المصفوفة انظر المحلق في هذه الوحدة. في المثال أعلاه:

$$[K]^{-1}=\begin{bmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{bmatrix}$$

يعبر عن أسلوب التشفير بالعلاقة الرياضية التالية:

$$[C]=E_k(m)=[K][p_m]\ mod\ 26 \quad \ldots\ldots\ 2.11$$

$$[m]=D_k(C)=[K]^{-1}[p_c]\ mod\ 26 \quad 2.12$$

تتمثل قوة أسلوب التشفير هذا وكما هو الحال مع أسلوب بلايفير في إخفائه لخصائص توزيع تكرار الأحرف في النص المشفر. وكلما كبرت أبعاد المصفوفة تم إخفاء خصائص أكثر عن تكرار الحرف.

2.6. التشفير باستخدام مجموعات الحروف المتعددة

أسلوب التشفير باستخدام مجموعات الحروف المتعددة polyalphabetic substitution ciphers يعزز من تامين الشفرة، حيث يصبح من الصعب على المحلل استنتاج التكرار النسبي للحروف، حيث يمكن استبدال نفس الحرف في النص الصريح بحروف مختلفة في النص المشفر. في هذا الأسلوب يتوفر عدد من القواعد لاستبدال حروف النص الصريح باستخدام مجموعة حروف

واحدة ويستخدم مفتاح لتحديد أي من هذه القواعد سيتم اختيارها لإجراء عملية استبدال الحرف في النص الصريح.

2.6.1. تشفير فيجينر Vigenere Cipher

هذا الأسلوب من ابسط أساليب التشفير باستخدام مجموعات الحروف المتعددة، وتتألف مجموعة الحروف (القواعد) المستخدمة في هذه الخوارزمية من 26 شفرة قيصر مختلفة، يتم تشكيلها عن طريق الإزاحة من 0 إلى 25، وتربط كل من هذه الشفرات بحرف مفتاحي والذي يحدد الحرف المشفر المقابل للحرف في النص الصريح. يكون المفتاح متعدد الأحرف وقد يمثل بالعلاقة $K=k_1k_2...k_d$ حيث الحرف الذي ترتيبه i المفتاح، يحدد الحرف الأبجدي i المستخدم في التشفير. فمثلا شفرة فيصر الناتجة عن الإزاحة بمقدار 3 أحرف ترتبط بالحرف المفتاح d. يعطى هذا الأسلوب 26 مفتاحاً، بواقع مفتاحا لكل حرف مفتاحي كما هو موضح في الجدول 2.3. هذا الجدول يعرف بجدول فيجينر. لتشفير النص الصريح نستخدم مفتاح بطول النص نفسه، وعادة يكون بتكرار كلمة مفتاحيه محددة، ويعطى هذا المفتاح الحرف ألمفتاحي لكل حرف في النص الصريح. لاستبدال الحرف في النص الصريح يحدد الحرف ألمفتاحي المقابل له تم يستبدل بالحرف المقابل له في مفتاح هذا الحرف ألمفتاحي.

جدول 2.3: جدول فيجينر

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	حروف النص الصريح / الحرف المفتاحي
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	a
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	b
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	c
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	d
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	e
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	f
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	g
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	h
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	i
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	j
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	k
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	l
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	m
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	n
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	o
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	p
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	q
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	r
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	s
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	t
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	u
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	v
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	w
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	x
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	y
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	z

مثال:

الكلمة المفتاحية: deceptive

- النص الصريح: we are discovered save yourself
- عملية التشفير:

المفتاح	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t	i	v	e	d
النص الصريح	f	l	e	s	r	u	o	y	e	d	s	a	v	e	d	r	e	r	e	v	o	c	s	i	d	e	r	a	e	w
النص المشفر	J	G	M	L	G	Y	Q	C	H	Z	A	V	W	T	V	G	Z	R	G	N	Q	W	T	V	Z	I	C	V	T	Z

عملية فك التشفير بسيطة أيضا، فيحدد الحرف ألمفتاحي المقابل للحرف المشفر ويستبدل الحرف المشرف في المفتاح المقابل لهذا الحرف المفتاحى بالحرف المقابل له في حروف النص الصريح. تكمن قوة أسلوب التشفير هذا في وجود عدة حروف لتشفير نفس الحرف النص الصريح وفقا للحرف المفتاحى المقابل له. مما يجعل التكرار النسبي للحروف في النص المشفر غير واضحة نهائياً.

يعتمد تحلل شفرة فيجينر على طول الكلمة المفتاحية N، عند استخدام الكلمة المفتاحية deceptive مثلا، سيتم استبدال الحروف الموجودة في الخانات 1 و 10 و 19و الخ باستخدام نفس مجموعة الحروف، ومن هنا يمكننا استنتاج التكرار النسبي للحروف في النص الصريح. يمكن التخلص من هذا الضعف باستخدام كلمة مفتاحيه غير مكررة وبطول مساوي لطول الرسالة نفسها، ويعرف هذا بالمفتاح الذاتي (أو الآلي)، والذي تتحصل عليه بوصل الكلمة المفتاحية مع النص الصريح.

مثال:

المفتاح	d	e	c	e	p	t	i	v	e	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v
النص الصريح	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
النص المشفر	Z	I	C	V	T	W	Q	N	G	K	Z	E	I	I	G	A	S	X	S	T	S	L	V	V	W	L	A

2.6.2. تشفير فيرنام Vernam

على الرغم من التحسينات التي يحدثها استخدام المفتاح الذاتي في تشفير فيجينر، مازال هذا الأسلوب يعانى من ضعفا اتجاه تحليل الشفرة، وذلك لأن لكل من المفتاح والنص الصريح نفس خصائص التكرار النسبي للحروف، مما يسمح بتطبيق الأساليب الإحصائية لتحليل الشفرة. فمثلا نتوقع أن يتكرر مجموعة الحروف المقابلة للحرف المفتاحى e أكثر من مجموعة الحروف المقابلة للحرف المفتاحى t.

في تشفير فيرنام والذي طوره حيلبرت فيرتام في العام 1918، يتم اختيار كلمة مفتاحيه بطول مساوي لطول النص الصريح وليس لديها أي علاقة إحصائية معه. ويعمل هذا الأسلوب على البيانات الثنائية بدلا عن الحروف، يمكن التعبير عنه بالتالي:

$$C_i = P_i \oplus K_i \qquad .....2.13$$

حيث:

P_i: الخانة ذات الرقم i في النص الصريح
K_i: الخانة ذات الرقم i في المفتاح
C_i: الخانة ذات الرقم i في النص المشفر
$\oplus$: عملية الجمع القسري (XOR)

باستخدام هذه العلاقة تتحصل على النص المشفر باستخدام عملية الجمع القسري بين خانات النص الصريح والمفتاح. وتتم عملية فك التشفير بتطبيق عملية الجمع القسري أيضا، ولكن بين خانات النص المشفر والمفتاح على النحو التالي:

$$P_i = C_i \oplus K_i \qquad .... 2.14$$

يعتمد أسلوب التشفير هذا بصورة رئيسة على بنية المفتاح، وقد اقترح فيرنام استخدام حلقة مغلقة لتكرار المفتاح، بحيث يعمل بمفتاح طويل جداً مؤلف من كلمة مفتاحيه متكررة.

2.6.3. تشفير الطبعة المستخدمة لمرة واحدة فقط One-Time Pad

يعتبر تشفير الطبعة المستخدمة لمرة واحدة فقط نسخة محسنة من أسلوب فيرنام، حيث يستخدم مفتاح عشوائي بطول النص الصريح ولا يتكرر استخدام المفتاح، مما يجعل النص

المشفر غير قابل للكسر. النص المشفر يكون عشوائيا ولا يحمل أي معلومات إحصائية مرتبطة بالنص الصريح. ويواجه هذا الأسلوب صعوبتان أساسيتان عند التطبيق وهما:

- تشكيل عدد كبير من المفاتيح العشوائية، والذي قد يتطلب استخدام ملايين الرموز العشوائية.
- التوزيع الأمن للمفتاح وحمايتها، حيث يجب أن يمتلك كل من المرسل والمستقبل مفتاحا وحيداً لكل رسالة.

نتيجة لهذه الصعوبات العملية أن تشفير الطبعة المستخدمة مرة واحدة فقط لا يستخدم بصورة شائعة ويقتصر استخدامه في بعض الخدمات الخاصة جداً والتي تتطلب مستوى أمان عالياً جداً.

2.7. تشفير النقل Transposition Ciphers:

تعتمد كل أساليب التشفير السابقة على إحلال (استبدال) الرموز. هناك أساليب أخرى للتشفير تعتمد على تبديل مواقع الحروف وترتيباها دون تغير قيمة الحرف الصريحة، وتعتبر هذه الأساليب كتلة البناء الأساسية الثانية لنظم التشفير الحديثة.

2.7.1. تشفير وضع السياج Rail Fence

يعتبر هذا الأسلوب من أبسط أساليب التشفير بنقل مواقع الحروف. يتم كتابة النص الصريح على هيئة متواليات قطرية من عدد من الصفوف ثم تتم قراءتها على هيئة متواليات أفقية (سطريه). عدد الصفوف المستخدمة يعطى عمق السياج. فمثالا لتشفير النص الصريح meet " me after the toga party" باستخدام عمق يساوى 2، تكتب أولا هذه الرسالة الصريحة بالطريقة التالية:

m e m a t r h t g p r y
e t e f e t e o a a t

ثم نقرأ الرسالة سطراً تلو الآخر للحصول على النص المشفر على النحو التالي:

MEMATRHTGPRYETEFETEOAAT

يمكن تحلل الشفرة الناتجة من هذا الأسلوب ببساطة، ويمكن استخدام أسلوب تشفير أكثر تعقيداً بكتابة الرسالة الصريحة على هيئة مستطيل يتكون من صفوف متتالية، ثم قراءة الرسالة عموداً تلو الآخر مع تبديل هذه الأعمدة. حيث يمثل ترتيب الأعمدة مفتاح التشفير.

مثال:

- تشفير النص الصريح: attack postponed until two a.m xyz

رقم العمود	7	6	5	2	1	3	4
النص الصريح المرتب	p	k	c	a	t	t	a
	e	n	o	p	t	s	o
	t	l	i	t	n	u	d
	z	y	x	m	a	o	w

- باستخدام ترتيب الأعمدة الموضح أعلاه تتحصل على النص المشفر:

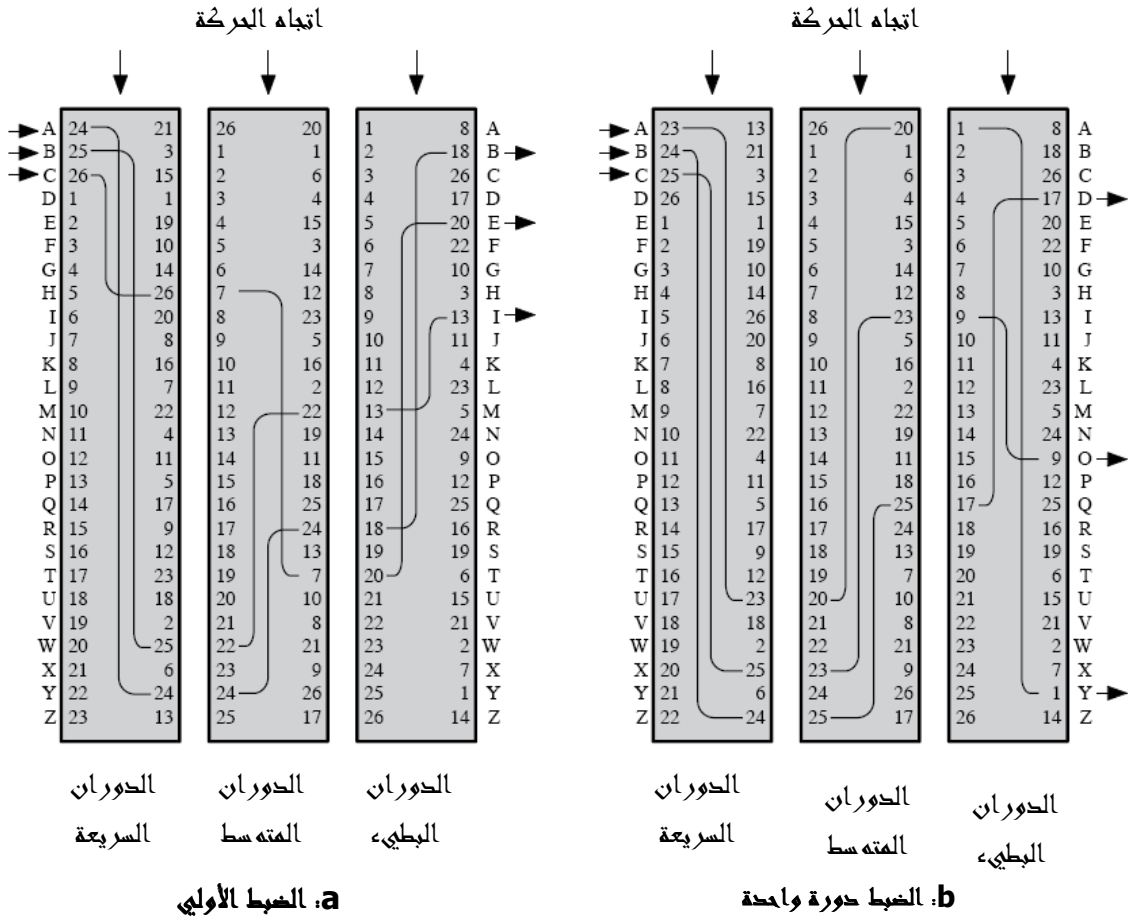
TTNAAPTMTSUOAODWCOIXKNLYPETZ

2.8. تشفير الناتج (المراحل المتعددة):

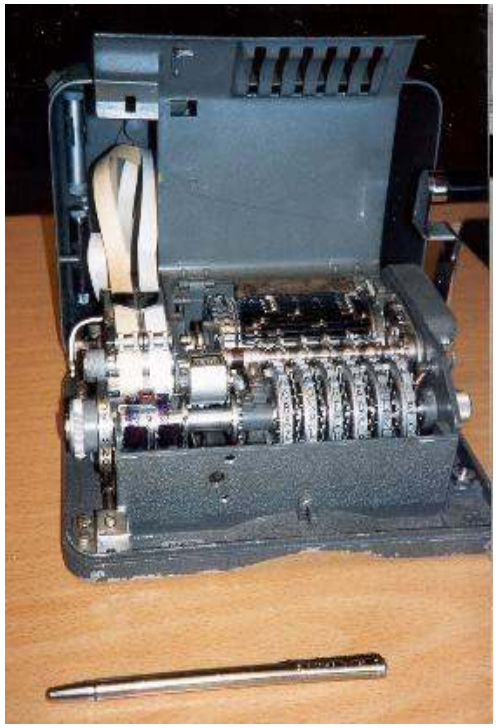
كل من أساليب التشفير بالإحلال أو النقل غير آمنة نتجه لخواص اللغة، حيث يمكن تحليلها بدراسة التكرار النسبي للحرف في النص المشفر واستنتاج النص الصريح. مما تتطلب استخدام كل من تشفير الإحلال والنقل معا لتصعيب عملية تحليل الشفرة. أن استخدام تشفير الإحلال والنقل مرتين قد يعقد من عملية التشفير ويجعلها بالغة الصعوبة. والحل العملي يتمثل في استخدام تشفير الإحلال واتباعيه بتشفير النقل. وهذا الأسلوب يعرف بأسلوب تشفير الناتج، ويمثل الأساس لكل أساليب التشفير الحديثة.

2.8.1. الآلات الدوارة

قبل استخدام أساليب التشفير الحديثة كان تشفير الآلات الدوارة Rotor Machines أكثر أساليب التشفير استخداما. يعتمد هذا الأسلوب على عدة مراحل للتشفير. حيث يستخدم عدد من الاسطوانات المستقلة عن بعضها البعض وتمر عبرها إشارات (نبضات) كهربائية. لكل اسطوانة 26 مدخلا و 26 مخرجاً، ويتم توصيل كل دخل بخرج وحيد داخلياً. كل اسطوانة تعطى تبديل واحد وتدور وتغيير بعد تشفير أي حرف. إن استخدمت ثلاثة اسطوانات على سبيل المثال تتحصل على 26^3 أي 17576 حرف أبجدي. يوضح الشكل 2.4 المبدأ الأساسي للآلات الدوارة. كما يوضح الشكل 2.5، صورة فوتوغرافية لآلة أليد هاجلين *Hagelin* Allied، *ويلاحظ هنا قلم قرب المقدمة وموضح فقط لإعطاء فكرة عن مقاس الآلة.*



الشكل 2.4: تشفير اللتة الدوارة



الشكل 2.5: لآلة أليد هاجلين

2.9: الإخفاء

يمثل الإخفاء (المواراة) أسلوباً بديلاً للتشفير، والذي يعمل على إخفاء الرسالة باستخدام بعض الأساليب الاختلاف بين الإخفاء والتشفير يتمثل في أن الإخفاء حقيقة وجود الرسالة أصلا، بينما تبقي أساليب التشفير النص ظاهرا، بعد تحويله إلى نص مبهم وغير مفهوم أو غير مقروء مباشرة. مقارنة مع التشفير يحتاج الإخفاء إلى مجهود كبير لإخفاء قليل من ثنائيات المعلومات، مما يمثل قصوراً لهذه الأسلوب. في بعض التطبيقات يتم تشفير الرسالة أولا ثم يتم إخفائها لمزيد من السرية.

يوجد عدد كبير من أساليب الإخفاء من هذه الأساليب:

- تعليم الحروف character marking، وهنا تتم الكتابة فوق الحروف المختارة المطبوعة وذلك باستخدام قلم رصاص مثلا، بحيث لا تكون الحروف المضافة مرئية ما لم تتوجه الورقة بزاوية محدد بالنسبة للضوء
- الحبر السري (غير المرئي) Invisible Ink، هناك العديد من المواد التي تستخدم بحيث لا تترك أي اثر عند الكتابة بها، ويتم إظهار الكتابة عند تعرض الورقة للحرارة أو مواد كيميائية معينة.
- التثقيب بالدبوس Pin Punctures، زهنا يتم إحداث ثقوب دقيقة فوق حروف مختارة في الرسالة المطبوعة بحيث لا تكون هذه الثقوب مرئية ما لم تتعرض الورقة مباشرة للضوء.
- إخفاء الرسالة في عناصر الصورة pixels الأقل أهمية في المناظر والصور.

ملخص:

ناقشنا في هذه الوحدة الأتي:

- أساليب التشفير التقليدية والتعبيرات المستخدمة في مجال التشفير
- أساليب تشفير الإحلال (الاستبدال) التقليدية
- تشفير الإحلال باستخدام مجموعة حروف واحدة
- تحليل الشفرة بدراسة تكرار الحروف
- التشفير باستخدام مجموعات حروف متعددة
- تشفير النقل

- تشفير الناتج والآلات الدوارة
- الإخفاء
-

أسئلة:

1. تعرف خوارزمية التشفير بالعناصر التالية:
   أ. المفتاح K
   ب. مجموعة النص الصريح P
   ج. مجموعة النص المشفر C

بحيث يوجد لكل k ∈ K دالة تشفير e_k: P ← C و دالة فك تشفير d_k: C ← P بحيث $d_x(e_x(x)=x$ لكل قيم x ∈ P. أفترض نظام تشفير للغة الإنجليزية يستخدم مفتاح (a,b) ويعرف بالعلاقة $e_k(x)=ax+b$ (mod M) علي مقياس M حيث تمثل M عدد الحروف الأبجدية. إن كانت الحروف الأبجدية تشتمل علي الحروف من A إلي Z ورمز الفراغ والنقطة.أوجد عدد المفاتيح التي يمكن أن تستخدم. هل عدد المفاتيح هذا اكبر أو اصغر من عدد المفاتيح الممكنة إن كانت الحروف الأبجدية تشتمل علي الحروف من A إلي Z فقط.

2. أفترض خوارزمية تشفير ينمو فيها تأدية المستخدمون الجيدون خطياً مع طول المفتاح. إذا كانت التأدية الحالية للخوارزمية على الحواسيب المستخدمة مناسبة باستخدام مفتاح طوله 64 ثنائية، وأيضا المستخدمون السيئون على وشك كسر هذه الخوارزمية باستخدام هجوم البحث الشامل. افترض أن التطور في نظم تقنيات الحاسوب ستنتج أجهزة أسرع بخمسة مرات بعد عامين مقارنة مع الأجهزة المستخدمة ألان. إذا احتفظ المستخدمون الجيدون والسيئون على نفس الحال الراهن، هل سيستفيد من هذا التطور المستخدمون السيئون أو الجيدون؟ هل توصي باستخدام طول جديد للمفتاح؟ أشرح.

3. أعتبر النص المشفر التالي :

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZVUEP
HZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFP
OMBZWPFUPZHMDJUDTMOHMQ

أ. أوجد التكرار النسبي للحروف في هذا النص وقارنه مع تكرار الحروف النسبي النموذجي الموضح في الشكل 2.3.
ب. إن استخدم التشفير بمجموعة حروف واحدة، استنتج حروف النص الصريح المقابلة للحروف P و Z في النص المشرف. ثم افحص أجواز الحروف واستنتج حروف النص الصريح المقابلة للحروف W و S في النص المشرف
ج. أذا كانت بداية النص الصريح هي: it was disclosed yesterday ، افترض أن استخدام التشفير الإحلال بمجموعة الحروف الواحدة والذي ببدء بالكلمة المفتاحية CIPHER تم تتبع ببقية الحروف الأبجدية ليعطي لاستبدال التالي.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	النص الصريح
C	I	P	H	E	R	A	B	D	F	G	J	K	L	M	N	O	Q	S	T	U	V	W	X	Y	Z	النص المشفر

هذا الإحلال لا يعطي مزج جيد للحروف، لتفادى ذلك استخدام الإحلال التالي والذي تحصل علية بكتابة الإحلال أعلاه في أعمدة (من اليسار إلى اليمن ابتداء من اعلي اليسار) ثم القراءة من الأعمدة (من أعلي إلي أسفل ابتداء من اعلي اليسار)

C I P H E R
A B D F G J

K L M N O Q
S T U V W X
Y Z

لتتحصل على سلسلة مجموعة حروف الاستبدال الواحدة التالية:
C A K S Y I B L T Z P D M U H ....

فك الشفرة واوجد بقية النص الصريح والكلمة المفتاحية للتشفير

4. *تمرين برمجة*: اكتب برنامج بلغة C++ أو أي لغة أخري، لتشفير وفك تشفير النص باستخدام تشفير فيجينر.

.5
الوحدة الثالثة: التشفير الكتلي ومعيار تشفير البيانات

أهداف الوحدة:
في نهاية هذه الوحدة سيكون بمقدورك:
- تحديد أسس تصميم التشفير الكتلي
- تحديد تفاصيل وقوة خوارزمية معيار تشفير البيانات DES
- شرح واستخدام تحليل الشفرة التفاضلي والخطى
- تحديد صيغ التشغيل المختلفة

3.1. مقدمة:

يستخدم أسلوب تشفير الكتلة block chipper بصورة واسعة اليوم لتشفير المعلومات ولتدقيق التشفير للتحقق من أن المعلومات لم تتغير. يفضل استخدام التشفير الكتلي نسبة لسرعته العالية نسبيا ومعرفتا المناسبة بمطلوبات تصميمه. يعالج التشفير التدفقي stream cipher حرف أو ثنائية أو ثمانية من النص الصريح في أي لحظة وبالمقابل يعالج التشفير الكتلي block cipher كتلة كاملة (مجموعة من الأحرف أو الثنائيات أو الثمانيات) من النص الصريح مرة واحدة، مثل إحلال رمز كبير قد يزيد حجمه عن 64 ثنائية. يتطلب تشفير الكتلة توفر البيانات قبل البدء في عملية التشفير. أساليب التشفير الكتلي المعتمدة على المفتاح المتناظر Symmetric-key block ciphers تعتبر من أكثر نظم التشفير أهمية واستخداما في كثير من التطبيقات اليوم. لا يوجد أسلوب تشفير كتلي واحد مناسب لجميع التطبيقات، حتى أن توفر مستوي عالي من الأمن والحماية لهذا لأسلوب. ويرجع السبب في ذلك إلى اختلاف مطلوب التشفير في التطبيقات المختلفة والتي قد تحددها العوامل التالية:

- السرعة المطلوبة ومحدودية الذاكرة الذي قد ينتج من حجم برنامج التشفير وحجم البيانات والذاكرة السريعة cache memory
- آليات التنفيذ مثل العتاد والبرمجيات وكروت الرقائق chipcards
- اختلاف تسامح التطبيقات مع خواص صيغ التشغيل المختلفة
- الضرورة إيجاد التوازن بين الكفاءة والأمن.

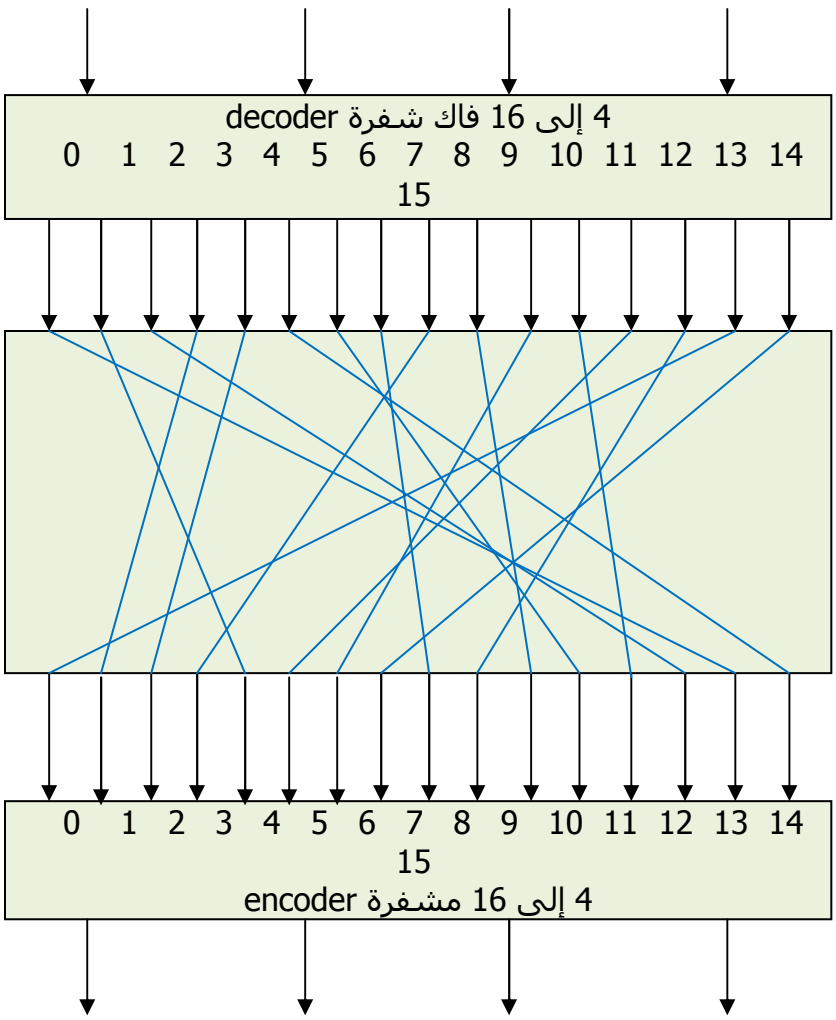
سنناقش في هذه الوحدة أساليب مختلفة للتشفير الكتلي لتحديد طريقة عملها وميزاتها ومواطن الضعف فيها. ولعل من أهم هذه الأساليب أسلوب معيار تشفير البيانات Data Encryption Standard (DES).

3.2. أساسيات التشفير الكتلي:

تعتمد أغلب خوارزميات التشفير الكتلي المتناظر المستخدمة اليوم على أسلوب تشفير يعرف بتشفير فيزتل الكتلي Feistel block cipher. يعمل التشفير الكتلي على كتلة من النص الصريح حجمها n ثنائية لإنتاج كتلة في النص المشفر متساوية لها في الحجم. استخدام تشفير الإحلال الاعتباطي العكسي يكون غير عملي بالنسبة للكتل الكبيرة، سواء من ناحية التحقيق (التنفيذ) أو الأداء. يحتاج تشفير كتلة حجمها n ثنائية إلى مفتاح طوله $nx2^n$، فمثلاً لكتلة حجمها 64 ثنائية، وهذا الحجم يعتبر مثاليا للحماية من الهجمات الإحصائية، تحتاج إلى مفتاح طوله $64x2^{64}$ ($10^{21} = 2^{70} =$1021) ثنائية. لتفادي هذه المشكلة اقترح فيزتل تقريب لنظام التشفير الكتلي المثالي لمعالجة n ثنائية، يمكن بناءه من مكونات سهلة التحقيق.

عرف فيزتل إحلال (استبدال) ثنائيات عددها 64 بالتشفير الكتلي المثالي، حيث يسمح بأقصى عدد من الربط التخطيطي بين النص الصريح والنص المشفر. فمثلا دخل طوله أربعة ثنائيات ينتج واحد من ستة عشر حالة دخل محتملة، والتي تربط تخطيطيا باستخدام تشفير الإحلال إلى حالة خرج واحدة وفريدة من حالات الخرج الستة عشر المحتملة، وكل حالة خرج تمثل بأربعة ثنائيات في نص مشفر. الربط التخطيطي للتشفير وفك التشفير يمكن أن يحدد باستخدام الجداول، كما هو موضح في الشكل 3.1. يوضح هذا الشكل إحلال بسيط لأربع

ثنائيات بحيث يربط تخطيطيا أي دخل محتمل وعشوائيا إلى خرج، مما يؤدى إلى تعقيد النظام بسرعة.



الشكل 3.1: مثال تشفير التشفير الكتلي المثالي

3.3. تشفير كلاود شانون وتشفير الاحلال والتعديل

احتوت الورقة العملية التي نشرها كلاود شانون Claude Shannon في العام 1949 علي أساسيات التشفير الكتلي الحديث، تحديا مفهوم شبكات الإحلال والتعديل substitution-permutation (S-P) networks. تعتمد شبكات الإحلال والتعديل على عملتين التشفير الأولية التي ناقشناها في الوحدة الثانية وهما:

- الإحلال (الاستبدال) (الصندوق S)
- التعديل (النقل) (الصندوق P)

تنشأ شبكات الإحلال والتعديل (شبكات S-P) من مجموعة من طبقات صناديق S منفصلة بطبقات من صناديق P، مما يعطى هيئة معقدة لتشفير المراحل المتعددة (المُنْتَج). أعطى شانون أيضاً فكرة رسائل الارتباك والانتشار، التي توفرها صناديق S وصناديق P. يقوم أسلوب

التشفير الكتلي بتحويل كتلة في النص الصريح إلى كتلة في النص المشفر، يعتمد هذا التحويل على مفتاح.

طور كلاود شانون أيضا فكرة الانتشار والارتباك confusion and diffusion، لزيادة صعوبة تحليل كتلة البناء الأساسية لنظام التشفير. يتحقق مفهوم الانتشار والارتباك باستخدام صناديق S بالاقتران مع صناديق P. تهدف آلية الانتشار إلى جعل العلاقة الإحصائية بين النص الصريح والنص المشفر أكثر تعقداً بحيث لا تسمح باستنتاج المفتاح بسهولة. بالمقابل يهدف الارتباك إلى جعل العلاقة الإحصائية بين النص المشفر والمفتاح معقدة إلى أقصى درجة ممكنة، حتى تحد من استنتاج المفتاح. آليات الانتشار والارتباك تمثل حجر الزاوية في تصميم نظم التشفير الحديثة.

3.4. تشفير فيزتل

أغلب أساليب التشفير الكتلي المتناظرة تعتمد على بنية تشفير فيزتل Feistel Cipher Structure، والذي يعتمد على مفهوم تشفير المنتج غير العكسي invertible product cipher. قد طور هورست فيزتل في بداية سبعينات القرن الماضي بنية التشفير هذه. حيث قام بتكيف شبكات الإحلال والتعديل في بنية بسيطة غير عكسية، انظر الشكل 3.1. يتلخص تشفير فيزتل على الخصائص التالية:

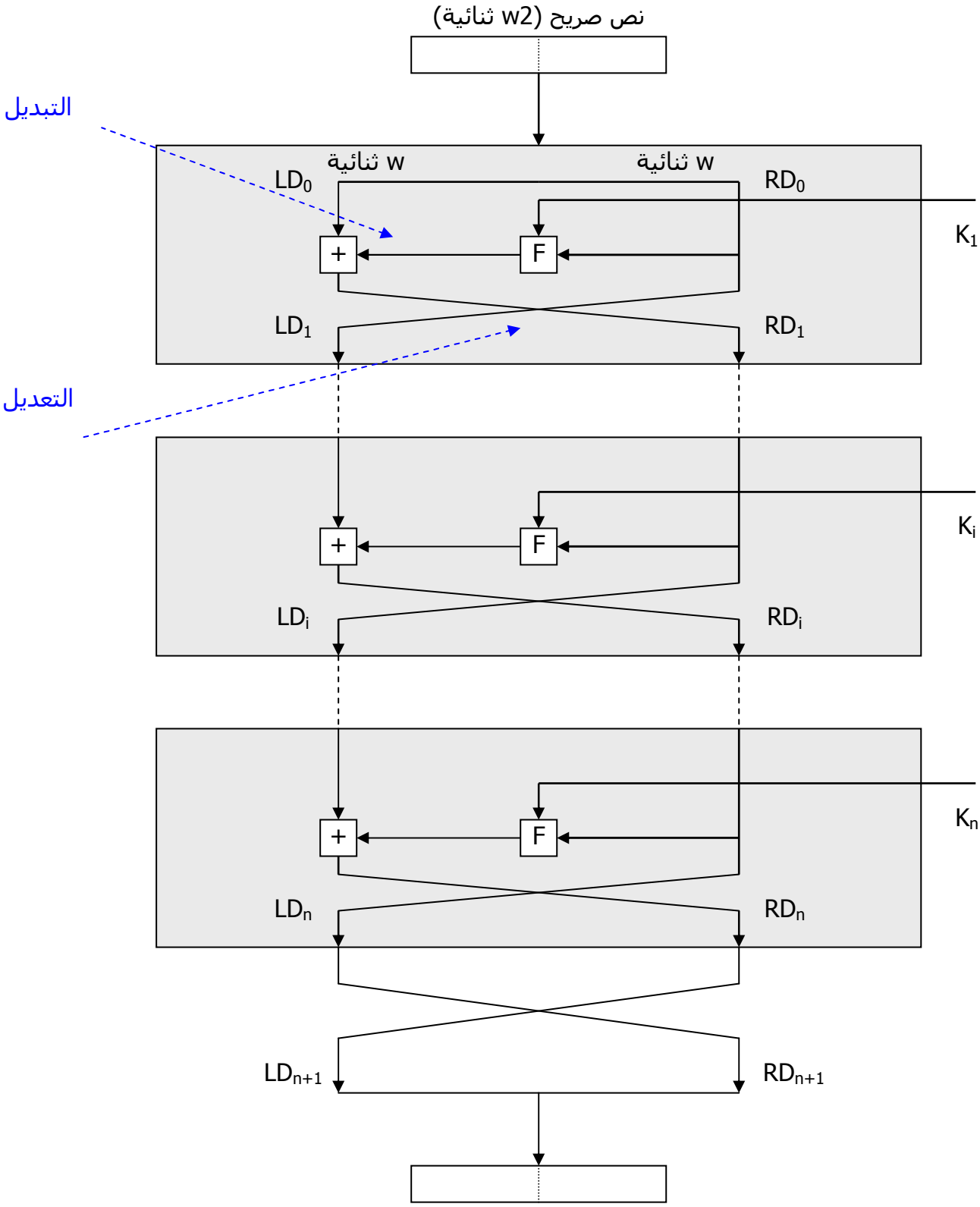
- توسعة المفتاح (تمديده) باستخدام مفاتيح فرعية ($K_1, K_2, \ldots$)
- تقسيم كتلة الدخل (البيانات) إلى نصفين ويعالجان في جولات متتالية، في كل جولة يعالج احد النصفين ثم تتم مقايضته مع النصف الأخر. يتم الإحلال في نصف البيانات الأيسر اعتماداً على دالة الجولات والنصف الأيمن للدخل ومفتاح الفرعي subkey. ثم يتم تعديل مواقع النصفين المتقاضيين
- المراحل متشابهة، كل مرحلة دالة اسطوانية F ومفتاح فرعى وعملية جمع قسري لتحقيق الإحلال والتعديل. ويمثل خرج الجولة دخل الجولة التي تليها.

يعطى خرج الجولة بالعلاقة التالية:

$$RD_i = LD_{i-1} \oplus F(RD_{i-1}, K_i)$$
$$LD_i = RD_{i-1} \qquad \ldots\ldots\ldots\ldots\ 3.1$$

حيث

- RD_{i-1} و RD_i نصف البيانات الأيمن عند دخل وخرج المرحلة i على التوالي
- LD_{i-1} و LD_i نصف البيانات الأيسر عند دخل وخرج المرحلة i على التوالي
- K_i المفتاح الفرعي للجولة i
- F الدالة الاسطوانية ويجب أن تكون غير عكسية MANGLER, INVERTIBLE



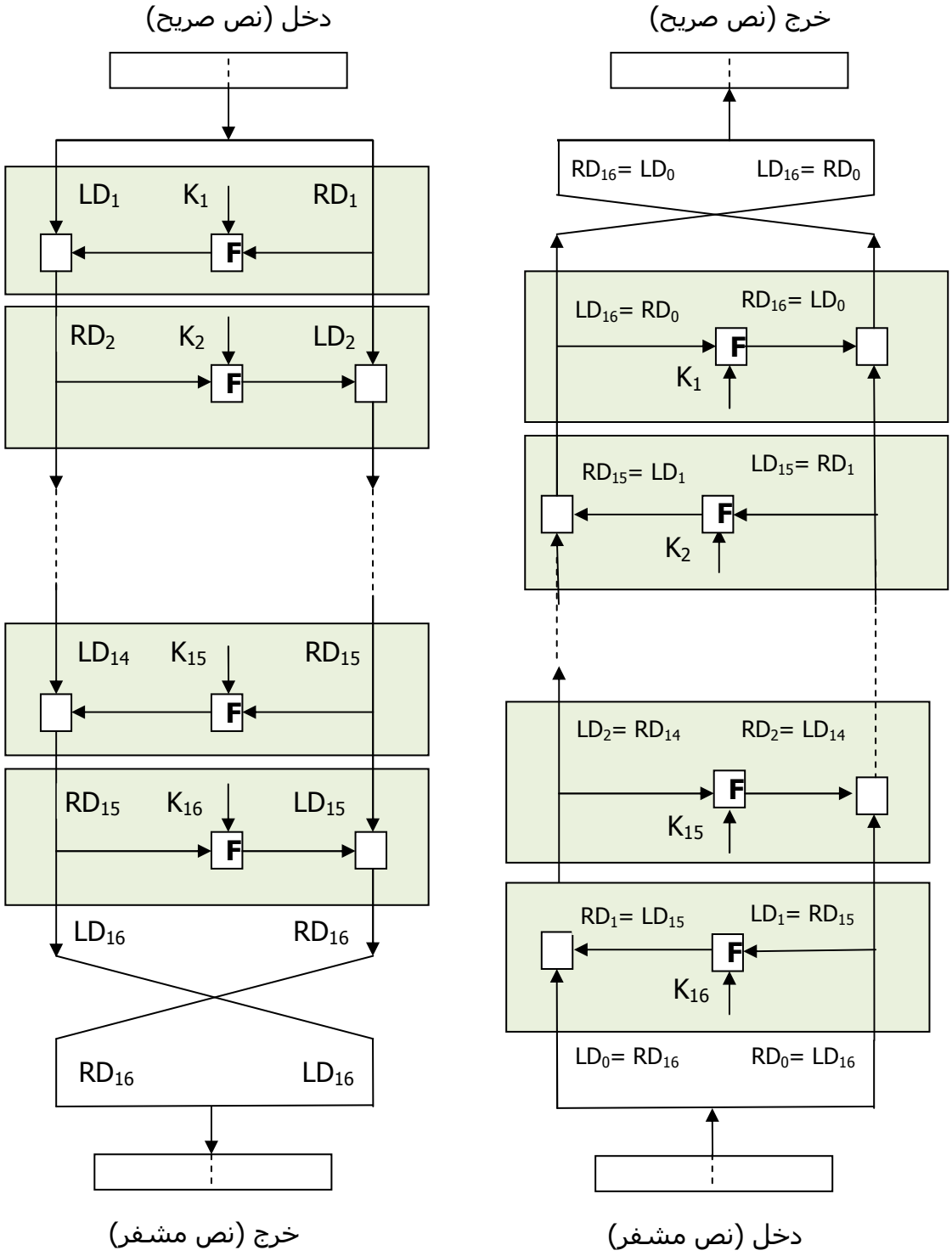
الشكل 3.1: تشفير فيزتل

يمكن تلخيص العوامل الأساسية في تصميم تشفير فيزتل في الآتي:

- حجم الكتلة: كلما ما زاد حجم الكتلة زاد امن التشفير والمقابل تتطلب عملية التشفير زمنا أطول
- حجم المفتاح: كلما ما زاد حجم المفتاح يتحسن امن الشفرة ويجعل استنتاج المفتاح أصعب والمقابل تتطلب عملية التشفير زمنا أطول.
- عدد الجولات: زيادة عدد الجولات يحسن امن التشفير، ولكنة يجعل عملية التشفير تأخذ زمنا أطول
- إنتاج المفتاح الفرعي: كلما كان المفتاح أكثر تعقيداً أصبح التحليل صعباً، ولكنه يؤدى إلى زمن تشفير أطول
- دالات الجولات: أيضا تعقيد الجولات يجعل التحليل صعباً، ولكنه يؤدى إلى زمن تشفير أطول

تشبه عملية فك التشفير في أسلوب فيزتل عملية التشفير. قانون فك التشفير يتلخص في الآتي: يمثل النص المشفر الدخل إلى الخوارزمية وتستخدم المفاتيح الفرعية K_i بترتيب معكوس، بحيث نستخدم المفتاح K_n في الجولة الأولى والمفتاح K_{n-1} في الجولة الثانية ونستمر هكذا حتى أن نستخدم المفتاح K_1 في الجولة الأخيرة، الشكل 3.2. فمن الواضح انه لا نحتاج إلى خوارزميات مختلفة للتشفير وفك التشمير مما يعتبر ميزة لهذا الأسلوب. فك التشفير يعطى بالعلاقة:

$$
\begin{aligned}
LD_1 &= RD_0 = LE_{16} = RE_{15} \\
RD_1 &= LD_0 \oplus F(RD_0, K_{16}) \\
&= RE_{16} \oplus F(RE_{15}, K_{16}) \\
&= (LE_{15} \oplus F(RE_{15}, K_{16})) \oplus F(RE_{15}, K_{16}) \\
&= LE_{15} \qquad \text{..... 3.2}
\end{aligned}
$$



الشكل 3.2:: عملية تشفير وفك تشفير فيزتل

3.5. معيار تشفير البيانات

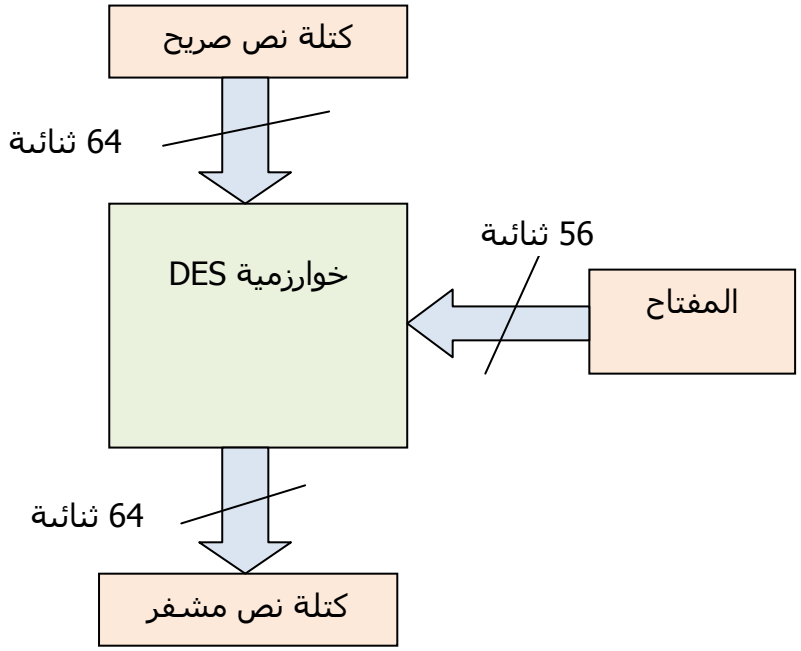
تعتبر خوارزمية معيار تشفير البيانات Data Encryption Standard (DES) من أكثر خوارزميات التشفير استخداما على نطاق العالم، منذ اعتمادها من مكتب المعايير الوطني بالولايات المتحدة الأمريكية NBS في العام 1977 بالوثيقة رقم FIPS PUB 46. تشفر الخوارزمية 64 ثنائية من البيانات باستخدام مفتاح طوله 56 ثنائية. هناك كثير من الجدل حول امن هذه الخوارزمية. نظرياً يمكن تحليل النص المشفر بخوارزمية DES باستخدام تحليل الشفرة التفاضلي أو الخطى، ورغم ذلك لا يمثل هذا مشكلة عملية في التطبيقات الواقعية.

يرجع تاريخ الخوارزمية إلى العام 1971 حين طور فريق تابع لشركة IBM خوارزمية لوسيفير والتي تعمل على كتلة معلومات حجمها 64 ثنائية ومفتاح طوله 120 ثنائية. ثم طور فريق أخر تابع لنفس الشركة هذه الخوارزمية لجعلها أكثر أمنا، كما تم تقليص طول المفتاح إلى 56 ثنائية. أعتمد المكتب الوطني للمعايير في الولايات المتحدة الأمريكية هذه الخوارزمية وأصبحت تعرف باسم معيار تشفير البيانات في العام 1977. هذه الخوارزمية ألان معتمد من قبل جهات كثيرة في العالم. كما اعتمدت نسخة معدلة منها لاحقا.

خوارزمية معيار تشفير البيانات متاحة للجميع، ومصممة بصورة جيدة، رغم ذلك فهناك جدل حول تصميم بعد جوانبها مثل اختيار الطول المناسب للمفتاح الذي يعطى نتائج أحسن، فهل يكون 56 ثنائية أم 128 ثنائية؟ هذا الجدل ناتج من أن تصميم الخوارزمية مازال سريا. أوضحت الأحداث والتحليلات بصورة عامة إن تصميم الخوارزمية مناسب. استخدمت خوارزمية DES في قطاعات مختلفة ولعل من أهمها قطاع التمويل والمصارف. التقدم في تحليل الشفرات والمقدرات الحاسوبية قد جعل طول المفتاح والذي يساوى 56 ثنائية غير امن بدرجة عالية. سوف ندرس في هذه الوحدة فقط الخواص الأساسية لخوارزمية DSE.

خوارزمية DES تعطى تشفير منتج (متعدد المراحل) Product Cipher، يتكون من عدد من جولات الإحلال والتعديل. تعتمد الخوارزمية على تشفير فيزتل الكتلي وتتعامل مع كتلة حجمها 64 ثنائية في كل مرة. صممت هذه الخوارزمية في الأساس لتنفذ باستخدام العتاد. في العام 1993 تم تنفيذها باستخدام البرمجيات. إن التشفير بواسطة البرمجيات وباستخدام هذه الخوارزمية يحتاج إلى زمناً طويلاً نسبياً (بطئ). الشكل 3.1 يعطى مخطط صندوقي لهذه الخوارزمية

خوارزمية DES لديها تأثير تتابعي كبير، حيث تغير ثنائية واحدة في الدخل يؤثر على متوسط كل ثنائيات نصف الدخل، مما يجعل الهجوم بالتخمين صعباً. صناديق S المستخدمة غير خطية، مما توفر الارتباك بجعل العلاقة الإحصائية بين النص المشفر والمفتاح غير واضحة بقدر كبير.



الشكل 3.3: تشفير خوارزمية DES

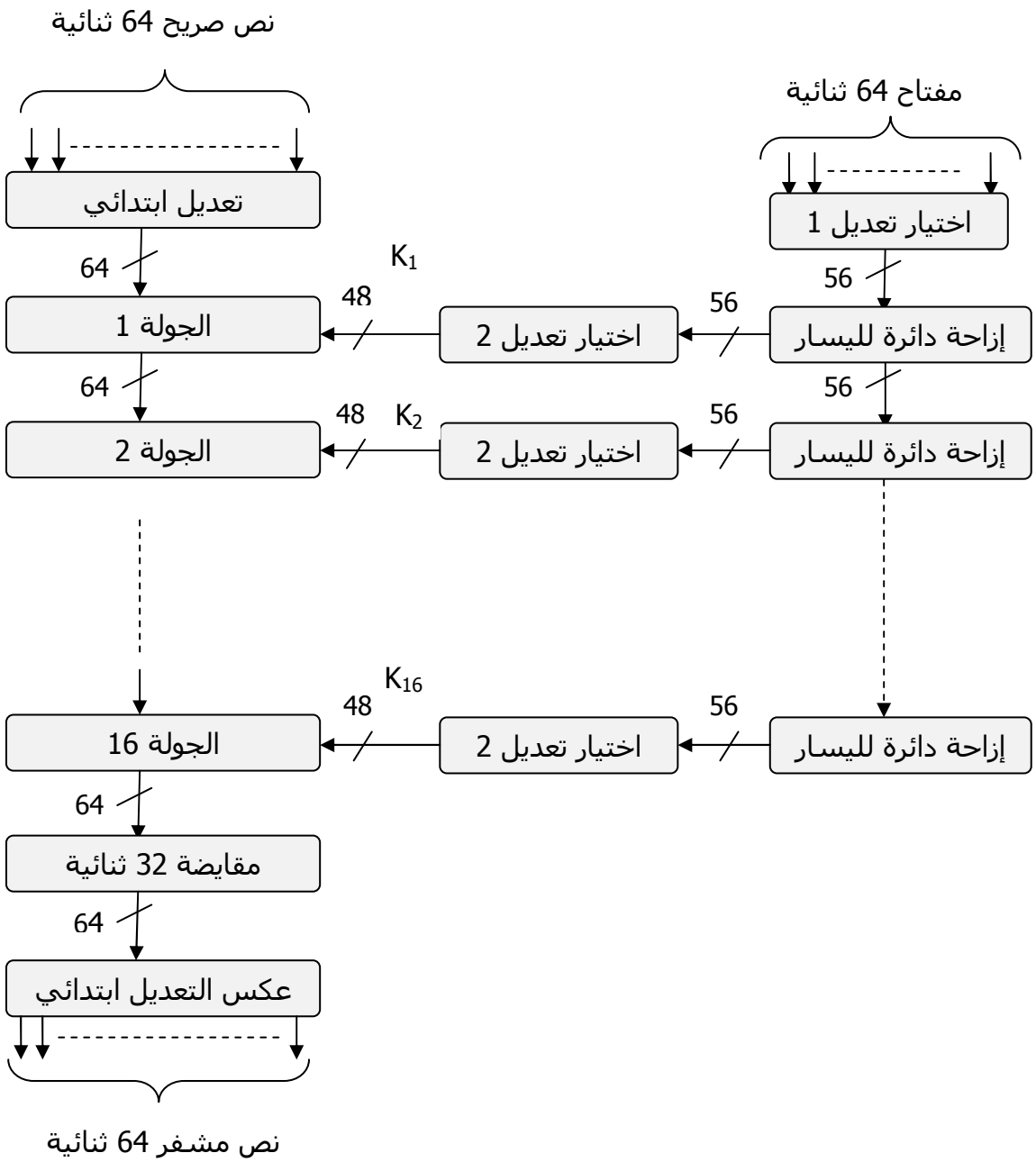
3.5.1. خوارزمية معيار تشفير البيانات:

العمليات الأساسية لتشفير كتلة بيانات حجمها 64 ثنائية باستخدام خوارزمية DES موضحة في الجهة أليسري من الشكل 3.3، وتشتمل على العمليات التالية:

- التعديل الأولي (الابتدائي) initial permutation IP
- 16 جولة من مهام مركبة تعتمد على المفتاح وتشتمل على وظائف الإحلال والتعديل
- التعديل نهائي، يمثل عكس التعديل الابتدائي final permutation IP

الجهة اليمني من الشكل توضح التعامل مع المفتاح والذي طوله 56 ثنائية، وتتكون من:

- التعديل الابتدائي للمفتاح (PC1) ويختار 56 ثنائية على نصفين كل منهم طوله 28 ثنائية
- ستة عشر مرحلة لإنتاج المفاتيح الفرعية subkeys باستخدام الإزاحة الدائرية والتعديل



الشكل 3.3: عمل خوارزمية DES

3.5.2. التعديل الابتدائي ومعكوسه

يعتبر التعديل الابتدائي الخطوة الأولى في معالجة البيانات، حيث يتم إعادة ترتب هذه البيانات بوضع الثنائيات في الخانات الزوجية even bits في النصف الأيسر والثنائيات في الخانات الفردية odd bits في النصف الأيمن. هذه العملية منتظمة البنية، ومن سهل تنفيذها باستخدام العتاد hardware.

يحدد التعديل الابتدائي ومعكوسة بواسطة جداول كما هو موضح في الجدول 3.1a والجدول 3.1b. تفسر هذه الجداول كالأتي:
دخل الجداول طوله 64 ثنائية ترقم من الشمال إلى اليمين بالأرقام العشرية من 1 إلى 64. الأربع وستون خانة في جدول التعديل تحتوى على تبديل الأرقام من 1 إلى 64. أي خانة في جدول التعديل تشير إلى موضع ثنائية الدخل المرقمة في الخرج، والذي يتكون أيضا من أربع وستون ثنائية. يلاحظ هنا أن ترقيم الثنائيات في خوارزمية DES يعكس ممارسة حواسيب IBM الكبيرة من رقم 1 (في أقصى اليسار وتمثل أقصى قيمة) إلى الثنائية رقم 64/48/32 الخ (أقصى اليمين وتمثل آدني قيمة)، وهذا عكس الترقيم الذي نستخدمه حاليا بكثرة. على سبيل المثال إن كانت بيانات الدخل تساوى "675a6967 5e5a6b5a" (القيم معطاة بالنظام السداسي العشري hexadecimal) وتمثل النصف الأيمن والأيسر للبيانات النص الصريح على التوالي بعد التعديل باستخدام IP تتحصل على "ffb2194d 004df6fb" . تعطى هذه العملية بالعلاقة التالية:

IP(675a6967 5e5a6b5a) = (ffb2194d 004df6fb)

الجدول 3.1: التعديل الابتدائي ومعكوسه

a: التعديل الابتدائي IP									b: معكوس التعديل الابتدائي IP^{-1}							
58	50	42	34	26	18	10	2		40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4		39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6		38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8		37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1		36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3		35	3	43	11	51	19	59	27
61	53	45	37	29	21	13	5		34	2	42	10	50	18	58	26
63	55	47	39	31	23	15	7		33	1	41	9	49	17	57	25

3.5.3. بنية جولات (مراحل) خوارزمية DES

تستخدم كل جولة (أو مرحلة) نصفين من البيانات طول كل منهم 32 ثنائية يعرفان بالنصف الأيسر LD_{i-1} والنصف الأيمن RD_{i-1} (i-1 رقم الجولة السابقة). مثل أي تشفير يعتمد طريقة فيزتل التقليدية يمكن توصيف نصفين خرج الجولة بالعلاقة التالية:

$$RD_i = LD_{i-1} \oplus F(RD_{i-1}, K_i)$$
$$LD_i = RD_{i-1} \quad \ldots 3.3$$

الدالة F تعمل على الوجه التالي، الشكل 3.4.

- يمدد النصف الأيمن من الدخل RD_{i-1} والذي طوله 32 ثنائية إلى 48 ثنائية باستخدام عملية التعديل E وفقاً للجدول 3.2a
- الناتج يجمع قسرياً مع المفتاح الفرعي K_i والذي طوله 48 ثنائية أيضا
- يمرر الناتج عبر ثمانية صناديق S للحصول على ناتج طوله 32 ثنائية
- أخيرا يعدل هذا الناتج والذي طوله 32 ثائية بعملية التبديل P، وفقا للجدول 3.2b

الجدول 3.2: تبديل الجولات

a: التمديد/التبديل (جدول E)					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

b: دالة التبديل P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

صناديق S تحقق الارتباك بين البيانات وقيمة المفتاح وبعدها يقوم التبديل بنشر هذا الارتباك على نطاق عريض، خرج أي صندوق S يؤثر على عدد كبير من دخول صناديق S في الجولة الثانية، مما ينتج الانتشار.

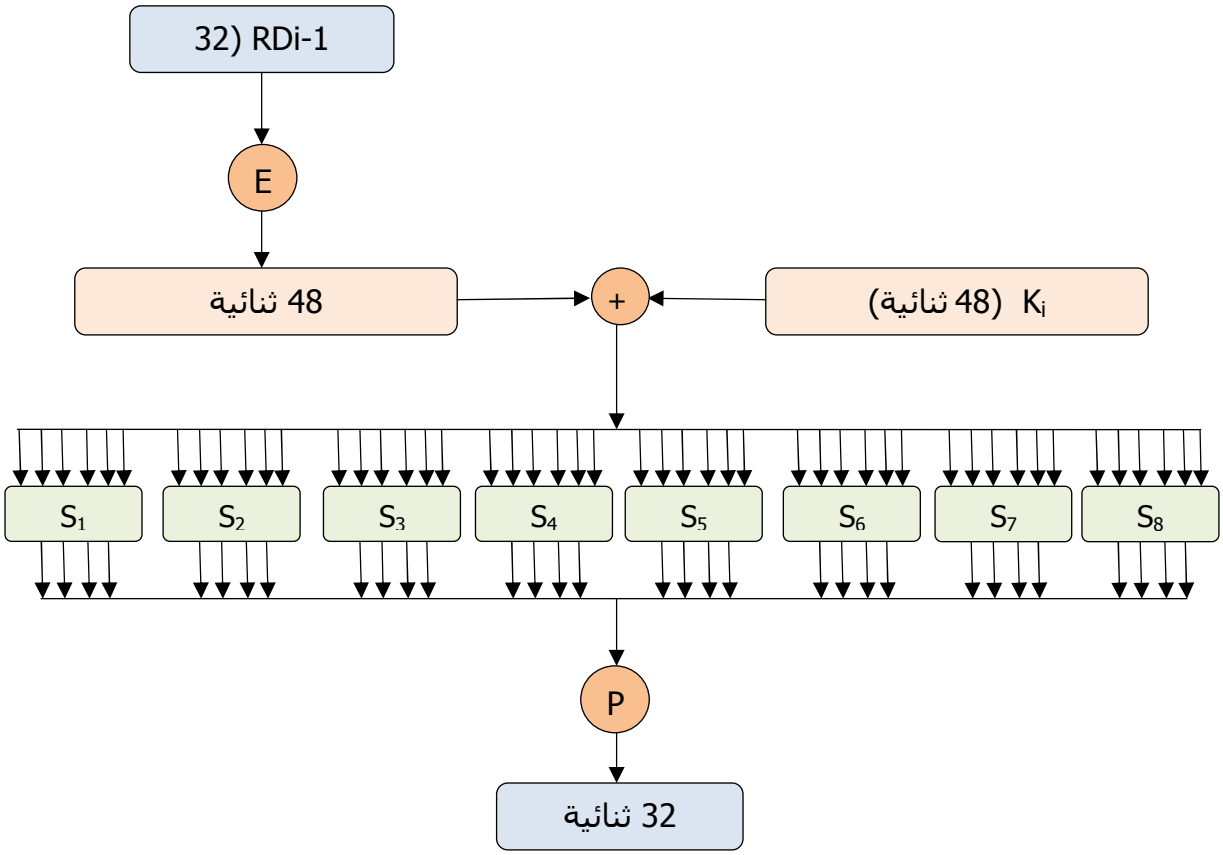
الإحلال (الاستبدال) يتحقق باستخدام ثمانية صناديق S، كل منها يقبل ست ثنائيات كدخل وينتج أربع ثنائيا في الخرج. هذا التحويل موضح في الجدول 3.4 والذي يفسر كالآتي: الثنائية الأولى والأخيرة في دخل الصندوق S_i يكونا رقم ثنائياً طوله ثنائيتان، يستخدم هذا الرقم لاختيار احد صفوف الإحلال الأربعة المحددة في الجدول. تستخدم الثنائيات الأربع الوسطى في الدخل لاختيار احد الست عشر عموداً. القيمة العشرية في الخليلة التي حددت أعلاه تحول إلى رقم ثنائي طوله أربعة ثنائيات لإنتاج الخرج. فمثلا للصندوق S_1 إن كان الدخل يساوى 011001، نختار الخلية المحددة بالصف 01 (الصف 1) والعمود 1100 (العمود 12)، القيمة العشرية في هذه الخلية 9، عليه يكون الخرج 1001. والذي يمكن أن نعبر عنه بالعلاقة:

S(18 09 12 3d 11 17 38 39) = 5fd25e03

المثال أعلاه يعطى ثمانية أرقام طول كل منهم ست ثنائيات، كل من هذه الأرقام تستبدل بإتباع العملية الموضحة أعلاه، وكما موضح في الجدول 3.3:

الجدول 3.3. إحلال صناديق S

رقم صندوق الإحلال	الدخل (ثنائي)		الصف	العمود	الناتج (الخرج ست عشري)
	ست عشري	ثنائي			
S_1	18	011000	00	1100	5
S_2	09	001001	01	0100	f
S_3	12	010010	00	1001	d
S_4	3d	111101	11	1110	2
S_5	11	010001	01	1000	5
S_6	17	010111	01	1011	e
S_7	38	111000	10	1100	0
S_8	39	111001	11	1100	3



الشكل 3.4: عمل الدالة F

3.5.4. إنتاج المفاتيح

اختير طول المفتاح ليكون 56 ثنائية وذلك بهدف تحسين امن الشفرة. يتكون مجال مفتاح خوارزمية DES من 64 ثنائية، 56 ثنائية تنتج عشوائيا وتستخدم مباشرة في الخوارزمية، الثنائيات الثمانية الأخرى والتي لا تستخدم من قبل الخوارزمية في المفتاح قد تستخدم لكشف الأخطاء، الجدول 3.5، حيث يتم ضبطها لتعطى تكافؤ فردى odd parity للمفتاح. يمكن أن يكون المفتاح أيضا مشفراً، وفى هذه الحالة ينتج رقم عشوائي طوله 64 ثنائية ثم يحدد المفتاح المشفر باستخدام مفتاح تشفير المفتاح Key Encryption KEY (KEK). ومن الواضح انه لا يمكن ضبط التكافؤ الفردي للمفتاح لكشف الأخطاء قبل تشفيره.

تختار 56 ثنائية من 64 ثنائية لتكوين المفتاح وذلك بتجاهل الثنائيات في المواقع: 8 و 16 و 24 و 32 و 40 و 48 و 56 و 64. بقية الثنائيات (56 ثنائية) تتعرض للتبديل باستخدام خيار التبديل الأول (PC1) والمحدد بالجدول 3.6. يتعامل مع المفتاح الناتج من تبديل الاختيار أعلاه مجموعتان منفصلتان طول كل منهما 28 ثنائية، تميز كل من هذه الكميات بالرموز C_0 و D_0. في كل جولة يزاح كل من C_{i-1} و D_{i-1} إزاحة يسارية الدوران بمقدار ثنائية واحدة أو ثنائيتان وفقاً لما هو موضح في الجدول 3.7. القيم المزاحة تستخدم كدخل للجولة التالية، كما تستخدم كدخل لتبديل الاختيار الثاني وفقاً للجدول 3.5 وذلك لإنتاج خرج طوله 48 ثنائية يستخدم كدخل للدالة $F(R_{i-1},K_i)$.

الشكل 3.5، يوضح تفاصيل عمليات خوارزمية DES الكاملة في أي جولة.

لجدول 3.4. تعريفات صناديق S في خوارزمية DES

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

الجدول 3.5. المفتاح

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

الجدول 3.6. تبديل الاختيار

a: تبديل الاختيار 1 (PC1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

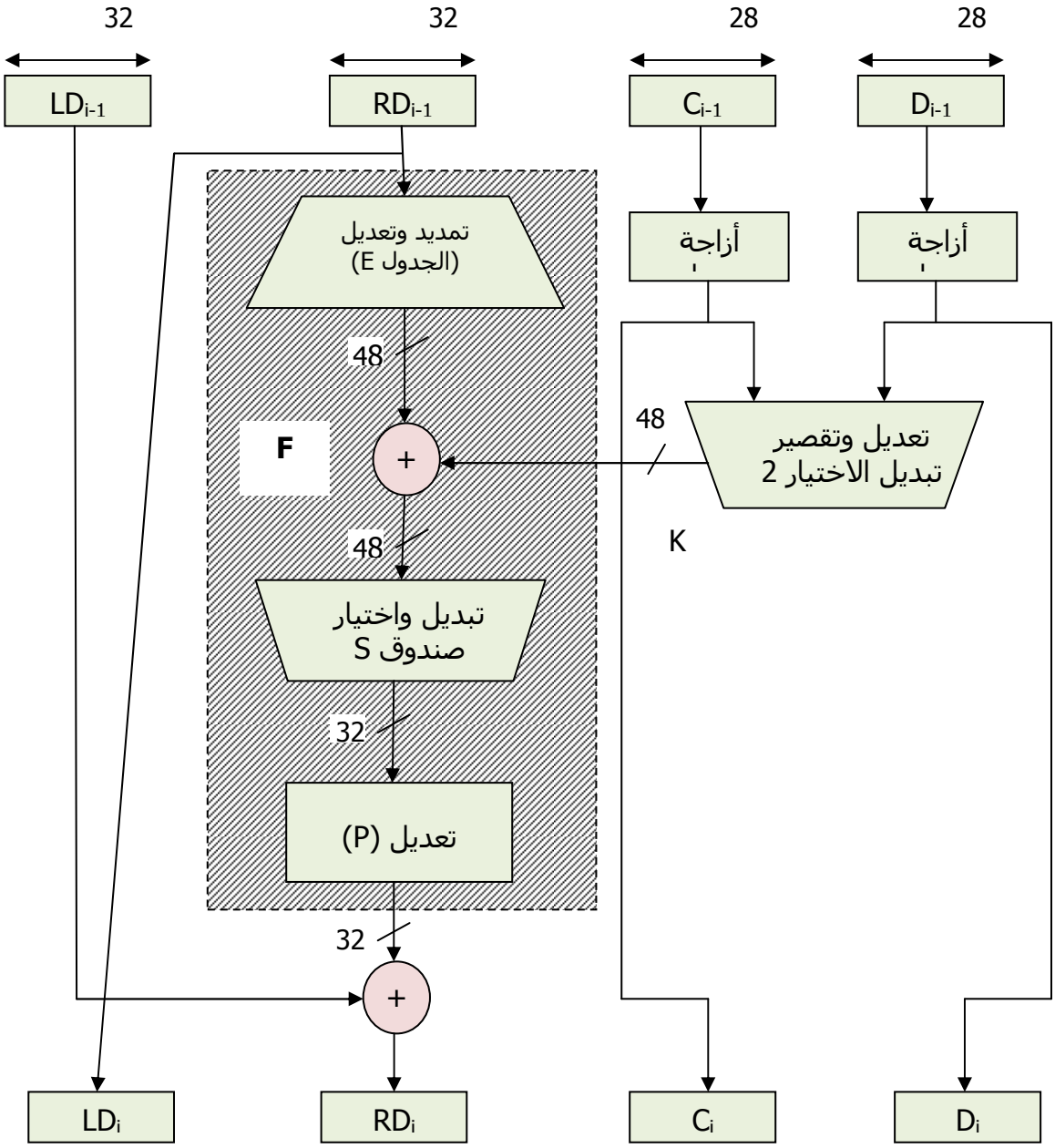
b: تبديل الاختيار 2 (PC2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

الجدول 3.7. جدولة الإزاحة لليسار

رقمة الجولة	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ثنائيات الدوران	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

مثله مثل تشفير فيزتل يستخدم تشفير خوارزمية DES نفس خوارزمية التشفير لفك التشفير، الاختلاف الوحيد بين التشفير وفك التشفير هو استخدام المفاتيح بترتيب عكسي ابتداءً من المفتاح K_{16} في الجولة الأولى وحتى المفتاح K_1 في الجولة الأخيرة.



الشكل 3.5: خوارزمية DES في جولة واحدة

3.5.5. تحليل شفرة خوارزمية DES التفاضلي:

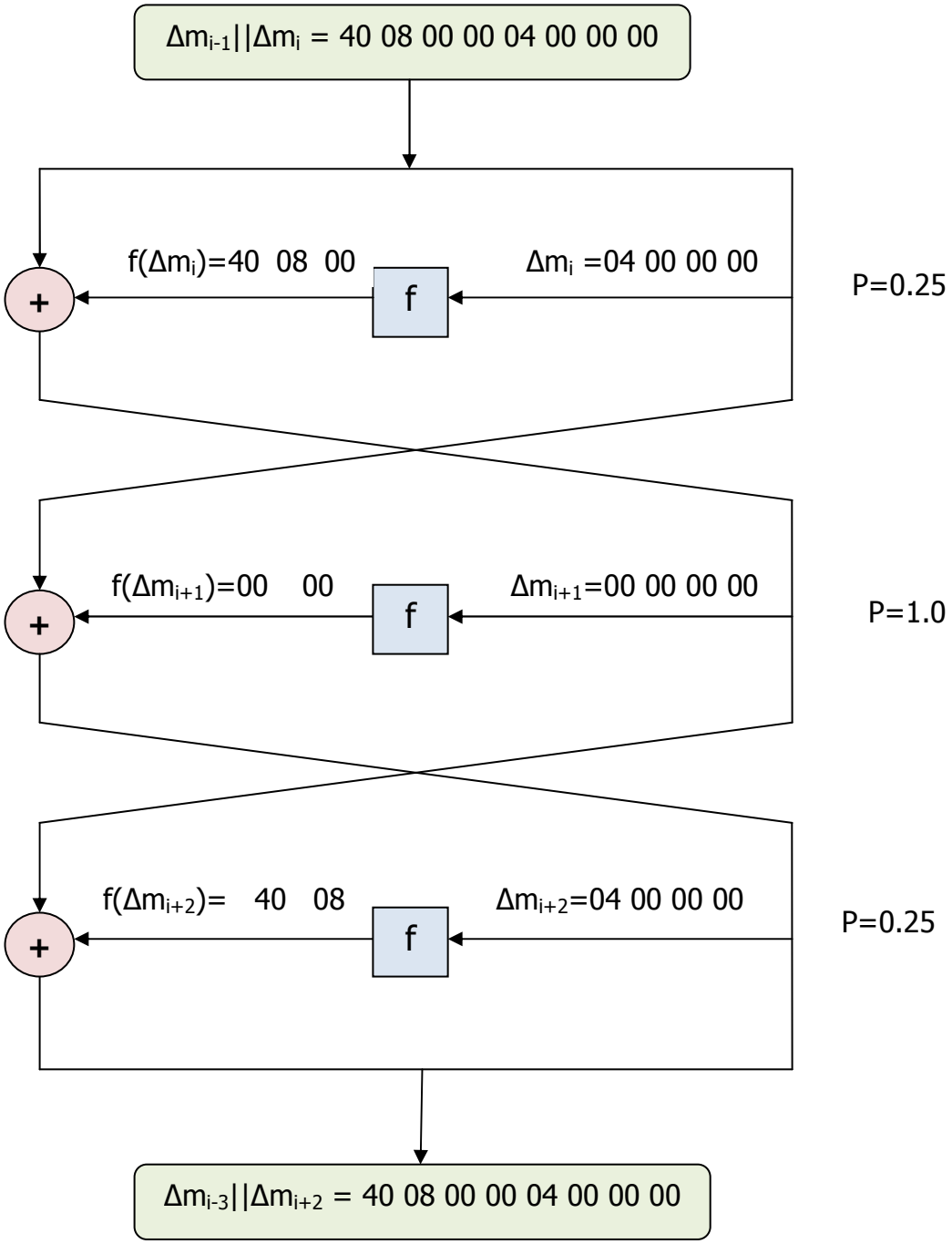
أوضح كل من بيهام وشامر Biham and Shamir إمكانية استخدم تحليل الشفرة التفاضلي Differential Cryptanalysis لتحليل وكسر تشفير خوارزمية DES. عرف تحليل الشفرة التفاضلي منذ العام 1974 باسم "تاتاك Tattack" من قبل فريق IBM لتصميم خوارزمية DES، حيث استخدم لتحسين امن تصميم صناديق S والتعديل P.

هجوم تحليل الشفرة التفاضلي معقد، والفكرة الأساسية لهذا التحليل تعتمد على مراقبة سلوك أجواز كتل نصية أثناء معالجتها في كل جولة من نظام التشفير، بدلا من مراقبة كتلة واحدة. في كل جولة تقوم خوارزمية DES بنقل نصف الدخل الأيمن إلى نصف الخرج الأيسر، ثم يتم إيجاد نصف الخرج الأيمن بدلالة نصف الدخل الأيسر والمفتاح الفرعي للجولة، مما يعنى أنة لايمكن استنتاج القيم بطريقة عكسية من غير معرفة قيمة المفتاح. يقارن تحليل الشفرة التفاضلي جوزين مرتبطين من النص المشفر، للحصول على المعلومات المتعلقة بالمفتاح.، إن استخدم عدد كبير من أجواز النص المشفر. بمقارنة الاختلاف بين شفرتان مرتبطتان والنظر للاختلافات المعروفة الدخل قد تتحصل باحتمال ما على الاختلافات في الخرج. المعادلات التالية توضح كيف يمكن إزالة تأثير المفتاح، وتمكن التحليل

$$\begin{aligned}\Delta m_{i+1} &= m_{i+1} \oplus m'_{i+1} \\ &= \left[m_{i-1} \oplus f\left(m_i, K_i\right)\right] \oplus \left[m'_{i-1} \oplus f\left(m'_i, K_i\right)\right] \\ &= \Delta\Delta m_1 \oplus \left[f\left(m_i, K_i\right) \oplus f\left(m'_i, K_i\right)\right] \qquad \text{..... 3.4}\end{aligned}$$

الاستراتيجية العامة لتحليل الشفرة التفاضلي تعتمد على التركيز على جولة واحدة. تبدأ العملية باستخدام نصين صريحين وهما الرسالة m والرسالة m′ بهما اختلافات، ونتتبع ونلاحظ النمط المحتمل للاختلافات بعد كل جولة للحصول على الاختلاف المحتمل للنص المشفر. ندخل كل من الرسالة m والرسالة m′ إلى نظام التشفير لتحديد الاختلاف الحقيقي في حالة عدم معرفة المفتاح، ومقارنة النتائج مع الاختلاف المحتمل. باستخدام هذه الافتراضات يمكننا الحصول على بعض الاستنتاجات عن المفتاح. يجب إعادة هذه العملية لعدد كبير من المحاولات لتحديد كل ثنائيات المفتاح. يحتاج أسلوب التحليل هذا إلى 2^{47} نص صريح.

الشكل 3.6 يوضح انتشار الاختلافات عبر ثلاث جولات من خوارزمية DES. قيم الاحتمالات الموضحة على اليمين، تشير احتمال أن تظهر الاختلافات الوسطية بدلالة اختلافات الدخل. بعد الجولة الثالثة يكون احتمال اختلاف الخرج يساوى 0.25x1x0.25=0.0625. حيث أن اختلاف الخرج هو نفسه اختلاف الدخل، يمكن إعادة نمط الجولات الثلاث هذا لعدد كبير من الجولات، بضرب الاحتمال لتصبح صغيراً تتابعاً.



3.5.6. تحليل الشفرة الخطى

يعتبر تحليل الشفرة الخطى تطوراً حديثاً في تحليل شفرة خوارزمية DES. هذا الهجوم يعتمد على إيجاد تقريب خطي لوصف التحويل الذي تقوم به خوارزمية DES. في هذه الطريقة يمكن إيجاد المفتاح بإعطاء 2^{43} نصاً صريحاً معروفاً، مقارنة مع اختيار 2^{47} نصاً في طريقة التحليل التفاضلي. والذي يعتبر تحسن في طريقة التحليل حيث من الأسهل التعامل مع نصوص معروفة بدلات عن اختيار نصوص اعتباطيا.

الهدف من تحليل الشفرة الخطى هو إيجاد معادلة خطية فعالة لربط بعض ثنائيات النص الصريح والنص المشفر والمفاتيح، باحتمال p يساوى حوالي 0.5. بعد تحديد هذه العلاقة، تحسب نتائج الجزء الأيسر من المعادلة لعدد كبير من أزواج النصوص الصريحة والمشفرة، لتحديد إن كان مجموع ثنائيات المفتاح تساوى 0 أو 1، عندها تتحصل على معلومة عن ثنائية واحدة في المفتاح. تكرر هذه العملية لمعادلات أخرى وعلي عدد من الأزواج للحصول على معلومات عن بقية ثنائيات المفتاح. تعاملنا مع معادلات خطية، يجعل من الممكن التعامل مع جولة واحدة من نظام التشفير في أي وقت، ودمج النتائج.

ملخص:

درسنا في هذه الوحدة المواضيع التالية:

- التشفير الكتلي والتشفير التدفقي
- تصميم وبنية تشفير فيزتل
- تشفير خوارزمية DES
- تحليل الشفرة التفاضلي والخطى

أسئلة:

1. تمثل الشفرة الوهمية التالية خوارزمية تشفير باستخدام أسلوب تشفير فيزتل. أعطى خوارزمية الشفرة الوهمية فك الشفرة الناتجة من هذا التشفير.

```
Input: plaintext = (left[0], right[0])

for round from 1 to 16 do
    left[round] := right[round-1]
    right[round] := left[round-1] ⊕ F(key[round-1], right[round-1])
end for

Output: ciphertext = (left[16], right[16])
```

2.
   أ. ما هو حجم كتلة النص الصريح في معاير تشفير البيانات؟
   ب. لماذا يجب أن تكون حجم كتلة النص المشفر مساويا لحجم كتلة النص الصريح لأي خوارزمية تشفير؟
   ج. كم عدد المفاتيح المستخدمة في معيار تشفير البيانات؟

3. يشتمل معيار تشفير البيانات علي التحول التالي في الجولة رقم i:
تأخذ النصف الأيسر L_{i-1} والنصف الأيمن R_{i-1} للبيانات ومفتاح الجولة K_i كدخل وتخرج L_i و R_i، حيث:

$$Li = Ri$$
$$R_{i+1} = L_i \oplus (K_i \text{ mangle } R_i)$$

وضح كيف يمكن استرجاع كل من L_{i-1} و R_{i-1} من L_i و R_i حتي إن كانت الدالة F غير عكسية. أوجد عدد محاولات هجوم البحث الشامل المطلوبة لكسر الشفرة في أسوء الحالات؟

4. تمرين برمجة: اكتب برنامج للتشفير وفك التشفير باستخدام خوارزمية المفتاح العام معيار تشفير البيانات DES.

أهداف الوحدة
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:

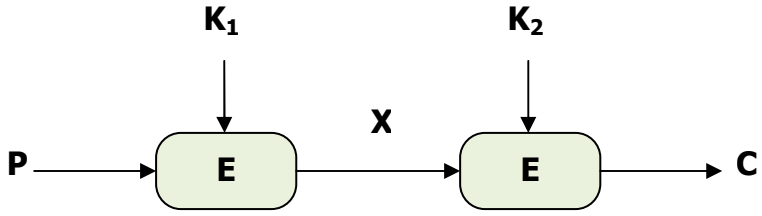
- استخدام خوارزمية معيار تشفير البيانات الثلاثية وتحديد ميزاتها ومحدوديتها ومستوى أمنها
- تحديد صيغ التشغيل المختلفة
- التعرف على عمليات تشفير التدفق ومقارنته بالتشفير الكتلي
- معرفة أسلوب تشفير RC4

4.1. مقدمة

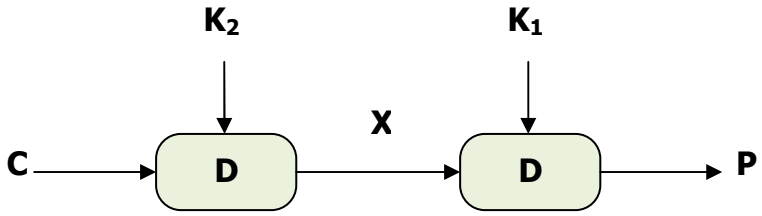
عدم تحصين خوارزمية DES ضد هجوم البحث الشامل brute-force attack، أدى إلى البحث عن بدائل لها. احد هذه البدائل تمثل في تصميم خوارزمية جديدة، فتم تصميم خوارزمية معيار التشفير المتقدم Advanced Encryption Standard (ASE). أما الخيار الأخر والذي يحافظ على الاستثمار الحالي في البرامج والمعدات، تمثل في استخدام تشفير متعدد مع خوارزمية DES ومع مفاتيح متعددة. سندرس في هذه الوحدة معيار تسفير البيانات الثلاثي Trible-DES والأكثر استخداما.

4.2. معيار تشفير البانات الثنائي:

ابسط هيئات التشفير المتعدد يستخدم مرحلتين تشفير ومفتاحين ويعرف باسم معيار تشفير البيانات التنائي Double-DES وموضح في الشكل 4.1.



a: التشفير



b: فك التشفير

الشكل 4.1: خوارزمية DES الثنائية

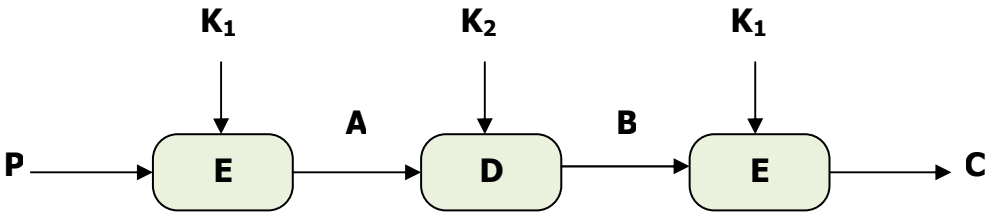
أسلوب التشفير هذا غير مناسب وغير امن، حيث انه غير محصن ضد الهجوم بالقابلة عند المنتصف meet-in-the-middle attack (هجوم النص الصريح). في هذا الهجوم وبمعرفة الثنائي (P,C) يمكن معرفة المفتاح عند منتصف عملية التشفير بعد محاولات متعددة. والذي يمكن وصفه كالأتي:
النص المشفر X بعد المرحلة الأولى يعطى بالعلاقة التالية:

$$X = E_{K1}[P] = D_{K2}[C] \quad \ldots\ldots \quad 4.1$$

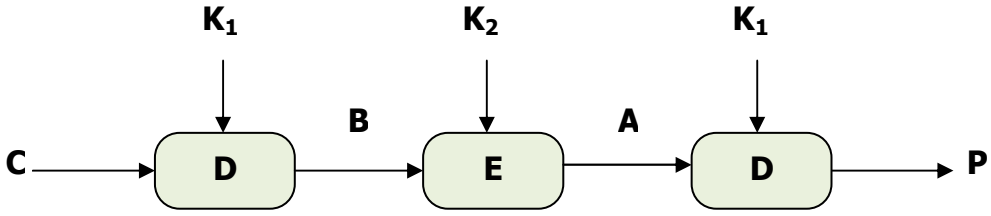
نحاول كل القيم الممكنة والمحتملة للمفتاح K_1 على P لإيجاد القيم المحتملة للنص المشفر X قبل المرحلة الثانية وتخزن هذه النتائج في جدول. ثم نحاول كل القيم المحتملة للمفتاح K_2 على C إيجاد أيضا القيم المحتملة للنص المشرف X بعد فك التشفير بعد المرحلة الأولى، ويخزن أيضا في جدول أخر، ويضاهي بقيم الجدول الأول. بإعادة المحاولة عددت مرات على أجواز من النصوص الصريحة والمشفرة قد تتحصل على قيم المفاتيح K_1 و K_2. إن تعقيد هجوم الهجوم بالقابلة عند المنتصف لا تزيد عن تعقيدات عن هجوم البحث الشامل.

4.3. معيار تشفير البيانات الثلاثي:

الشكل 3.2 يوضح تشفير معيار تشفير البيانات الثلاثي Trible-DES باستخدام مفتاحين، استخدام هذا الأسلوب شائع كبديل لأسلوب معيار تشفير البيانات المفرد. هذا التشفير ثلاثة مرات أبطء من تشفير DES المفرد.



a: التشفير



b: فك التشفير

الشكل 4.2: خوارزمية DES الثلاثي بمفتاحين

استخدام مراحل تشفير وفك تشفير يجعل بنية التشفير مكافئة لتشفير معيار تشفير البيانات المفرد. يمكن لهذا الأسلوب فك شفرة معيار تسفير البيانات المفرد بجعل $K_1=K_2$. نظرياً يمكن مهاجمة هذا التشفير، لكن هذا الهجوم غير عملي، حيث يحتاج إلى عدد كبير من المحاولات. اعتمد معيار تشفير البيانات الثلاثي باستخدام مفتاحين للاستخدام في معايير إدارة المفتاح ANS X9.17 و ISO 8732.

للحصول على مزيد من امن الشفرة يمكن استخدام معيار تشفير البيانات الثلاثي مع ثلاثة مفاتيح، طول كل منم 128 ثنائية. حيث يعطى النص المشفر بالعلاقة التالية:

$$C = E_{K3}[D_{K2}[E_{K1}[P]]] \quad \ldots\ldots \quad 4.2$$

يستخدم هذا التشفير في بعض تطبيقات الانترنت بكثرة.

4.4. صيغ التشغيل

يمثل معيار تشفير البيانات مثله مثل أي تشفير كتلي أخر، وحدة البناء الأساسية لتشفير وفك تشفير كتلة بيانات حجمها ثابت. عملياً نتعامل مع كمية اعتباطية من البيانات قد تكون موجودة مقدماً (وفى هذه الحالة تكون صيغة الكتلة مناسبة)، أو تتحصل عليه ثنائية أو ثمانية في أي وقت، (وفى هذه الحالة تكون صيغة التدفق أكثر ملائمة). لاستخدام التشفير الكتلي في التطبيقات المختلفة حددت يئة NIST في الوثيقة FIPS 81 أربعة صيغ (أنماط) تشغيل modes of operation. تهدف هذه الصيغ إلى تغطية كل التطبيقات التي قد يستخدم التشفير الكتلي فيها. نتيجة لظهور تطبيقات واحتياجات جديدة، زيدت صيغ التشغيل إلى خمسة في الوثيقة الخاصة 800-38A. تستخدم هذه الصيغ مع التشفير الكتلي المتناظر، مثل معيار تشفير البيانات الثلاثي ومعيار التشفير المتقدم. قائمة صيغ التشغيل تشتمل على:

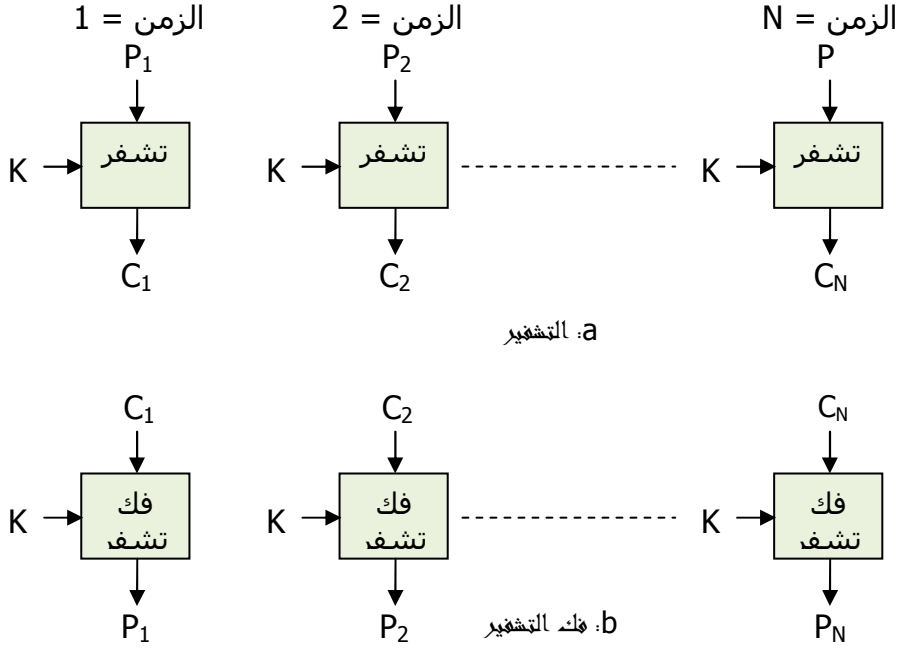
- صيغة كتاب الشفرة الإلكتروني Electronic Codebook Book (ECB)
- صيغة ربط الكتل المشفرة Cipher Block Chaining (CBC)
- صيغة التغذية العكسية بالشفرة Cipher FeedBack (CFB)
- صيغة التغذية العكسية بالخرج Output FeedBack (CFB)
- صيغة العداد Counter (CTR)

4.5. صيغة كتاب الشفرة الإلكتروني

ابسط صيغة تشغيل هي صيغة كتاب التشفير الالكتروني، في هذه الصيغة تقسم الرسالة إلى كتل مستقلة وتشفر أي كتلة من النص الصريح في إي وقت. أي كتلة من النص الصريح تشفر باستخدام نفس المفتاح. تعطى الكتلة المشفرة بمعيار تشفير البيات المفرد بالعلاقة، الشكل 4.3.:

$$C_i = DES_K(P_i) \qquad \ldots\ldots 4.3$$

تستخدم هذه الصيغة فقط عندما نحتاج إلى إرسال كتلة واحدة من المعلومات مثل مفتاح الجلسة (الدورة) session key المشفر بمفتاح رئيسي. صيغة الكتاب الالكتروني لا تناسب كل كميات البيانات، نسبة تكرار الرسالة الذي يمكن ملاحظته في النص المشفر وخاصة مع التخطيطات والرسالات التي يكون فيها التغييرات صغيرة. الضعف الرئيسي لهذه الصيغة يكمن في أن الكتل المشفرة مستقلة عن بعضها البعض. حيث يمكن أن تخلط وتقحم الكتلة دون أن توثر على تشفير وفك تشفير أي كتلة أخري.



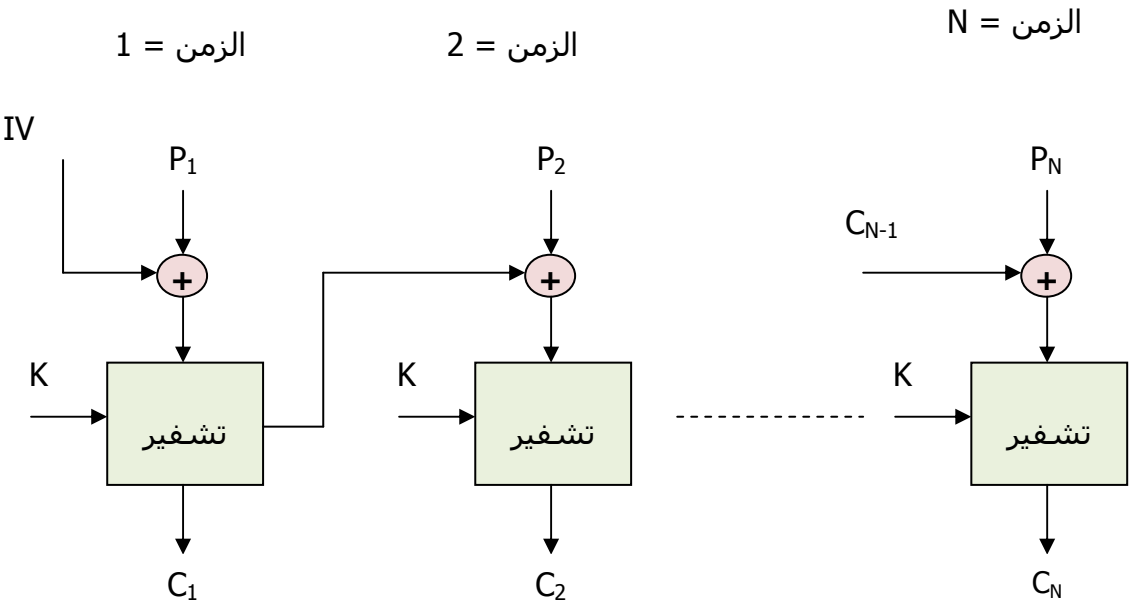
الشكل 4.3: صيغة كتاب التشفير الالكتروني

4.6. صيغة ربط الكتل المشفرة

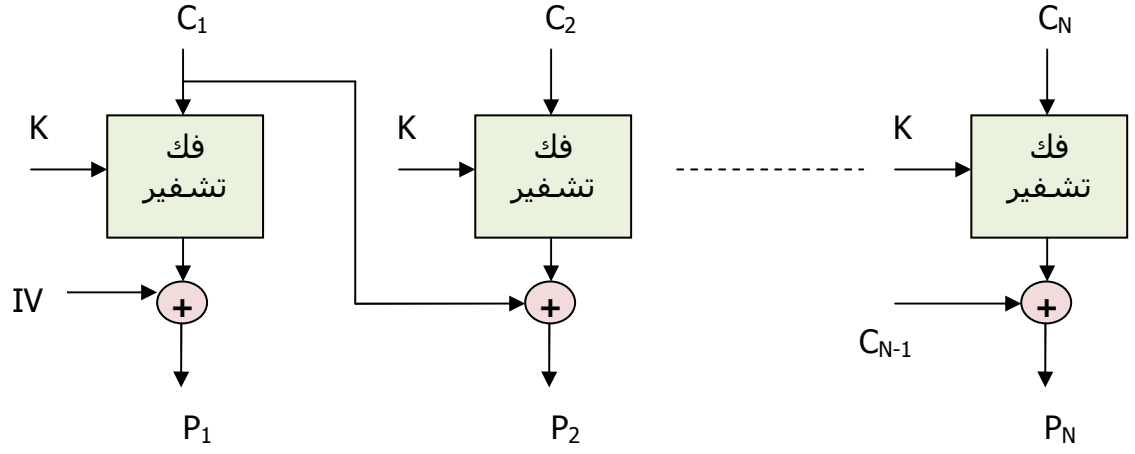
يتطلب تخطى مشكلتي التكرار و الاستغلالية في صيغة كتاب الشفرة الالكتروني، جعل النص المشفر غير مستقلاً عن كل الكتل السابقة. هذا ما تعطيه صيغة ربط الكتل المشفرة. يقسم النص الصريح إلى كتل، تربط ببعضها البعض في عملية التشفير. تدمج الكتلة المشفرة سابقا مع كتلة الرسالة الحالية قبل تشفيرها لبداية عملية التشفير. تستخدم قيمة ابتدائية Initial Value (IV)، وعادة ما تكون معرفة (غالبا كلها أصفار)، ونعبر عن المشفرة بمعيار تشفير البيات المفرد بالعلاقة، الشكل 4.4.:

$$C_i = DES_K(P_i \text{ XOR } C_{i-1}) \quad \ldots 4.4a$$
$$C_{-1} = IV \quad \ldots 4.4b$$

تستخدم صيغة ربط الكتل المشفرة عند الحاجة إلى إرسال كميات كبيرة من البيانات بأمان، شريطة أن تكون البيانات موجودة مقدماً مثل البريد الالكتروني وبرتوكول تبادل الملفات FTP والويب web.



a: التشفير



b: فك التشفير

الشكل 4.3: صيغة ربط الكتل المشفرة

احد المواضيع المهمة في صيغة ربط الكتل المشفرة يتمثل في كيفية التعامل مع الكتلة الأخيرة، التي قد تكون غير مكتملة وحجمها اصغر من حجم الكتلة المشفرة. عامة يتم حشو هذه الكتلة (نموذجياً بأصفار) ويجب تمييز الحشو في الطرف الثاني. تستخدم الثمانية الأخيرة في الكتلة لحساب عدد الحشو المستخدم.

فمثلا [b1 b2 b3 0 0 0 0 5] في هذه الكتلة توجد 4 حشوات. الثمانية الخيرة تساوى خمسة أي عدد الحشو زائد العداد. إن كانت أخر ثمانية في الكتلة احد المضاعَفات الزوجية للرقم 8 أو إن كانت يساوى تماما عدد الحشو زائد العداد عندها يجب إضافة كتلة إضافية. توجد صيغ أخرى أكثر سرية تتفادى الحاجة إلى كتلة إضافية.

ربط الكتل يعطى تأثير انهيار تراكمي avalanche effect مما يعنى أن النص المشفر لا يمكن تغيره أو إعادة ترتيبه دون تدمير كل البيانات السابقة. القيمة الابتدائية يجب أن تكون معروفة للمرسل والمستقبل، وان أرسلت دون تشفير يمكن للمهاجم تغير ثنائيات الكتلة الأولى وتغيير القيمة الابتدائية للتعويض وتحليل التشفير، عليه يجب أن تكون القيمة الابتدائية ثابتة أو ترسل مشفرة باستخدام صيغة كتاب الشفرة الالكتروني قبل إرسال الرسالة.

4.7. صيغة التغذية العكسية بالشفرة

إن كانت البيانات متاحة فقط كثنائية أو ثمانية في إي وقت (مثلا جولة طرفية أو قيمة مجس) يجب استخدام أسلوب أخر للتشفير غير أسلوب تشفير الكتلة حتى لا تتأخر المعلومات. الفكرة هنا استخدام التشفير الكتلي كمولد أرقام عشوائي زائف pseudo-random number (انظر الوحدة 6 عن تشفير التدفق)، ودمج هذه الثنائيات العشوائية في الرسالة. ويلاحظ هنا عملية الجمع القسرى يمكن عكسها بسهولة، تتطلب فقط جمع الناتج قسيريا مع نفس الكمية للحصول على الدخل.

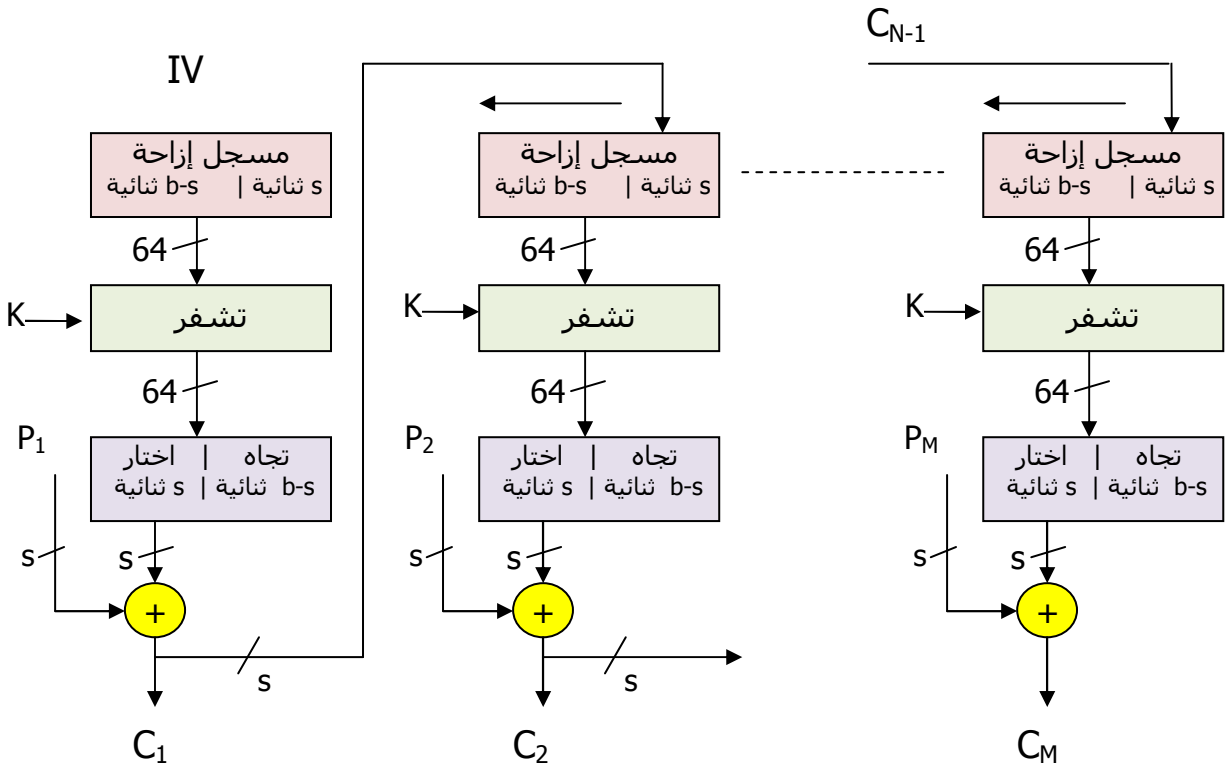
تعتمد هذه الصيغة على الاستخدام العشوائي لأي عدد من وحدت الخرج (ثنائيات أو ثمانيات) قبل ضخ الثنائيات من الصف وإعادة التشفير. هذا الأسلوب به كثير من الفاقد الذي يبطئ عملية التشفير. طريقة بديلة تتمثل في إنتاج كتلة من الثنائيات عشوائيا، عدد الثنائيات بها يساوى 1 أو 8 أو 64 أو 128، (يرمز إليها باستخدام CFB-1, CFB-8, CFB-64, CFB-128) نجمعها فسريا مع ثنائية أو ثمانية الرسالة التي تعالج كتدفق ثنائيات. حيث تتم التغذية العكسية بكتلة كاملة من النص المشفر. حجم الكتلة CFB-1, CFB-8, CFB-64, CFB-128 يعتمد على حجم كتلة المشفر مثل معيار تشفير البيانات أو معيار التشفير المتقدم.

صيغة التغذية العكسية بالشفرة مناسبة للاستخدام عندما يكون وصول البيانات (الثنائيات أو الثمانيات) تتابعي. تعانى هذه الصيغة من المشاكل عندما تستخدم في قنوات عالية الضجيج noisy Channels، عندها أي ثنائية غير صحيحة (خربة) تدمر القيم في الكتلة الحالية والكتل المستقبلية.

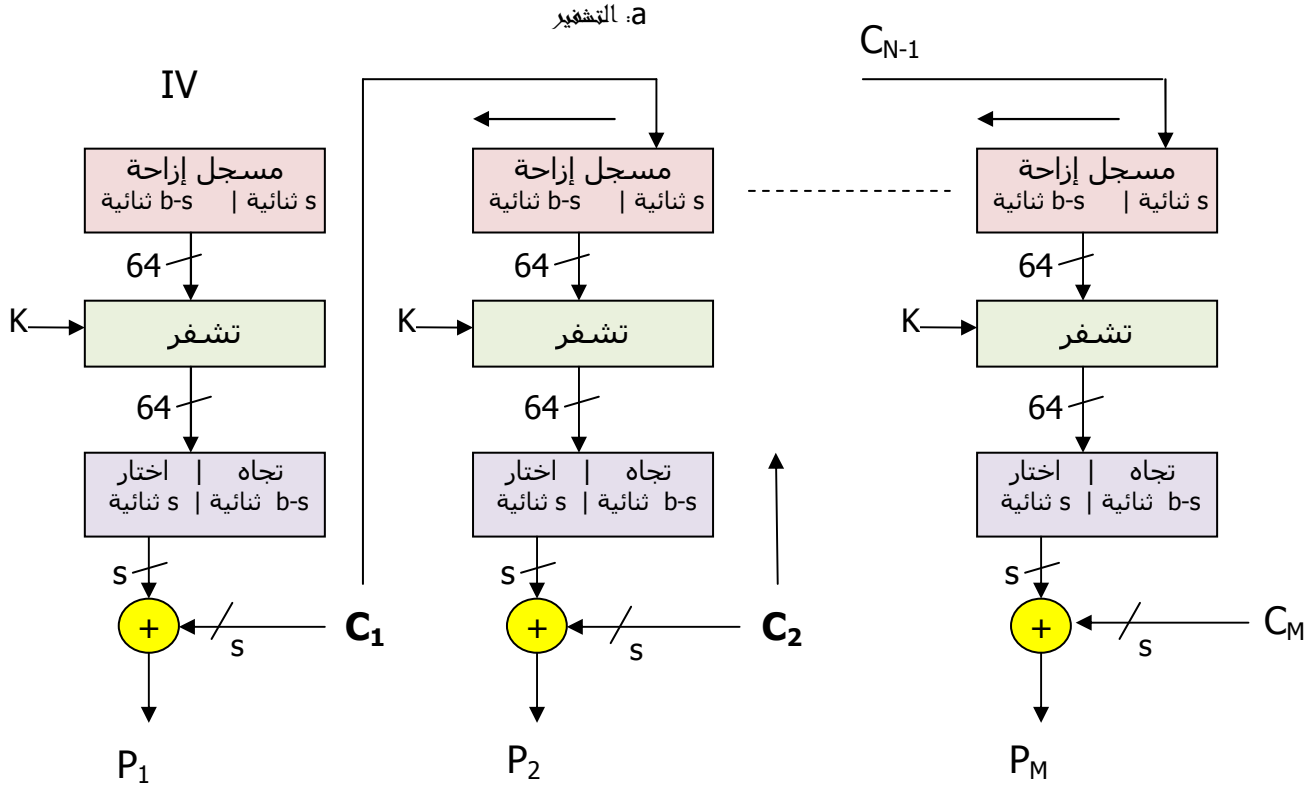
4.8. صيغة التغذية العكسية بالخرج

تعتبر صيغة التغذية العكسية بالخرج صيغة بديلة لصيغة التغذية العكسية بالشفرة. يتم التعامل من الرسالة كتدفق ثنائيات. في هذه الصيغة يكون الإنتاج العشوائي للثنائيات مستقلا عن الرسالة التي تم تشفيرها، مما يعطيها ميزات تتمثل في أمكانية حساب هذه الأرقام مقدماً والميزة الثانية إن الخطاء في إي ثنائية يؤثر فقط على تنائيه واحدة. مما يجعل هذه الصيغة مناسبة للاستخدام في القنوات ذات الضجيج العالي مثل التوابع الاصطناعية والإرسال التلفزيوني. يمكن تحديد القيم مقدماً باستخدام العلاقات التالية:

$$C_i = P_i \text{ XOR } O_i \quad \ldots 4.5a$$
$$O_i = DES_{K1}(O_{i-1}) \quad \ldots 4.5b$$
$$O_{-1} = IV \quad \ldots 4.5c$$

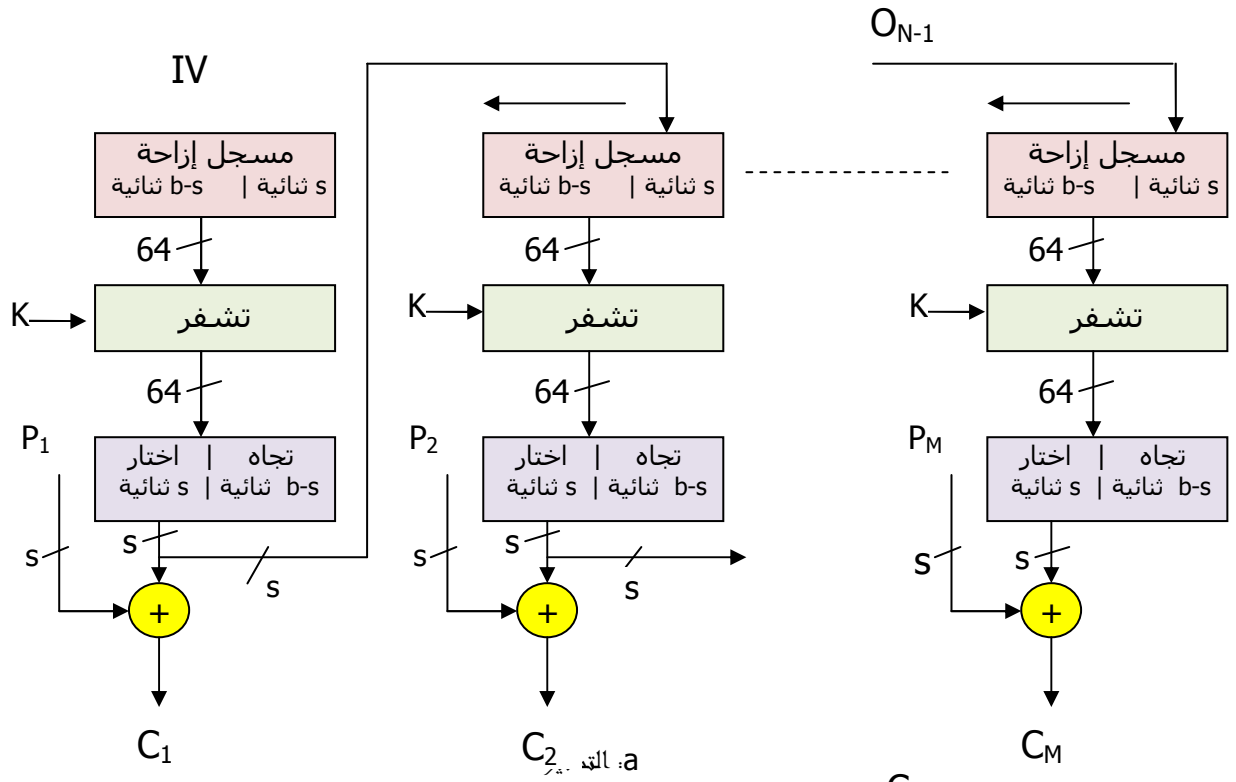


a: التشفير

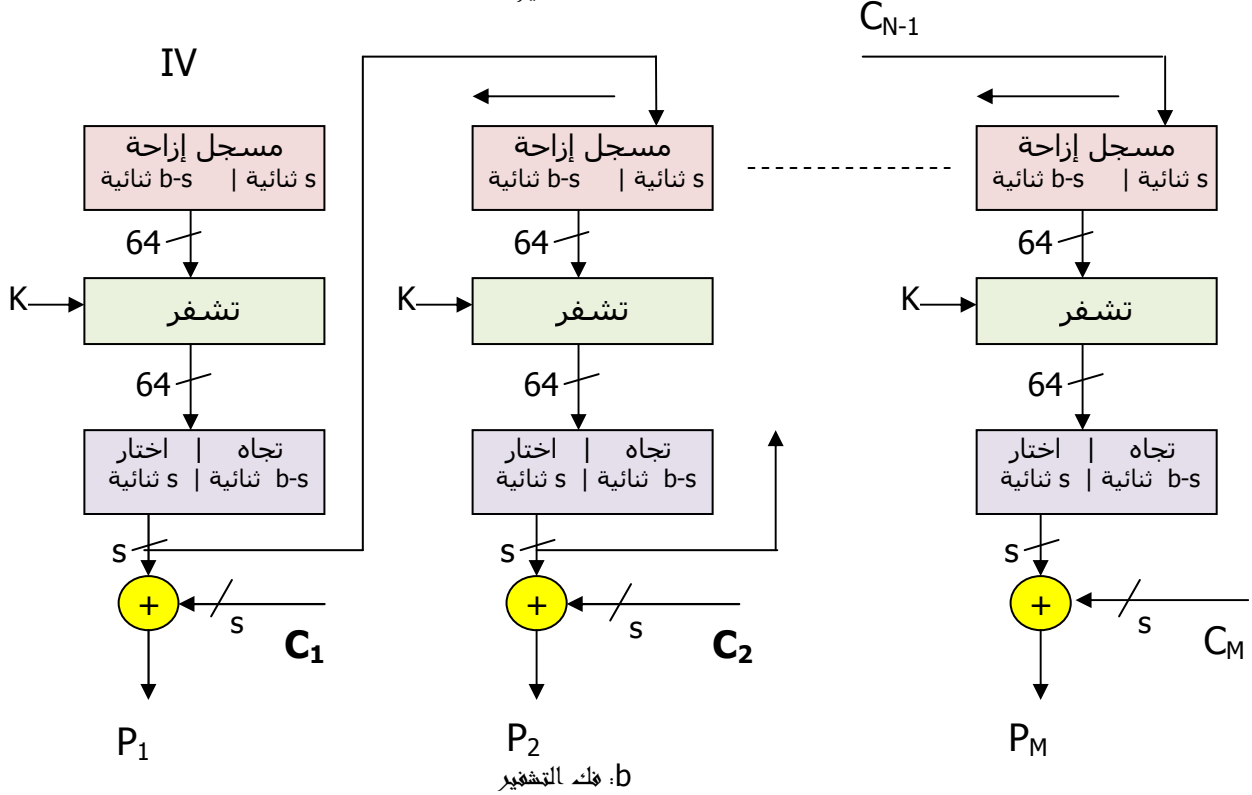


b: فك التشفير

الشكل 4.3: صيغة التغذية العكسية بالشفرة



a: التشفير



b: فك التشفير

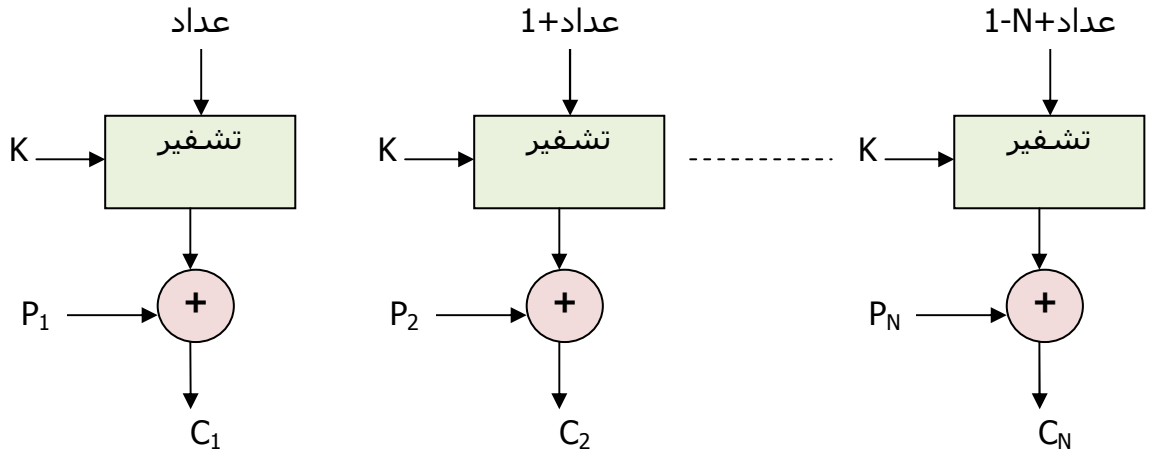
الشكل 4.3: صيغة التغذية العكسية بالشفرة

لتقوية امن تشفير صيغة التغذية العكسية بالخرج يجب عدم استخدام التدفق أكثر من مرة، حيث لا يتم دمج نصين مشفرين وبإلغاء الثائيات يمكن تحليل النص المشفر. كما يجب ان يتزامن كل من المرسل والمستقبل حتى لا تفقد البيانات. أوضحت الأبحاث انه من الضروري استخدام الكتل الكاملة فقط (CFB-64 أو CFB-128).

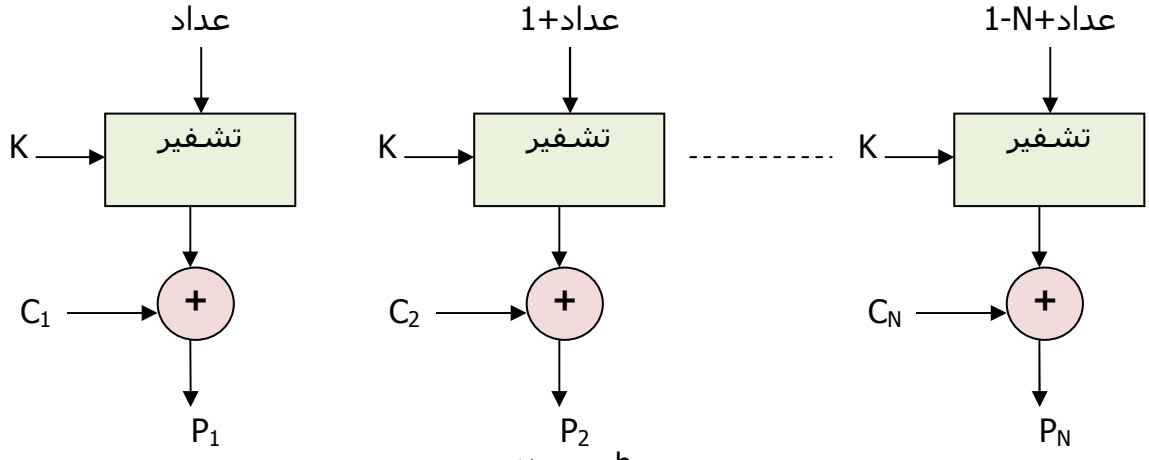
4.9. صيغة العداد

صيغة العداد نسخة مختلفة من صيغة التغذية العكسية بالخرج، تستخدم في التشفير قيم عداد بدلا عن الخرج. رغم أن هذه الصيغة قد اقترحت منذ سنوات عديدة، لم يتم معيرتها إلا قريبا لاستخدامها في معيار التشفير المتقدم AES مع صيغ التشغيل الأربعة التي تم مناقشتها سابقا في هذه الوحدة. تستخدم هذه الصيغة في تامين تطبيقات شبكات صيغة الانتقال الغير متزامن asynchronous transfer mode (ATM) وامن برتوكول الانترنت IP security (IPSec) . طول خرج العداد يساوى حجم كتلة النص الصريح المستخدم. يجب استخدام قيمة عداد مختلفة ومفتاح مختلف لتشفير أي كتلة في النص الصريح. يعبر عن هذه الصيغة باستخدام العلاقات التالية:

$$Ci = Pi \text{ XOR } Oi$$
$$Oi = DESK1(i)$$



a: التشفير



b: فك التشفير

الشكل 4.3: صيغة العداد

من أهم ميزات صيغة العداد يمكن تلخيصها في التالي:

- مقدرتها على تنفيذ التشفير المتوازي باستخدام العتاد و/أو البرمجيات بكفاءة عالية
- مقدرتها المعالجة قبل الحاجة للتشفير
- النفاذ العشوائي للكتل المشفرة

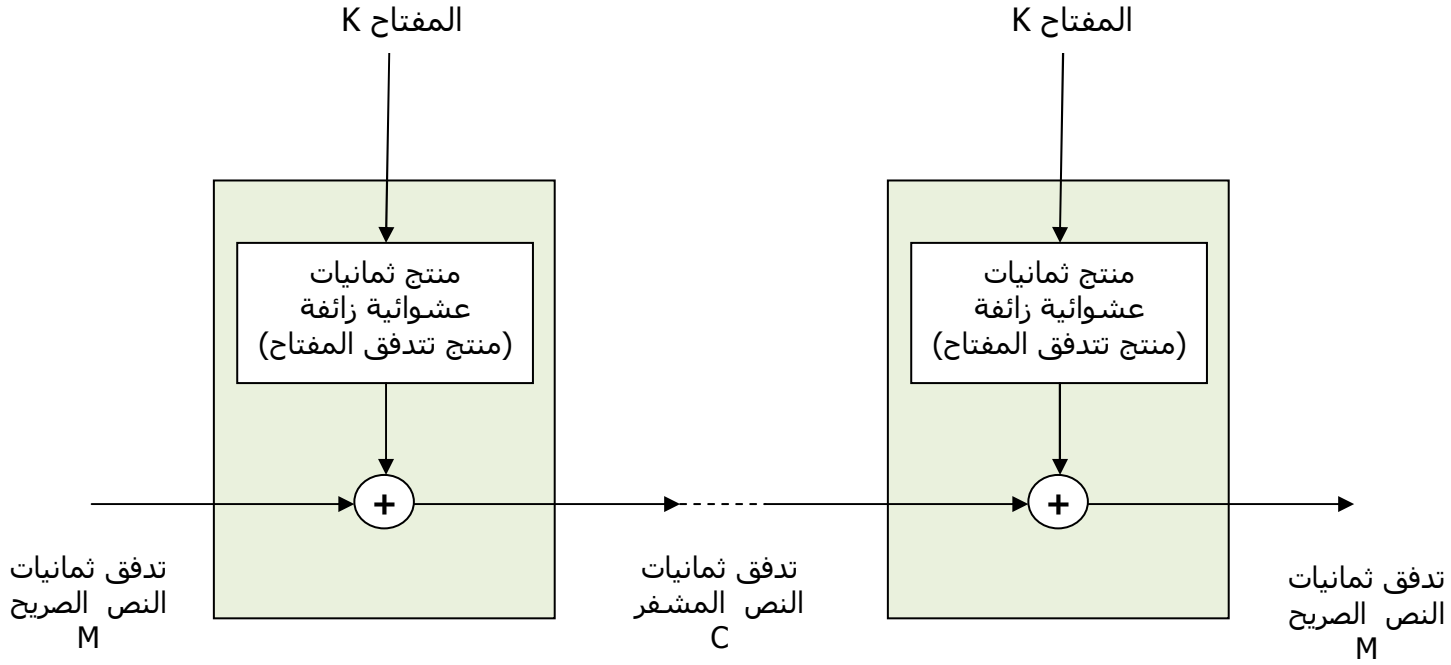
هذه الصيغة مناسبة للاستخدام في قنوات الاتصال العالية السرعة والتي تنقل حركة متفجرة. تامين التشفير يتطلب عدم استخدام المفتاح وقيمة العداد.

4.10. التشفير التدفقي

يشفر أسلوب التشفير التدفقي النص الصريح بمعالجة ثمانية (أو تنائيه) في أي وقت ثم تتبع بوحدة أخرى من النص الصريح. وذلك باستخدام الجمع القسرى مع تتدفق مفتاحي عشوائي وزائف pseudo-random keystream. التشفير التدفقي شبيه لتشفير الطبعة والواحدة الذي تمت دراسته في الوحدة الثانية، الفرق الوحيد أن تشفير الطبعة الواحدة يستخدم تتدفق حقيقي (غير زائف) والمقابل يستخدم التشفير التدفقي تدفق أرقام عشوائي زائف. استخدام تتدفق المفتاح العشوائي يدمر (يلغي) بالكامل خواص الرسالة الإحصائية. وحدة النص المشرف تعطى بالعلاقة التالية:

$$C_i = M_i \text{ XOR } StreamKey_i \quad \ldots 4.6$$

يتطلب تامين التشفير التدفقي عدم إعادة استخدام تتدفق المفتاح، حتى لا يتم تحليل النص المشفر بسهولة. الشكل 3.8 يوضح البنية العامة لتشفير التدفق. يدخل مفتاح إلى منتج الثنائيات العشوائية الزائفة والذي ينتج بدوره تدفق مفتاحي عشوائي من الثنائيات. والذي يجمع قسريا مع ثنائيات النص الصريح ومراد تشفيره. تستخدم أيضا عملية الجمع القسرى لدى المستقبل لفك التشفير.



الشكل 4.3: بنية تشفير التدفق

للحصول على تشفير تدفق امن لابد من اخذ النقاط التالية في الاعتبار عند تصميم أسلوب التشفير:

- سلسلة التشفير يجب أن تكون دورتها كبيرة، لإعطاء فترة طويلة دون تكرار. كلما ما طالت دورة الإعادة (التكرار) كل ما أصبح من الصعب تحليل الشفرة
- يجب أن يقارب تتدفق المفتاح خصائص تدفق الأرقام العشوائية الحقيقي، كلما ما كان تدفق المفتاح أكثر عشوائية أصبح النص المشفر أكثر عشوائية، مما يصعب تحليل الشفرة.

- الحماية من هجوم تكرار المحاولة يتطلب أن يكون طول المفتاح كافياً، ونفس الاعتبارات بالنسبة للتشفير الكتلي تطبق هنا. في ظل التقنيات الحالية قد يستخدم مفتاح طوله 128 ثنائية.

إن صمم منتج الأرقام العشوائية الزائفة بصورة جيدة، يكون امن تشفير التدفق معادل لأمن التشفير الكتلي يستخدم طول مفتاح مقارن. تشفير التدفق ابسط من التشفير الكتلي وعادة ما يكون تشفير التدفق أسرع منه ويحتاج إلى برامج ابسط.

4.11. تشفير RC4

صمم أسلوب تشفير RC4 في العام 1987. يستخدم تشفير RC4 مفتاح متغير الحجم ويعمل على ثمانيات النص الصريح. تعتمد الخوارزمية على التعديل العشوائي random permutation لإنتاج المفتاح الذي يستخدم لاحقا لتشفير بيانات الدخل ثمانية في أي وقت. ويحتاج من ثمانية إلى ستة عشر عملية آلة machine operations لكل ثمانية خرج من نظام التشفير. تشفير RC4 أوسع نظام تشفير استخداما، وبالأخص في برتوكولات امن الويب مثل SSL/TSL, و برتوكولات تامين الشبكات المحلية اللاسلكية.

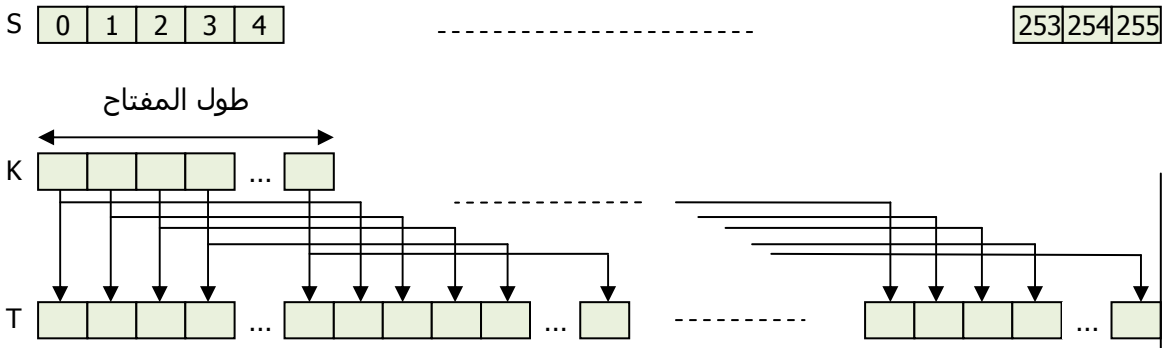
يبدأ جدول تحديد مفتاح تشفير RC4 بإعطاء الحالة (الصف array) S الأرقام 255..0. ثم يتعامل مع كل دخل على التوالي، وباستخدام القيمة الحالية بالإضافة إلى الثمانية التالية في المفتاح يأخذ دخل أخر في الصف array ويتم مقاضية القيم. بعد إتمام هذه العملية 256 مرة تتحصل على مفتاح مخلوط بصورة جيدة. نفس المفتاح يستخدم في التشفير وفك التشفير. مقطع البرنامج التالي يوضح إنتاج المفتاح.

```
 for i = 0 to 255 do
S[i] = i
T[i] = K[i mod keylen])
j = 0
for i = 0 to 255 do
j = (j + S[i] + T[i]) (mod 256)
swap (S[i], S[j])
```

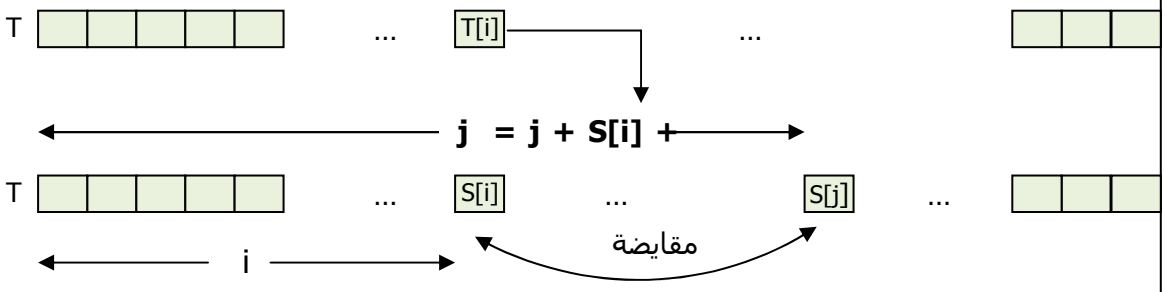
تستخدم عملية الجمع القسرى لجمع النتاج للمفتاح S[t] مع الثمانية التالية في الرسالة (النص الصريح) . مقطع البرنامج التالي يوضح عملية التشفير

```
i = j = 0
for each message byte Mi
i = (i + 1) (mod 256)
j = (j + S[i]) (mod 256)
swap(S[i], S[j])
t = (S[i] + S[j]) (mod 256)
Ci = Mi XOR S[t]
```

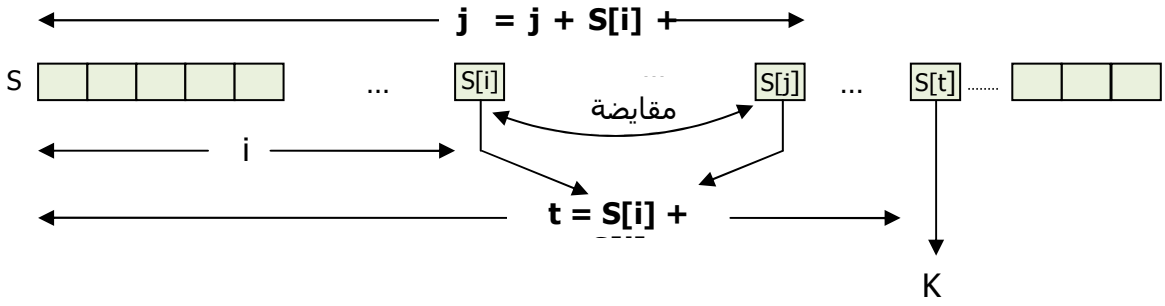
الشكل 6.9 يوضح البنية العامة لتشفير RC4



a: المرحلة الابتدائية لكل من S وT



b: التبديل الابتدائي S



c: إنتاج التدفق

الشكل 9.3: بنية تشفير RC4

تناولت العديد من الأبحاث تحليل الهجوم على تشفير RC4، لم توضح أي من هذه البحوث خطورة عملية على امن تشفير RC4 والذي يستخدم طول مناسب للمفتاح مثل 128 ثنائية. توجد بعض المحاذير عند استخدام هذا التشفير في تامين الشبكات المحلية اللاسلكية WEP، وذلك ليست لأسباب متعلقة بأسلوب التشفير بل بأسباب متعلقة بالتعامل مع المفتاح.

ملخص

تم في هذه الوحدة دراسة المواضيع التالية:

- معيار تشفير البيانات الثنائي والثلاثي
  - صيغ التشغيل المختلفة التالية:
  - صيغة كتاب الشفرة الإلكتروني
  - صيغة ربط الكتل المشفرة
  - صيغة التغذية العكسية بالشفرة
  - صيغة التغذية العكسية بالخرج
  - صيغة التغذية العكسية بالخرج
- تشفير التدفق
- تشفير RC4

أسئلة:

1. باختصار اشرح الاختلاف بين معيار تشفير البيانات المفرد والثلاثي. لماذا يستخدم في الجزء الوسط من معيار تشفير البيانات الثلاثي فك تشفير بدلا عن تشفير.

2. إن حدث خطاء في ثنائية خلال الإرسال في حرف مشفر باستخدام ثمانية ثنائيات في صيغة التغذية العكسية بالشفرة، إلى إي مدي ينتشر هذا الخطاء؟ أشرح.

3. تم الجدول التالي:

الصيغة	التشفير	فك التشفير
كتاب الشفرة الإلكتروني	$Cj = EK [Pj] \; j = 1, \ldots, N$	$Pj = DK [Cj] \; j = 1, \ldots, N$
ربط الكتل المشفرة	$C1 = EK [P1 \oplus IV]$ $Cj = EK [Pj \oplus Cj - 1] \; j = 1, \ldots, N$	
التغذية العكسية بالشفرة		
التغذية العكسية بالخرج		
التغذية العكسية بالخرج		

4. اكتب برنامج للتشفير وفك التشفير باستخدام أسلوب التشفير RC4

الوحدة الخامسة: السرية باستخدام التشفير المتناظر

أهداف الوحدة

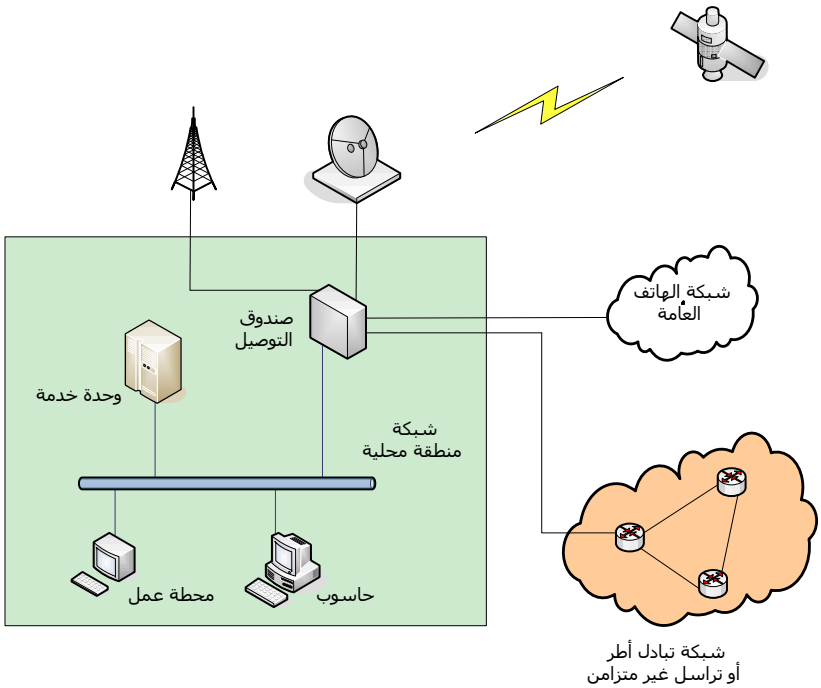
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:

- استخدام التشفير المتناظر لحماية السرية والخصوصية في الشبكات واختيار الموقع المناسب للتشفير
- تحديد مطلوبات توزيع مفتاح التشفير المتناظر
- شرح واستخدام مراكز توزيع المفتاح وإدارته وتحديد مطلوبات التشغيل
- تحديد أهمية الأعداد العشوائية في التشفير وتحديد خواصها
- شرح عمل بعض خوارزميات توليد العدد العشوائي.

5.1. مقدمة:

استخدم التشفير المتناظر تقليديا لحماية سرية المعلومات وخصوصيتها سواء في حالة تخزينها في وحدات الخدمة أو خلال نقلها عبر الشبكات. إن استخدام التشفير لمكافحة الهجمات على السرية والخصوصية في الشبكات، يتطلب تحديد ما يجب تشفيره وأين نضع أجهزة ووظائف التشفير في الشبكة. توجد كثير من المواقع في أي شبكة التي قد تمثل ثغرات أمنية, الشكل 5.1 يوضح الثغرات المحتملة في الشبكات التي قد يحدث من خلالها الهجوم على سرية وخصوصية المعلومات. وتتلخص هذه الثغرات الأمنية في الأتي:

- أجهزة الحاسوب في الشبكة المحلية التي تتصل بأجهزة أخرى أو وحدات خدمة في نفس الشبكة
- الشبكات المحلية المرتبطة بمبدلات أو موجهات مع خطوط اتصالات خارجية أو وصلات رادوية أو وصلات توابع اصطناعية



الشكل 5.1: الثغرات الأمنية في الشبكات

أنوع الهجمات على سرية المعلومات في هذه الشبكة وأماكنها، يمكن تلخيصها في التالي:

- التطفل snooping من حاسوب آخر
- استخدام الاتصال الهاتفي إلى شبكة المنطقة المحلية أو وحدة الخدمة للتطفل
- تفريع خط مادي (كيبل) من صندوق التوصيل
- استخدام وصلة موجه خارجي للنفاذ والتطفل
- مراقبة الحركة في الوصلات الخارجية وتعديلها

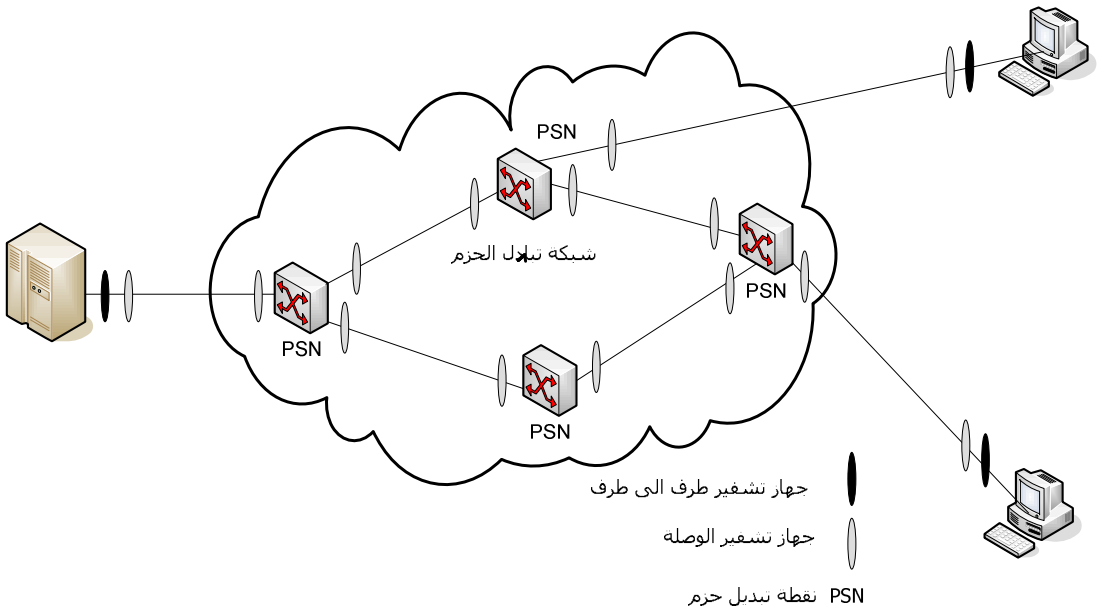
في هذه الوحدة سندرس مطلوبات التشفير في الشبكات وارتباطه برتوكولات الطبقات المختلفة. كما سندرس توزيع مفتاح التشفير وإدارته في نظم تشفير المفتاح الواحد (التشفير المتناظر).

5.2. أنماط التشفير في الشبكات

عادة يستخدم التشفير في موضوعين أساسين وبديلين في الشبكات وهما: على مستوى الوصلة (تشفير الوصلة link encryption) وعلى مستوى طرفيات الاتصال (تشفير النهاية إلى النهاية end-to-end encryption).

في تشفير الوصلة تستخدم أجهزة تشفير encryption device في طرفي أي وصلة اتصالات تكون معرضة للهجوم والتطفل، كما يستخدم تشفير الوصلة في كل الوصلات التي تحدد المسار من المصدر إلى المقصد، حيث يتم التشفير على مستوي الوصلة وباستقلالية عن التشفير في الوصلات الآخري. إن تشارك أي نقطتين (مركزين) nodes بالشبكة في وصلة يتطلب أن يتشاركا في مفتاح تشفير مفرد، ولا بد من استخدام مفاتيح مختلفة لكل وصلة، مما يتطلب توفير عدد كبير من مفاتيح التشفير. نمط التشفير هذا يشفر أيضا وضمنياً الحركة بين نقاط الشبكة.

أما في حالة تشفير النهاية إلى النهاية، تجرى عمليات التشفير في نهايتي (طرفي) النظام بين المصدر الأصلي للبيانات والمقصد الأخير، مما يزيح عن المستخدم الطرفي عبء الاهتمام بدرجة أمان وصلات الاتصالات. هذا الأسلوب يحمى سرية البيانات، وليست نمط الحركة حث أن ترويسة الحزم ترسل دون تشفير للسماح بتوجيه الحركة في الموجهات. يتشارك مصدر البيانات ومقصدها فقط في مفتاح التشفير. الشكل 5.2 يوضح أنماط التشفير هذه.



الشكل 5.2: أنماط التشفير في شبكات تبديل الحزم

يوفر نمط تشفير النهاية إلى النهاية موثوقية أعلى من نمط تشفير الوصلة، حيث انه في تشفير النهاية إلى النهاية يكون المستقبل متأكدا من أن مصدر أي رسالة مستلمة حقيقي وغير زائف، ويشاركه مفتاح التشفير. لتحقيق درجة أمنية عالية نحتاج إلى الاستخدام المتزامن لكل من تشفير الوصلة وتشفير النهاية إلى النهاية، بحيث تتوفر حماية البيانات وتتحقق موثوقية أعلى وحماية للحركة من المراقبة. كما هو موضح في الشكل 5.2.

5.3. التشفير وبرتوكولات الطبقات

يمكن أن نقوم بمهمة التشفير في أي عدد من الطبقات في نموذج ربط النظم المفتوحة المرجعي OSI Reference Model. تشفير الوصلة يمكن أن يتم ضمن وظائف الطبقة الفيزيائية physical layer (طبقة رقم 1) أو طبقة الوصلة link layer (طبقة رقم 2). أما تشفير النهاية إلى النهاية قد يتم ضمن وظائف طبقة الشبكة network layer (الطبقة رقم 3، لكل العمليات في النظام ويمكن أيضا في عمليات الواجهة الخلفية)، أو ضمن وظائف طبقة النقل Transport layer (الطبقة رقم 4، قد يكون لكل عملية على حدة) أو ضمن وظائف طبقتي العرض والتطبيقات (الطبقة رقم 2 و الطبقة رقم 1، خاصة إن تتطلب أن تتعدى الحماية بوابات (منافذ) التطبيقات). كلما ما تم التشفير في الطبقات العليا يقل حجم البيانات المشفرة وتتحصل بالمقابل علي درجة تامين أعلى.

الشكل 5.3 يوضح العلاقة بين التشفير برتوكولات الطبقة، باستخدام بنية برتوكول ضبط الانتقال وبرتوكول الانترنت TCP/IP كمثال. يوضح الشكل كيف يتم حماية المعلومات في الحزمة.

مقطورة الوصلة	البيانات	ترويسة TCP	ترويسة IP	ترويسة الشبكة	ترويسة الوصلة

a: تشفير طبقة التطبيقات (على الوصلة والموجهات والمنافذ)

مقطورة الوصلة	البيانات	ترويسة TCP	ترويسة IP	ترويسة الشبكة	ترويسة الوصلة

على الوصلة والموجهات

مقطورة الوصلة	البيانات	ترويسة TCP	ترويسة IP	ترويسة الشبكة	ترويسة الوصلة

على المنافذ

b: تشفير طبقة النقل TCP

مقطورة الوصلة	البيانات	ترويسة TCP	ترويسة IP	ترويسة الشبكة	ترويسة الوصلة

على الوصلة

مقطورة الوصلة	البيانات	ترويسة TCP	ترويسة IP	ترويسة الشبكة	ترويسة الوصلة

على الموجهات والمنافذ

c: تشفير طبقة الوصلة

الشكل 5.3: التشفير وبرتوكولات الطبقة

يهتم بعض المستخدمين بتحليل الحركة التي قد توفر معلومات عن عدد الرسائل بين نقاط الشبكة وأطوالها. هذه المعلومات قد تمكن المهاجم من تحديد أطراف الاتصال، ثم يستنتج أهمية المعلومات المتبادلة، أو يربطها بأحداث محددة. عند استخدام تشفير الوصلة تشفر ترويسات طبقة الشبكة أيضاً، مما يقلل من فرص تحليل الحركة. يعتبر أسلوب الحشو padding أسلوب فعال لمكافحة هذا النوع من الهجمات (جوم تحليل الحركة). استخدام تشفير النهاية إلى النهاية، يتيح فرص اكبر للمهاجم لتحليل الحركة، نتيجة لعدم تشفير ترويسات البرتوكولات. يمكن هنا استخدام حشو بيانات التطبيقات والرسائل الفارغة، ويكون استخدام الحشو على حساب استمرار الحركة.

5.4. توزيع مفتاح التشفير المتناظر

يتطلب عمل التشفير المتناظر أن يكون للشريكين في الاتصال مفتاح مشترك وسرى. ويجب حماية سرية هذا المفتاح ومنع الآخرين من الوصول إليه. يعتبر توزيع المفتاح وحمايته من أكثر المواضيع حساسية وأهمية في نظم التشفير عامة. ففي كثير من الأحيان يكسر التشفير ليست كنتيجة لضعف التشفير ولكن كنتيجة للاختيار السيئ للمفتاح وسوء إدارته.

قوة أي نظام تشفير تعتمد بدرجة كبيرة على تقنيات توزيع المفتاح. توزيع المفتاح بين الأطراف A و B قد يتم بعدة طرق، نلخصها في التالي:

- التسليم المادي للمفتاح، والذي يعتبر أسلوب بسيط، ولكن يمكن استخدامه فقط إن توفر اتصال شخصي ومباشر بين المستلم ومصدر المفتاح. هذا الأسلوب مناسب لتشفير الوصلة، لان أجهزة التشفير والمفاتيح تكون أجوازا، هناك صعوبة عملية في استخدام هذا الأسلوب في حالة مشاركة أطراف عديدة في الاتصال.
- اختيار طرف ثالث تثق فيه جميع الإطراف لتوزيع المفتاح وتسليمه للأطراف A و B, يعمل الطرف الثالث كوسيط موثوق به لا يسئ استخدام معلومات المفاتيح.
- إذا كان هناك اتصال سابق بين الطرفين A و B، يمكن استخدام المفتاح السابق لتشفير المفتاح الجديد.
- إذا كان لكل من الإطراف A و B اتصال امن مع طرف ثالث C، يمكن استخدام الطرف الثالث لتمرير المفتاح بين A و B.

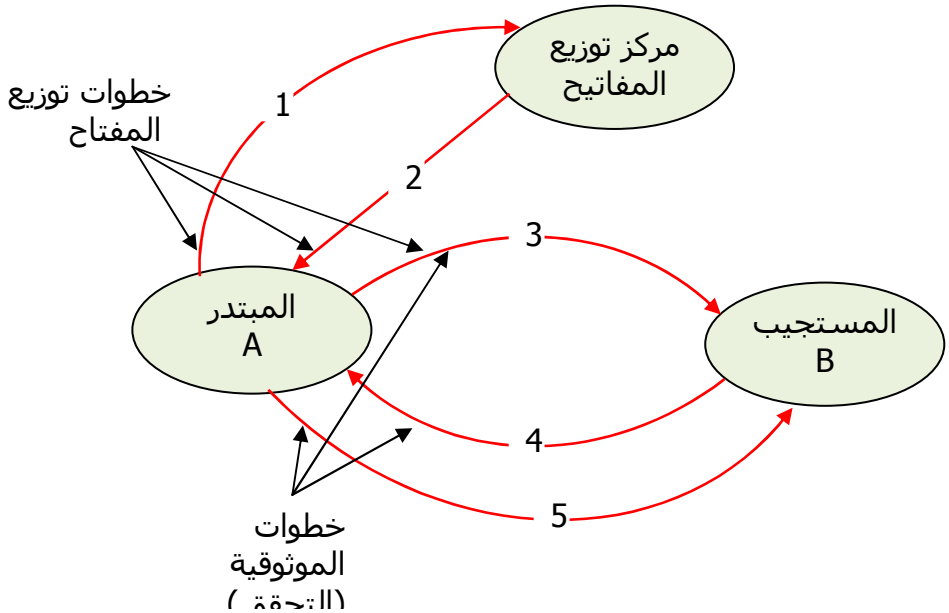
كل أساليب توزيع وتسليم المفاتيح هذه تكون غير عملية في حالة مشاركة عدد كبير من الإطراف في الاتصال. وفى هذه الحالة يكون استخدام مراكز توزيع المفاتيح هي الحل العملي. إن استخدام مركز توزيع المفتاح يعتمد على استخدام هرم للمفاتيح، أو مستوين من المفاتيح وهما مفتاح الجلسة session key والذي يستخدم خلال فترة التوصيل المنطقي والمفتاح الرئيسي master key يكون مشتركا بين مركز توزيع المفتاح والنظام النهائي أو المستخدم، ويستخدم المفتاح الرئيسي لتشفير مفتاح الجلسة.

مفهوم توزيع المفتاح يمكن تنفيذه بعدة طرق، الشكل 5.4 يوضح احد الطرق النموذجية لتوزيع المفتاح، في هذه الطريقة مركز توزيع المفتاح (KDC) "Key Distribution Center يتشارك مع كل مستخدم (طرف) مفتاح فريد، ويتم تسليم المفتاح بعد التوثق من الأطراف.

بالنسبة للشبكات الكبيرة ينشاء هرم لمراكز توزيع المفتاح. يجب أن تثق كل المراكز في بعضها البعض. للاتصال بين أطراف في نفس النطاق المحلى، يكون مركز توزيع المفتاح المحلى مسئولا عن توزيع المفتاح. إذا كان الاتصال بين إطراف في نطاقات مختلفة، يتم الاتصال بين مراكز توزيع المفتاح المحلية عبر مركز معلومات عالمي في مستوى أعلى من الهرم، لتوزيع المفتاح وإدارته.

عادة يستخدم مفتاح جديد يدعى مفتاح الجلسة لإيجاد التوازن بين الأمن ومجهود توزيع وإدارة المفاتيح. الحصول على مستوى امن عالي يتطلب تحديد المدى الزمني لمفتاح الجلسة. في حالة الاتصالات المتجهة للربط connection-oriented يستخدم مفتاح جلسة جديد لكل

جلسة ربط جديدة، أما في حالة البرتوكولات غير المتجهة للربط connectionless protocol يستخدم مفتاح الجلسة فقط لفترة زمنية محددة أو لعدد محدد من المعاملات. فصل المفاتيح الرئيسة من مفاتيح الجلسات قد يتطلب ضبط لاستخدام المفتاح، مما قد يتطلب تحديد أنواع مختلفة من مفاتيح الجلسات على أساس التطبيقات.



الشكل 5.4: مثال لاسلوب توزيع المفتاح عبر مركز توزيع المفتاح

أسلوب التوزيع المفتاح الذاتي automated key distribution يعطى مرونة وحركية اكبر في إدارة المفاتيح، هذه الخاصية مطلوبة للسماح لعدد من الأطراف بالنفاذ (الوصول) إلى الجهاز المضيف host وأيضا للسماح للأجهزة المضيفة بتبادل البيانات فيما بينها، يتطلب التوزيع الذاتي للمفتاح أن تثق كل الأطراف في النظام الذي يعمل بالنيابة عنهم، كما يجب حماية هذه المركز من التخريب والعبث بها، ما يمكن تجنبه أن كان نظام توزيع المفتاح الذاتي غير ممركز بالكامل.

5.5. الأعداد العشوائية:

تقوم الأعداد العشوائية بادوار هامة عند استخدام التشفير في تطبيقات المختلفة لتامين وحماية الشبكات. وبالرغم الصعوبة العملية فمن المهم الحصول على أعداد عشوائية جيدة، حتى لا يمكن تحليل الشفرة بسهولة. وتتلخص صفات الأعداد العشوائية الجيدة بالنقاط التالية:

- أن تكون إحصائيا عشوائية وتوزيعها منتظما ومستقلة
- لا يمكن التنبؤ يقيمها المستقبلية من قيمها السابقة

تستخدم الأعداد العشوائية في مجالات التشفير التالية:

- برتوكولات التوثيق لمنع الإجابة والتمرير
- مفاتيح الجلسات
- توليد المفتاح العام
- تدفق المفتاح في الطبعة الواحدة

تستخدم تطبيقات التشفير عادة تقنيات الخوارزمية المحددة لتوليد الأعداد العشوائية، التي تنتج سلاسل من الأعداد التي قد تكون غير عشوائية إحصائيا، ولن أن كانت الخوارزمية جيدة، تستوفى هذه السلاسل المتحصل عليها كثير من اختبارات العشوائية، مثل هذه الأعداد تعرف

باسم الأعداد العشوائية الوهمية (الزائفة) pseudorandom numbers وتنتج باستخدام مولد العدد العشوائي الوهمي "Pseudorandom Number Generators (PRNGs)".

5.5.1. مولد التطابق الخطى

يعتبر مولد التطابق الخطي Linear Congruential Generator أكثر التقنيات استخداماً لتوليد العدد العشوائي الوهمي. يستخدم هذا الأسلوب قيم متتابعة X_i على مقياس m من المعادلة التكرارية التالية:

$$X_{n+1} = (aX_n + c) \bmod m \qquad \ldots\ldots\ldots \quad 5.1$$

بإعطاء قيم مناسبة للعوامل a و c يمكن إنتاج سلسلة طويلة شبه عشوائية، تكمن الصعوبة هنا في وجود بدائل محدودة لاختيارات العوامل الجيدة. رغم أن السلسة تبدو عشوائية، يمكن التبوء بها، ويستطيع المهاجم إعادة إنشاء السلسلة من معرفة عدد محدود من القيم فقط. توجد بعض الطرق التي يمكن استخدامها جعل التبوء بالسلسة صعبا، ولكننا سوف لا نناقشها في هذا المقرر.

5.5.2. تشفير الكتلة كمولد أعداد عشوائية وهمية

بالنسبة لتطبيقات التشفير قد يكون من المنطقي الاستفادة من أي من وظائف التشفير الكتلي لإنتاج أعداد عشوائية. يمكن استخدام نمط العداد أو نمط التغذية العكسية بالخرج لتوليد مفتاح الجلسة من المفتاح الرئيسي.

في حالة استخدام نمط العداد تتحصل على العدد العشوائي X_i على مقياس m باستخدام المعادلة:

$$X_i = EK_m[i] \qquad \ldots\ldots\ldots \quad 5.2$$

أما في حالة استخدام نمط التغذية العكسية بالخرج تتحصل على العدد العشوائي X_i على مقياس m باستخدام المعادلة:

$$Xi = EKm[Xi\text{-}1] \qquad \ldots\ldots\ldots \quad 5.3$$

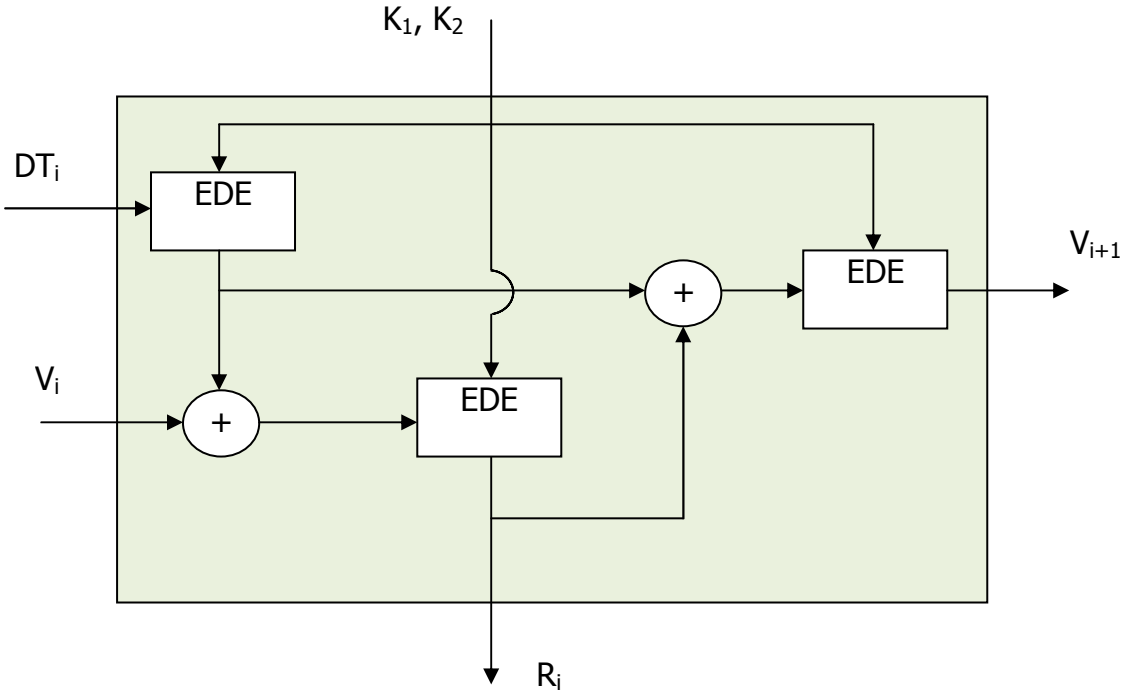
5.5.3. مولد انسى X9.17

يعتبر مولد العدد العشوائي الوهمي انسى ANSI X9.17 X9.17 من اقوي مولدات الأعداد العشوائية الوهمية لتطبيقات التشفير. يستخدم هذا الأسلوب التاريخ والزمن (DT_i) بالإضافة إلى بذرة دخل (V_i) وثلاثة تشفيرات علي اساس معيار تشفير البيانات الثلاثي بالمفاتيح K_1 و K_2 ($EDE[K_1,K_2]$) لتوليد بذرة جديدة (V_{i+1}) وقيمة عشوائية (R_i) تحسب باستخدام المعادلات التكرارية التالية:

$$R_i = EDE([K_1, K_2], [V_i \text{ XOR } EDE([K_1, K_2], DT_i)]) \qquad \ldots 5.4a$$
$$V_{i+1} = EDE([K_1, K_2], [R_i \text{ XOR } EDE([K_1, K_2], DT_i)]) \qquad \ldots 5.4b$$

كثير من العوامل تؤثر على قوة التشفير بهذه الطريقة. تستخدم هذا الأسلوب مفتاح طوله 112 ثنائية وثلاثة تشفيرات EDE لانجاز تسعة تشفيرات DES. يدفع هذا الأسلوب بدخلين من

الأعداد العشوائية الوهمية، وقيمة التاريخ والزمن وبذرة تنتج بمولد مستقل من مولد العدد العشوائي الوهمي المنتج بالمولد، الشكل 5.5.



الشكل 5.5: مولد مولد انسي X9.17

5.5.4. مولد بلوم بلوم شوب

مولد بلوم بلوم شوب Blum Blum Shub Generator أسلوب شائع لتوليد عدد عشوائي وهمي امن. يعتمد هذا الأسلوب على خوارزميات المفتاح العام (انظر الوحدة السادسة)، مما يجعله بطيئاً جداً. يستخدم الأسلوب ادني ثنائية ذات قيمة من المعادلة التكرارية التالية علي مقياس n:

$$x_i = x_{i-1}2 \bmod n \qquad \ldots 5.5$$

حيث n=p.q وأعداد أولية تعطى بالتالي p,q=3 mod 4

عمليا لا يمكن التنبؤ بالعدد العشوائي الوهمي المولد بهذا الأسلوب.

ملخص

درسنا في هذه الوحدة

- استخدام التشفير المتناظر لحماية السرية والخصوصية في الشبكات واختيار مكان وضع أجهزة التشفير
- التوزيع الجيد للمفتاح
- استخدام مراكز توزيع المفتاح وإدارته
- بعض المواضيع المرتبطة بالأعداد العشوائية وتوليدها.

أسئلة

1. أفترض أن محمد ومريم يستخدمون بالبرتوكول التالي للتأكد من امتلاك كل منهما نفس المفتاح السري المتناظر: محمد ينتج سلسلة من الثنائيات العشوائية يساوي طولها طول المفتاح، ثم يجمعها قسريا مع المفتاح ويرسل الناتج إلي مريم. تقوم مريم بجمع الرسالة المستقبلة من محمد قسريا مع مفتاحها (والذي يجب أن يكون شبيهاً لمفتاح محمد) تم ترسل الناتج إلي محمد. يفحص محمد الرسالة المستلمة من مريم للتأكد من استلام سلسلة البيانات العشوائية الأصلية. أشرح كيف يتأكد محمد بان مريم لديها نفس المفتاح، مع ملاحظة أن كل من محمد ومريم لم يتبادلا المفتاح مسبقاً. هل يوجد خلل في هذا الأسلوب؟ وإذا كان هناك خلل اشرحه
2. أفترض أن مريم تريد الحديث مع محمد عبر سلسلة من ثلاثة مراكز توزيع مفاتيح (مركز توزيع مفاتيح مريم ومركز توزيع مفاتيح محمد ومركز توزيع المفاتيح الذي يشارك المفاتيح مع مركز مفاتيح مريم ومركز مفاتيح محمد) . أعطي الأحداث المتتابعة والضرورية لإنشاء هذا الاتصال.،
3. أساليب توزيع المفتاح التي تستخدم مركز ضبط النفاذ و/أو مركز توزيع المفتاح لديها نقاط مركزية غير حصينة وتكون معرضة للهجوم. ناقش الآثار الأمنية لهذا لأساليب توزيع المفتاح المركزي هذاـ ووضح كيف يمكن تحسين الأمن في هذه الحالة.

الوحدة السادسة: تشفير المفتاح العام وخوارزمية **RSA**

أهداف الوحدة
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:

- تحديد خصائص وصفات تشفير المفتاح العام (التشفير غير المتناظر)
- معرفة طبيعة الأعداد الأولية واستخدامها في عمليات تشفير المفتاح العام
- معرفة واستخدام نظريات الأعداد المرتبطة بتشفير المفتاح العام
- معرفة خصائص وطريقة عمل خوارزمية RSA
- معرفة طرق توليد المفتاح العام والخاص في خوارزمية RSA
- تحديد مهددات امن خوارزمية RAS وطرق مكافحتها

6.1. مقدمة:

كل أساليب التشفير التي تعرضنا لها في الوحدات السابقة تصنف كأساليب تشفير متناظر (تشفير المفتاح الخاص أو الأمن أو الوحيد). وتعتمد هذه الأساليب على عمليات الإحلال والتبديل (الانتقال) ويتشارك المرسل والمستقبل في المفتاح. كشف المفتاح يعرض الاتصالات للمخاطر. في حالة التشفير المتناظر يتساوى الشركاء (إطراف الاتصال)، مما لا يحمى المرسل من تزوير المستقبل للرسالة وإدعاءه استلامها من المرسل.

سندرس في هذه الوحدة نظام تشفير مفتاح عام مختلف كليا عن النظم التشفير التي قمنا بدراستها في الوحدات السابقة. تطوير تشفير المفتاح العام public-key cryptography يعتبر من أهم الإحداث في تاريخ التشفير. أسلوب التشفير هذا غير متناظر ويستخدم مفتاحين عكس أساليب التشفير المتناظر والتي يستخدم مفتاح واحد. المفتاح العام يستخدم لتشفير الرسالة أو لتتحقق من التوقيع، ولا يمكن أن يستطيع لفك التشفير أو إنتاج التوقيع. تعتمد نظم تشفير المفتاح العام على الاستخدام الذكي لعدد من المفاهيم النظرية. لا تعتبر نظم تشفير المفتاح العام أكثر (أو اقل) أمنا من نظم التشفير الخاص ولا تهدف إلى إحلالها، بل تعتبر متمة لها.

التشفير بالمفتاح غير المتناظر (Asymmetric key encryption) هو أسلوب من أساليب التشفير يتم فيه تشفير البيانات باستخدام مفتاح ما وفك تشفيرها باستخدام مفتاح آخر، ولهذا السبب سمي بالتشفير غير المتناظر، لأن مفتاح التشفير يختلف عن مفتاح فك التشفير، وبالتالي فإنه يسمح بتوزيع صلاحيات التشفير وفك التشفير على الجهات المختلفة بأن يعطي لبعضهم مفاتيح التشفير فقط ويعطي للآخرين مفاتيح فك التشفير. ويسمى هذا النوع من التشفير أيضا بالتشفير بالمفتاح العلني أو العام (encryption public-key)، لأنك تستطيع أن تنشر أحد المفتاحين وهو يسمى المفتاح العلني (public-key)، وتحتفظ بالآخر سريا، ويسمى المفتاح الخاص (private-key). وعندما تقوم الجهة A مثلا بنشر مفتاح علني، أي طرف في الاتصال يستطيع استخدام هذا المفتاح لتشفير البيانات المراد إرسالها إلي A، لكنه لن يتمكن من فك تشفير هذه البيانات باستخدام هذا المفتاح العلني، (المفتاح العلني يستخدم للتشفير فقط ولا يمكن استخدامه لفك التشفير)، أما فك التشفير فيكون باستخدام المفتاح الخاص الذي يكون بحوزة الطرف A فقط، وبالتالي فهو الجهة الوحيدة الذي يمكنها قراءة الرسائل التي شفرت باستخدام مفتاحه العلني.

وأشهر خوارزميات هذا النوع من التشفير هي خوارزمية (RSA- Rivest, Shamir and Adleman) نسبة إلى العلماء الثلاثة الذين وضعوا هذه الخوارزمية.

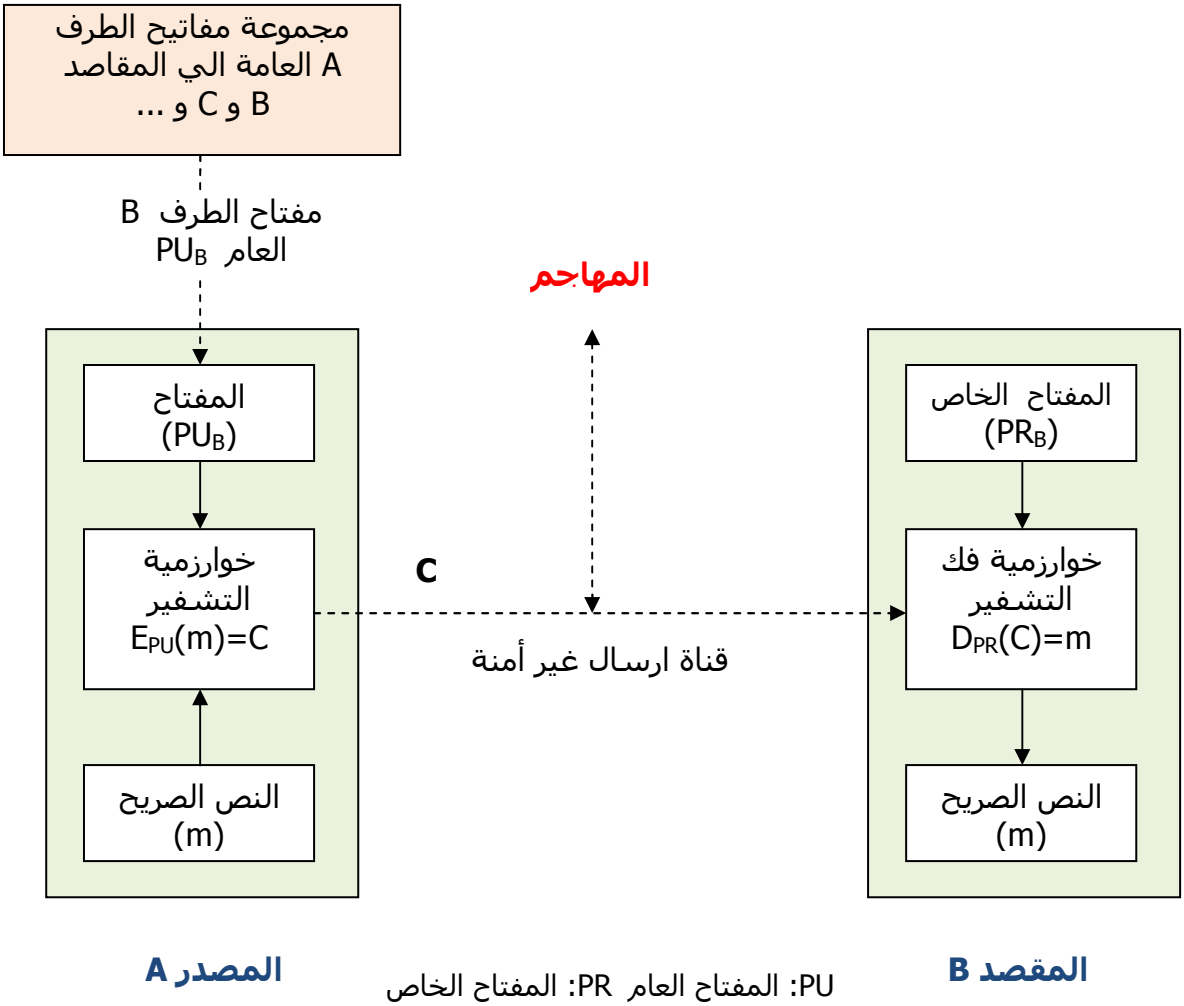
كثير من المفاهيم في نظرية الأرقام ذات أهمية في تصميم خوارزميات تشفير المفتاح العام، ولذل سنتعرض لنظرية الأرقام في هذه الوحدة.

6.2. تشفير المفتاح العام

تتطور مفهوم تشفير المفتاح العام من المحاولة لمعالجة مشكلتان صعبتان يلازمان التشفير المتناظر وهما: توزيع المفتاح والحصول على اتصالات أمنة لا تحتاج إلى مركز توزيع المفاتيح.

يستخدم أسلوب تشفير المفتاح العام مفتاحين مرتبطين، لهم ادوار ومقدرات مختلفة. أي شخص يعرف المفتاح العام يمكنهم تشفير الرسائل والتحقق من التوقيعات ولكنه لا يستطيع فك التشفير أو إنتاج التوقيعات، وتتحصل على هذه الخاصية بالاستخدام الذكي لنظرية الأرقام.

الشكل 6.1 يوضح بنية نظام تشفير المفتاح العام. يتكون هذا النظام من ستة عناصر وهى: النص الصريح و خوارزمية التشفير والمفتاح العام والخاص والنص المشفر وخوارزمية فك التشفير.



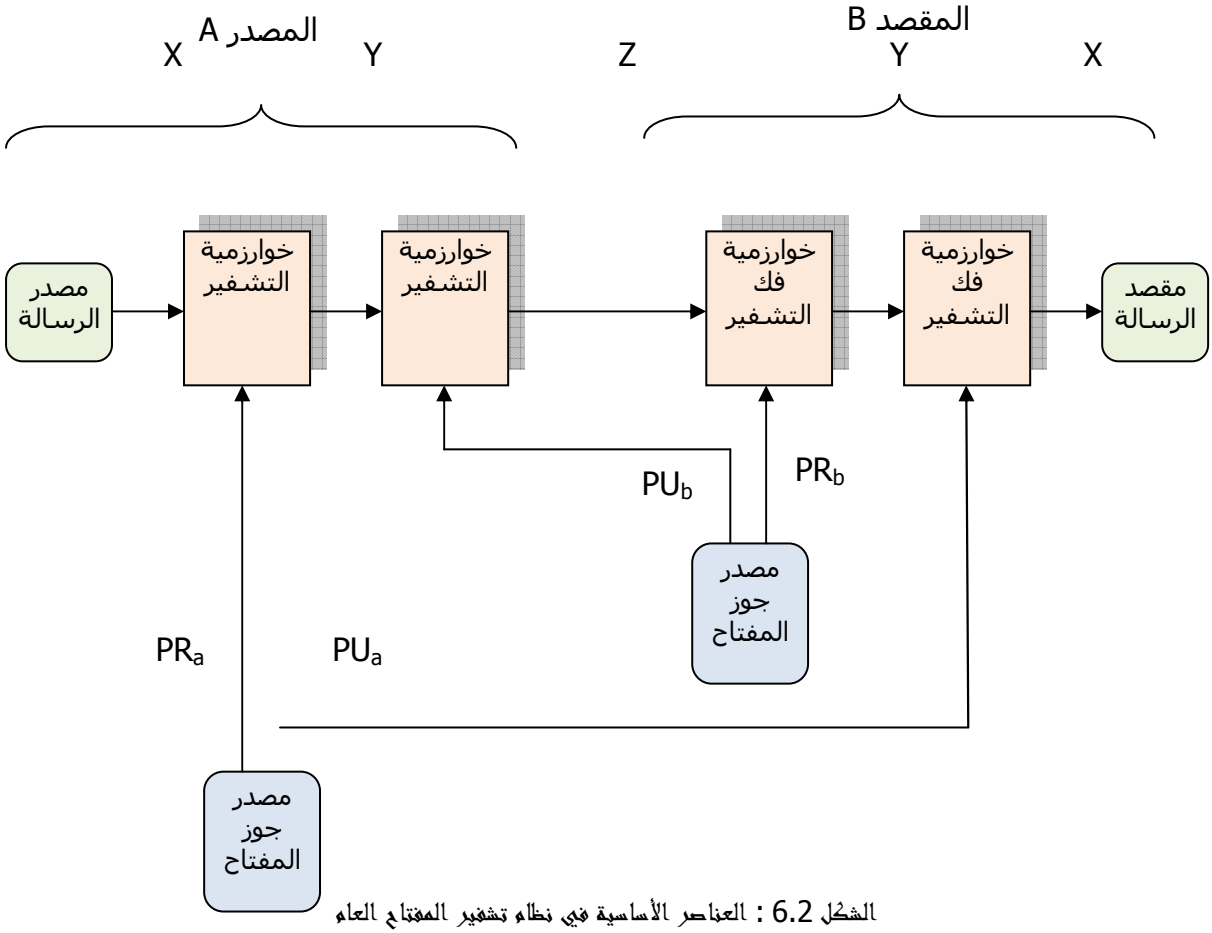
PU: المفتاح العام PR: المفتاح الخاص

الشكل 6.1: بنية نظام تشفير المفتاح العام

تعتمد خوارزميات التشفير غير المتناظر على استخدام مفتاح للتشفير ومفتاح أخر مختلف ومرتبط به لفك التشفير. هذه الخوارزميات لديها الخواص المهمة التالية: من غير المجدي حسابيا محاولة استنتاج مفتاح فك التشفير بمعرفة خوارزمية التشفير ومفتاح التشفير فقط. تنتفع أساليب تشفير المفتاح العام من المعضلات التي تكون سهلة من جهة معينة وصعبة من الجهة الأخرى، مثل الدوال الآسية مقابل الدوال اللوقرثمية و الضرب مقابل إيجاد العوامل. بعض الخوارزميات لديها المقدرة على استخدام أي المفتاحين كمفتاح عام أو مفتاح خاص.

الشكل 6.2 يوضح العناصر الأساسية في نظام تشفير المفتاح العام والذي قد يقوم بالتكتم (السرية) Secrecy او الموثوقية Authentication وكلاهما. في حالة النظام الموضح في الشكل 6.2 يستخدم مفتاحين منفصلين للتكتم والموثقية. حيث ينتج المستقبل مفتاح التكتم ويمتلكه وينتج المرسل مفتاح الموقوقية ويمتلكه. لا يحدث هذا عمليا، نسبة للتكلفة الحسابية

العالية لأساليب المفتاح العام. حيث يتم تشفير مفتاح جلسة الذي يستخدم لاحقا مع التشفير الكتلي لتشفير الرسالة، ويوقع بانفصال الرسالة المشفرة (المفرومة) كتوقيع رقمي، وهذا ما سندرسه في الوحدة التاسعة.



الشكل 6.2 : العناصر الأساسية في نظام تشفير المفتاح العام

طبيعة التطبيقات تحدد استخدام المفتاح العام، فيمكن للمرسل أن يستخدم مفتاحه الخاص أو مفتاح المستقبل العام أو كلاهما للقيام ببعض أنواع وظائف التشفير. بصورة عامة يمكننا تصنيف نظم تشفير المفتاح العام إلى ثلاثة أنواع:

- نظم التشفير وفك التشفير: حيث يقوم المرسل بتشفير الرسالة والمستقبل بفك التشفير
- التوقيع الرقمي: يوقع المرسل الرسالة باستخدام المفتاح الخاص سواء كان كل الرسالة أو كتلة صغيرة من لبيانات تمثل وظيفة للرسالة.
- تبادل المفتاح: يتعاون الطرفين لتبادل مفتاح الجلسة. توجد أساليب مختلفة يمكن استخدامها لتبادل مفتاح الجلسة، تعتمد على المفتاح الخاص لأحد الطرفين أو كلاهما.

بعض خوارزميات تشفير المفتاح العام يمكن استخدامها في التطبيقات المذكورة أعلاه، وبعضها تكون محددة لتطبيق محدد.

لا يمكن التحديد إن كان تشفير المفتاح العام أكثر أو اقل أمانا مقارنة مع تشفير المفتاح الخاص، فامن الشفرة في كلا الحالتين يعتمد على حجم المفتاح. يمكن استنتاج المفتاح العام أو المفتاح الخاص إن توفرت للمهاجم معلومات وإمكانيات كافية. على المستوى النظري قد

يتعرض المفتاح العام مثل المفتاح الخاص إلى هجوم التكرار. في حالة المفتاح العام يوجد أساس نظري لتحديد امن المفتاح، حيث انه يعتمد نظرية الأرقام المعروفة بصورة جيدة.

6.3. نظرية الأرقام

للأرقام الأولية (الأساسية) prime numbers أهمية خاصة في نظرية الأرقام number theory. العدد الصحيح p > 1 يكون عدد أولى (أساسي) أذا وفقط إذا كان يقبل القسمة علي 1 أو العدد نفسه، أي لا يمكن التعبير عنه كحاصل ضرب أعداد أخرى. ونلاحظ أن الرقم 1 رقم أولى، وان كان ليس ذو أهمية. الأرقام 2 و 3 و 5 و 7 أمثلة لأرقام أولية والأرقام 4 و 6 و 8 و 9 و 10 أرقام ليست أولية. تقوم الأعداد الأولية بدور محوري ومهم في نظرية الأرقام .

تحليل الرقم تهدف إلى تحديد الأرقام الأولية التي يقبل القسمة عليها. وبتحليل الرقم يمكننا التعبير عنه كحاصل ضرب أرقام أولية (قد تكون باس معين). إذا كانت a و b و c العوامل الأولية للرقم n، عندها يكون n=a x b x c. فمثلا $3600=2^4x3^2x5^2$; 91=7x13. يعبر عن الرقم بدلالة عوامله الأولية بالمعادلة التالية:

$$n = \prod_{p \in P} p^{a_p} \qquad \ldots\ldots \quad 6.1$$

تكون الأعداد a و b نسبيا أولية إذا لم يتشاركا في عامل مشترك غير 1، مثل 8 و 15 حيث عوامل 8 هي 1 و 2 و 4 و 8 وعوامل 15 هي 1 و 3 و 5 و 15 والعدد 1 هو العامل المشترك بينهما. يحدد القاسم المشترك الأعظم GCD(a,b) "greatest common divisor" (اكبر عدد يقبل كل من a , b القسمة عليه) بين الأعداد التي تكون نسبيا أولية بمقارنة عواملهم الأولية واستخدام أدنى أس. فمثلا $300=2^1x3^1x5^2$ $18=2^1x3^2$، علية يكون $GCD(18,300)=2^1x3^1x5^0=6$.

نظرية فيرمات

نظرية فيرمات Fermat's theorem تحدد خاصية هامة للأعداد الأولية، وتعطى بالعلاقة التالية:

$$a^{p-1} = 1 \pmod p$$

حيث p عدد أولى وأيضا GCD(a,p)=1

وأيضا نجد أن

$$a^p = p \pmod p$$

هذه النظرية مفيدة وتستخدم في المفتاح العام واختبار الأولية.

6.3.1. نظرية أيلر

دالة ايلر توتينت ø(n) Euler's Totient function تعرف عدد الأعداد الصحيحة الموجبة التي تقل عن n و أولية نسبيا للعدد n. يستخدم التعبير "متبقي residue" للإشارة إلى الأعداد التي اقل من أساسmodulus محدد ، عندما نجرى العملية الحسابية على أساس n، كما يستخدم التعبير "مجموعة البواقي المختصرة reduced set of residues" للإشارة إلى الأعداد (المتبقيات) التي تكون أولية نسبياً إلى الأساس (n)، ويساوى ø(n). يلاحظ هنا أن ø(1) = 1. مثلا إن أخذنا n=10 تتحصل على

- مجموعة الكاملة للبواقي: {0,1,2,3,4,5,6,7,8,9}
- مجموعة البواقي المختصرة: {1,3,7,9}

العناصر في مجموعة البواقي المختصرة تسمى دالة ايلر توتينت Euler's Totient function ø(n). لحساب هذه الدالة نحتاج إلى عد عدد البواقي التي سوف ستستثني. عامة نحتاج أن نستخدم معادلة معقدة على تحليل n لعواملها الأولية، وهنا نلاحظ التالي:

- بالنسبة إلى p (عدد أولى) ← ø(p) = p-1،
- بالنسبة الى p و q (اعداد أولية) ← ø(pq) =(p-1)x(q-1).

مثال:

$$ø(37) = 36$$
$$ø(21) = (3–1)x(7–1) = 2x6 = 12$$

تعتبر نظرية أيلر Euler's Theorem تعميم لنظرية فيرمات لأي عدد n. ويمكن عن نعبر هنا بالاتي:

$$a^{ø(n)} = 1 \pmod n$$

بالنسبة لأي a و n وعند GCD(a,n)=1

مثال:

$\rightarrow 3^4 = 81 = 1 \bmod 10$ a=3;n=10; ø(10)=4;
a=2;n=11; ø(11)=10; $\rightarrow 2^{10} = 1024 = 1 \bmod 11$

6.3.2. اختبار الأولية

تتطلب كثير من وظائف التشفير اختيار أعداد أولية كبيرة جداً بطريقة عشوائية. مما يجعل من الضرورة التأكد من العدد الكبير العشوائي أن يكون أولي. يتم اختبار الأعداد تقليديا بالقسمة التجريبية، حيث بقسم العدد على كل العوامل الأولية. هذا الأسلوب غير عملي بالنسبة للأعداد الكبيرة. أسلوب بديل لإختبار الأولية يستخدم اختبارات أولية إحصائية متكررة، تعتمد هذه الاختبارات على خواص الأعداد الأولية ولكن هناك بعض الأعداد تدعي الإعداد الأولية الزائفة (الوهمية) pseudo-primes أيضا تستوفى مطلوبات هذا الاختبار وللتأكد نستخدم بعد ذلك اختبارات أولية محددة ولكنها بطيئة مثل اختبار ASK.

تستخدم خوارزمية ميلر رابين Rabin Algorithm لاختبار أولية الأعداد الكبيرة. يعتمد هذا الاختبار على نظرية فيرمات، ويمكن تلخيصه في الخطوات التالية:

1. أوجد الاعداد الصحيحة k و q، $k > 0$ و q عدد فردي، بحيث $(n-1)=2^k q$
2. إختار عدد صحيح عشوائي a، $1 < a < n-1$
3. إذا كان $a^q \bmod n = 1$، حينها أرجع "قد يكون عدد أولي"
4. كرر لقيمة j=0 الي قيمة j=k-1
5. إذا كان $a^{2/q} \bmod n = n-1$، حينها أرجع "قد يكون عدد أولي"
6. أرجع "عدد مركب"

1. Find integers k, q, $k > 0$, q odd, so that $(n–1)=2^k q$
2. Select a random integer a, $1<a<n–1$
3. if $a^q \bmod n = 1$ then return ("maybe prime");
4. for $j = 0$ to $k – 1$ do
5. if ($a^{2jq} \bmod n = n$-1)
   then return(" maybe prime ")
6. return ("composite")

أذا أعادت خوارزمية ميلر رابين "composite" مركب يكون أكيد أن العدد غير أولى، غير ذلك قد يكون أولى أو أولى زائف، احتمال اكتشاف العدد الأولى الزائف تقل عن 0.25. بإعادة الاختبار بعشوائية مختلفة، تكون فرصة العدد n أن يكون أولى بعد t اختبار تعطى بالاتي:

$$\Pr(\text{n عدد أولى بعد t اختبار}) = 1\text{-}4^{-t}$$

نتيجة لنظرية الأعداد، تعرف باسم نظرية الأعداد الأولية prime number theorem، تنص على أن الأعداد الأولية بقرب n توزع في المتوسط عدد لكل (ln n) عدد صحيح. حيث إننا نستطيع تجاهل الأعداد الزوجية، نحتاج في المتوسط فقط اختبار 0.5 ln(n) عدد من حجم n لتحديد الأعداد الأولية. فمثلا للأعداد حول 2^{200} نفحص 0.5ln(2^200) = 69 عدداً في المتوسط.

6.3.3. نظرية الباقي الصينية

احد أهم نتائج نظرية الأعداد نظرية الباقي الصينية. والتي تساعد في تسريع بعض العمليات في تشفير المفتاح العام RSA. إذا كان أساس العمل حاصل ضرب أعداد مثل $m_1m_2..m_k$، باستخدام نظرية الباقي الصينية يمكن أن نعمل في كل أساس m_i منفصلاً ، ثم ندمج النتائج لنحصل على النتيجة الفعلية. بهذا الأسلوب يمكننا معالجة الأعداد (التي قد تكون كبيرة) على أساس M بدلالة إعداد صغيرة، وتكون هذه الطريقة فعالة أن كانت M تساوى أو تزيد عن 150 ثنائية. لحساب A(mod M) نتبع الخطوات التالية:

- اولاً احسب منفصلا كل القيم $a_i = A \bmod m_i$
- حدد الثوابت c_i من المعادلة التالية عندما يكون $M_i = M/m_i$

$$c_i = M_i \times \left(M_i^{-1} \bmod m_i\right) \qquad for\ 1 \le i \le k$$

- ادمج النتائج للتحصل على الاجابة باستخدام المعادلة التالية:

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i\right) (\bmod\ M)$$

6.3.4. الجذور الابتدائية

اعتبر أسس من أعداد صحيحة على مقياس n. باستخدام نظرية ايلير، لكل عدد نسبيا أولى a، يوجد على الأقل آس واحد يساوى 1 (يكون) ولكن قد يكون هناك قيمة أصغر. من نظرية ايلير تتحصل على $a^{ø(n)} \bmod n = 1$. اعتبر $a^m = 1 \pmod n$ و GCD(a,n)=1 فلا بد من وجود m = ø(n)، ولكن قد لا تكون أصغر قيمة، عندما تصل الأسس قيمة m نعيد الدورة. إذا كانت قيمة m = ø(n) أصغر قيمة، عندها a تدعى الجذر الابتدائي. إذا كان p عدد أولى، عندها أسس a المتتابعة تولد كل البواقي على أساس n.

اللوغارثمات المنفصلة:

تعتبر اللوغارثمات المنفصلة Discrete Logarithms من العمليات الجوهرية في عدد من خوارزميات المفتاح العام، مثل تبادل مفتاح دبفى وهيلمان Diffie-Hellman key exchange وخوارزمية التشفير الرقمي digital signature algorithm (DSA).

اللوغارثمات المنفصلة (أو الدلالات indices) تشارك خواص اللوغارثمات العادية. أعتبر العلاقة:

$$y = g^x \pmod p$$

نعيد كتابة هذه العلاقة كالأتي

$$x = \log_g y \pmod p$$

إذا كان g جذر ابتدائي فيكون دائما موجوداً وغير لا يكون موجود، مثلا:

$$x = \log_3 4 \bmod 13$$

لا يوجد جواب

$$x = \log_2 3 \bmod 13 = 4$$

محاولة أسس متتابعة

6.4. خوارزمية RSA

تعتبر خوارزمية RSA من أكثر خوارزميات تشفير المفتاح العام استخداما، نشرت هذه الخوارزمية لأول مرة في العام 1978 من قبل ريفيست و شامير و ادليمان Rivest, Shamir & Adleman التابعين لمعهد مسشيقين التقني MIT. منذ ذلك التاريخ أصبحت هذه الخوارزمية مقبولة بصورة واسعة لإنتاج تشفير المفتاح العام لإغراض متعددة. تعتمد الخوارزمية على ألآس في مجال محدد على الأعداد الصحيحة على أساس العدد الأولى a. تستخدم الخوارزمية أعداد صحية كبيرة، مما يوفر امن كبير لها نتيجة المجود والتكلفة الحسابية الكبيرة المطلوبة لتحليل العدد.

ينشا مفتاح خوارزمية RSA مرة واحدة فقط (نادرا) عندما ينشئ المستخدم مفتاحه العام أو استبداله. كل مستخدم ينتج مفاتحين، مفتاح عام ومفتاح خاص وفقاً للخطوات التالية:

- اختيار عددين أولين كبيرين عشوائيا، لنفترضهما p و q
- تحسب أساس نظامهما $p.q = n$. ويلاحظ هنا وباستخدام نظرية أيلر أن $\phi(n)=(p-1)(q-1)$
- اختار عشوائيا مفتاح التشفير e، بحيث $1<e<\phi(n), GCD(e,\phi(n))=1$
- حل المعادلة التالية لإيجاد مفتاح فك التشفير d $e.d=1 \bmod \phi(n)$ and $0 \le d \le n$
- انشر مفتاح التشفير العام PU= {e,n}
- احتفظ مفتاح فك التشفير سرا: PR= {d,n}

الآس e يكون عادة صغيرا، فقط أن يكون أولى نسبيا إلى ø(n)، ونحتاج إلى حساب معكوسة على أساس ø(n) ((mod ø(n) لإيجاد d. من الأهمية أن نحافظ على سرية بالعوامل p و q على أساس n، نسبة لاحتمال استخدامهما في كسر التشفير.

حسابات تشفير وفك تشفير خوارزمية RAS الفعلية تكون ببساطة أس واحد على مقياس n. ويجب أن تكون الرسالة اصفر من المقياس (modulus)، مما يتطلب استخدام كتل من النص الصريح. لتشفير الرسالة M يتحصل المرسل على المفتاح العام PU={e,n} من المستقبل، ثم يحسب الرسالة المشفرة باستخدام $C = M^e \bmod$ ، عندما يكون $0 \le M < n$. لفك النص المشفر C، يقوم المالك باستخدام مفتاحه الخاص PR={d,n} ليحسب النص الصريح باستخدام العلاقة $M = C^d \bmod n$.

من الواضح أن خوارزمية RSA تعمل كنتاج مباشر لنظرية أيلر، وعلية برفع العدد بالآس e ثم بالآسن d (أو العكس) ينتج العدد الأصلي. وهذا ما قد نعبر عنه بالخطوات التالية:

- نظرية أيلير
  - $a^{\phi(n)} \bmod n = 1$ حيث $GCD(a,n)=1$
- في خوارزمية RSA
  - $n=p.q$
  - $\phi(n)=(p-1)(q-1)$
  - اختار كل من e و d بعناية لتكون معكوس $\bmod \phi(n)$
  - عندعا يكون $e.d=1+k.\phi(n)$ لبعض قيم k

بناءً على ما تقدم، تتحصل على النص المشفر C بالعلاقة التالية:

$$C^d = M^{e.d} = M^{1+k.\phi(n)} = M^1.(M^{\phi(n)})^k$$
$$= M^1.(1)^k = M^1 = M \bmod n$$

قبل تطبيق تشفير المفتاح العام، كل طرف في الاتصالات يجب أن يولد (ينتج) مفاتيحين، مما تتطلب إيجاد أعداد أولية وحساب المعكوس. كل من توليد الأعداد الأولية واشتقاق جوز مناسب من الآسس العكسية قد يتطلب محاولة عدد من البدائل. نخمن عشوائياً لقيم محتملة لكل من p و q ثم نفحص باستخدام اختبار الأولية الاحتمالي لتحديد أن كان العدد حقيقا أولى. توضح نظرية الأعداد الأولية بان متوسط عدد التخمينات كبيراً جداً، مما يتطلب استخدام خوارزمية الانعكاس.

6.4.1. مثال لخوارزمية RSA

أنشاء المفتاح

سنأخذ هنا مثالا لتوليد مفتاح خوارزمية RSA باستخدام حجم أعداد عادى (صغير). اختيار الإعداد الأولية يحتاج إلى استخدام اختبار الأولية والذي تعرضنا له في القسم السابق. إيجاد d معكوس e mod ø(*n*)، وتتحصل على المفتاح بالخطوات التالية:

- اختار أعداد أولية: لنفترض p=17 و q=11
- احسب n = pq = 17 × 11 = 187
- أحسب ø(*n*) = (*p*–1)(*q*-1) = 16 × 10 = 160
- اختار e بحيث: GCD(e,160) =1، عليه e = 7
- أوجد d بحيث *de*=1 mod 160 و d < 160، علية d = 23 حيث 1+160×10=161=7×23
- انشر المفتاح العام: PU = {7,187}
- احتفظ بالمفتاح الخاص سريا وهو: PR = {23,187}

التشفير وفك التشفير

عملتي التشفير وفك التشفير تمثل آسي على مقياس 187 بسيطة. نفترض رسالة M = 88 (لاحظ 88 < 187) يتم إنتاج الرسالة المشرفة كالأتي:

:

$$C = 88^7 \bmod 187 = 11$$

أما فك التشفير فيتم كالأتي:

$$M = 11^{23} \bmod 187 = 88$$

بدلا من عمليا الضرب المكررة والمرهقة، نستخدم خوارزمية التربيع والضرب "square and multiply" algorithm مع خصم الأساس لتنفيذ الأسس بسرعة وكفاءة. تتمحور فكرة هذه الخوارزمية بتكرار تربيع الأساس ثم نضرب عند الحاجة لحساب النتيجة. مثلا:

$$7^5 = 7^4.7^1 = 3.7 = 10 \bmod 11$$
$$3^{129} = 3^{128}.3^1 = 5.3 = 4 \bmod 11$$

مقطع البرنامج التالي ينفد خوارزمية التربيع والضرب

```
c = 0; f = 1
for i = k downto 0
do c = 2 x c
f = (f x f) mod n
if bi == 1 then
c = c + 1
f = (f x a) mod n
return f
```

6.4.2. كفاءة التشفير وفك التشفير

لتسريع عملية خوارزمية RSA المستخدمة للمفتاح العام، يمكننا اختيار قيمة صغيرة لتمثل e، على أن لا تكون صغيرة جداً بحيث تكون ثغرة للهجوم). ثم نتأكد من القيم المختارة لكل من p و q قيم أولية نسبيا للثابت e. ولتسريع الخوارزمية يمكننا أيضا استخدام نظرية المتبقي الصينية لحساب mod p و mod q كل على حدة، ثم ندمج النتائج لتتحصل على الجواب المطلوب. هذه الطريقة أسرع بأربع مرات مقارنة مع حساب $C^d \bmod n$ مباشرة. ونلاحظ هنا فقط مالك المفتاح الخاص والذي يعرف قيم p و q يمكنه استخدام هذه الطريقة.

6.5. أمن خوارزمية RSA

أساليب مهاجمة خوارزمية RSA يمكن تلخيصها في التالي:

- هجوم البحث الشامل على المفتاح، ويمكن الحد من هذا الهجوم باستخدام حجم مفتاح كبير. ويجب الانتباه هنا إلى تعقيدات العمليات الرياضية المصاحبة لتوليد المفتاح والتشفير وفك التشفير، مما يجعل النظام بطيئاً أن استخدم مفتاحا كبيراً.
- الهجمات الرياضية والتي تعتمد على صعوبة حساب ø(n) بتحليل المقياس n
- الهجمات الزمنية وتكون في القيام بفك التشفير
- هجمات النص المشفر المختار والتي تعتمد على خواص خوارزمية RSA المعروفة.

6.5.1. مشكلة التحليل:

تعتمد هذه الهجمات على تحليل الشفرة رياضيا، وتحليل الأعداد. العمليات الرياضية في هذه الخوارزمية تأخذ ثلاثة أشكال وهى:

- تحليل $p.q = n$ ثم حساب ø(n) وحساب d منها
- تحديد ø(n) مباشرة وحساب d
- إيجاد قيمة d مباشرة

كل هذه الإشكال مكافئة لتحليل العدد، والذي شهد تحسن بطيئا على مر السنوات، واكبر تحسين من تحسين الخوارزمية، أحسن خوارزمية مستخدمة حاليا هي خوارزمية "Lattice Sieve" والتي أحلت مكان خوارزمية "Generalized Number Field Sieve" (GNFS) والتي كانت على أحلت مكان خوارزمية "Quadratic Sieve"(QS).

يعتبر حاليا مناسبا استخدام حجم يساوى مابين 1024 و 2048 ثنائية للحصول على خوارزمية أمنة لتأكيد أن كل من p و q لديهم نفس الحجم وتتوافق مع التعقيدات الأخرى.

6.5.2. الهجمات الزمنية:

يعتبر الهجوم الزمني نوع جديد من الهجمات طور بواسطة بول كوشر فى Paul Kocher في منتصف تسعينات القرن الماضي، ويعتمد هذا الهجوم على مراقبة الفترة الزمنية المطلوبة لإنهاء عمليات فك التشفير. والتي قد يستنتج منها بعض الخواص مثل الضرب بعدد صغير أو كبير. هجمات الزمن تنطبق على كل نظم تشفير المفتاح العام وليست فقط تشفير خوارزمية RSA. تتمثل خطورة هذا الهجوم في سببين وهما:

- يحدث من جهة غير متوقعة
- ويعتمد فقط على النص المشفر

رغم خطورة الهجوم الزمني، توجد أساليب بسيطة لمكافحته، مثل استخدام خوارزميات آس زمني ثابت constant exponentiation time algorithms و إضافة تأخير عشوائي لعملية فك الشفرة، واستخدام قيم عمياء في الحسابات.

6.5.3. هجوم النص المشفر المختار

خوارزمية RSA معرضة لهجمات النص المشفر المختار، والذي يعرف بالهجوم يقوم فيه المهاجم (الخصم) باختيار عدد من النصوص المشفرة، وبمعرفة النصوص الصريحة المقابل لها ويفك التشفير بمفتاح الهدف الخاص. يستغل المهاجم خواص خوارزمية RSA والكتل المختارة من البيانات، عند الاستمرار في استخدام مفتاح الهدف الخاص، مما ينتج المعلومات الضرورية له لتحليل (كسر) التشفير.

يمكن مكافحة هذا الهجمات البسيطة باستخدام حشوه عشوائية من النص الصريح. أما مكافحة الهجمات الأكثر تعقيداً تحتاج إلى تعديل النص الصريح باستخدام أسلوب يدعى حشو التشفير غير المتناظر الأمثل asymmetric encryption padding (OAEP) .

ملخص:

درسنا في هذه الوحدة:

- أسس تشفير المفتاح العام
- خصائص الأعداد الأولية نظريات الأعداد المرتبطة بتشفير المفتاح العام
- وخصائص خوارزمية RSA وتنفيذها وأمنها

اسئلة

1. ما قيمة $3^{2007} \bmod 17$ (أعطي الإجابة في الصيغة 0.... 16)
2. أعتبر الأرقام 1..16، وضح لكل عدد I يوجد معكوس وهو الرقم J بحيث $I*J = 1 \bmod 17$.
3. إن كانت S(n) مجموعة أعداد (1..n-1) أولية للعدد n. وضح لكل عدد I في S(n) يوجد عدد J في S(n) بحيث $I*J = 1 \bmod n$.
4. أوجد $3^8 \bmod 14$. أوجد قيمة x بحيث $3^x = 14 \bmod 17$. أيهما أسهل في الحساب الأس أو اللوقيرثمات المنفصلة.
5. إذا كان العدد p عدد أولي، أثبت ان
$$\emptyset(p^i) = p^i - p^{i-1}$$
6. إذا كان GCD(m,n)=1 يمكن اثبات الأتي:
$$\emptyset(m * n) = \emptyset(m) * \emptyset(n)$$
وتعرف ايضا Ø(p)=p-1 ان كان p عدد أولي. بافتراض هذه النتائج ونتيجة السؤال 5 أعلا، أوجد: Ø(108) و Ø(64) و Ø(231) و Ø(91) و Ø(550) .
7. هل العدد 2047 عدد أولي؟ إذا كان كذلك أثبت. إذا كان غير أولي وضح كيف يمكن استخدام نظرية فيرمات لإثبات ذلك.
8. أشرح بالتفصيل عمل خوارزمية RSA في التشفير. ماهو المفتاح العام (العلني) والمفتاح الخاص، كيف يتم التشفير وفك شفرة النص المشفر؟
9. أيهما أكثر أمانا: معايير التشفير البيانات الثلاثي طوله 112 ثنائية أم تشفير RSA طوله 112 ثنائية ولماذا؟
10. قوم بعملية التشفير وفك التشفير باستخدام خوارزمية RSA والعوامل التالية: p=5, q=11, e=3, M=9

الوحدة السابعة: إدارة المفتاح وأنواع تشفير المفتاح العام الأخرى

أهداف الوحدة
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:
- شرح أساليب وطرق توزيع المفتاح العام وخصائصها
- شرح مطلوبات توزيع المفتاح السري باستخدام المفتاح العام
- استخدام تبادل المفاتيح باستخدام أسلوب ديفي وهلمن
- القيام بتشفير النص الصريح باستخدام أسلوب المنحنى الهليلجيّ
-

7.1: مقدمة:

تعتبر طرق توزيع المفتاح من المهام الأساسية والمحورية في تشفير المفتاح العام. تحتوى عمليات توزيع المفتاح وإدارته على عمليتين أساسيتين وهما:
- توزيع المفتاح العام
- استخدام تشفير المفتاح العام لتوزيع المفاتيح السرية

سندرس هذه العمليات في هذه الوحدة.

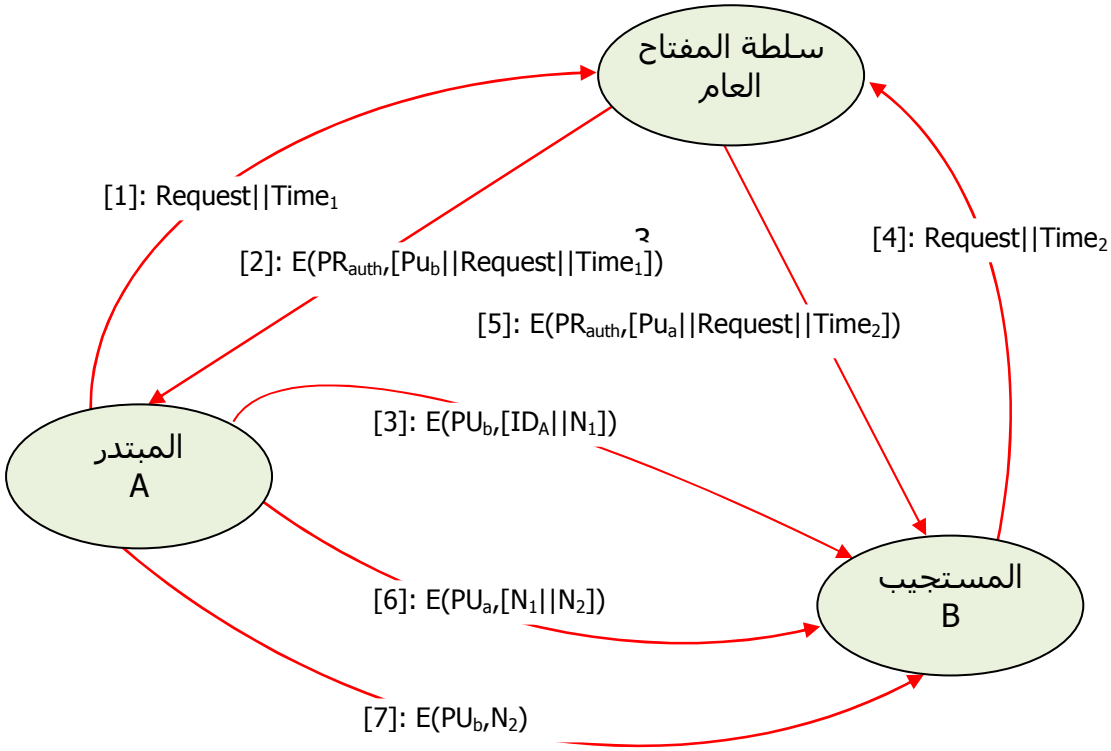
7.2: توزيع المفاتيح العامة:

يوجد العديد من التقنيات التي قد تستخدم في توزيع المفاتيح العامة، ويمكن تجميع هذه التقنيات في الفئات التالية:
- الإعلان العام
- الدليل العام
- سلطة المفتاح العام
- شهادات المفتاح العام

الإعلان العام
من صفات تشفير المفتاح العام أن المفتاح العام يكون متاحا للجميع، فكل مشارك (طرف) يمكنه إرسال مفتاحه العام لأي مشارك (طرف) أخر أو إذاعة هذا المفتاح لكل الأطراف وجعله مشاعاً. الضعف هذا الأسلوب يكمن في إمكانية التزوير. حيث أي شخص يمكنه إنتاج مفتاح ويدعى انه شخص أخر ويوزعه على الجميع. وينتحل المزور الشخصية المذكورة حتى اكتشاف التزوير.

الدليل العام
قد تتحصل على مستوى أعلى من الأمن بإدارة دليل عام يكون متاح للجميع المفاتيح العامة. الاحتفاظ بهذا الدليل العام وتوزيعه يكون مسئولية كيان أو مؤسسة محددة موثوق فيها. رغم أن هذا الأسلوب أكثر أمنا من الإعلان الفردي عن المفاتيح، ولكنه أيضا به بعض الثغرات الأمنية التي قد تسمح بالتلاعب أو التزوير. تتلخص خصائص الدليل العام في التالي:
- يحتوى على {*السم، المفتاح العام*}
- يسجل المشاركين بأمان في الدليل
- يمكن للمشاركين استبدال المفتاح في أي وقت
- ينشر الدليل دورياً
- يمكن النفاذ إلى الدليل الكترونياً

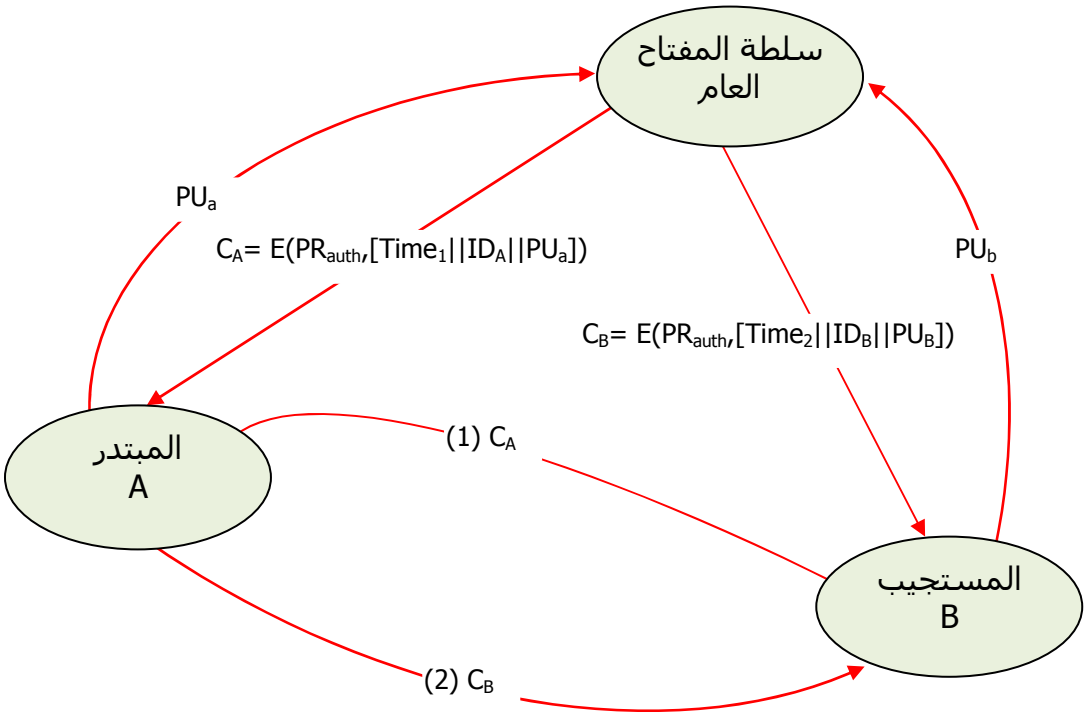
سلطة المفتاح العام:
قد تتحصل على امن وحماية اقوي لتوزيع المفتاح العام بوضع ضوابط محكمة على التوزيع من خلال الدليل العام. يتطلب هذا أن يعرف المستخدم مفتاح العام للدليل، ويتم تعامل المستخدم مع الدليل في الزمن الفعلي للحصول على المفتاح العام بأمان. الشكل 7.1 يوضح تداخل البرتوكولات المستخدمة في أسلوب سلطة المفتاح العام.



الشكل 7.1 : البرتوكولات المستخدمة في أسلوب سلطة المفتاح العام

<u>شهادة المفتاح العام:</u>

استخدام الشهادات يؤدي إلى تحسين إضافي في امن توزيع المفتاح العام. حيث يمكن هذا الأسلوب من تبادل المفاتيح دون الاتصال المباشر أو النفاذ في الزمن الفعلي إلى سلطة المفتاح العام، وذلك بنفس درجة الاعتمادية كما أن كان المفتاح متحصل عليه مباشرة من السلطة. تضيف الشهادة إلى المفتاح العام هوية بالإضافة معلومات أخرى مثل فترة الصلاحية والحقوق وغيره، مع توقيع كل المحتويات من قبل مفتاح عام موثوق فيه أو سلطة الشهادات Certificate Authority (CA). ويمكن التحقيق من هذه البيانات لدي سلطة المفتاح العام من قبل أي شخص يعرف المفتاح العام. الشكل 7.2 يوضح نظام شهادات المفتاح العام.



الشكل 7.2: نظام شهادات المفتاح العام

7.3: توزيع المفاتيح السرية باستخدام المفتاح العام

بعد توزيع المفتاح العام أو جعل الوصول إليه ممكناً يصبح بالمكان الاتصال بطريقة أمنة تمنع التطفل والتلاعب، مما يوفر سرية وموثوقية، رغم ذلك عدد قليل من المستخدمين يستفيدون من اتصالات تشفير المفتاح العام بصورة شاملة، نسبة لمعدل إرسال البيانات المنخفض لهذه الطريقة للاتصالات. ولهذا السبب يستخدم تشفير المفتاح العام لتوزيع مفتاح خاص (سري) يستخدم في التشفير المعتاد وحماية محتويات الرسالة.

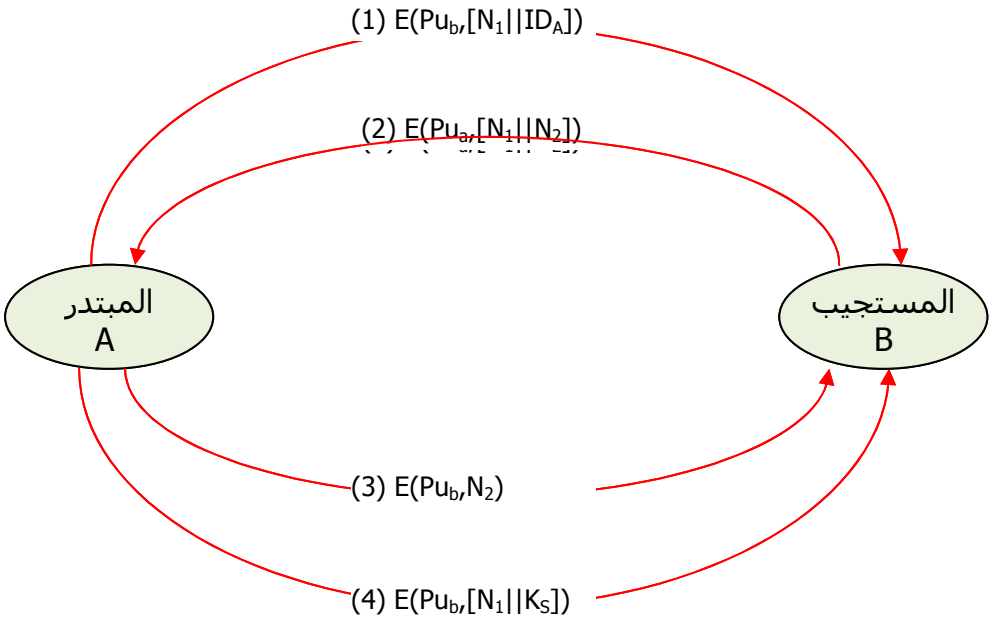
أسلوب توزيع المفتاح السرى البسيط

اقترح من قبل ميركيل في العام 1979 احد الأساليب البسيطة لتوزيع المفتاح السري (مفتاح الجلسة). وتحدد الطريقة بالخطوات التالية:

- الطرف A يولد جوز جديد من المفاتيح العامة المؤقتة
- يرسل A إلى B المفتاح العامة وهوايتهما
- يولد B مفتاح الجلسة K ويرسله إلى B بعد تشفيره بالمفتاح العام المرسل من A
- يقوم الطرف A بفك شفرة مفتاح الجلسة، ثم يستخدم في تشفير الرسائل.

هذا الأسلوب غير مؤمن ضد هجمات الاعتراض، حيث يمكن للمهاجم اعتراض الرسالة ثم يقوم بتعديلها أو استبدالها برسالة أخرى. هذا هجوم يعرف أيضا باسم بهجوم رجل الوسط man-in-the-middle attack.

الشكل 7.3 يوضح برتوكول تبادل المفتاح السري باستخدام المفتاح العام، يقوم هذا البرتوكول بكل من السرية والمثوقية.



الشكل 7.3 : تبادل المفتاح السري باستخدام المفتاح العام

<u>التوزيع الهجين للمفتاح</u>

التوزيع الهجين أسلوب أخر يستخدم لتوزيع المفتاح السري باستخدام المفتاح العام. استخدم هذا الأسلوب في حواسيب IBM الرئيسية. يعتمد الأسلوب على مركز توزيع المفتاح الذي يشارك المستخدمين في مفتاح رئيسي سرى ويوزع مفاتيح جلسات سرية مشفرة باستخدام المفتاح الرئيسي. ويستخدم أسلوب المفتاح العام لتوزيع المفتاح الرئيسي.

7.4: أسلوب ديفي وهلمن لتوزيع المفتاح

أول أسلوب عملي لتوزيع المفاتيح باستخدام المفتاح العام أعلن في العام 1977 من قبل ديفي وهلمن Diffie & Hellman. هذا الأسلوب مستخدم في عدد من المنتجات التجارية. الغاية من هذه الخوارزمية تمكين المستخدمين من تبادل المفتاح بأمان والذي يستخدم لاحقا لتشفير الرسائل. تعتمد الخوارزمية على تبادل قيم سرية (رسائل اعتباطية)، وتعتمد على قيم المفاتيح العامة والخاصة للشركاء، بدلا عن إنشاء مفتاح مشترك. يستخدم أسلوب آس في مدى محدد (الحساب على أولى modulo a prime أو polynomial)، تعتمد كفاءة الخوارزمية على صعوبة حساب اللوغرثميات المنفصلة.

استخدام خوارزمية ديفي وهلمن لتبادل المفتاح يعتمد على الإعلان عن عددين: عدد أولى كبير أو متسلسلة q وعدد صحيح a يكون جذر ابتدائي للعدد q. هذه الأعداد قد تكون مشتركة بين جميع المستخدمين. تولد أسس الجذر الابتدائي a كل عناصر mod q تتابعاً. المستخدمون A و B يختارون أعدد عشوائية سرية (×) ثم تحمى هذه الأعداد باستخدام الأسس لإنتاج مفاتيحهم العامة (y). فمثلا المستخدم A يولد مفاتيحه كالأتي:

- يختار مفتاح (عدد) سرى x_A ($x_A < q$)
- يحسب مفتاحه العام y_A ($y_A = a^{xA} \bmod q$)
- الإعلان العام عن المفتاح y_A

التبادل الفعلي للمفتاح لكل طرف يحتوى على رفع مفاتيح الآخرين العامة بآس يساوى المفتاح الخاص. العدد الناتج يستخدم كمفتاح للتشفير الكتلي أو أساليب تشفير المفتاح الأخرى. يعطى مفتاح الجلسة K_{AB} للمستخدمين A و B بالعلاقة التالية:

$$K_{AB} = a^{xA.xB} \bmod q$$

عندما يحسب المفتاح من قبل المستخدم A يعطى المعادلة:

$$K_{AB} = y_B^{xA} \bmod q$$

وعندما يحسب المفتاح من قبل المستخدم B يعطى المعادلة:

$$K_{AB} = y_A^{xB} \bmod q$$

يستخدم K_{AB} كمفتاح جلسة لتشفير المفتاح الخاص بين المستخدمون A و B. إذا كان هناك اتصال سابق يبين المستخدمون A و B، سيكون لهم نفس المفتاح السابق في حالة الاتصال الجديد، إلا إذا تم اختيار مفاتيح عامة جديدة. حتى يتمكن المهاجم من الحصول على نفس القيمة يحتاج على الأقل معرفة احد الأعداد السرية، ما يعني حل لوغراثماية منفصلة، والتي تحتاج إلى مجهود حسابي كبير للأعداد الكبيرة.

مثال

- المستخدمون A و B الراغبون في مقايضة المفاتيح يتفقون على العدد الأولي q=353 والعدد الصحيح a=3
- لاختيار مفاتيح سرية و عشوائية، يختار المستخدم A قيمة x_A تساوى 97 ويختار المستخدم B قيمة x_B تساوى 233.
- يحسب مفتاح الجلسة المشترك من ناحية A و B كالأتي:

$$K_{AB} = y_B^{xA} \bmod 353 = 248^{97} = 160$$
$$K_{AB} = y_A^{xB} \bmod 353 = 40^{233} = 160$$

خوارزمية التشفير هذه أيضا معرضة لهجوم رجل الوسط، وتتطلب موثوقية المفتاح.

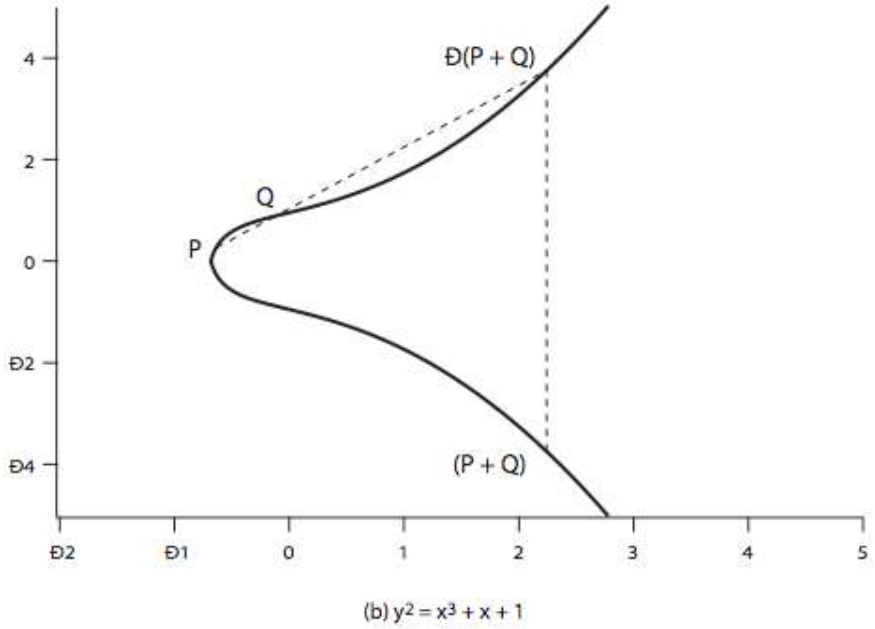
7.5: تشفير المنحنى الهليلجيّ

يمثل حجم الأعداد المستخدمة أكثر المواضيع أهمية في تشفير المفتاح العام، والتي تتطلب جهداً كبيراً لتخزين ومعالجة المفتاح والرسالة. في الفترة الأخيرة طور أسلوب بديل وهو تشفير المنحنى الهليلجيّ، والذي تنجز فيه العمليات الحسابية باستخدام حساب المنحنى الهليلجيّ elliptic curve arithmetic بدلا عن حسابات الأعداد الصحيحة أو المتسلسلات. مستوي السرية في هذه الخوارزمية ليست في مستوى امن خوارزمية RSA.

يحدد المنحنى الهليلجيّ بمعادلة من متغيرين x و y مع عوامل. المنحنى الهليلجيّ التكعيبيّ cubic elliptic curve يحدد بالمعادلة التالية:

$$y^2 = x^3 + ax + b$$

حيث x و y و a و b كلها أعداد صحيحة، كما يحدد أيضا نقطة صفر zero point O. عملية الجمع في المنحنى الهليلجيّ هي جمع هندسي لكل من Q+R وهو انعكاس لتقاطع R. الشكل 7.4 يوضح المنحنى الهليلجيّ التكعيبيّ حين يكون a=b=1، كما يوضح أيضا عملية الجمع.



الشكل 7.4 : المنحنى الهليلجيّ التكعيبيّ

تشفير المنحنى الهليلجيّ يستخدم المنحنيات الهليلجيّة التي تكون فيها المتغيرات والعوامل محددة بعناصر مجال محدد. وتستخدم عائلتان من المنحنيات الهليلجيّة في تطبيقات التشفير، وهما:

- المنحنيات الأولية $E_p(a,b)$ prime curves المحددة على Z_p (مناسب جداً للبرمجيات) وتستخدم أعادا صحيحة integers modulo a prime
- المنحنيات الثنائية $E_{2m}(a,b)$ binary curves المحددة على $GF(2^m)$ (مناسبة لتطبيقات العتاد) ويستخدم متسلسلات بعوامل ثنائية.

جمع المنحنى الهليلجيّ مماثل لضرب المقياس، أما تكرار الجمع فيكون مماثل إلى modulo exponentiation. وتعتبر لغوريثمات المنحنى الهليلجيّ من المشاكل الصعبة. فمثلا إن كان $Q=kP$ عندما ينتمي كل من Q و P إلى منحني أولي، فمن السهل حساب Q إن أعطيت k و P انظر الشكل 7.4، ولكن من الصعب إيجاد k إن أعطيت Q و P.

يمكن استخدام المنحنى الهليلجيّ لتبادل المفتاح وذلك كالأتي:

- يختار المستخدمون منحني $E_p(a,b)$ مناسب
- تختار نقطة أساس $G=(x_1,y_1)$ لديها رتبة n كبيرة بحيث $nG=O$
- يختار كل من A و B مفاتيح خاصة $n_A<n$, $n_B<n$
- يحسب المفتاح المشترك: $K=n_An_BG$ ، حيث $K=n_AP_B$, $K=n_BP_A$

يوجد العديد من الأساليب للتشفير وفك التشفير باستخدام المنحنى الهليلجيّ. سندر هنا أسلوب واحد مماثل خوارزمية الجمال لتشفير المفتاح العام. ويعمل هذا الأسلوب على الوجه التالي:

- يقوم المرسل أولا بتمثيل إي رسالة كنقطة P_m في المنحنى الهليلجيّ، وتوجد تقنيات برمجية لهذه العملية.
- اختار منحني مناسب والنقطة G في ديفي وهلمن
- يختار أي مستخدم مفتاح خاص $n_A<n$
- يحسب المفتاح العام $P_A=n_AG$
- تشفر النقطة P_m إلى النقطة $C_m=\{kG, P_m+kP_b\}$ المشفرة ، حيث K عشوائي.

- كما يرسل المرسل إمارة تسمح للمستقبل والذي يعرف المفتاح الخاص لاسترجاع k وفك الشفرة على النحو التالي: $P_m+kP_b-n_B(kG) = P_m+k(n_BG)-n_B(kG) = P_m$

يعتمد امن خوارزمية المنحنى الهليلجيّ على مستوى صعوبة تحديد قيمة k ان عرفت قيم kP و P، يشار إلى هذا باسم مشكلة لوغراثماية المنحنى الهليلجيّ. أحد الأساليب السريعة لتحليل خوارزمية المنحنى الهليلجيّ هي طريقة بولارد رهو Pollard rho method. بمقارنة هذا الأسلوب مع أسلوب تحليل الأعداد الصحيحة أو المتسلسلات، قد نحتاج إلى مفتاح اصغر من المفتاح المستخدم في خوارزمية RSA، وعليه للحصول على نفس مستوى الأمن تتطلب خوارزمية المنحنى الهليلجيّ لمجهود حسابي أقل.

ملخص:

درسنا في هذه الوحدة:

- توزيع المفتاح العام
- توزيع المفتاح السري باستخدام المفتاح العام
- تبادل ديفي وهلمن
- تشفير المنحنى الهليلجيّ

أسئلة

1. أشرح بالتفصيل استخدام أسلوب ديف-هيلمات Diffie-Hellman في التشفير. ما هو المفتاح العام (العلني) والمفتاح الخاص، كيف يتم التشفير وفك شفرة النص المشفر؟

الوحدة الثامنة: الموثوقية ودوال الفرم (الهاش)

أهداف الوحدة
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:
- شرح موثوقية الرسالة والعلاقة بين تشفير الرسالة والموثوقية
- إنتاج شفرات موثوقية الرسالة
- إنتاج واستخدام دوال الفرم (الهش)

8.1: مقدمة:

في سياق الاتصالات عبر الشبكات، لابد من حماية الرسائل من الهجمات التالية: إفشاء المحتوى و تحليل الحركة و التنكر والتزوير و تعديل المحتوى و تعديل التسلسل و تعديل التزامن وتزوير للمصدر والمقصد.

في كل الوحدات السابقة كان اهتمامنا على استخدام التشفير حماية محتويات الرسالة (السرية وعدم إفشاء محتواها) وتحليل الحركة. في هذه الوحدة سندرس كيف نحمى سلامة الرسالة وتكاملها وعدم تعديلها، أي حمايتها من التعديل، وإثبات شخصية المرسل. في بعض التطبيقات، مثل التجارة الالكترونية، تكون موثوقية الرسالة أكثر أهمية من حماية محتوياتها. تهتم أساليب موثوقية الرسالة بحماية سلامة (كمال) الرسالة و إثبات شخصية مصدرها وعدم تكرار المصدر (قرار التنازع). يوجد ثلاثة أساليب قد تستخدم لإنتاج الموثوقية وهى تشفير الرسالة وشفرة موثوقية الرسالة message authentication code (MAC) ودالة الهش hash function.

إما التحقق من المصدر والمقصد فيمكن أن يتم باستخدام التوقيع الرقمي والذي سندرسه في الوحدات القادمة.

8.2: التشفير والموثوقية:

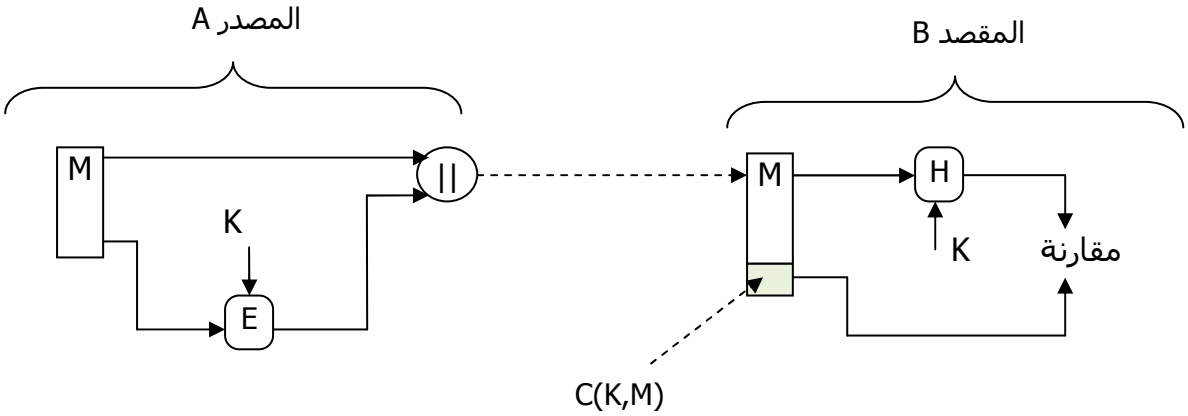
يمكن أن يكون التشفير مقياس لموثوقية الرسالة، وذلك على أساس أن فقط الذين يعرفون المفاتيح الضرورية لديهم شرعية وحق تشفير الرسالة. عند استخدم التشفير المتناظر لابد أن تكون الرسالة منتجة من قبل المرسل، حيث أن المرسل والمستقبل فقط يعرفون المفتاح، وعليه لا يمكن تغيير المحتويات، وقد تستخدم بنية الرسالة والفائض فيها ومجموع الفحص checksum لاكتشاف إي تغيير حدث فيها. في حالة تشفير المفتاح العام لا يعطى التشفير إي تأكيد عن الجهة المرسلة حيث إي شخص (طرف) يكون ملم بالمفتاح العام. لتأكيد مصدر الرسالة قد نستخدم التوقيع الرقمي الذي ينتج بالمفتاح المملوك (الخاص)، حيث يقوم المرسل بتوقيع الرسالة باستخدام مفتاحه الخاص ثم يشفرها بمفتاح المستقبل مما يعطى الرسالة سرية وسلامة. فمن الواضح استخدام هذا الأسلوب ويتطلب عمليتي مفتاح عام على الرسالة في كل طرف.

بصورة عامة إن استخدام التشفير لتحقيق موثوقية الرسالة يتطلب عمليات إضافية مما يمثل عب حسابي إضافي على نظام التشفير ويؤثر على سرعته وأداءه.

8.3: شفرة موثوقية الرسالة

أسلوب أخر لتحقيق موثوقية الرسالة هو استخدام المفتاح السري لتوليد كتلة بيانات صغيرة وحجمها ثابت تلحق بالرسالة وتسمى مجموع فحص التشفير أو شفرة موثوقية الرسالة message authentication code (MAC). يقوم المستقبل ببعض الحسابات على الرسالة وشفرة موثوقية الرسالة للتأكد أن الرسالة لم تتغير ومصدرها المرسل المحدد. هذا الأسلوب يفترض إن الطرفين المشاركين في الاتصال، A و B، يتشاركون في مفتاح سرى عام K. وظيفة وشفرة موثوقية الرسالة شبيهة بوظيفة التشفير، مع الاختلاف أن خوارزمية شفرة موثوقية

الرسالة لا تحتاج أن تكون عكسية، كما هو الحال مع فك التشفير. الشكل 8.1 يوضح تحقيق موثوقية الرسالة باستخدام فقط شفرة موثوقية الرسالة.



الشكل 8.1: موثوقية الرسالة باستخدام شفرة موثوقية الرسالة

يمكن دمج شفرة موثوقية الرسالة مع التشفير بطرق مختلفة لتحقيق السرية والسلامة (التكامل)، في هذه الحالة من المعتاد استخدام مفاتيح منفصلة لكل عملية، ويمكن حساب شفرة موثوقية الرسالة قبل أو بعد التشفير، وان كان من المفضل القيام بذلك قبل التشفير.

شفرة موثوقية الرسالة ليست توقيعاً رقمياً، حيث كل من المرسل والمستقبل يتشاركان المفتاح ويمكنهما إنتاجه.الحاجة لاستخدام شفرة موثوقية الرسالة يمكن تلخيصها في الأتي:

- في بعض الأحيان نحتاج فقط إلى الموثوقية
- في بعض الأحيان نحتاج أن تبقى الموثوقية لفترة أطول من التشفير، لاستخدامات الأرشفة مثلا

كما ذكر أعلاه شفرة موثوقية الرسالة MAC عبارة مجموع فحص للتشفير وتلحق بالرسالة عندما نفترض أو نعلم إنها صحيحة. يمكن توليده بالدالة C على النحو التالي:

$$MAC = C_K(M) \quad \ldots\ldots\ldots \quad 8.1$$

حيث M الطول المتغير للرسالة. هذه الدالة تنقل العديد إلى واحد، حيث من المحتمل كثير من الرسائل الطويلة الاعتباطية يمكن أن توجز إلى نفس قيم الملخص، إيجاد هذا الملخص والذي يصف رسائل مختلفة قد يكون عملية صعبة. المستقبل يتوثق من الرسالة بإعادة حساب شفرة موثوقية الرسالة.

تقيم امن وظيفة شفرة موثوقية الرسالة يتطلب التعرف على الهجمات التي قد تتعرض لها. ولتحقق امن عالي لهذه الخوارزمية يجب استيفاء المطلوبات التالية:

1. أن لا تكمن معرفة الرسالة و شفرة موثوقية الرسالة من إيجاد رسالة أخرى بنفس شفرة موثوقية الرسالة.
2. يجب أن يكون توزيع شفرة موثوقية الرسالة منتظماً.
3. يجب أن تعتمد شفرة موثوقية الرسالة على كل ثنائيات الرسالة بالتساوي.

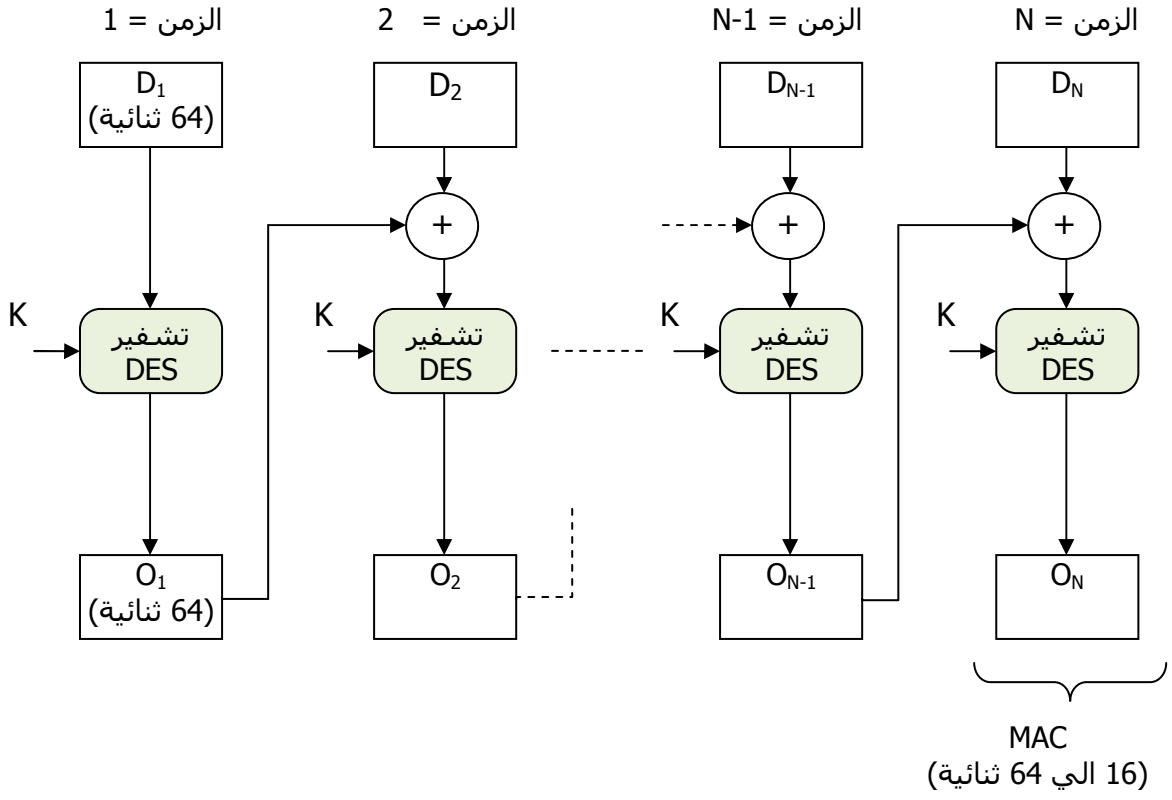
المطلوب الأول أعلاه يتعامل مع هجوم إحلال الرسالة، الذي يتمكن فيه المهاجم من إنشاء رسالة جديدة لملائمة شفرة موثوقية الرسالة الحقيقة دون الحاجة إلى معرفة المفتاح. المطلوب الثاني مهم لمكافحة هجوم البحث الشامل brute-force attack المعتمد على نص صريح مختار. أما المطلوب الأخير مهم للتأكد من أن خوارزمية الموثوقية ليست ضعيفة لأجزاء محددة من الرسالة أو لبعض ثنائياتها.

8.3.1: التشفير المتناظر و شفرة موثوقية الرسالة

يمكن استخدام صيغة ربط الكتل المشفرة Cipher Block Chaining (CBC) لإنتاج موثوقية منفصلة للرسالة وعادة تكون الكتلة الأخيرة، يتم هذا باستخدام خوارزمية موثوقية البيانات Data Authentication Algorithm (DAA)، وأكثر الخوارزميات استخداما هي خوارزمية شفرة موثوقية الرسالة المعتمدة على معيار تشفير البيانات في صيغة ربط الكتل المشفرة DES-CBC والتي توصف كالأتي:

- استخدم قيمة ابتدائية IV=0 وحشوه أصفار في الكتلة الأخيرة
- شفر الرسالة باستخدام معيار تشفير البيانات في صيغة ربط الكتل المشفرة DES-CBC
- أرسل كشفرة موثوقية الرسالة فقط الكتلة الخيرة أو أخر M ثنائية من اليسار في الكتلة الأخيرة (64≥M≥16)، وفى هذه الحالة تكون كشفرة موثوقية الرسالة صغيرة للمطلوبات الأمنية.

الشكل 8.2 يوضح عمل مثال لخوارزمية موثوقية البيانات.



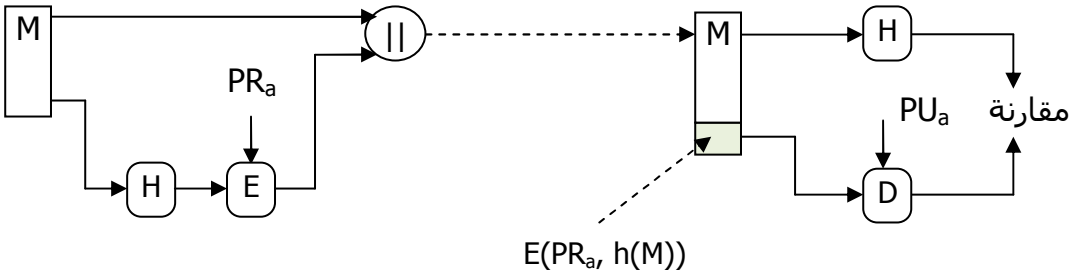
الشكل 8.2: خوارزمية موثوقية البيانات

8.4: دوال الَفْرم (الهش)

الاختلاف في شفرة موثوقية الرسالة يمثل دالة الفرم ذات الاتجاه الواحد. مثلها مثل شفرة موثوقية الرسالة، تتقبل دالة الَفْرم رسالة متغير حجمها (M) كدخل وتنتج خرج حجمه ثابت، يشار إليه باسم شفرة الَفْرم H(M). تختلف شفرة الَفْرم عن شفرة موثوقية الرسالة في عدم استخدامها لمفتاح. توجز شفرة الَفْرم الرسالة إلى h يعطى بالعلاقة التالية:

$$h = H(M) \quad \ldots\ldots 8.2$$

يستخدم الَفْرم لاكتشاف التغييرات في الرسالة، ويمكن استخدامه بطرق مختلفة مع الرسالة، أكثرها استخداما إنتاج توقيع رقمي (الاستخدام الأساسي لدوال الفرم). الشكل 8.3 يوضح استخدام الفرم للتوقيع باستخدام مفتاح المرسل الخاص، مما ينشئ توقيع رقمي.



الشكل 8.3: دوال الفرم والتوقيع الرقمي

الغاية الأساسية من استخدام دوال الفرم هي إنتاج بصمة للملف أو الرسالة أو كتل بيانات أخري. مواصفات دوال الفرم الجيدة تتلخص في الأتي:

- يمكن تطبيقها على أي حجم رسالة M
- تنتج خرج طوله ثابت
- سهولة حساب موجز الرسالة h [h=H(M)] لأي رسالة M
- أن يكون من غير العملي إيجاد x أن عرفت قيمة h، لا يمكن حل المعادلة H(x)=h, بمعنى أخر أن يكون للدوال خاصية الاتجاه الواحد.
- أن يكون من غير العملي إيجاد y أن عرفت قيمة x، لا يمكن حل المعادلة H(y)=H(x)، بمعنى أخر أن يكون للدوال مقاومة قوية للتصادُم.
- أن يكون من غير العملي إيجاد أي x و y ، لا يمكن حل المعادلة H(y)=H(x)، بمعنى أخر أن يكون للدوال مقاومة قوية للتصادُم.

من الضرورة أن نجعل من الصعب جداً إيجاد رسالتين يكون لديهما نفس الفرم، وان لا يكون الفرم مرتبط بالرسالة بأي صورة واضحة، بمعني أخر أن تكون العلاقة علاقة لاخطية ومعقدة. يوجد قليل من التشابه في تقويم دوال الفرم وتشفير الكتلة.

تعمل كل دوال الفرم باستخدام القواعد العامة التالية:

- النظر إلى الدخل (رسالة أو ملف الخ) كسلسلة من كتل حجمها كل منها n ثنائية
- تعالج كتلة في إي وقت بنهج تكراري لإنتاج دالة فرم حجمها n ثنائية
- يمكن إنتاج عدد من دوال الفرم البسيطة فقط بالجمع القسري مع الدوران
- تحتاج إلي نظام تشفير قوى (انظر الوحدة التاسعة)

8.4.1: هجوم تاريخ الميلاد

هجوم تاريخ الميلاد يعتمد على فرضية تاريخ الميلاد والتي تنص علي: في مجموعة من 23 شخص فرصة أن يكون لشخصين نفس تاريخ الميلاد تكون باحتمال يزيد عن 0.5 (Pr>0.5). يتلخص هجوم تاريخ الميلاد في النقاط التالية:

- يولد المهاجم $2^{m/2}$ اختلافاً من رسالة صحيحة وكل هذه الاختلافات لديها نفس المعنى
- يولد المهاجم أيضا $2^{m/2}$ اختلافاً من رسالة الأساسية المطلوبة
- تقارن مجمعتي الرسائل لإيجاد جوز لديهم نفس الفرم (الاحتمال يزيد عن 0.5 بفرضية تاريخ الميلاد)
- يستخدم توقيع المستخدم في الرسالة الصحيحة بإحلاله في الرسالة المزورة ويصبح توقيعها صحيح

لمكافحة هذا الهجوم نحتاج إلى استخدام شفرة موثوقية الرسالة أو دالة فرم كبيرة

8.5: تشفير الكتلة كدوال فرم

توجد العديد من الأساليب المستخدمة للحصول على دوال الفرم التي تعتمد على استخدام تقنية ربط الكتل المشفرة ولكن دون مفتاح سرى (بدلا تستخدم كتل الرسالة كمفاتيح). يمكن وصف هذا الأسلوب على النحو التالي:

- استخدم $H_0=0$ و حشوه أصفار في الكتلة الأخيرة
- احسب: $H_i = E_{Mi} [H_{i-1}]$
- استخدم الكتلة الأخيرة كقيمة فرم

هذا الأسلوب به ثغرات قد تعرضه لهجوم تاريخ الميلاد وهجوم رجل الوسط.

يمكننا تصنيف الهجمات على دوال الفرم وشفرات موثوقية الرسالة إلى فئتان: هجوم البحث الشامل وهجوم تحليل الشفرة. تعتمد قوة دوال الفرم وصدها لهجوم البحث الشامل فقط على طول شفرة الفرم التي تنتج باستخدام الخوارزمية. فتكلفة الفرم للمقاومة الشديدة للتصادم تساوى $2^{m/2}$ (m طول الشفرة) اقل قيمة عملية m=128 وتكون الشفرة غير محصنة بالكامل ويستحسن استخدام m=160. من الصعب قيام بهجوم البحث الشامل على الشفرات يكون أكثر صعوبة حيث انه يحتاج معرفة أجواز من الرسالة وشفرة الموثوقية. ومن المعتاد استخدام شفرة موثوقية رسالة طولها يساوى 128 ثنائية تحقيق مستوى عالي من الأمن.

كما مع خوارزميات التشفير يهدف هجوم تحليل الشفرة على دوام الفرم وشفرة موثوقية الرسالة استغلال بعض خواص الخوارزمية لتحليل التشفير. احد الأساليب لقياس مقاومة خوارزميات الفرم وشفرة موثوقية الرسالة لهجوم لتحليل الشفرة يكون بمقارنة قوتها إلى المجهود المطلوب بهجوم البحث الشامل. وعادة تحتاج خوارزميات الفرم وشفرة موثوقية الرسالة المثالية تحتاج إلى مجهود تحليل شفرة اكبر أو يساوى مجهود البحث الشامل. هجوم تحليل الشفرة يركز على البنية الداخلية لدالة الضغط f ويعتمد على المحاولات لإيجاد أساليب ذات كفاءة لإنتاج التصادم التصادمات لتنفيذ واحد.

ملخص:

درسنا في هذه الوحدة:

- استخدام موثوقية الرسالة
- تشفير الرسالة والموثوقية
- شفرات موثوقية الرسالة
- دوال الفرم
- الأسلوب العام والأمن

اسئلة

1. ألصق مصمم فرم الرسالة لأي رسالة لتصميم أسلوب لحماية الرسالة من التعديل من قبل المتطفلين. لماذا لا يحل هذا الأسلوب مشكلة تعديل الرسالة. ما هي مقترحاتك لحل هذه المشكلة

الوحدة التاسعة: التوقيعات الرقمية وبرتوكولات الموثوقية

أهداف الوحدة
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:

- شرح التوقيع الرقمي وتحديد مطلوباته وخصائصه
- شرح وتحديد خصائص برتوكولات الموثوقية ذات الاتجاه الواجد والمشتركة
- تحديد خصائص معيار وخوارزمية التوقيع الرقمي واستخدامها في بغض التطبيقات

9.1: مقدمة:

تعتبر التوقيعات الرقمية من أكثر التطورات أهمية في مجال امن الشبكات. كما ذكر في الوحدة السابقة إن موثوقية الرسالة تحمى الطرفين المتبادلين للرسالة من إي طرف ثالث، ولكنه لا تحمي هذه الأطراف من بعضها البعض. التوقيع الرقمي متماثل للتوقيع المتعارف عليه باليد، ويوفر مجموعة من المقدرات الأمنية التي يصعب تنفيذها بأي طريقة أخري. يجب أن يكون للتوقيع الرقمي الصفات التالية:

- أن يتحقق من الكاتب وتاريخ وزمن التوقيع
- أن يوثق المحتويات في لحظة التوقيع
- أن يمكنٌ إثباتُهُ (أو التحقّق منه) من قبل طرف ثالث لحل النزاعات

تحتوى وظائف التوقيعات الرقمية على وظائف توثيق.

9.2: التوقيع الرقمي

يوجد العديد من الأساليب والطرق للقيام بإجراءات التوقيع الرقمي والتي يمكن تصنيفها في مجموعتين: التوقيعات الرقمية المباشرة direct والتوقيعات الرقمية التحكّميّة arbitrated. ويمكن تلخيص خواص التوقيع الرقمي في النقاط التالية:

- أن يعتمد التوقيع الرقمي على الرسالة الموقعة
- أن يستخدم معلومات مرسل فريدة لمنع التزوير والإنكار.
- أن يكون إنتاج التوقيع الرقمي وتميزه والتحقق منه سهلاً.
- أن تكون حساباته صعبة للمزور لكل من توقيع الرسائل الجديد و تزوير التوقيع الرقمي في رسالة محددة
- أن يمكن حفظه بأمان

تتطلب التوقيعات الرقمية المباشرة التطبيق المباشر لخوارزميات المفتاح العام بين إطراف الاتصال فقط. ويشارك فيه المرسل والمستقبل، ويفترض أن المستقبل على درية بمفتاح المرسل العام. يمكن إنشاء التوقيع الرقمي بتشفير كل الرسالة باستخدام مفتاح المرسل الخاص، أو تشفير شفرة الفرم أيضا باستخدام مفتاح المرسل الخاص. علاوة على ذلك تتحصل على السرية بتشفير الرسالة كاملة بالإضافة إلى التوقيع باستخدام أسلوب المفتاح العام أو أسلوب المفتاح الخاص. ويفك التشفير باستخدام مفتاح المستقبل العام. من المهم أن نقوم أولا بتوقيع الرسالة، وذلك للسماح، وفي حالة النزاعات، لطرف ثالث بالإطلاع على الرسالة والتوقيع. يعتمد امن أسلوب التوقيع المباشر على امن مفتاح المرسل الخاص، وتصبح هناك مشكلة أن تم فقد هذا المفتاح أو سرقته، حيث يعرض التوقيع للتزوير. وذلك نحتاج إلى أختام (طوابع) زمنية وإلغاء مؤقت للمفتاح.

المشاكل المرتبطة بالتوقيعات الرقمية المباشرة يمكن حلها باستخدام والتوقيعات الرقمية التحكّميّة، وبترتيبات مختلفة. يتطلب هذا الأسلوب وجود حكم (طرف ثالث) تتمثل مهمته في التصديق (يصادق رسميّاً) على الرسالة الموقعة ويؤرخها ثم يرسلها إلى المستلم. يقوم الحكم بدور حساس وحاسم في هذه الطريقة، ويجب أن يكون لدي جميع الأطراف ثقة أن آلية

التحكيم تعمل كما ينبغي. يتحقق التوقيعات الرقمية التحكّميّة باستخدام خوارزميات المفتاح العام ويمكن للحكم الاطلاع أو عدم الاطلاع على محتويات الرسالة.

9.3: برتوكولات الموثوقية

تستخدم برتوكولات الموثوقية لإقناع الأطراف بشخصية كل طرف أخر ولتبادل مفاتيح الجلسات. قد تكون هذه البرتوكولات ذات اتجاه واحد أو مشتركة. هناك موضوعين محورين مرتبطين بتبادل مفاتيح التوثيق وهما:

- السرية، وهى ضرورية لحماية مفاتيح الجلسات. لمكافحة الإنكار، واستنتاج مفاتيح الجلسات من الضروري إرسال معلومات مفتاح الجلسة وتعرفاته بنسق مشفر، مما يتطلب تواجد المفتاح السري أو المفتاح العام مسبقاً.
- وخطوط الزمن وهى ضرورية لمنع هجوم وتهديدات إعادة الإرسال.

كل برتوكولات الموثوقية المستخدمة حالياً تعاني من عدة عيوب وتحتاج إلى تعديلات.

هجمات إعادة الإرسال:

في هجوم إعادة الإرسال Replay Attacks تنسخ رسالة موقعة صحيحة (سارية المفعول) ثم يعاد إرسالها لاحقاً. مما قد يسمح للمهاجم، في الحد الأقصى، باستنتاج مفتاح الجلسة أو انتحال شخصية طرف أخر. أما في الحد الأدنى قد يصيب العمليات بالخلل وذلك بإرسال رسائل إلى إطراف الاتصال تبدو أصلية رغم أنها غير ذلك.

مكافحة هذا التهديد الأمني قد يشتمل على استخدام:

- أعداد متسلسلة sequence numbers، وعادة يكون هذا الأسلوب غير عملي، حيث يجب تذكر العدد الاخير المستخدم في الاتصال مع كل طرف.
- أختام زمنية timestamps، ويحتاج هذا الأسلوب إلى ساعات متزامنة في كل الإطراف المشاركة في الاتصال، مما قد يمثل مشكلة.
- التحدي والاستجابة challenge/response، وهنا يستخدم طابع فريد وعشوائي غير قابل للتنبؤ وذلك للتحدي من قبل المستقبل والاستجابة من ناحية المرسل. هذا الأسلوب غير مناسب التطبيقات غير الموجهة للربط نسبة لمطلوبات المصافحة handshake overhead.

استخدام التشفير المتناظر

كما ذكر سابقا انه يمكن استخدام مستوين هرمين من مفاتيح التشفير المتناظر لتوفير السرية للاتصالات في بيئة موزعة distributed environment. ويتطلب هذا عادة استخدام مركز توزيع مفتاح موثوق فيه. أي طرف في الشبكة يتشارك في مفتاح رئيسي سري مع مركز توزيع المفتاح. يكون المركز مسئولا عن توليد مفاتيح الجلسات وتوزيعها على الأطراف المشاركة في الاتصال وذلك باستخدام المفاتيح الرئيسية لحمايتها.

برتوكول نيدهام وشرويدر

يمثل برتوكول نيدهام وشرويدر Needham-Schroeder Protocol برتوكول تبادل المفتاح الأصلي والأساسي. يستخدم هذا البرتوكول من قبل طرفين يثق كل منهما في وحدة خدمة مفتاح مشترك، حيث تعطى وحدة الخدمة احد الأطراف المعلومات الضرورية لإنشاء مفتاح جلسة مع الطرف الأخر. ويلاحظ هنا، حيث أن وحدة خدمة المفاتيح تختار مفتاح الجلسة، فسيكون بمقدورها قراءة وتزوير أي رسالة بين طرفي الاتصال، مما يتطلب ثقة مطلقة في وحدة خدمات المفاتيح. كل الاتصالات بين الأطراف بعضها البعض ومع مركز توزيع المفتاح تتم بصورة غير مباشرة، فمثلا تمرر الرسالة من مركز توزيع المفتاح عبر الطرف A إلى الطرف B، حيث يتم تشفيرها بمفتاح الطرف B ولا يمكن للطرف A قراءة الرسالة أو تعديلها.

يعمل البرتوكول على النحو التالي:

- من الطرف A إلى مركز توزيع المفتاح: $ID_A \parallel ID_B \parallel N_1$
- من مركز توزيع المفتاح إلى الطرف A: $E_{Ka}[Ks \parallel ID_B \parallel N_1 \parallel E_{Kb}[Ks \| ID_A]\ ]$

- من الطرف A إلى الطرف B: $E_{Kb}[Ks||ID_A]$
- من الطرف B إلى الطرف A:$E_{Ks}[N_2]$
- من الطرف A إلى الطرف B: $E_{Ks}[f(N_2)]$

يعانى هذا البرتوكول من خلل أساسي وهو ضعفه أمام هجمات إعادة الإرسال. يمكن معالجة هذا الخلل باستخدام أختام زمنية أو طوابع إضافية والتي بدورهما لديهما ميزات وقصور. وفى العموم ليست من السهل تصميم برتوكول امن ويحتاج تصمي برتوكول امن إلى كثير من المجهود والتحليل.

استخدام تشفير المفتاح العام

يوجد العديد من الأساليب تعتمد على استخدام تشفير المفتاح العام والتي تفترض أن أي من الطرفين يمتلك المفتاح العام الحالي للطرف الأخر. من المهم التأكد من تواجد المفتاح العام الصحيح لكل الأطراف. النظام المركزي يعرف باسم وحدة خدمة التوثيق Authentication Server (AS). يوجد برتوكولات مختلفة تستخدم الأختام الزمنية أو الطوابع، كما يوجد أيضا خلل في عدد من هذه البرتوكولات.

الخطوات التالية توضح برتوكول ديبين لوحدة خدمة التوثيق Denning AS Protocol والذي يستخدم أختام زمنية

- من A إلى AS: $ID_A || ID_B$
- من AS إلى A: $E_{PRas}[ID_A||PU_a||T] || E_{PRas}[ID_B||PU_b||T]$
- من A إلى B: $E_{PRas}[ID_A||PU_a||T] || E_{PRas}[ID_B||PU_b||T] || E_{PUb}[E_{PRas}[K_s||T]]$

وحدة خدمة التوثيق المركزية يوفر فقط شهادات المفتاح العام، يختار مفتاح الجلسة ويشفر من قبل الطرف A، وعندها لا يحتاج إلى الثقة في AS لحمايته، والأختام الزمنية تمنع هجوم إعادة الإرسال وان كان يحتاج إلى تزامن الساعات.

9.3: موثوقية الاتجاه الواحد

البريد الالكتروني احد التطبيقات التي ينمو فيها استخدام التشفير. طبيعة البريد الالكتروني واحد مكاسبه الكبيرة تتمثل في عدم الحاجة أن يكون المرسل والمستقبل على الخط في نفس الوقت. رسائل البريد الالكتروني ترسل إلى صندوق البريد الالكتروني الخاص بالمستقبل، حيث يتم حفظها حتى يطلع عليها لاحقاً. ظرف (أو ترويسة) رسالة البريد الالكتروني يجب أن يكون واضحاً وغير مشفر حتى يتم التعامل معه باستخدام برتوكول البريد الالكتروني للحفظ والإرسال للأمام store-and-forward e-mail protocol. في كثير من الأحيان قد نحتاج إلى تشفير رسالة البريد الالكتروني وقد نحتاج أيضا إلى موثوقية الرسالة. تكمن المشكلة هنا في أن نظام البريد الالكتروني لا يمتلك مفتاح فك التشفير. للحصول على السرية والموثوقية في نظام البريد الالكتروني يمكن أن نستخدم موثوقية الاتجاه الواحد، والتي توفر تحقق الخصائص التالية:

- لا تحتاج أن يكون المرسل والمستقبل على خط مباشرة في نفس الوقت
- تكون الترويسة غير مشفرة حتى يمكن التعامل معها من قبل نظام البريد الالكتروني
- يمكن حماية محتويات جسم الرسالة والتوثق من المرسل

استخدام التشفير المتناظر مع بعد التعديل للقيام بده الممة. حيث تعتمد استراتيجية مركز توزيع المفتاح على خوارزمية برتوكول نيدهام وشرويدر المذكورة أعلاه والتي تعتبر مناسبة جداً لتشفير البريد الالكتروني. حيث إننا نرغب في تفادى أن يكون المرسل والمستلم في خط مباشرة في نفس اللحظة، يجب علينا إلغاء بعض الخطوات في برتوكول (لا يوجد تبادل نهائي للطوابع) لتتحصل على الخوارزمية التالية للتشفير والتوثيق في اتجاه واحد:

- من الطرف A إلى مركز توزيع المفتاح: $ID_A || ID_B || N_1$
- من مركز توزيع المفتاح إلى الطرف A: $E_{Ka}[Ks || ID_B || N_1 || E_{Kb}[Ks||ID_A]$]

- من الطرف A إلى الطرف B: $E_{Kb}[Ks||ID_A]$

هذا الأسلوب يضمن أن يطلع المستقبل المقصود فقط على الرسالة ، كما انه يحقق الموثوقية عن المراسل A. هذا البرتوكول لا يحمى من تهديدات هجوم إعادة الإرسال، ويمكن مكافحة هذا النوع من الهجمات باستخدام الأختام الزمنية في الرسالة كما ذكر أعلاه. إن استخدام هذا الأسلوب يعرض رسالة البريد الالكتروني للتأخير.

ناقشنا في هذه الوحدة تشفير المفتاح العام والمناسب للبريد الالكتروني، ويشتمل على تشفير صريح ومباشر لكل الرسالة لتحقيق السرية أو الموثوقية أو كلاهما. يتطلب هذا الأسلوب أن يعرف المرسل مفتاح المستقبل العام (لتحقيق السرية) أو أن يعرف المستلم مفتاح المرسل العام (لتحقيق موثوقية الرسالة) أو كل من المرسل والمستلم يعرف مفتاح الآخر العام (لتحقيق كل من السرية والموثوقية). بالإضافة إلى ذلك تطبيق خوارزمية المفتاح مرة واحدة أو مرتين في حالة الرسائل الطويلة.

إذا كانت السرية هي الأهم عندها يمكن تشفير الرسالة باستخدام مفتاح سرى لمرة واحدة والذي يشفر بدوره باستخدام المفتاح العام للطرف الثاني B ، وذلك باستخدام العلاقة التالية:

من A إلى B: $E_{PUb}[Ks] \;||\; E_{Ks}[M]$

للحصول على موثوقية الرسالة والتحقق من مفتاح المرسل العام، يمكن تشفير التوقيع باستخدام مفتاح المستلم العام، ولتأكيد أن مفتاح الطرف A العام مرسل في الشهادة الرقمية، وذلك كالأتي:

من A إلى B: $M \;||\; E_{PRa}[H(M)] \;||\; E_{PRas}[T||ID_A||PU_a]$

للحصول على كل من سرية وموثوقية الرسالة نستخدم الخيارين أعلاه.

9.4: معيار التوقيع الرقمي

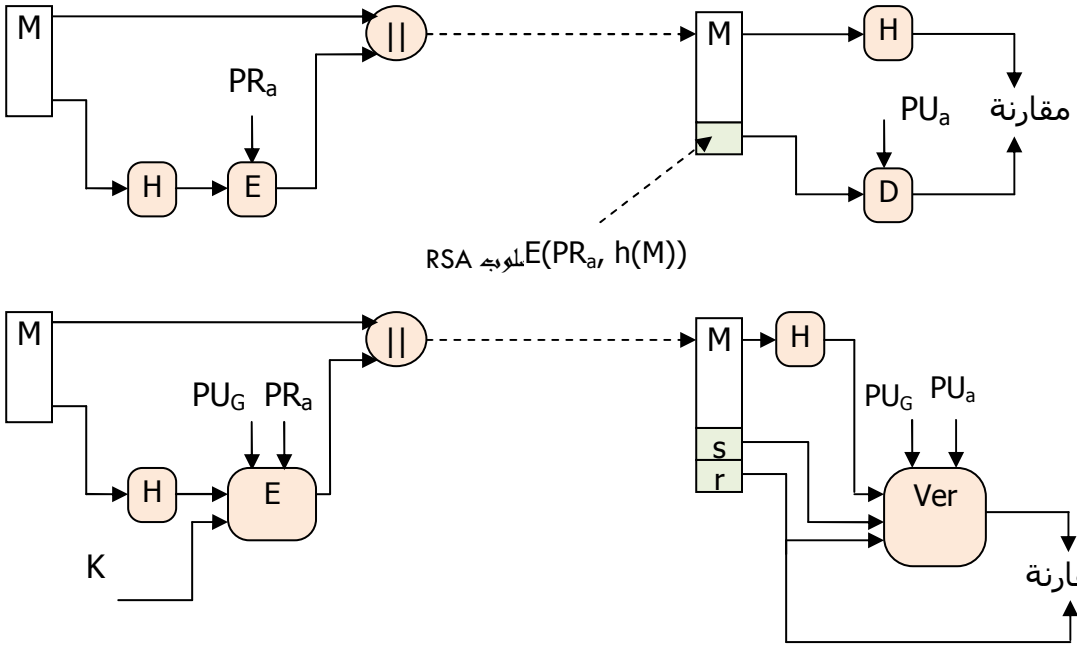
معيار التوقيع الرقمي Digital Signature Standard (DSS) يستخدم خوارزمية فرم أمنة ويقدم أسلوب توقيع رقمي جديد يعرف باسم خوارزمية التوقيع الرقمي Digital Signature Algorithm (DSA). صممت هذه الخوارزمية لتوفير توقيع رقمي قوى دون السماح باستخدام سهل للتشفير. خوارزمية التوقيع الرقمي هو نظام التوقيع الرقمي المعتمد علي نطاق واسع من العالم. اقترحت هذه الخوارزمية أولا في العام 1991 وتمت مراجعتها في العام 1993 كاستجابة للردود الفعل العامة عن امن الخوارزمية. تمت بعض المراجعات الطفيفة للخوارزمية في العام 1996. في العام 2000 تم نشر نسخة ممتدة من المعيار، والذي شمل خوارزميات توقيع رقمي على أساس خوارزمية RSA وعلى تشفير المنحنى الهليلجي.

9.4.1: خوارزمية التوقيع الرقمي

مقارنة مع خوارزمية RSA نجد أن خوارزمية التوقيع الرقمي لديها ميزات، فإنها اصغر من خوارزمية RSA حيث تستخدم توقيع طوله 320 ثنائية (مقابل512-1024 ثنائية تامين في خوارزمية RSA) وأسرع منها. خوارزمية التوقيع الرقمي ليست مثل خوارزمية RSA، حيث لا يمكن استخدامها للتشفير أو تبادل المفاتيح. ومع ذلك فان خوارزمية DSA تعتبر تقنية مفتاح عام. تعتمد خوارزمية DSA على صعوبة حساب اللوغارثمات المنفصلة وتعتمد على نظام اقترح من قبل الجمال في العام 1985 وشنور في العام 1991.

الاختلاف بين خوارزميات DAS و RSA يتمثل توليد توقيع الرسالة والتصديق عليه، كما هو موضح في الشكل 8.1. توقيعات خوارزمية RSA تشفر فرم الرسالة باستخدام مفتاح خاص لإنتاج التوقيع والذي يتحقق منه لاحقا بفك التشفير باستخدام المفتاح العام لمقارنته مع قيمة الفرم

مجددة. أما في خوارزمية التوقيع الرقمي تستخدم فرم الرسالة وقيمة عامة عالمية ومفتاح خاص وعدد عشوائي k لإنتاج توقيع مكون من جزئيين (s,r). يتحقق من التوقيع بحساب دالة فرم الرسالة والمفتاح العام و r و s ثم تقارن النتائج مع r. إثبات هذه الخوارزمية صعب وسوف لا نتعرض له في هذا المقرر.



b: اسلوب DSS

الشكل 8.1: أساليب التوقيع الرقمي

9.4.2: توليد مفتاح خوارزمية التوقيع الرقمي

نموذجيا تستخدم خوارزمية التوقيع الرقمي مجموعة مشتركة من العوامل (p,q,g) لمجموعة من الزبائن (المستخدمين). ثم يختار مفتاح خاص عشوائي × لكل مستخدم لخوارزمية التوقيع الرقمي ويحسب المفاتيح العامة كالآتي:

- اختار q، طوله 160 ثنائية
- اختار عدد أولي كبير p، $p = 2^L$، حيث طول L من 512 إلى 1024 ثنائية وتكون من مضاعفات العدد 64، والعدد Q عامل أولى للعدد (P-1)
- اختار g، $g = h^{(p-1)/q}$ حيث $h^{(p-1)/q} \pmod p > 1$,h<p-1

حساب المفتاح العام y بإعطاء قيمة × نسبيا مباشرة وصريحة حيث انه اللوغريثمات المنفصلة لعدد y على قاعدة g و mod p وعلى النحو التالي:

- اختار $x < q$
- احسب y، $y = g^x \pmod p$

لتوليد التوقيع يحسب المستخدم الكميتان r و s دلالة مكونات المفتاح العام (p,q,g) والمفتاح الخاص (×) وشفرة فرم الرسالة H(M) وعدد صحيح إضافي k والذي يكون عشوائي أو عشوائي وهمي وفريد لكل توقيع، وذلك على النحو التالي:

- ولد مفتاح توقيع عشوائي k، $k < q$ (يكون k عشوائي ويدمر بعد الاستخدام ولا يعاد استخدامه ابداً مرة ثانية)

- احسب جوز التوقيع على النحو التالي:

$$r = (g^k (\text{mod } p))(\text{mod } q)$$
$$s = (k^{-1}.H(M) + x.r)(\text{mod } q)$$

- أرسل التوقيع (s,r) مع الرسالة

يلاحظ هنا إن حساب قيمة r يتطلب فقط الحساب على mod p ولا يعتمد على الرسالة ومما يعنى إن هذه الحساب يمكن أن نقوم به مقدماً، وهذا شبيه للاختيار العشوائي لقيمة k وحساب معكوسه.
يتم التحقق من التوقيع عند المستقبل بعد استلام الرسالة M و التوقيع (s,r) باستخدام المعادلات التالية:

$$w = s^{-1}(\text{mod } q)$$
$$u1 = (H(M).w)(\text{mod } q)$$
$$u2 = (r.w)(\text{mod } q)$$
$$v = (g^{u1}.y^{u2}(\text{mod } p))\ (\text{mod } q)$$

هذه المعادلات يولد العدد v بدلالة مكونات المفتاح العام ومفتاح المرسل العام وفرم رسالة الدخل. إذا كانت قيمة r= v عندها يؤكد التوقيع. يلاحظ هنا صعوبة حسابات اللوغرثمات المنفصلة مما يجعل من الصعب على المهاجم استرجاع قيمة k من قيمة r أو قيمة × من s.

ملخص

ناقشنا في هذه الوحدة:

- التوقيع الرقمي
- برتوكولات الموثوقية ذات الاتجاه الواجد والمشتركة
- معيار وخوارزمية التوقيع الرقمي.

اسئلة

1. أشرح كيف تستخدم خوارزمية RSA في التوقيع.
2. باعتبار التشفير (التعمية)، ما هو الفرق بين موثوقية الرسالة واستخدام التوقيع الرقمي؟ ماهي الخطوات المطلوبة للتحقيق من شفرة موثوقية الرسالة والتوقيع الرقمي؟
3. يعيش كل من مريم ومحمد في بلد يمنع تشفير الرسائل ويسمح فقط بتوقيعها. نسبة لهذا التقيد، الخورازميات التي يمكن استخداما تنحصر في أساليب التوقيع ودوال الفرم (بحيث تفرم الرسالة قبل توقيعها) رغم ذلك يحتاج كل من مريم ومحمد إلي تشفير بعض المعلومات الحساسة والهامة، ولعمل ذلك قررا أن يتقابلا شخصيا أولا لتبادل مفتاح سري وبعدها يستخدما دالة الفرم لتشفير الرسائل مستقبلا. وضح كيف يمكن لمريم ومحمد تشفير الرسائل باستخدام دالة الفرم فقط. يجب أن يقاوم التشفير أي هجوم نشط.

الوحدة العاشرة: تطبيقات الموثوقية

أهداف الوحدة
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:
- شرح نظام وحدة المفاتيح الموثوق فيها كيربيروس ومعرفة خواصه
- شرح موثوقية X.509 والشهادات (التصاديق) وتحديد خواصهما

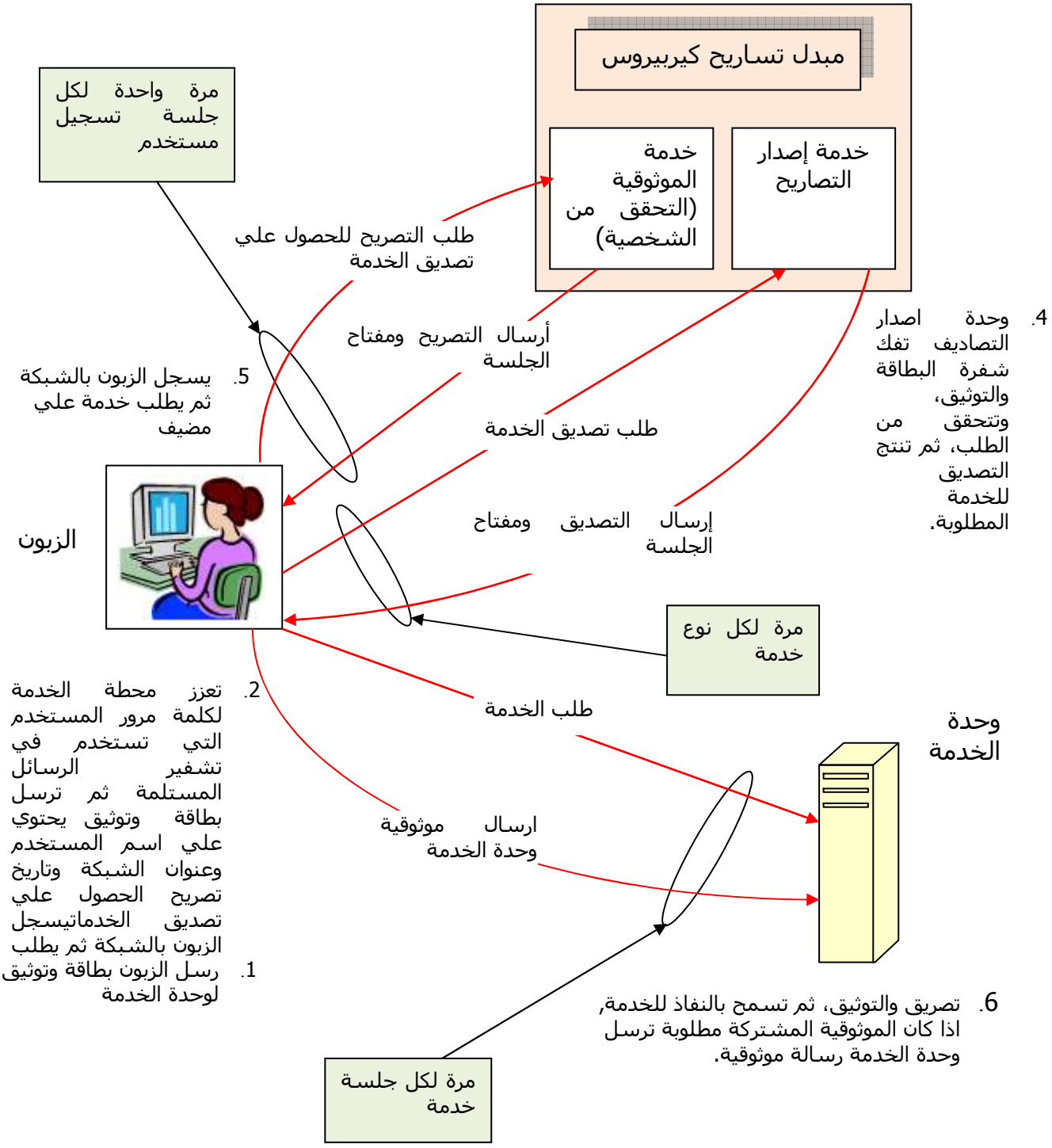
10.1: مقدمة:
في هذه الوحدة سنناقش بعض وظائف الموثوقية التي طورت لدعم موثوفية طبقة التطبيقات (الطبقة رقم 7) والتوقيعات الرقمية. ستدرس أولا احد الخدمات الموثوقية الأولى وأكثرها شيوعا وهى خدمة كيربيروس Kerberos، والذي بصنف كخدمة موثوقية مفتاح خاص. ثم نختبر خدمة دليل الموثوقية X.509 والذى يصنف دليل خدمة موثوقية مفتاح عام.

10.2: كيربيروس
كيربيروس Kerberos خدمة توثيق طورت كجزء من مشروع اثنا Project Athena في معهد مستشبى التقني MIT، ويعتبر احد أحسن نظم توزيع المفتاح عبر طرف ثالث موثوق به وأكثرها أنشارا. يوفر كيربيروس وحدة خدمة موثوقية مركزية مهمتها الأساسية أن توثّق المستخدمين لوحدة الخدمة ووحدة الخدمة إلى المستخدمين. يوفر النظام موثوقية مفتاح خاص مركزية عبر طرف ثالث في الشبكات الموزعة، حيث يسمح لكل المستخدمين بالنفاذ للخدمة الموزعة عبر الشبكة دون الحاجة إلى الثقة في كل محطات العمل (الحواسيب) في الشبكة، مُفضّلاً ذلك على أن تثق جميع محطات العمل في وحدة موثوقية مركزية. وليست مثل نظم الموثوقية الأخرى، يعتمد كيربيروس بصورة شاملة على التشفير المتناظر مستفيدا من تشفير المفتاح العام. توجد نسختين من كيربيروس شائعتا الاستخدام: النسخة رقم 4 (v4) والنسخة رقم 5 (v5). الاسم كيربيروس يرجع إلى كلب لديه ثلاثة رؤوس في الأساطير الإغريقية.

أول تقرير عن كيربيروس نشر في العام 1988 حدد المطلوبات التالية للنظام : أن يكون أمنا ويمكن الاعتماد عليه وان يكون شفافا وواضحا وقابل للتوسع. لدعم هذه المطلوبات صمم كيربيروس كخدمة موثوقية عبر طرف ثالث موثوق فيه، ويستخدم برتوكول يعتمد على مقترح نيدهام وشرويدر والذى ناقشناه في الوحدة السادسة. يعتمد امن البرتوكول بصورة كبيرة على أن يحافظ المشاركين على تزامن زمني مرن وعلى إعطاء فترة صلاحية قصيرة للموثق ويدعى تذكرة كيربيروس.

يتكون برتوكول كيربيروس من ثلاثة عناصر رئيسة وهى: مركز توزيع المفتاح والمستخدم ووحدة الخدمة المنصب فيها الخدمة المطلوب النفاذ إليها. يقوم مركز توزيع المفتاح بمهمتين وهما خدمة الموثوقية وخدمة منح التذاكر. يتطلب البرتوكول ثلاثة تبادلات عندما يريد الزبون النفاذ إلى إمكانيات (خدمات) على وحدة الخدمة وهى انظر الشكل 10.1:
- تبادل خدمة الموثوقية، للحصول على تسريح الحصول على تصديق الخدمات
- تبادل خدمة منح (إصدار) التصديق، للحصول على تصديق الحصول على الخدمات
- نبادل الزبون ووحدة الخدمة، للحصول على الخدمات

4. خدمة الموثوقية تحقق من حق المستخدم فى النفاذ فى قاعدة البيانات، تنتج تصريح لتخويله للحصول على تصاديق الخدمات ومفتاح جلسة. يشفر النتاج باستخدام المفتاح المشتق من كلمة مرور المستخدم؟



الشكل 10.1: التبادل في نظام كيربيروس

10.2.1: النسخة الرابعة:

يتناقش المستخدم ابتداءً مع وحدة خدمة الموثوقية لتحديد أنفسهم،

- بتوفير اسم مستخدم وكلمة مرور حتى يتحقق منه من قبل قسم خدمة الموثوقية في مركز توزيع المفتاح.
- يقوم الزبون بتنفيذ وظيفة ذات اتجاه واحد على كلمة المرور المدخلة لتصبح المفتاح الخاص (السري) للزبون
-

عندما يستوثق من المستخدم بنجاح، يمنح المستخدم الموثوقية أوراق اعتماد صحيحة للمستخدم في الشبكة أو تذكرة تخوله بالحصول على تذاكر صالحة للاستخدام في نطاق الشبكة المحلى (تذكرة الحصول على تذاكر ticket granting ticket TGT). عادة يكون لهذه التذكرة فترة صلاحية محددة وقد تجدد خلال جلسة الاستخدام دون الحاجة إلى إعادة إدخال كلمة المرور. تبادل خدمة الموثوقية قد يوصف بالعلاقات التالية:

- من الزبون لخدمة الموثوقية: $ID_c \,||\, ID_{tgs} \,||TS_1$
- من خدمة الموثوقية إلى الزبون: $E_{Kc}\,[K_{c,tgs}|| \, ID_{tgs} \,||\, TS_2 \,||\, Lifetime_2 \,||\, Ticket_{tgs}]$

وتتلخص خطوات موثوقية الزبون في التالي:

- يرسل الزبون نص واضح (غير مشفر) إلى وحدة خدمة الموثوقية نيابة عن المستخدم لطلب التخويل بالنفاذ إلى الخدمات (التطبيقات) في الشبكة، ولا يرسل مفتاح الزبون الخاص (السري) ولا كلمة مروره
- تفحص وحدة خدمة الموثوقية الطلب للتأكد من أن الزبون متواجد في قاعدة البيانات، فإن وجده يرسل إلى الزبون رسالتين وهما
  - الرسالة A: مفتاح التبادل بين الزبون ووحدة خدمة تسليم (إصدار) التذاكر ويكون مشفرا بمفتاح المستخدم السري
  - الرسالة B: تذكرة الحصول على التذاكر والتي تشتمل على هوية الزبون، وعنوان الزبون على الشبكة وفترة صلاحية التذكرة ومفتاح جلسة الزبون وحدة خدمة إصدار التذاكر مشفرا بمفتاح وحدة إصدار التذاكر الخاص.
- بعد استلام الرسالتين،يفك الزبون شفرة الرسالة الأولي للحصول على مفتاح جلسة بين الزبون ووحدة إصدار التذاكر والذي يستخدم لاحقا للاتصال مع وحدة إصدار التذاكر. ويلاحظ أن الزبون لا يستطيع فك شفرة الرسالة الثانية، حيث إنها مشفرة بمفتاح وحدة إصدار التذاكر. وبهذا يمتلك الزبون المعلومات الكافية للتوثيق لدى وحدة إصدار المفاتيح.

باستخدام وحدة خدمة تسليم (إصدار) التذاكر، يطلب المستخدم النفاذ إلى خدمات أخرى من الوحدة على أساس تذكرة الحصول على تذاكر. تقوم وحدة تسليم التذاكر بالتوثق من تذكرة الحصول التذاكر المقدمة من قبل الزبون باستخدام مفتاحه الوحدة الخاص، إن تم التصديق تنتج تذكرة ومفتاح جلسة بين الزبون ووحدة الخدمة المراد النفاذ إليها. تعرف هذه المعلومات بخدمة التذاكر. تحفظ التذكرة الصادرة مؤقتا علي حاسوب الزبون. هذا التبادل يعبر عنه بالعلاقة التالية:

- من الزبون إلى خدمة إصدار التذاكر: $ID_v \,||Ticket_{tgs} \,||Authenticator_c$
- من خدمة إصدار التذاكر إلى الزبون: $EK_c\,[Kc,¨v|| \, ID_v \,||\, TS_4 \,||\, Ticket_v]$

يمكن تلخيص خطوات في الأتي:

- لطلب الخدمات يرسل الزبون الرسالتان التاليتان إلى وحدة إصدار التذاكر
  - الرسالة الأولى C: وتتكون من تذكرة التخويل للحصول على التذاكر من الرسالة B أعلاه وهوية (تعريف) الخدمة المطلوبة
  - الرسالة الثانية D: الموثق والتي تتكون من هوية (تعريف) الزبون والأختام الزمنية، ومشفرة بمفتاح جلسة الزبون ووحدة خدمة إصدار التذاكر
- عند استلام الرسائل C و D تسترد وحدة خدمة إصدار التذاكر الرسالة B من الرسالة C، حيث يتم فك شفرة الرسالة B باستخدام مفتاح وحدة إصدار المفاتيح السري، ممل

يعطى مفتاح الجلية للزبون ووحدة إصدار التذاكر. باستخدام هذا تفك وحدة إصدار التذاكر شفرة الرسالة D، الموثق. ثم ير سل الرسالتان التاليتان إلى الزبون:

- الرسالة E: تذكرة الزبون إلى وحدة خدمة التطبيقات وتحتوى على تعريف الزبون وعنوان الزبون الشبكي وفترة الصلاحية مفتاح جلسة الزبون ووحدة الخدمة مشفرا باستخدام مفتاح الخدمة الخاص (السري)
- الرسالة F: وتحتوى على مفتاح جلسة الزبون ووحدة الخدمة مشفرة باستخدام مفتاح جلسة الزبون ووحدة خدمة إصدار التذاكر.

عند يستلم الزبون تذكرة الزبون/وحدة الخدمة، يمكنه إنشاء جلسات للاستفادة من خدمات وحدة الخدمة وتبادل المعلومات معه. تشفر وحدة الخدمة المعلومات الواردة بصورة غير مباشرة من خدمة إصدار التذاكر باستخدام مفتاحه الخاص مع مركز توزيع المفاتيح. ثم تستخدم تذكرة الخدمة للتوثق من المستخدم وإنشاء جلسة خدمة بين وحدة الخدمة والزبون. عند انتهاء صلاحية التذكرة لابد من تجديدها للاستمرار في تبادل المعلومات. يمكن التعبير عن هذا التبادل بالعلاقات التالية:

- من الزبون إلى وحدة الخدمة: Ticketv || Authenticatorc
- من وحدة الخدمة إلى الزبون: $EK_{c,v}[TS_5 +1]$

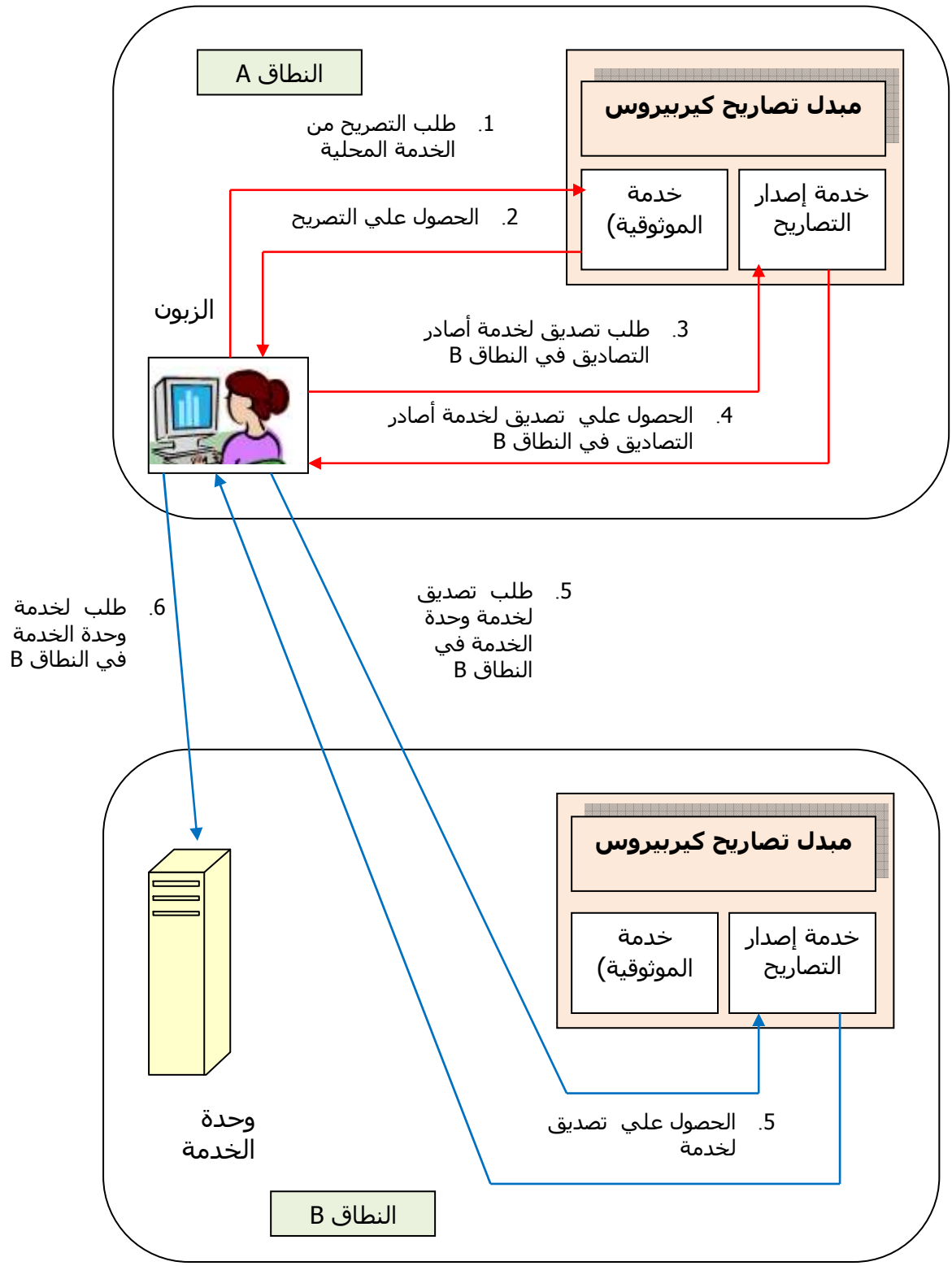
تتلخص خطوات طلب الزبون للخدمة في التالي:

- عند استلام الرسائل E و F من وحدة خدمة إصدار التذاكر، تتوفر معلومات كافية للزبون لتوثيق نفسه عند وحدة خدمة التطبيقات. يربط الزبون بوحدة خدمات التطبيقات (الخدمات) ويرسل الرسائل التالية:
  - الرسالة E من المرحلة السابقة أعلاه، والتي تشتمل على تذكرة الزبون إلى وحدة الخدمة مشفرة باستخدام مفتاح الخدمات السري.
  - الرسالة G: وهى موثق جديد ويحتوى على تعريف الزبون والختام الزمنية ومشفرة باستخدام مفتاح جلسة الزبون ووحدة الخدمة.
- تفك ووحدة خدمات التطبيقات تشفير التذكرة باستخدام مفتاحه السري ثم يرسل الرسالة التالية إلى الزبون للتوثيق (التأكيد) على انه حقيقي وراغب في خدمة الزبون:
  - الرسالة H: وتحتوى على قيمة الأختام الزمنية المتواجدة في رسالة موثوقية الزبون الأخيرة بإضافة واحد كختم زمني جديد، وتشفر هذه الرسالة باستخدام مفتاح جلسة الزبون ووحدة الخدمة.
- يفك الزبون تشفير رسالة التوثيق (التأكيد) باستخدام مفتاح جلسة الزبون ووحدة الخدمة ويتأكد من الأختام الزمنية، فان كانت مجددة بصورة صحيحة يثق عندها الزبون في وحدة الخدمة ويمكنه عند إذن إصدار الطلبات إلى وحدة الخدمة
- تقدم ووحدة الخدمة الخدمة المطلوبة للزبون

10.2.2: بيئة كيربيروس

بيئة خدمات كيربيروس الكاملة تتكون من وحدات خدمة كيربيروس وعدد من الزبائن وعدد من وحدات خدمة التطبيقات، ويشار إلى هذه البيئة باسم عالم كيربيروس. عالم كيربيروس مجموعة من نقاط الشبكة المدارة وتتشارك في نفس قاعدة بيانات كيربيروس وتكون جزء من النطاق الإداري. وفى حالة تواجد عدد من عوالم كيربيروس يجب أن تتشارك وحدات قواعد بيانات كيربيروس في هذه العوالم في نفس المفاتيح وان تثق في بعضها البعض.

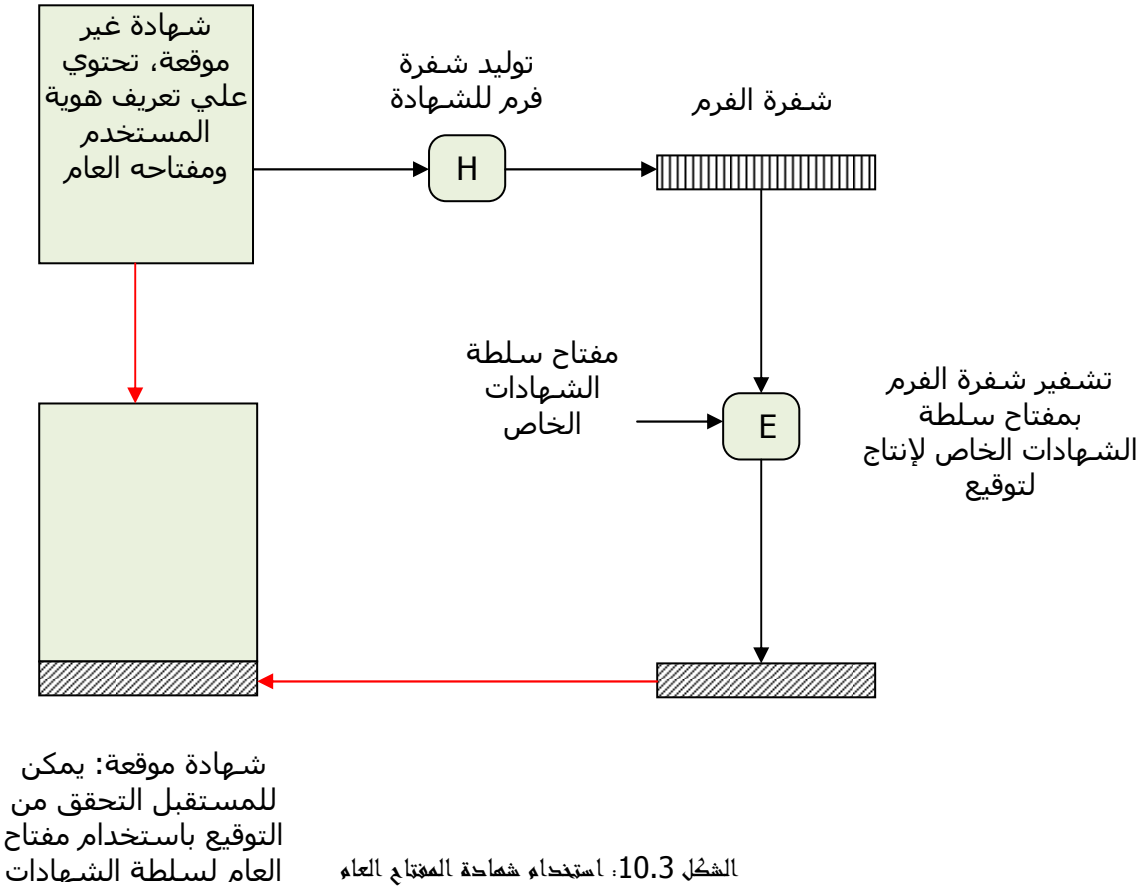
الشكل 10.2 يوضح رسائل الموثوقية عندما تتطلب الخدمة من نطاق أخر. التذكرة المقدمة إلى وحدة الخدمة البعيدة تحتوي العالم الأصلي للمستخدم. يختار وحدة الخدمة أن كان سيقبل الطلب عن بعد. احد قصور هذا الأسلوب انه لا يمكن تمديده بصورة جيدة إلى كثير من العوالم حيث أي عالمين يحتاجان إلى المشاركة في مفتاح.



الشكل 10.2: تبادل رسائل الموثوقية بين نطاقين

10.3: خدمة موثوقية X.509

خدمة X.509 جزء من سلسلة توصيات X.500 CCITT والتي تعرف معايير دليل خدمة. وتتكون من مجموعة وحدات الخدمة أو مجموعة وحدات الخدمة موزعة تحتفظ بقواعد بيانات تحتوى على معلومات عن المستخدمين. التوصية X.509 تحدد الأطر لتوفير خدمة الموثوقية عبر دليل X.500 للمستخدمين. قد يخدم الدليل كمستودع لشهادات المفتاح العام مع توقيع مفتاح المستخدم العام من قبل سلطة اصدار الشهادات، الشكل 10.3. بالإضافة يعرف X.509 برتوكول موثوقية بديل يعتمد على استخدام شهادات المفتاح العام. وتعتمد أيضا على تشفير المفتاح العام والتوقيع الرقمي. لا تحدد المعايير استخدام خوارزمية محددة ولكن من المفضل استخدام خوارزم RSA.



الشكل 10.3: استخدام شهادة المفتاح العام

10.3.1: شهادات X.509

تمثل شهادات X.509 جوهر المعيار. توجد ثلاثة نسخ من الشهادات مع معلومات أكثر في كل نسخة شهادة تتابعاً. تصدر هذه الشهادات من سلطة إصدار الشهادات الموثوق فيها trusted certification authority (CA) وثم تضع في الدليل من قبل تلك السلطة أو المستخدم. وحدة خدمة الدليل غير مسئولة عن إنتاج المفاتيح العامة آو وظائف إصدار الشهادات، فقط يوفر موضع نفاذ سهل وسلس للمستخدمين للحصول على الشهادات. تحتوى الشهادة على العناصر التالية:

- النسخة (1 أو 2 أو 3)
- الرقم المتسلسل (فريد في سلطة إصدار الشهادات) لتعريف الشهادة
- مصدر X.500: اسم سلطة إصدار الشهادات
- فترة الصلاحية (من تاريخ البداية إلى تاريخ النهاية)
- موضوع X.500: اسم المالك
- معرف المصدر الفريد (فقط في النسخ رقم 2 ورقم 3)
- معرف الموضوع الفريد (فقط في النسخ رقم 2 ورقم 3)
- حقول التمديد (فقط في النسخة رقم 3)

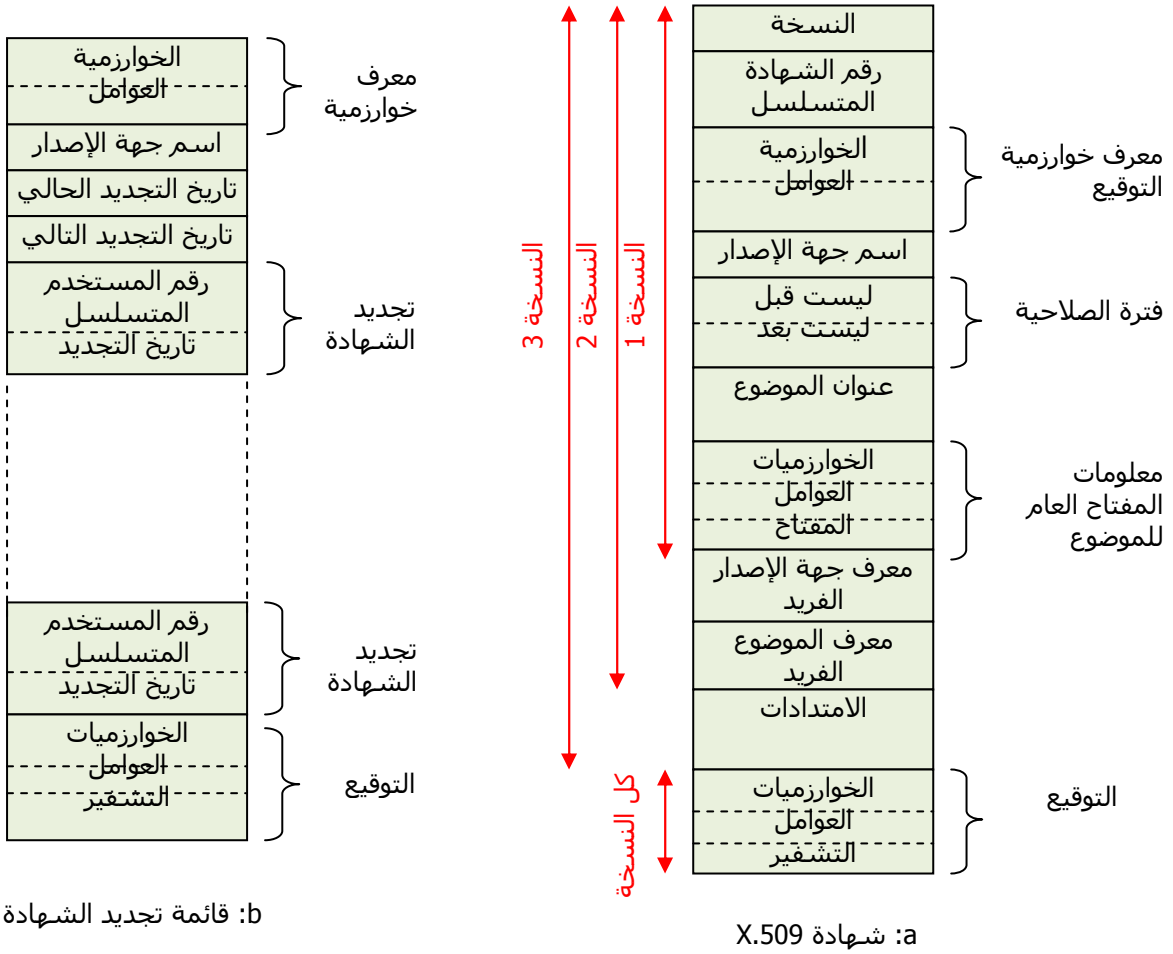
- التوقيع (فرم كل الحقول في الشهادة)

وعادة يستخدم الترميز A>>CA>> للإشارة إلى الشهادة A الموقعة من قبل سلطة إصدار الشهادات CA. الشكل 8.3 يوضح نسق شهادة X.509.

شهادات المستخدمين المولدة من قبل سلطة إصدار الشهادات لديها الخواص أن أي مستخدم لديه نفاذ إلى مفتاح سلطة إصدار الشهادات العام يمكنه التحقق من مفتاح مستخدم عام مصدق علية من قبل السلطة.، ولا يمكن لأي جهة أخرى ما عدا سلطة إصدار الشهادات تغير الشهادة (التصديق) دون أن يكشف. حيث أن الشهادات لا يمكن تزويرها، فيمكن وضعها في الدليل دون أن يقوم الدليل بمجهود إضافي لحمياتها.

10.3.2: هرمية سلطة إصدار الشهادات:

في حالة تشارك أطراف الاتصال نفس سلطة إصدار الشهادات، يعرف جميع الإطراف مفتاح السلطة العام ويمكنه التحقق من صحة شهادة الآخرين مباشرة. أما في حالة إصدار الشهادات من سلطات مختلفة فلا بد من إيجاد طريقة (أو هرمية) ما لإنشاء سلسة تصديقات بين سلطات إصدار الشهادات المختلفة للاستخدام بين الإطراف المختلفة، ويتم ذلك باستخدام شهادات الزبون و والأب (الأصل) client and parent certificates. تستخدم هذه الشهادات لربط الأطراف في السلطات المختلفة للتحقق من صحة التصديقات.
فكل سلطة إصدار لديها شهادات زبائن (للأمام) وشهادات أصل (للخلف). إي زبون يثق في شهادات الأصل.



الشكل 10.3: نسق شهادة X.509 والتجديدات

الشكل 10.4 يوضح استخدام هرمية X.509 للمشاركة في التحقق من شهادات الزبائن. مسلك تسلل الشهادات يكون على النحو التالي:

- يتحصل A على شهادة B باستخدام السلسلة:

X<<W>>W<<V>>V<<Y>>Y<<Z>>Z<<B>>

- يتحصل B على شهادة A باستخدام السلسلة:

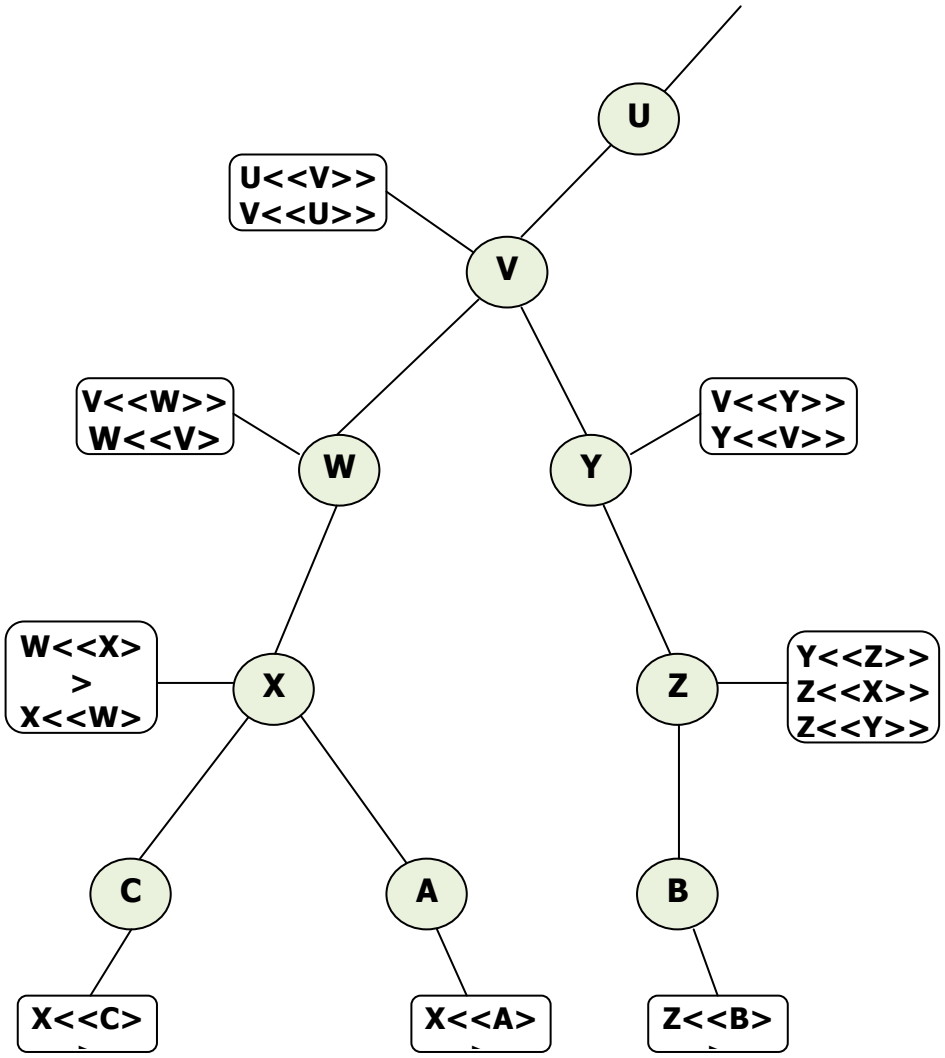
Z<<Y>>Y<<V>>V<<W>>W<<X>>X<<A>>

10.3.3: تجديد الشهادات

أي شهادة تحتوى على فترة صلاحية، فمن الضرورة إنشاء شهادة جديدة بمجرد انتهاء صلاحية الشهادة القديمة. عامة قد يكون من الضرورة تجديد صلاحية الشهادة لأحد أسباب أخري مثل:

- تغيير مفتاح المستخدم الخاص
- توقف التصديق على المستخدم من قبل السلطة
- تغيير شهادة سلطة إصدار الشهادات

تحتفظ سلطة إصدار الشهادات بقائمة الشهادات المجددة Certificate Revocation List (CRL). وعلى المستخدم فحص الشهادات في هذه القائمة.



الشكل 10.4: هرمية X.509 للتحقق من الشهادات

10.3.4: إجراءات الموثوقية

تشتمل التوصية X.509 على ثلاثة بدائل لإجراءات الموثوقية والتي تستخدم في تطبيقات مختلفة للحصول على الشهادات واستخدامها. وتصنف هذه البدائل في الأتي انظر الشكل 10.2:

- موثوقية الاتجاه الواحد، وتستخدم في الرسائل الأحادية الاتجاه مثل البريد الالكتروني
- مووقية الاتجاهين وتستخدم في الجلسات التفاعلية مع استخدام الأختام الزمنية
- موثوقية الاتجاهات الثلاثة وتستخدم في الجلسات التفاعلية من دون الحاجة إلى الأختام الزمنية

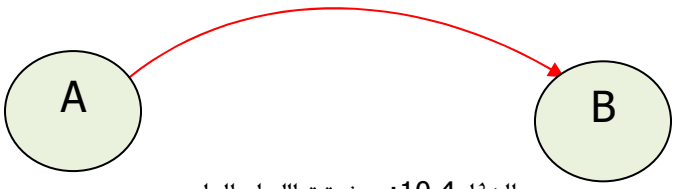
كل هذه البدائل توقيعات المفتاح العام.

تشتمل موثوقية الاتجاه الواحد على نقلة وحيدة للمعلومات من مستخدم (A) إلى أخر (B). تستخدم رسالة واحدة من A الى B لانشاء الأتي:

- هوية المستخدم A والرسالة من A
- مقصد الرسالة المستخدم B
- سلامة (تكاملية) الرسالة وأصالتها

ونلاحظ هنا أن هذا الإجراء يتحقق فقط من هوية المرسل وليست المستقبل. في الحد الأدنى تشتمل الرسالة على ختم التاريخ وطابعة وهوية المستلم وتوقع بواسطة مفتاح الطرف A الخاص. قد تحتوى الرسالة على معلومات إضافية تنقل للمستخدم B مثل مفتاح الجلسة.

1. A{t_A, r_A, ID_B, sgnData, E[PU_b, K_{ab}]}



الشكل 10.4: موثوقية الاتجاه الواحد

تتيح موثوقية الاتجاهين لطرفي الاتصال من التحقق من هوية بعضهما البعض، تستخدم رسالتين من A إلى B شبيهة بالرسالة أعلاه ورسالة أخرى من B إلى A، تنشئ بالإضافة إلى ما قامت به الرسالة الأولى الأتي:

- هوية المستخدم B والجواب من B
- مقصد الجواب المستخدم A
- سلامة (تكاملية) الجواب وأصالته

تشتمل رسالة الجواب على طابعة المستخدم A الأصلية لتصديق الجواب وختم الزمن وطابعة مولدة من قبل المستخدم. ك قد تحتوى على معلومات إضافية مرسلة للمستخدم A.

موثوقية الاتجاهات الثلاثة يشتمل بالإضافة إلى الرسالتين المذكورتان أعلاه إلى رسالة نهائية من المستخدم A إلى المستخدم B تحتوى على نسخة موقعة من الطابعة، مما لا يتطلب فحص الختام الزمنية. ويستخدم هذا الأسلوب في حالة عدم توفر ساعات متزامنة في طرفي الاتصال.

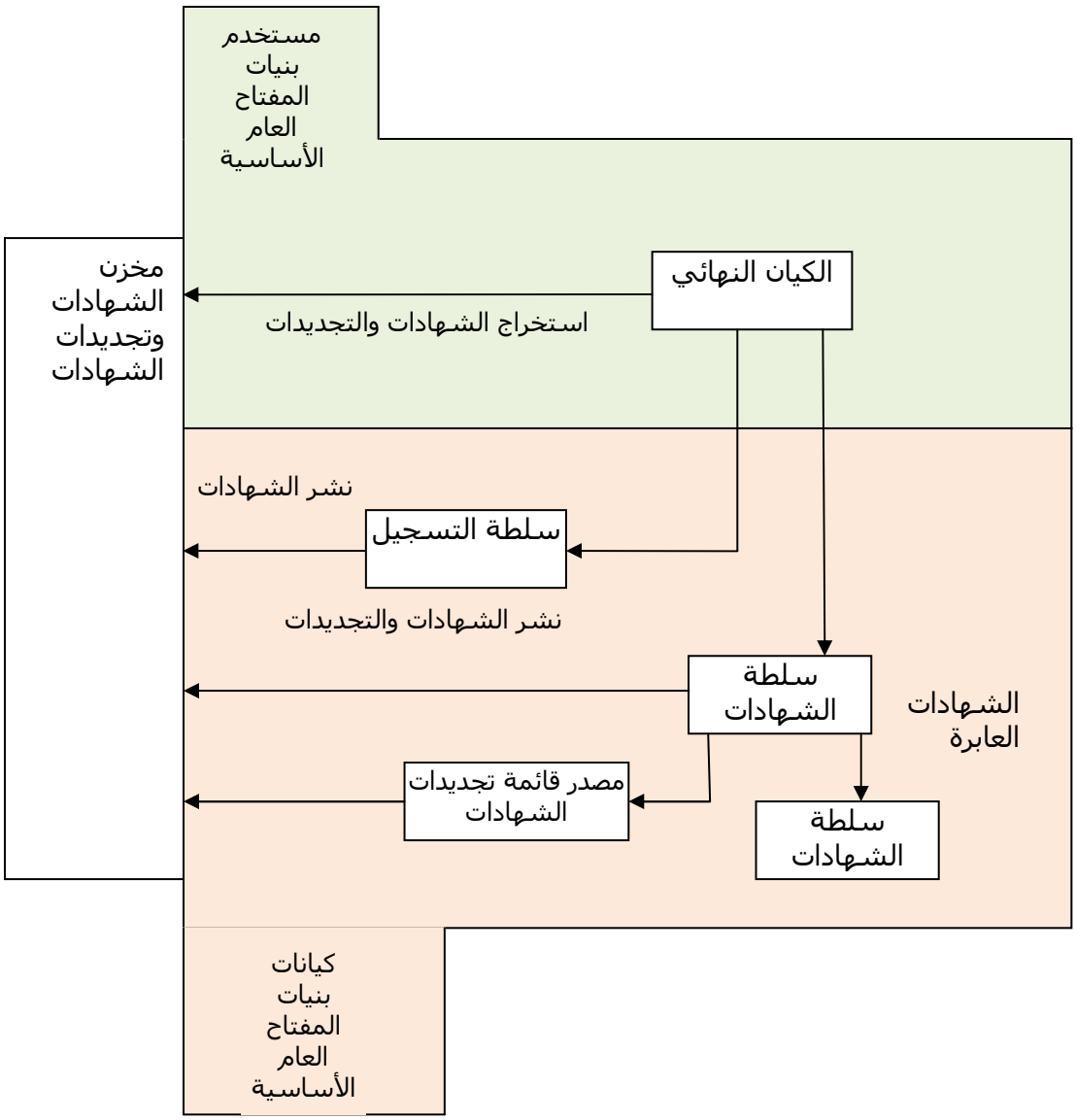
النسخة الثانية من برتوكول X.509 لا يوصل (ينقل) كل المعلومات التي قد يحتاجها بعض التطبيقات الحديثة، مثل البريد الالكتروني على محدد الإمكانات المنتظم وتفاصيل السياسات وتعقيدات الاستخدام والتي تتطلب معلومات إضافية في الشهادة. إضافة حقول إلى النسق الثابت لنقل هذه المعلومات الإضافية أسلوب غير مرن. النسخة الثالثة من برتوكول X.509 شملت على عدد من الامتدادات والتي يمكن أن تضاف إلى نسق النسخة الثانية. أي امتداد يتكون من محدد هوية الامتداد ومؤشر الأهمية وقيمة الامتداد. مؤشر الأهمية يحدد سواء أن كان من الممكن تجاهل الامتداد بأمان ودون التأثير على عمل البرتوكول وصلاحية الشهادة.

امتدادات الشهادة قد تصنف إلى ثلاثة مجموعات:

- المفتاح ومعلومات السياسية، وتنقل معلومات إضافية عن الموضوع مفاتيح المصدَر بالإضافة إلى مؤشرات عن سياسة الشهادة
- الموضوع وخواص مصدَرها، لدعم أسماء بديلة في انساق بديلة لموضوع الشهادة أو مصدرها كما يمكنه نقل معلومات إضافية عن موضوع الشهادة.
- مطلوبات مسار الشهادة، يسمح بمواصفات المطلوبات التي يجب أن تضمن الشهادات الصادرة إلى سلطة إصدار الشهادات من قبل سلطات أخرى.

10.3.5: البنيات الأساسية للمفتاح العام

عرفت الوثيقة RFC 2822 (مَسْرَد امن الانترنت) البنيات الأساسية للمفتاح العام كمجموعة من العتاد والبرمجيات والإفراد والسياسات والإجراءات الضرورية لإنتاج وإدارة وتخزين وتوزيع وتجديد الشهادات (التصديقات) الرقمية على أساس التشفير غير المتناظر. وضعت مجموعة عمل البنيات الأساسية للمفتاح العامX.509 (PKIX) Public Key Infrastructure X.509 تحت مظلة IEFT نموذجاً رسمياً (أصليا) على أساس برتوكول X.509، هذا النموذج مناسب لنشر البنيات المعتمدة على الشهادات (التصاديق) في الانترنت, الشكل 10.5 يوضح العلاقات الداخلية بين عناصر نموذج PKIX كما يعطى قائمة بالوظائف الادارية المطلوبة,



الشكل 10.5: البنيات الأساسية للمفتاح العام

ملخص

في هذه الوحدة ناقشنا

- نظام وحدة المفاتيح الموثوق فيها كيربيروس
- موثوقية X.509 والشهادات (التصاديق)

أسئلة

1. في برتوكول كيربيروس، لماذا لا يكون مجال الموثوقية ليس ذات جدوه أمنية عندما نطلب تصريح للوصول إلي الطرف A والمقابل يكون مفيداً عند الدخول login إلي (أو إنشاء اتصال مع) الطرف A.
2. أعطي مخطط لانسياب الرسالة في برتوكول موثوقية كيربيروس عندما ينفذ المستخدم خدمات الشبكة. أفترض إن المستخدم تحصل علي تصريح الحصول التصديق TGT. أكتب المعلومات الأساسية المتبادلة في كل انسياب.

3. في نطاق كيربيروس، افترض انتهاء صلاحية المفتاح السري المخزن في وحدة خدمات الشبكة. أشرح كيف للمخترق ان يتعرف (يختلس) الاتصالات السابقة والمستقبلية إلي وحدة الخدمة هذه بالإطلاع وتسجيل الحركة في الشبكة.
4. في نطاق كيربيروس، افترض انتهاء صلاحية المفتاح السري المخزن في مركز توزيع المفتاح KDC. أشرح كيف للمخترق ان يتعرف (يختلس) الاتصالات السابقة والمستقبلية إلي وحدة الخدمة هذه بالإطلاع وتسجيل الحركة في الشبكة.
5. عندما يتحطم (يتعطل) مركز توزيع المفتاح لا يستطيع كل المستخدمين توثيق أنفسهم لاستخدام خدمات الشبكة. وضح بالتفصيل كيف يمكنك تصميم نطاق كيربيروس ليس لديه نقطة إخفاق واحدة؟ ما هي الآثار الأمنية لتصميمك، وهل هذا التصميم عرضة للتهديدات الامنية؟

الوحدة الحادية عشر: امن الويب

أهداف الوحدة
عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:

- تحديد اهمية امن الويب والتطبيقات المرتبطة ب
- شرح برتوكولات طبقة النقل SSL/TLS وتحديد خواص واستخدام
- شرح برتوكول الدفع الأمن عبر بطاقات الاعتماد وتحديد خواص واستخدام

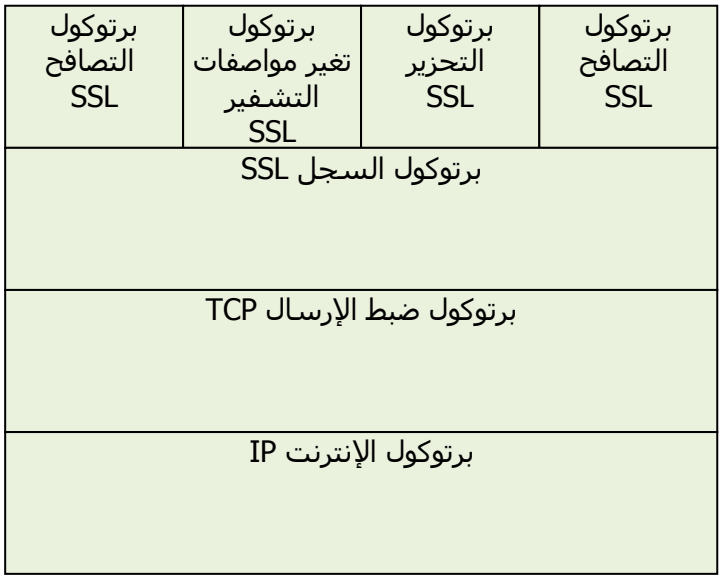
11.1: مقدمة:

تستخدم الشبكة العنكبوتية العالمية (الويب) World Wide Web على نحو واسع في الإعمال والمؤسسات الحكومية وشركات القطاع الخاص. الانترنت والويب بصورة عامة معرضة للهجمات والتهديدات الأمنية مما يعرضها لمخاطر من أنواع مختلفة. قد تصنف التهديدات الأمنية التي قد تتعرض لها الانترنت والويب في المجموعات التالية: السلامة (الاستقامة) والسرية ومنع الخدمة والموثوقية. ناقشنا هذه التهديدات والمخاطر الأمنية بإسهاب في الوحدة الأولي.

11.2: طبقة المَغْرز الأمن

طبقة المَغْرز الأمن SSL (Secure Socket Layer) من أكثر آليات تامين وحماية الويب استخداما. تنفذ هذه الإلية في طبقة النقل، وصممت للاستفادة من برتوكول ضبط الانتقال TCP لتوفير خدمة أمنة ويعتمد عليها من النهاية إلى النهاية. كانت نتاسكيب Netscape أول مطور لهذه الآلية. صممت النسخة الثالثة من هذا الآلية بمراجعة علانية ومشاركة القطاع الصناعي ونشرت على مسودة وثيقة انترنت، ثم طورت مجموعة عمل IETF TLS معيار مشترك لهذه الإلية. آلية SSL ليست برتوكول واحد بل طبقتين من البرتوكولات.

الشكل 11.1 يوضح بنية برتوكولات SSL. برتوكول تسجيل SSL يوفر خدمات الأمن الأساسية لبرتوكولات الطبقات العليا المختلفة. بالتحديد برتوكول نقل النص المتشعب Hypertext Transfer Protocol (HTTP) والذي يوفر خدمة النقل لتفاعل الزبون ووحدة الخدمة في الويب، ويمكن أن يعمل أعلى SSL. ثلاثة من برتوكولات الطبقات الأعلى والتي يمكن أيضا أن تعرف كجزء من SSL: برتوكول التصافح Handshake Protocol و وبرتوكول تغير مواصفات التشفير Change Cipher Spec Protocol وبرتوكول الاحتراس من الخطر Alert Protocol. هذه البرتوكولات المحددة إلى SSL تستخدم في إدارة تبادلات آلية SSL.



الشكل 11.1: بنية برتوكولات SSL

أكثر عنصران مهمان في آلية SSL هما توصيل SSL وجلسة SSL. توصيل عبارة عن نقل شبكي يوفر نوع مناسب من الخدمة، مثل شفافية الربط وعلاقة النِّدَ إلى النِّد ، ويرتبط بجلسة واحدة. أما جلسة آلية SSL هي المشاركة بين الزبون ووحدة الخدمة وتنتجها برتوكول المصافحة. تعرف الجلسات مجموعة عوامل تامين التشفير، والتي قد يشترك فيها روابط متعددة. تستخدم الجلسات للحد التفاوض المكلف لتحديد عوامل التأمين لكل توصيل جديد.

11.2.1: برتوكولاتSSL

يعرف برتوكول تسجيل SSL خدمات لتوصيلات SSL، هذه الخدمات تشتمل على:

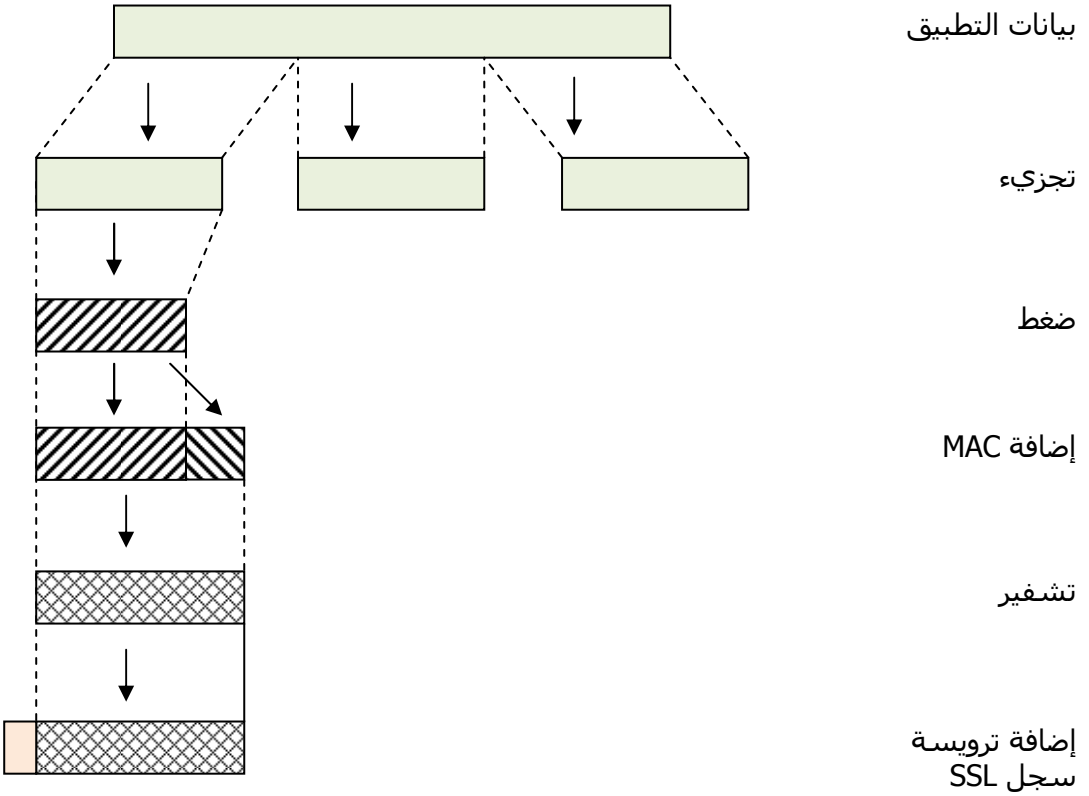
- سلامة الرسالة، يعرف أيضا برتوكول المصافحة مفتاح سري مشترك يستخدم لإنشاء شفرة موثوقية الرسالة MAC الشبيه بشفرة الفرم HMAC مع اختلاف الحشو.
- السرية، يعرف أيضا برتوكول المصافحة مفتاح سري مشترك يستخدم لتشفير جزء البيانات في حزم SSL، مجال واسع من نظم التشفير المتناظر قد تستخدم. الرسالة تضغط قبل أن تسلسل بشفرة موثوقية الرسالة وتشفر.

الشكل 11.2 يوضح العمليات الكاملة لبرتوكول تسجيل SSL. في جهة المرسل نقوم بالعمليات التالية:

- يستلم برتوكول التسجيل رسالة التطبيق المراد إرسالها من تطبيقات الطبقة العليا
- يتم تجزئة البيانات إلى كتل يسهل إدارتها،
- يمكن ضغط البيانات (اختياريا).
- تضاف شفرة موثوقية الرسالة ثم نشفرها
- تضاف ترويسة برتوكول التسجيل،
- ترسل وحدة بيانات البرتوكول المتحصل عليها في مقطع برتوكول TCP.

أما في جهة المستقبل فنقوم بالعمليات التالية:

- تفك شفرة البيانات المستلمة،
- يتحقق من صحتها
- نمدد الرسالة)فك الضغط)
- إعادة تجميع الرسالة
- تسليم الرسالة لتطبيقات الطبقات العليا



الشكل 11.2: العمليات الكاملة لبرتوكول تسجيل SSL

برتوكول تغيير مواصفات التشفير احد برتوكولات SSL المتخصصة والتي تستخدم برتوكول تسجيل SSL. برتوكول تغيير مواصفات بسيط ويستخدم رسالة واحدة. مهمته نقل الحالة المنتظرة لتصبح الحالة الراهنة، حيث يحدث مجموعة التشفير لاستخدامها في توصيل SSL.

يستخدم برتوكول الاحتراس من الخطر لنقل التحذيرات المرتبة بآليةSSL لكيانات النِّدَ. مثل التطبيقات الأخرى التي تستخدم SSL, رسالة التحذير تضغط وتشفر وتحدد بالحالة الراهنة. أي رسالة في هذا البرتوكول تتكون من ثمانيتان. تأخذ الثمانية الأولى القيمة 1 (تحذير) أو القيمة 2 (مُهْلِك) وذلك لنقل الخطورة. الثمانية الثانية تحتوى على شفرة تشير إلى تحذير محدد.

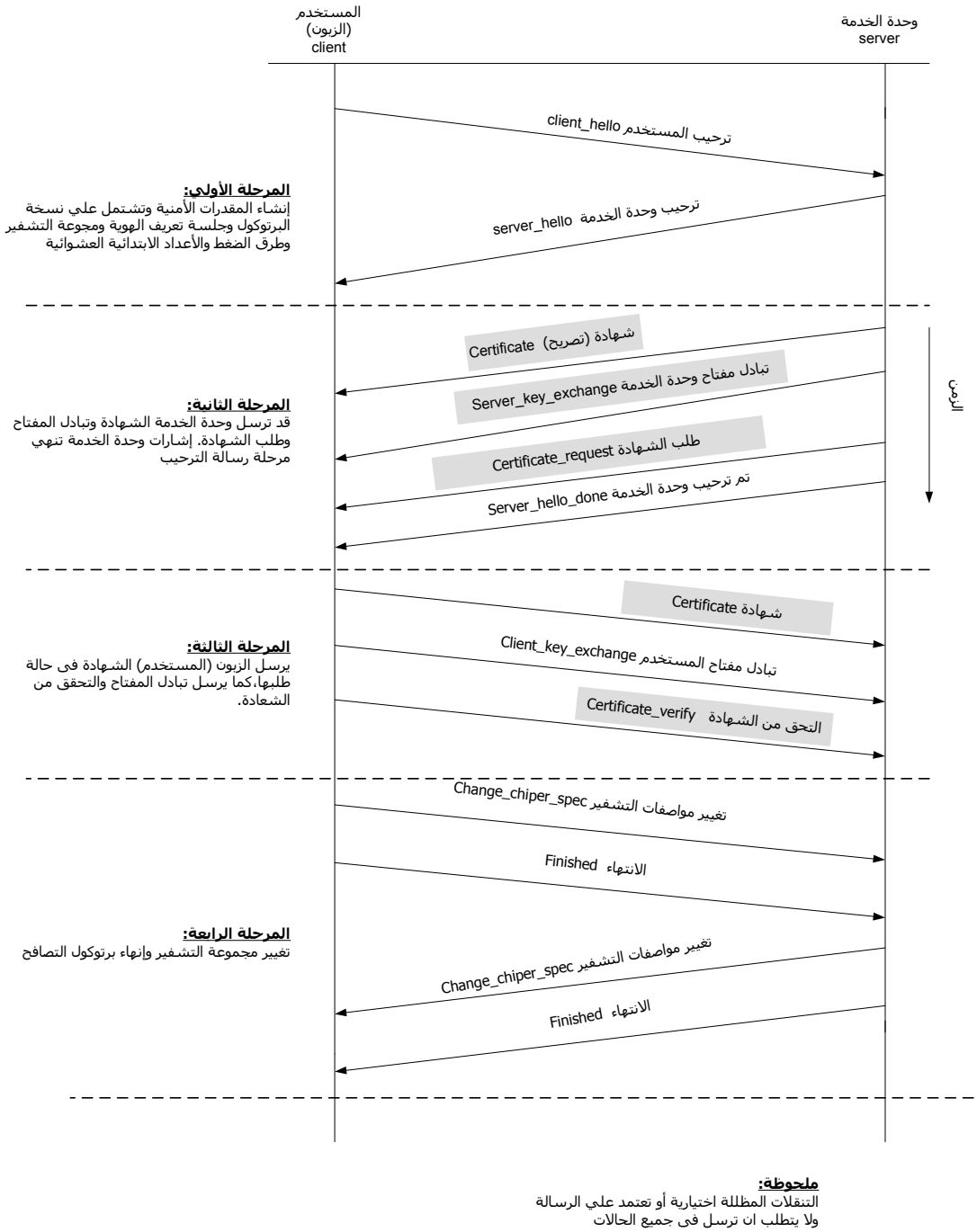
يعتبر برتوكول المصافحة من أكثر الأجزاء تعقيداً في آلية SSL. يسمح هذا البرتوكول بالوظائف التالية:

- موثوفية الزبون ووحدة الخدمة في بعضهما البعض
- التفاوض على التشفير وخوارزمية شفرة موثوقية الرسالة
- التفاوض على مفتاح التشفير الذي سوف يستخدم لحماية البيانات المرسلة في سجل آلية SSL.

يشتمل برتوكول المصافحة على سلسلة من الرسائل المتبادلة بين الزبون ووحدة الخدمة والتي يمكن النظر إليها في مراحل كالآتي الشكل 11.3:

- المرحلة الأولي: إنشاء المقدرات الأمنية. وتستخدم هذه المرحلة من قبل الزبون لبدء التوصيل المنطقي وإنشاء المقدرات الأمنية المرتبطة بهذا التوصيل.
- المرحلة الثانية: موثوقية وحدة الخدمة وتبادل المفتاح. يبدأ هذه المرحلة وحدة الخدمة بإرسال شهادته للتوثيق، في حالة الحاجة إليها

- المرحلة الثالثة: موثوقية الزبون وتبادل المفتاح. ع الزبون أن يتحقق بان وحدة الخدمة وفرت شهادة صالحة وتفحص إن عوامل بدء الاتصال بوحدة الخدمة server_hello parameters لقبولها.
- المرحلة الرابعة: النهاية. هذه المرحلة تتم ضبط التوصيل الآمن. يرسل الزبون رسالة تغير مواصفات التشفير وينسخ مواصفات التشفير المنتظرة إلى مواصفات التشفير الراهنة.



الشكل 11.3: رسائل برتوكول المصافحة

11.3: امن طبقة النقل

امن طبقة النقل (Transport Layer Security) TLS احد معايير IETF ويهدف ان تحدد معاير الانترنت لاستخدام آلية SSL. امن طبقة النقل شبيهاً لحد بعيد بالنسخة الثالثة من SSL، وغن كان هناك عدد من الاختلافات الطفيفة بينهما يمكن تلخيصها في الآتي:

- استخدام نسق تسجيل رقم النسخة مختلف.
- استخدام خوارزمية HMAC لموثوقية الرسالة.
- استخدام عملية عشوائية وهمية لتمديد الأسرار.
- استخدام المزيد من شفرات التحذير
- بعض التغييرات في التشفير الداعم للبرتوكول
- تغيير في نوع الشهادة والتفاوض
- تغيير في حسابات التشفير والحشو.

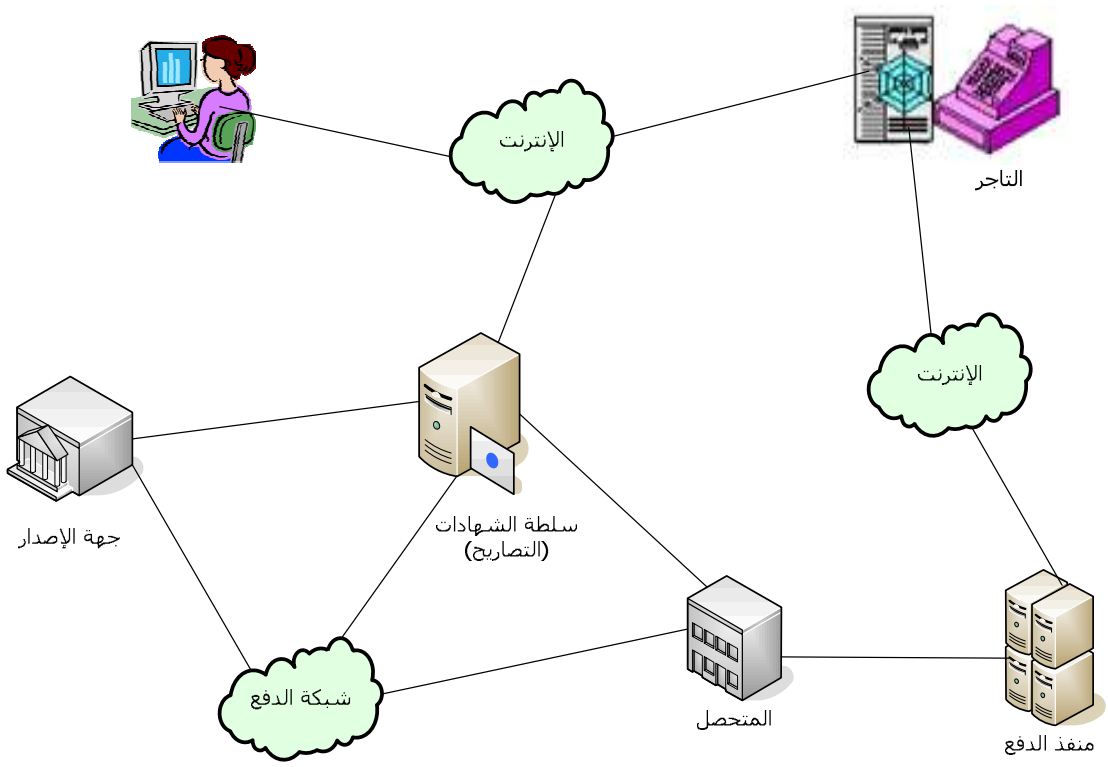
11.4: المعاملات الالكترونية الآمنة:

المعاملات الالكترونية الآمنة Secure Electronic Transactions (SET) نظام تشفير مفتوح ومواصفات أمنية صممت لحماية معاملات بطاقات الاعتماد على الانترنت. منذ العام 1996 تعرضت النسخة الأولى من نظام المعاملات الالكترونية الآمنة للعديد من الاختبارات حتى العام 1998 حين تم طرح أول منتجات مسايرة لنظام المعاملات الالكترونية الآمنة المقترح. المعاملات الالكترونية الآمنة في حد ذاته ليست نظام دفع، بالأحرى هو مجموعة من البرتوكولات الأمنية والأنساق (الهيئات) تمكن المستخدمين من توظيف البنيات الأساسية المتوفرة ألان للدفع عبر بطاقات الاعتماد واستخدامها في الشبكات المفتوحة (الانترنت)، بصورة أمنة وذلك بتوفير التالي:

- قناة اتصال أمنة بين كل الأطراف المشاركة في المعاملة
- الثقة من خلال استخدام الشهادات الرقمية التي توفرها النسخة الثالثة من X.509
- توفير الخصوصية بحيث تكون المعلومات متوفرة فقط للأطراف المشاركة في المعاملة وفى المكان والزمان المناسب.

الشكل 11.4 يوضح المشاركين في نظام المعاملات الالكترونية الآمنة، والذي يتكون من الأتي:

- حامل البطاقة: المشترون الذين يتفاعلون مع التجار من حواسيب شخصية عبر الانترنت.
- التاجر: شخص أو مؤسسة تمتلك السلع أو الخدمات المباعة لحامل البطاقة
- المصدر: مؤسسة مالية مثل المصرف والتي توفر حامل البطاقة بطاقة الدفع.
- المحْزر: المؤسسة المالية التي تنشئ حساب مع التاجر وتعالج موثوقية بطاقات الدفع والدفعيات.
- منافذ الدفع: عمليات ينفذها المحْزر أو تصمم من قبل طرف ثالث لمعالجة رسائل دفع التاجر
- سلطة اصدار الشهادات (التصاديق): كيان موثوق به يصدر شهادات (تصاديق) المفتاح العام على X.509v3 لحاملي البطاقات والتجار ومنافذ الدفع.



الشكل 11.4: نظام المعاملات الالكترونية الآمنة

يكون تسلسل المعاملات الالكترونية الآمنة على النحو التالي:

- يفتح الزبون حساب
- يستلم الزبون شهادة (تصديق)
- يكون للتجار شهاداتهم الخاصة
- يقدم الزبون طلب الشراء
- يتحقق من التاجر
- يرسل الطلب والدفع
- يطلب التاجر موثوقية الدفع
- يؤكد التاجر الطلب
- يوفر التاجر السلعة أو الخدمة
- يطلب التاجر الدفع

غاية نظام المعاملات الالكترونية الآمنة المزدوج التوقيع ربط رسالتان مقصود بها مستلمين مختلفين، وهما معلومات الطلب من التاجر order information (OI) ومعلومات الدفع من المصرف payment information (PI). لا يحتاج التاجر معرفة رقم بطاقة اعتماد الزبون، ولكن من الضرورة ربط البندين بصورة تمكن من فض التنازع عند الحاجة. يأخذ الزبون فرم (هاش) رسالة معلومات الدفع ورسالة معلومات الطلب باستخدام الخوارزمية SHA-1 ثم يتم تركيزهم ويأخذ فرم (هاش) الناتج. اخيراً يشفر الزبون الفرم (الهاش) النهائى باستخدام مفتاح توقيعه الخاص مما ينتج توقيع مزدوج. يمكن تلخيص هذا بالاتي:

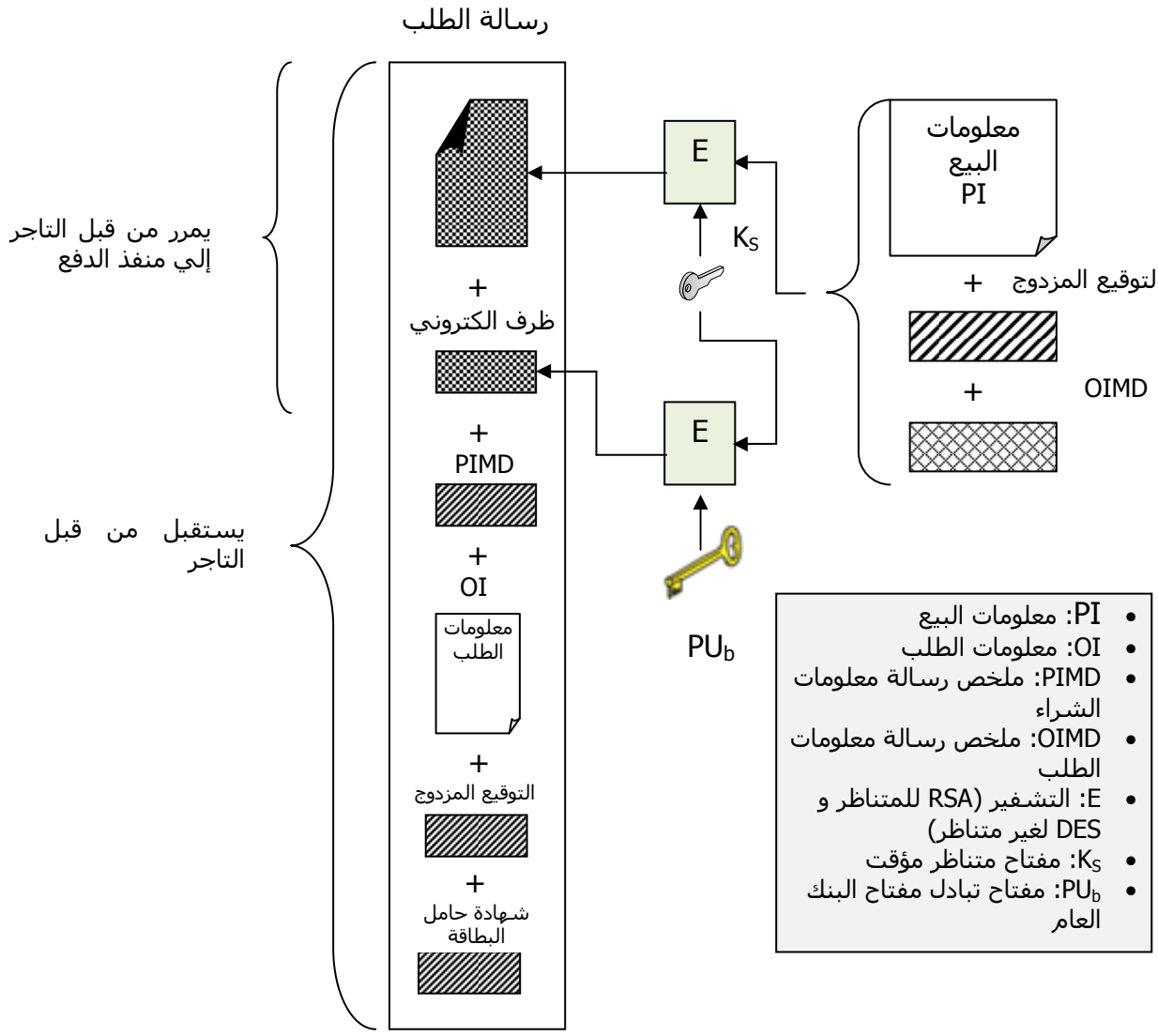
$$DS=E(PRc, [H(H(PI)||H(OI))])$$

تبادل طلب الشراء يتكون من أربعة رسائل وهي:

- الطلب المبدئي: إرسال رسائل المعاملات الالكترونية الآمنة للتاجر يجب أن يتحصل الزبون على نسخة من شهادات التاجر ومنافذ الدفع. رسالة الطلب المبدئي وهو طلب الزبون لهذه الشهادات
- الاستجابة المبدئية: تحتوى على استجابة (جواب) التاجر وتكون موقعة مفتاح توقيعه الخاص. يتحقق الزبون من شهادات التاجر ومنفذ الدفع باستخدام توقيعات سلطة إصدار الشهادات.
- طلب الشراء: يحضر الزبون طلب الشراء والذي تحتوي على رسائل معلومات الطلب والدفع OI and PI.
- استجابة الشراء: تحتوى رسالة استجابة الشراء على كتلة معلومات تقر الطلب ورقم المعاملة المرجعي.

الشكل 11.5 يوضح تفاصيل محتويات رسالة طلب الشراء المولدة من قبل الزبون، وتحتوى الرسالة على الأتي:

- المعلومات المتعلقة بالشراء، والتي يعيد إرسالها التاجر إلى منفذ البيع وتتكون هذه المعلومات من معلومات البيع PI والتوقيع المزدوج وملخص (مصنف) رسالة معلومات الطلب OI message digest (OIMD).
- المعلومات المتعلقة بالطلب والتي يحتاجها التاجر وتحتوى على: معلومات الطلب OI والتوقيع المزدوج و وملخص (مصنف) رسالة معلومات الشراء PI message digest (PIMD).
- شهادة حامل البطاقة وتحتوى على مفتاح التوقيع العام لحامل البطاقة.

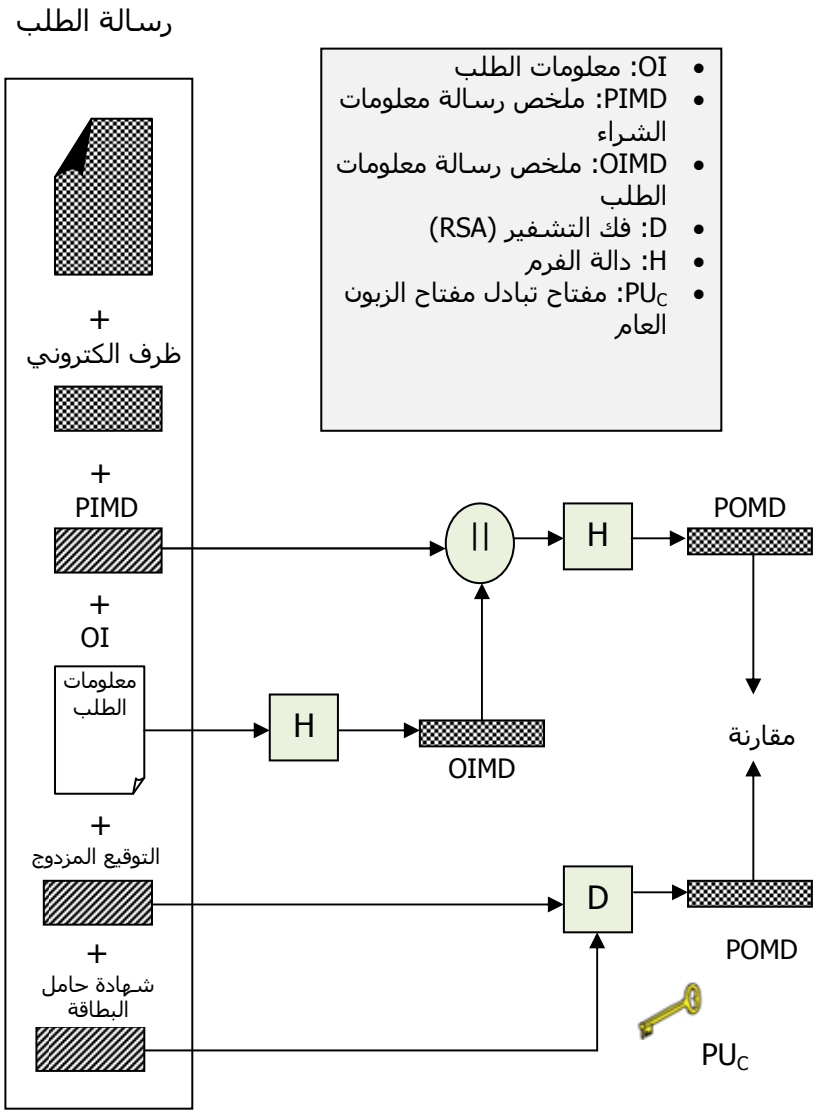


الشكل 11.5 : محتويات رسالة طلب الشراء المولدة من قبل الزبون

عند استلام التاجر رسالة طلب الشراء يقوم بالأنشطة التالية:

- التحقق من شهادة حامل البطاقة باستخدام توقيعات سلطة إصدار الشهادات
- التحقق من التوقيع المزدوج باستخدام مفتاح التوقيع العام والخاص بالزبون لتأكيد الطلب لم يتعرض للتلاعب والتزوير خلال الإرسال وان الطلب موقع باستخدام مفتاح التوقيع الخاص من قبل الزبون.
- معالجة طلب الشراء وإعادة إرسال معلومات الدفع إلى منفذ الدفع للموثوقية.
- يرسل الاستجابة على الطلب إلى حامل الطاقة

الشكل 11.6 يوضح الخطوات التي يقوم بها التاجر للتحقيق من طلب شراء الزبون المذكورة أعلاه.



الشكل 11.6 : التحقيق من طلب شراء الزبون

خلال معالجة طلب الزبون، يوثق التاجر المعاملة مع منفذ الدفع كما ذكر أعلاه. توثيق الدفع يؤكد أن المعاملة مصدقة من قبل مصدر البطاقة، وتضمن أن التاجر سوف يستلم الدفع (السعر)، مما يمكن للتاجر بتقديم السلعة أو الخدمة للزبون. تبادل موثوقية الدفع تحتوى على رسالتان: طلب الموثوقية واستجابة الموثوقية. يقوم منفذ الدفع بالمهام التالية عند استلام رسالة طلب الموثوقية:

- التحقق من الشهادات
- فك تشفير الظرف كتلة الموثوقية الرقمي للحصول على المفتاح المتناظر ثم يفك شفرة كتلة الموثوقية
- يتحقق من توقيع التاجر على كتلة الموثوقية
- يفك شفرة ظرف كتلة الدفع الرقمي للحصول على المفتاح المتناظر ثم يفك شفرة كتلة الدفع
- يتحقق من التوقيع المزدوج في كتلة الدفع
- يتحقق من أن هوية المعاملة المستلمة من التاجر متوافقة مع معلومات الدفع المستلمة بصورة غير مباشرة من الزبون
- يطلب ويستلم التوثيق من مصدر الشهادات

- يرسل استجابة الموثوقية إلى التاجر

للحصول على الدفع (السعر) يرسل التاجر طلب قبض إلى منفذ الدفع والذي يقوم فيه التاجر بتوليد وتوقيع وتشفير كتلة طلب القبض ويحتوى الطلب قيمة وهوية المعاملة. يستلم منفذ الدفع رسالة طلب القبض ثم يقوم بفك شفرتها ويتحقق من كتلة طلب القبض. ثم يفك شفرة أمارة (علامة) كتلة القبض ويتحقق منها. يقوم منفذ الدفع بفحص الاتساق بين طلب القبض وإمارة القبض. ثم ينتج طلب سحب يرسل لمصدر البطاقة على شبكة الدفع الخاصة والتي تجعل المبلغ يتحول لحساب التاجر. يقوم منفذ البيع بعد ذلك بإخطار التاجر بقبض السعر بواسطة رسالة استجابة القبض والتي تحتوى على كتلة استجابة القبض الموقعة مشفراً وموقعاً من قبل منفذ الدفع، بالإضافة إلى شهادة مفتاح التوقيع الخاصة بمنفذ الدفع. يحتفظ برنامج التاجر باستجابة القبض للمراجعة مع المحْزر لاحقاً.

ملخص:

ناقشنا في هذه الوحدة:

- الحاجة إلى امن الويب
- برتوكولات طبقة النقل SSL/TLS
- برتوكول دفع الأمن عبر بطاقات الاعتماد

اسئلة

1. أشرح تصافح SSL الأساسي.
2. عند استخدام المتصفح للربط بوحدة خدمة المصرف باستخدام برتوكول https لماذا لا يحتاج الزبون (المتصفح) باستخدام مفاتيحه (العامة و الخاصة)
3. أفترض شرائك من موقع للتجارة الالكترونية. وافترض بأنك تمتلك حساب علي ذلك الموقع ومعلوماتك الشخصية (*مثل الاسم وعنوان الشحن وعنوان إرسال الفواتير ورقم بطاقة الاتمان واسم المستخدم وكلمة المرور وغيره*) مخزنة في قاعدة بيانات الموقع.

يتم الشراء باختيار التاجر والدخول للموقع باستخدام اسم المستخدم وكلمة المرور ثم اختيار بطاقة الاتمان وثم يتم نقر رابط التسليم "submit". من العادة إن يتم تبادل البيانات بين حاسوبك الشخصي ووحدة خدمة الشركة عبر الانترنت، حيث من العادة تواجد مهاجم منحرف في الانترنت يحاول سرقة رقم بطاقة الاتمان الخاصة بك.

أشرح عدد من التهديدات الأمنية التي يتعرض لها موقع التجارة الالكترونية ومستخدميه في الحالة الموضحة أعلاه. (لا تفترض أن موقع التجارة الالكترونية هذا يستخدم أحسن أساليب وتقنيات الحماية). أذكر أسلوب حماية يمكن استخدامه لكل من التهديدات التي ذكرتها. يمكنك استخدام احد أو اكثر من هذه التعابير في إجابتك: الزبون وحدة الخدمة المتصفح الكعكات الجلسات، مقدم خدمة الانترنت، وعنوان برتوكول الانترنت ، الموجه، المنفذ، الحزمة، ترشيح الحزم، اسم المستخدم، كلمة المرور، قواعد البيانات، التشفير، حجب الخدمة.

الوحدة الثانية عشر: امن برتوكول الانترنت

أهداف الوحدة

عند الانتهاء من دراسة هذه الوحدة سيكون بمقدورك:

- شرح واستخدام اطر امن آلية امن برتوكول الانترنت
- شرح واستخدام برتوكول ترويسة الموثوقية
- شرح واستخدام برتوكول حمولة امن التغليف
- شرح واستخدام برتوكولات إدارة المفتاح المستخدمة في امن برتوكول الانترنت

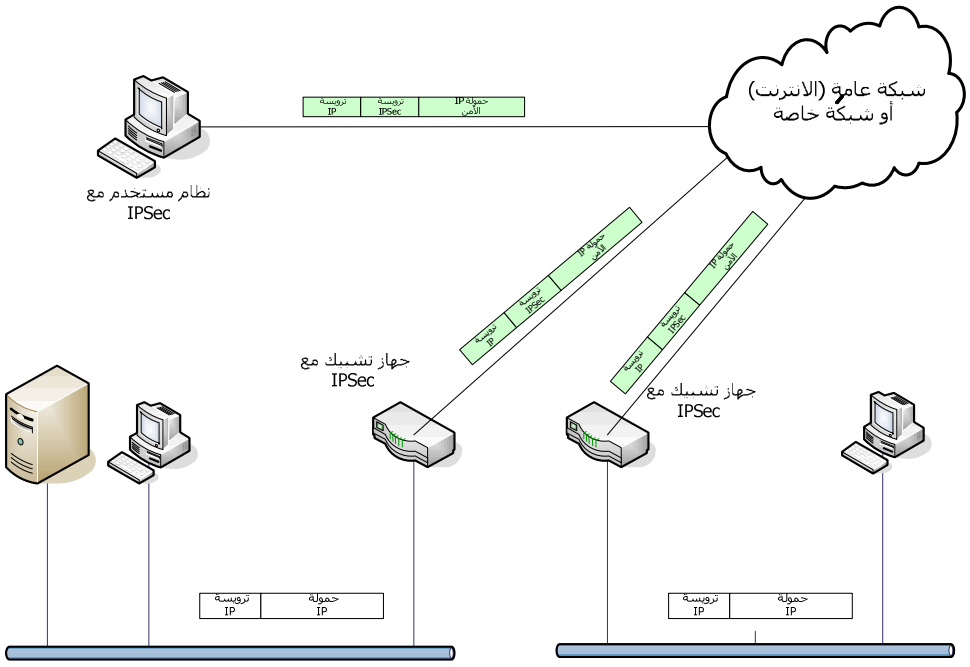
12.1: مقدمة:

درسنا في الوحدة السابقة بعض آليات التامين والتي تعمل على مستوى التطبيقات في نموذج ربط النظم المفتوحة المرجعي لتوفير قناة اتصال أمنة بين أطراف الاتصال. جميع هذه الوسائل وظائفها محدده جدا ، لا تستطيع تشفير إلا ما بنيت لأجله، لذلك كان لا بد من إيجاد طريقة تمكننا من تشفير كل الحزم Packets المرسلة من إي جهاز حتى نتمكن من تامين كل البنيات الأساسية للشبكة من المراقبة الحركة غير المشروعة وضبطها.

12.2: امن برتوكول الانترنت

طورت آلية امن برتوكول الانترنت IP Security (IPSec) وهو أسلوب تامين يعمل في طبقة برتوكول الانترنت في نموذج DOD (أو طبقة الشبكة في نموذج OSI. يدعم امن برتوكول الانترنت كل التطبيقات بمقدرته على تشفير وتوثيق كل الحركة على مستوى برتوكول الانترنت. توفر آلية تامين برتوكول الانترنت اتصالات آمنة عبر شبكات المناطق المحلية LAN وعبر شبكات المناطق الواسعة WAN الخاصة والعامة وعبر الانترنت، كما هو موضح فى الشكل 12.1 ويقدم الخدمات التالية:

- موثوقية المصدر وتشتمل على سلامة وتكامل الرسائل
- السرية وذلك بتشفير الرسائل
- وإدارة المفاتيح (تبادل امن للمفتاح)



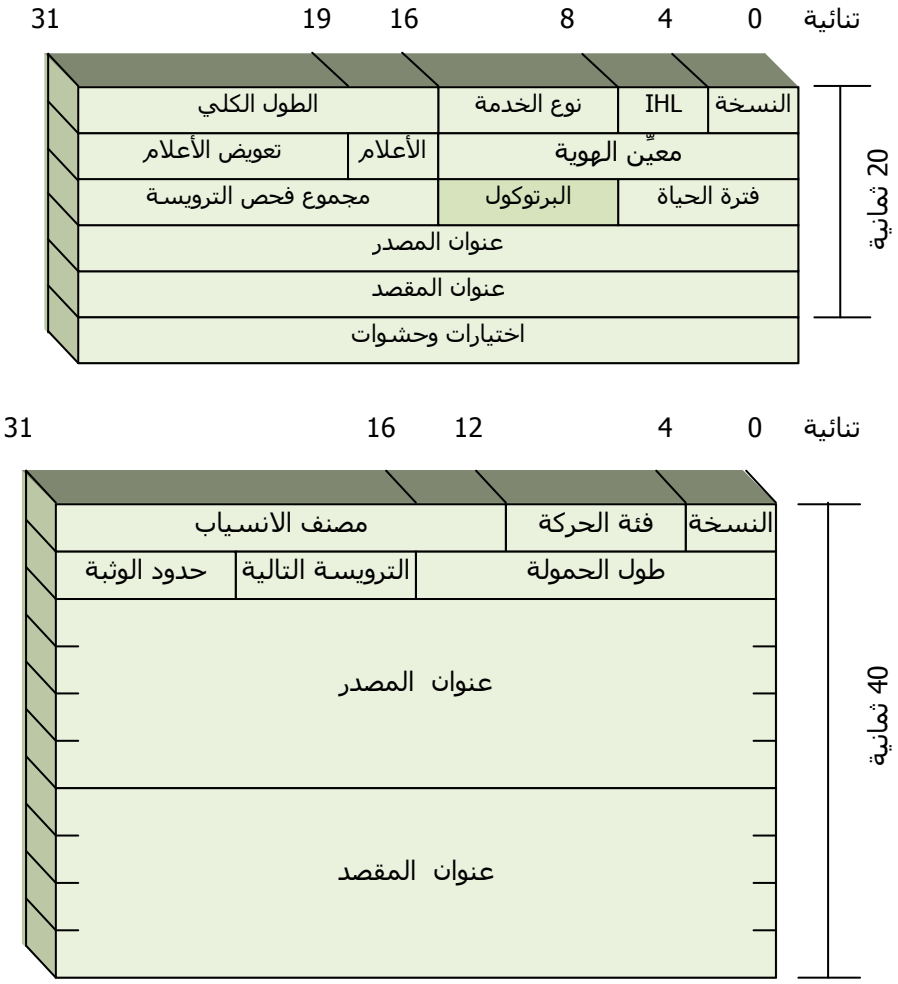
الشكل 12.1: آلية امن برتوكول الانترنت

المكاسب التي قد تتحصل عليها من استخدام امن برتوكول الانترنت يمكن تلخيصها في الأتي:

- يمكن استخدامه في جدار النار Firewall أو الموجه Router، حيث يوفر امن برتوكول الانترنت امن قوى وحماية شاملة لكل الحركة العابرة من والى المؤسسة دون التأثير على الحركة داخل المؤسسة
- استخدام امن برتوكول الانترنت في جدار النار يقاوم الالتفاف، حيث لابد أن تستخدم كل الحركة القادمة من خارج المؤسسة برتوكول الانترنت
- يعمل امن برتوكول الانترنت تحت طبقة الانتقال مما يجعله شفاف بالنسبة للتطبيقات ولا يؤثر على عمل برتوكولاتها أو عمل برمجيات التطبيقات
- امن برتوكول الانترنت شفافاً أيضا للمستخدم الأخير، مما لا يتطلب تدريب المستخدمين على آلية التامين
- عند الحاجة يمكن استخدام امن برتوكول الانترنت لتوفير الأمن والحماية لمجموعة مستخدمين مستقلة، مما يعتبر مفيداً للعاملين خارج الموقع.

12.3: امن برتوكول الانترنت

يوفر برتوكول الانترنت خدمات الربط البيني بين النظم الطرفية عبر شبكات متعددة. حيث يتم تنفيذه في كل نظام طرفي وفى الموجهات. تغليف بيانات الطبقة العليا في المصدر (تضع في كبسولة) في وحدة بيانات البرتوكول protocol data unit (PDU) قبل الإرسال. باستخدام الموجهات تمرر وحدات البيانات عبر الشبكة إلى مقصدها. من الضروري أن تكون الموجهات قادرة على التعامل نع اختلافات الشبكات والتي قد تحدث في نظام العنونة والترقيم وحجم الحزمة والربط البيني والاعتمادية. عمل الموجهات يعتمد على برتوكول الانترنت. الشكل 12.2 يوضح ترويسة برتوكول الانترنت للنسخة IPv4 4 والنسخة IPv6 6. مواصفات امن برتوكول الانترنت معقدة إلى حدٍ كبير. ويوفر آلية امن الانترنت خدمات موثوقية الحزم فقط أو تشفير وموثوقية المشتركة للحزم، وإدارة المفتاح. يعمل امن برتوكول الانترنت مع حزم برتوكول الانترنت النسخة الرابعة والنسخة السادسة. دعم مطلوبات التامين إجباري في النسخة السادسة واختياري في النسخة الرابعة.



الشكل 12.2 يوضح ترويسة برتوكول الانترنت

يوفر امن برتوكول الانترنت خدمات الأمن والحماية بتمكين النظم من اختيار برتوكولات الأمن وتحديد الخوارزميات المستخدمة وضع أي مفتاح ضروري لأي خدمة مطلوبة في مكانه الصحيح. وتشتمل الخدمات على:

- ضبط النفاذ
- تكاملية الربط غير موصل
- موثوقية مصدر البيانات
- رفض إعادة إرسال الحزم (سلامة التسلسل الجزئي)
- السرية (التشفير)
- سرية محدودة لانسياب حركة

تستخدم آلية امن برتوكول الانترنت برتوكولين لتوفير خدمات الآمن: برتوكول الموثوقية (ترويسة الموثوقي (Authentication Header – AH) وبرتوكول التشفير والموثوقية المشترك (حمولة امن التغليف Encapsulation Security Payload - ESP) . الجدول 12.1 يحدد الخدمات التي يدعمها كل من هذه البرتوكولات.

الجدول 12.1: برتوكولات وخدمات آلية امن الانترنت

الخدمة/ البرتوكول	AH	ESP (تشفير فقط)	ESP (تشفير وموثوقية)
ضبط النفاذ	√	√	√
سلامة الربط غير الموصل	√		√
موثوقية مصدر البيانات	√		√
رفض إعادة إرسال الحزم	√	√	√
السرية		√	√
السرية المحدودة لإنسيات الحركة		√	√

تزاملات الآمن security association (SA) علاقة ذات اتجاه واحد بين المرسل والمستقبل ويوفر الآمن لانسياب الحركة، ويستخدم تزامل الآمن برتوكول AH أو برتوكول ESP فقط وليس كلاهما. يحدد تزامل الآمن بالعوامل الثلاثة التالية:

- مؤشر عوامل الآمن Security Parameters Index (SPI)، صف ثنائيات يحمل في ترويسات AH و ESP يمكن المستخدم الأخير من اختيار تزامل الأمن الذي سيستخدم لمعالجة الحزمة المستقبلة.
- عنوان مقصد برتوكول الانترنت IP Destination Address، قد تكون نقطة نهاية تزامل الآمن هي نظام المستخدم الأخير أو نظام الشبكة (جدار النار والموجهات)
- محدد برتوكول الآمن ، يشير إذا كان تزامل الأمن تزامل AH أو تزامل ESP

في حزمة برتوكول الانترنت يحدد تزامل الأمن باستخدام عنوان المقصد في ترويسة برتوكول الانترنت وباستخدام مؤشر عوامل الأمن في ترويسة الامتداد.

12.4: صيغ الاستخدام

كل من برتوكول AH وبرتوكول ESP تدعم صيغتان للاستخدام وهما صبغة النقل Transport mode وضيغة النفق tunnel mode.

توفر صيغة النقل الحماية لبرتوكولات الطبقات العليا وتمتد إلى حمولة payload حزمة برتوكول الانترنت. في النسخة الرابعة من برتوكول الانترنت تعرف الحمولة بكل البيانات التي تتبع ترويسة برتوكول الانترنت. أما في النسخة السادسة من برتوكول الانترنت تعرف الحمولة بكل البيانات التي تتبع ترويسة برتوكول الانترنت وأي ترويسة امتداد وقد تستثنى ترويسة المقصد. تعتمد صيغة النقل على الاتصال من النهاية إلى النهاية في نموذج الزبون ووحدة الخدمة أو الزبون والزبون. برتوكول AH في صيغة النقل يوثق حمولة برتوكول الانترنت وحقول مختارة من الترويسة، أما برتوكول ESP يشفر الحمولة وقد يوثقها اختياريا وليس ترويسة برتوكول الانترنت.

صيغة النفق توفر الحماية لكل حزمة برتوكول الانترنت، ولتحقيق هذا يتعامل مع كل حزمة برتوكول الانترنت بالإضافة إلى حقول الأمن كحمولة لحزمة برتوكول انترنت جديدة (خارجية(لديها ترويسة جديدة. تنتقل كل حزمة برتوكول الانترنت الأصلية عبر نفق من نقطة في الشبكة إلى نقطة أخري. وفي هذه الحالة لا يمكن للموجه اختبار ترويسة برتوكول الانترنت الداخلية. قد يكون للحزمة الخارجية عناوين مصدر ومقصد مختلفين بالكامل عن الحزمة الأساسية. تستخدم هذا الأسلوب عندما يكون نهايات (أطراف) تزامل الأمن منافذ (جدار نار أو موجهات تستخدم امن برتوكول الانترنت). ويمكن للحواسيب ووحدات الخدمة خلف جدار النار تتراسل باتصالات أمنة دون استخدام امن برتوكول الانترنت فيها مباشرة.
الخطوات التالية توضح مثال لعمل صيغة النفق:

- الحاسوب (المضيف) A يولد حزمة برتوكول انترنت لإرسالها إلى الحاسوب B في شبكة أخري

- أولا توجه الحزمة من الحاسوب A إلى جدار النار في حدود شبكة الحاسوب A والذي يرشح كل الحزم الخارجة لأمن برتوكول الانترنت
- إن كانت الحزمة من A إلى B تحتاج امن برتوكول الانترنت، عندها تغلف الحزمة ببترويسة برتوكول انترنت خارجية
- يكون عنوان المصدر في حزمة برتوكول الانترنت الخارجية عنوان جدار النار في حدود شبكة A وعنوان المقصد عنوان جدار النار على حدود شبكة الحاسوب B
- توجه الحزمة الخارجية إلى جدار النار في حدود شبكة B
- الموجهات الوسيطة تختبر فقط ترويسة برتوكول الانترنت الخارجية
- جدار النار في حدود شبكة B ينزع ترويسة برتوكول الانترنت الخارجية وتنقل حزمة الانترنت الداخلية إلى الحاسوب B

الجدول 12.2 يوضح وظائف الصيغ مع البرتوكولات المختلفة.

الجدول 12.2: صيغ استخدام وبرتوكولات امن برتوكول الأمن

	تزامل الأمن صيغة النقل	تزامل الأمن صيغة النفق
AH	يوثق حمولة برتوكول الانترنت وجزء مختار من الترويسة وترويسات امتداد برتوكول الانترنت النسخة السادسة	يوثق كامل حزمة برتوكول الانترنت الداخلية (توريسة الحزمة الداخلية و الحمولة) بالاضافة الى اجزاء مختارة من الترويسة الخارجية و والترويسات امتداد برتوكول الانترنت النسخة السادسة الخارجية
ESP (تشفير فقط)	يشفر حمولة برتوكول الانترنت وأى ترويسة امتداد برتوكول الانترنت النسخة السادسة تتبع ترويسة ESP	يشفر كل حزمة برتوكول الانترنت الداخلية
ESP (تشفير وموثوقية)	يشفر حمولة برتوكول الانترنت وأى ترويسة امتداد برتوكول الانترنت النسخة السادسة تتبع ترويسة ESP. ويوثق حمولة برتوكول الانترنت ولبست الترويسة	يشفر كل حزمة برتوكول الانترنت الداخلية. ويوثق الحزمة الداخلية.

12.5: برتوكول موثوقية الترويسة:

برتوكول موثوقية الترويسة يوفر الدعم لسلامة البيانات وموثوقية حزم برتوكول الانترنت، وذلك على النحو التالي:

- لا ترسل تعديلات الحزم الغير مكتشفة
- النظام النهائي والموجهات يمكن أن تستوثق من المستخدم أو التطبيق وترشح الحركة على أساس ذلك
- تمنع هجوم تزوير العنوان address spoofing attacks

تتحصل على الموثوقية باستخدام شفرة موثوقية الرسالة مما يتطلب مشاركة الأطراف في مفتاح سرى. وعادة تستخدم أسلوب فرم شفرة موثوقية الرسالة HMAC باستخدام الخوارزميات MD5 آو SHA للفرم. تخزن شفرة موثوقية الرسالة في حقل بيانات الموثوقية Authentication Data field في ترويسة الموثوقية، انظر الشكل 12.3.

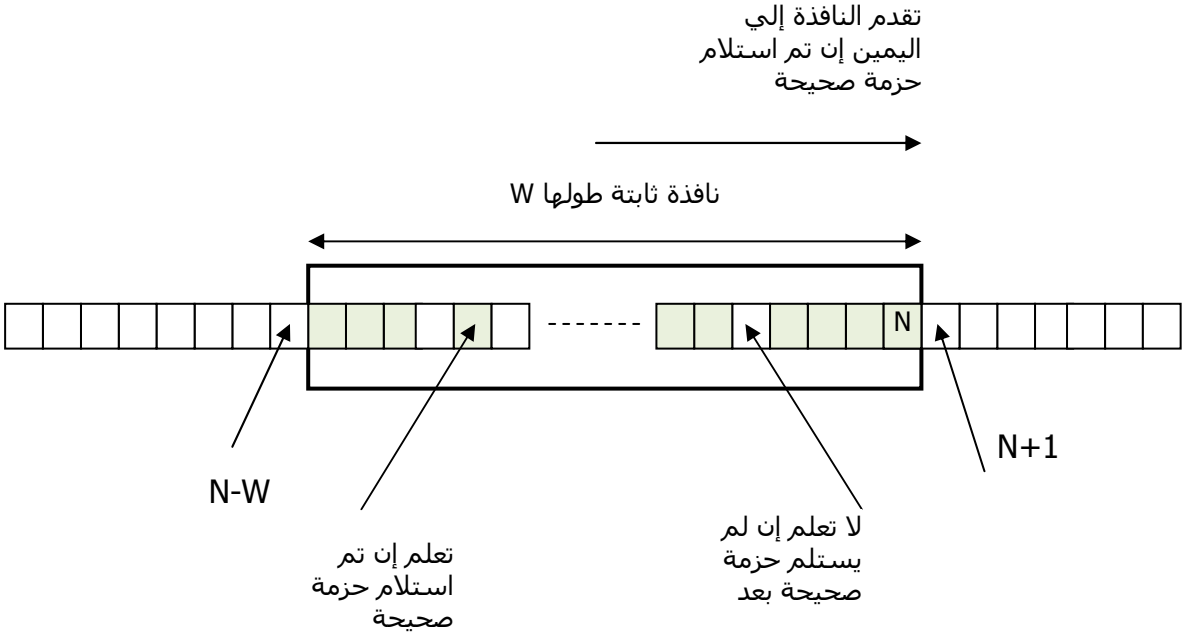
تنائية 0	8	16	31
الترويسة التالية	طول الحمولة	محجوز	
مصنف عوامل التامين (SPI)			
الرقم المتسلسل			
بيانات الموثوقية (متغيرة)			

الشكل 12.3: ترويسة الموثوقية،

12.5.1: خدمة منع إعادة الإرسال

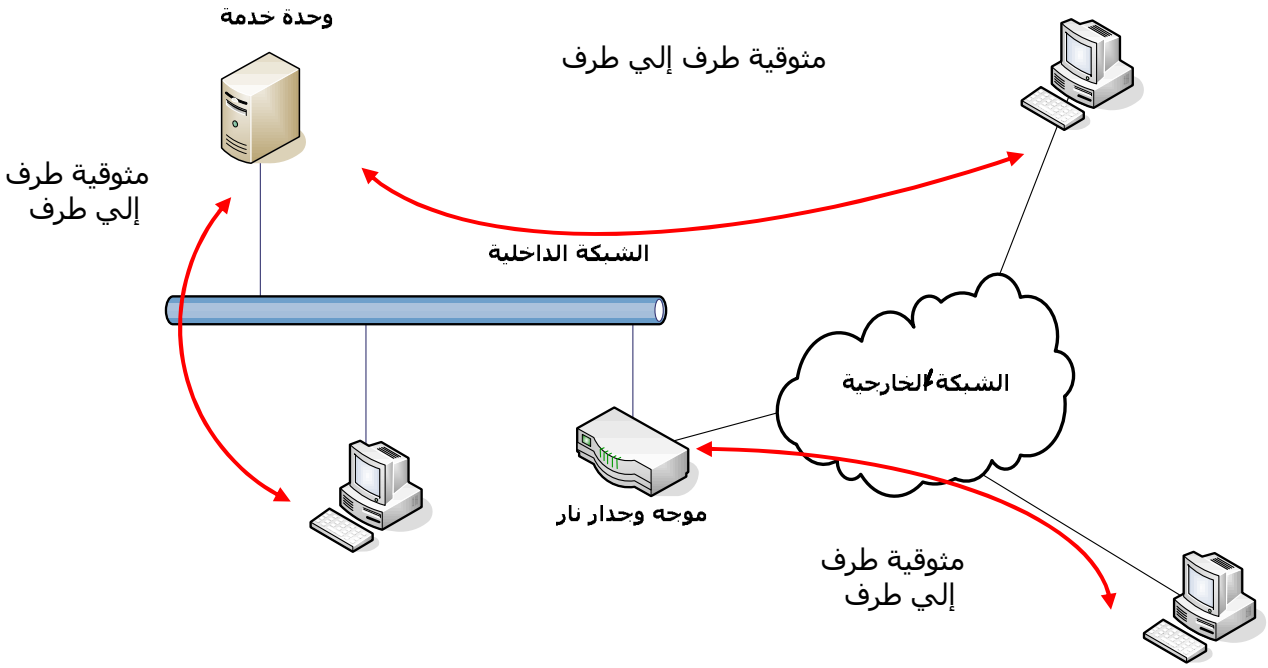
برتوكول موثوقية الترويسة يحمي من هجمات إعادة الإرسال Replay. في هجوم إعادة الإرسال يحتفظ المهاجم بنسخة من حزمة توثيق ويعيد إرسالها لاحقا للمقصد المراد (أو المقصود) حيث يمكن أن يعكر الخدمة أو يتسبب في العديد من المشاكل. صمم حقل رقم التسلسل لاعتراض هجوم إعادة الإرسال، حيث يقوم المرسل بالضبط الأولى لعداد رقم التسلسل إلى القيمة صفر (0)، تزداد قيمة العداد كل مرة بالقيمة 1 كلما تم إرسال حزمة جديدة على تزامل الأمن، عندما نصل إلى الحد 232-1 ينشا تزامل امن جديد بمفتاح جديد. لا يوجد ضمان لاستلام الحزم أو استلامها وفق لترتيب إرسالها. مما يتطلب أن يتعامل امن برتوكول الانترنت مع الحزم المستلمة. تستخدم نافذة حجمها W (القيمة الأساسية تساوى 64)، طرف النافذة الأيمن يمثل أعلى رقم حزمة N استلمت حتى اللحظة. في إي وقت تستلم فيه حزمة تنفذ عملية منع إعادة الإرسال. آلية منع إعادة الإرسال يمكن تلخيصها في النقاط التالية (انظر الشكل 12.4):

- إذا كانت الحزمة المستلمة في نطاق النافذة (رقم التسلسل بين N-W+1 و N) وجديدة، تفحص شفرة موثوقية الرسالة، إذا كانت نتيجة الفحص ايجابية يعلم الشَّقْب المقابل لرقم الحزمة في النافذة
- إذا كانت الحزمة على يمين النافذة وجديدة، تفحص شفرة موثوقية الرسالة، إذا كانت نتيجة الفحص ايجابية تقدم النافذة (تحدث N)
- إذا كانت الحزمة على يسار النافذة أو فشلت الموثوقية يتخلص من الحزمة.



الشكل 12.4: آلية منع إعادة الإرسال

الشكل 12.5 يوضح مقارنة بين عمل صيغة النقل وصيغة النفق عند استخدام برتوكول موثوقية الترويسة. كما يوضح الشكل 12.6 بنية الحزم قبل استخدام برتوكول موثوقية الترويسة للنسخة 4 والنسخة 6 وبعد استخدامه في كل من صيغة النقل وصيغة النفق.



الشكل 12.5 : عمل صيغة النقل وصيغة النفق

IP النسخة 4

ترويسة IP الاصلية	TCP	البيانات

IP النسخة 6

ترويسة IP الاصلية	إمتداد الترويسة	TCP	البيانات

الشكل 12.6: حزمة برتوكول الانترنت قبل استخدام برتوكول موثوقية الترويسة

IP النسخة 4

ترويسة IP الاصلية	AH	TCP	البيانات

IP النسخة 6

ترويسة IP الأصلية	Hop-to-hop, dest, routing, fragment	AH	المقصد	TCP	البيانات

الشكل 12.7: حزمة برتوكول الانترنت بعد استخدام برتوكول موثوقية الترويسة في صيغة النقل

IP النسخة 4

ترويسة IP الجديدة	AH	ترويسة IP الأصلية	TCP	البيانات

IP النسخة 6

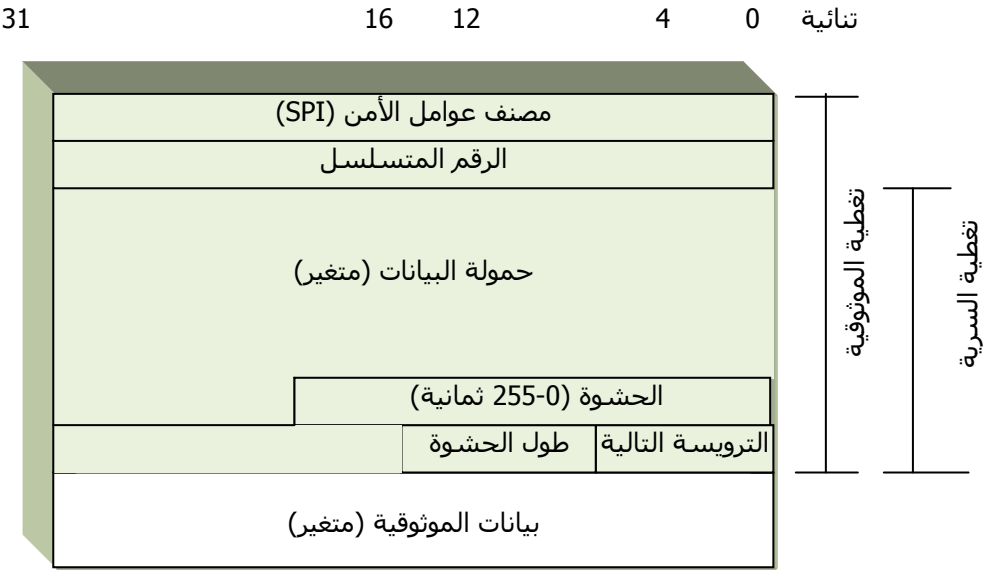
ترويسة IP الجديدة	امتداد الترويسات	AH	ترويسة IP الأصلية	امتداد الترويسات	TCP	البيانات

الشكل 12.8: حزمة برتوكول الانترنت بعد استخدام برتوكول موثوقية الترويسة في صيغة النقل

12.6: حمولة امن التغليف

برتوكول حمولة امن التغليف Encapsulating Security Payload يوفر السرية لمحتويات الرسالة كما يوفر سرية محدودة لانسياب الحركة. كما يمكنه أن يوفر اختيارياً بعض خدمات الموثوقية مثل برتوكول موثوقية الترويسة، وعندها تخزن شفرة موثوقية الرسالة في حقل بيانات الموثوقية Authentication Data field في ترويسة الموثوقية، انظر الشكل والذى يوضح ترويسة البرتوكول12.4. يدعم برتوكول حمولة امن التغليف عدد من نظم التشفير وصيغ الاستخدام والحشو مثل معيار تشفير البيانات ومعيار تشفير البيانات الثلاثى و RC5 و IDEA وغيره. يستخدم حقل الحشو في برتوكول حمولة امن التغليف ترويسة للاتي:

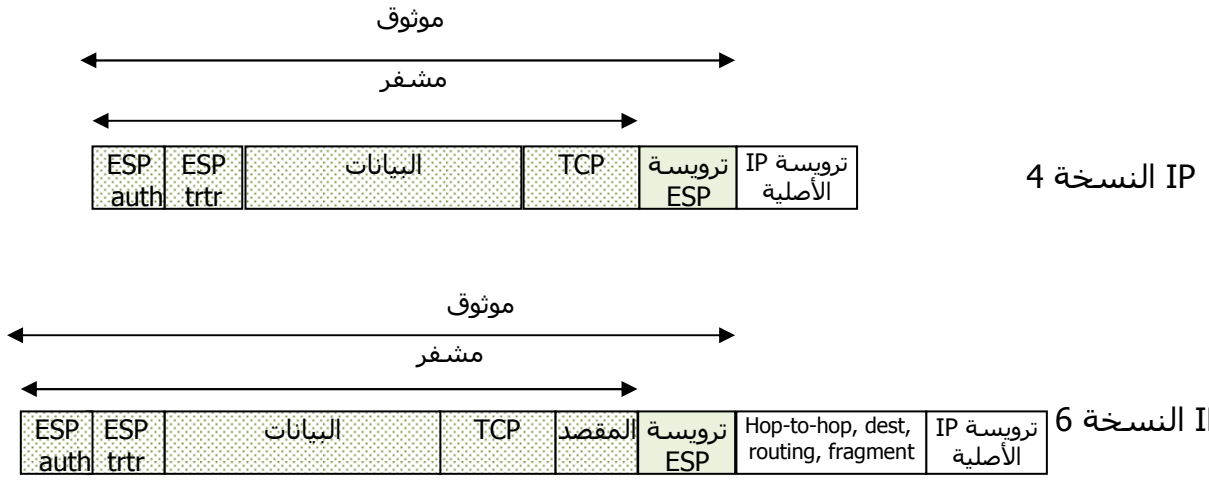
- تمديد النص الصريح للحجم المطلوب للتشفير، للحصول على كتل مكتملة
- تأكيد الاصطفاف (مثلا استخدام كلمة طولها 32 ثنائية لتسريع الحسابات في 32 ثنائية معالج دقيق)
- توفير سرية انسياب الحركة بالتكتم على الطول الحقيقي للحمولة.



الشكل 12.9: ترويسة برتوكول حمولة امن التغليف

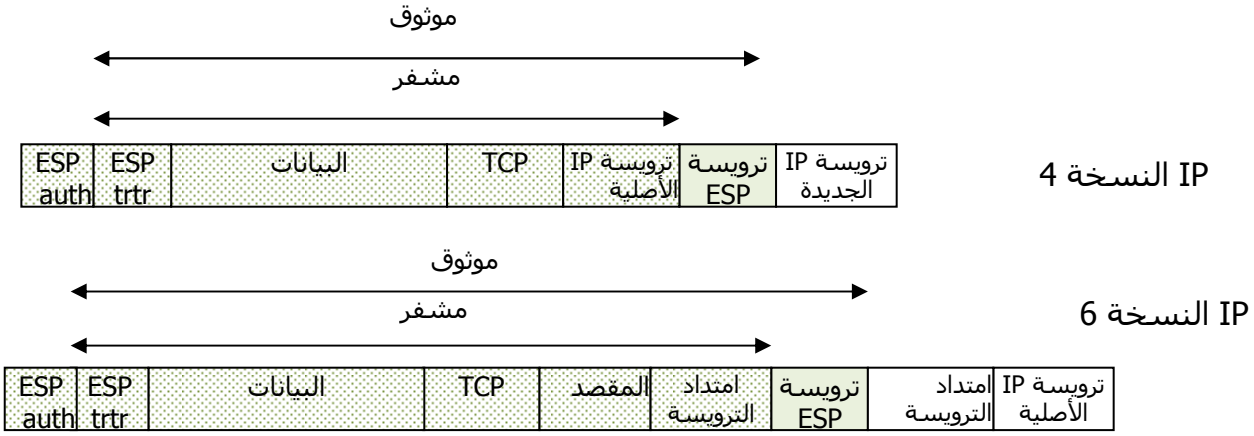
الشكل 12.8 يوضح إدخال ترويسة ومقطورة (الحشة وطول الحشو وحقول الترويسة التالية) برتوكول حمولة امن التغليف في حزمة برتوكول الانترنت عند استخدام صيغة النقل. استخدام

شفرة موثوقية الرسالة يكون اختيارياً. تشفر نقطة المصدر الحمولة وتشتمل على مقطورة ESP. توجة حزمة برتوكول الانترنت الى مقصدها، حيث تقوم الموجهات الوسطية باختبار ومعالجة ترويسة برتوكول الانترنت، تختبر عقدة المقصد ترويسة برتوكول الانترنت وتعالجها، ثم تفك شفرة الحمولة على أساس مؤشر عوامل الأمن في ترويسة ESP.



الشكل 12.10 ترويسة ومقطورة برتوكول حمولة امن التغليف في صيغة النقل.

الشكل 12.8 يوضح إدخال ترويسة ومقطورة برتوكول حمولة امن التغليف في حزمة برتوكول الانترنت عند استخدام صيغة النفق. استخدام شفرة موثوقية الرسالة يكون اختيارياً. الحزمة المتحصل عليها تغلف باستخدام ترويسة برتوكول الانترنت خارجية. توجه الحزمة الخارجية إلى جدار نار المقصد، وتقوم الموجهات الوسطية باختبار ومعالجة ترويسى برتوكول الانترنت الخارجية. يختبر جدار النار الحزمة الخاجية ويعالجها، ثم يفك شفرة حزمة برتوكول الانترنت الداخلية على أساس مؤشر عوامل الأمن في ترويسة ESP. ثم توجه الحزمة الداخلية عبر الشبكة الداخلية إلى مقصدها.



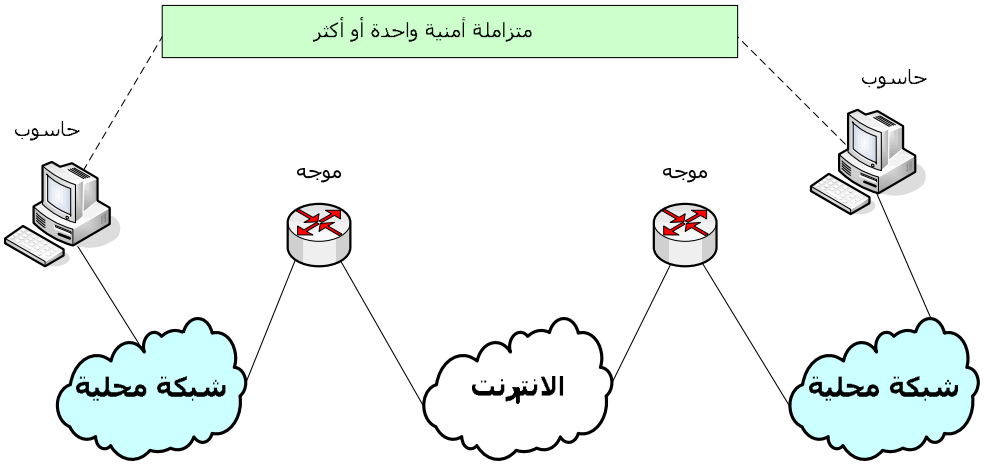
الشكل 12.11 ترويسة ومقطورة برتوكول حمولة امن التغليف في صيغة النفق.

12.7: المتزاملات الأمنية المدمجة

يمكن للتزامل الأمني أن ينفذ برتوكول ترويسة الموثوقية أو برتوكول حمولة تغليف الأمن. ولتنفيذ البرتوكولين معاً نحتاج إلى دمج المتزاملات الأمنية combine SAs. ونستخدم لتحقيق

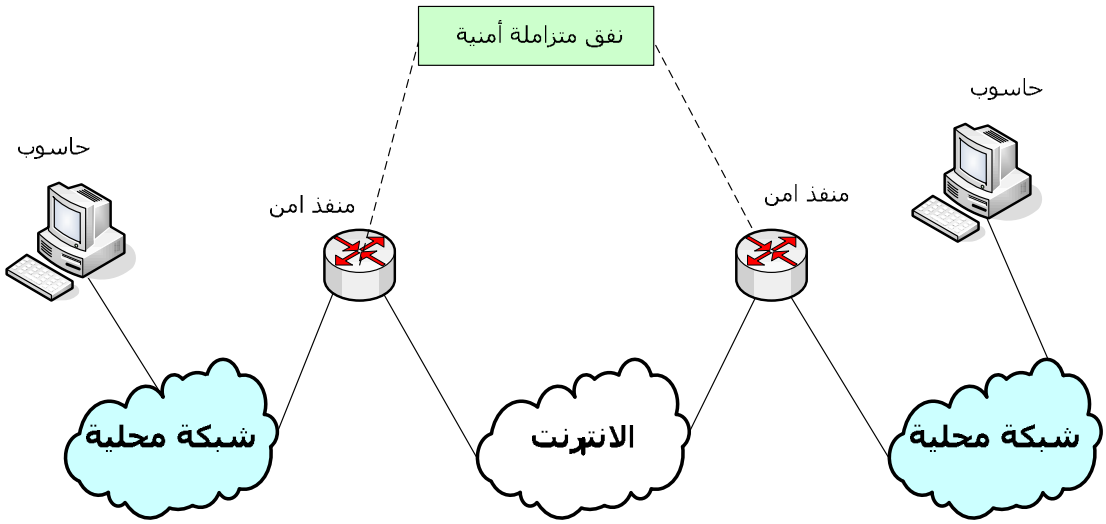
ذلك حزمة التزامل الأمني ***security association bundle*** وهى عبارة عن تسلسل متزاملات أمنية تعالج عبرها الحركة. مما ينتج تجاور النقل Transport adjacency ، والذي يطبق أكثر من برتوكول امني على نفس حزمة برتوكول الانترنت دون استخدام نفق، ويعرف هذا الأسلوب بدمج المستوى الواحد، أو أسلوب الأنفاق المتكررة Iterated tunneling ، والذي يتكون من مستويات برتوكولات أمنية متعدد تؤثر عبر شق أنفاق برتوكول الانترنت، أي نفق يمكن لن يبتدئ وينتهي في مواقع مختلفة.

الشكل 12.7، يوضح دمج بسيط للمتزاملات الأمنية، حيث يوفر هذا الدمج الأمن بين النظم النهائية (الحواسيب) باستخدام امن برتوكول الانترنت، ويجب على طرفي الاتصال باستخدام التزامل الأمني المشاركة في مفتاح سري مناسب.



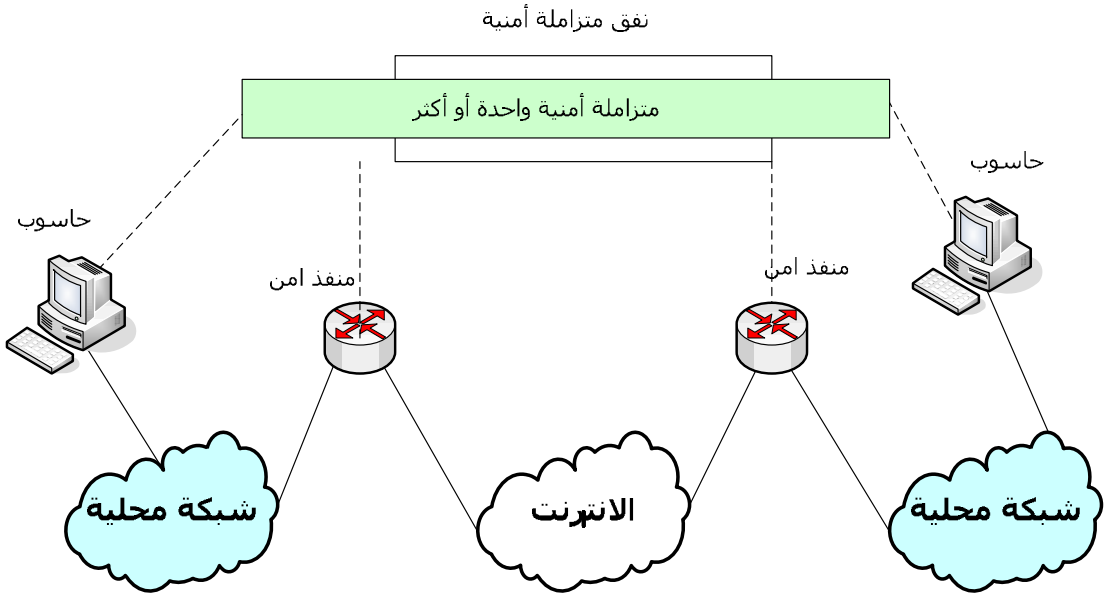
الشكل 12.12، دمج بسيط للمتزاملات الأمنية

قد يستخدم دمج المتزاملات الأمنية لتوفير الأمن والحماية فقط بين المنافذ كما هو موضح في الشكل 12.1. لا يستخدم إي حاسوب امن برتوكول الانترنت، ولا يوجد مجموعة أنفاق nested tunnels حيث يطبق امن برتوكول الانترنت IPSec على كامل الحزمة الداخلية.



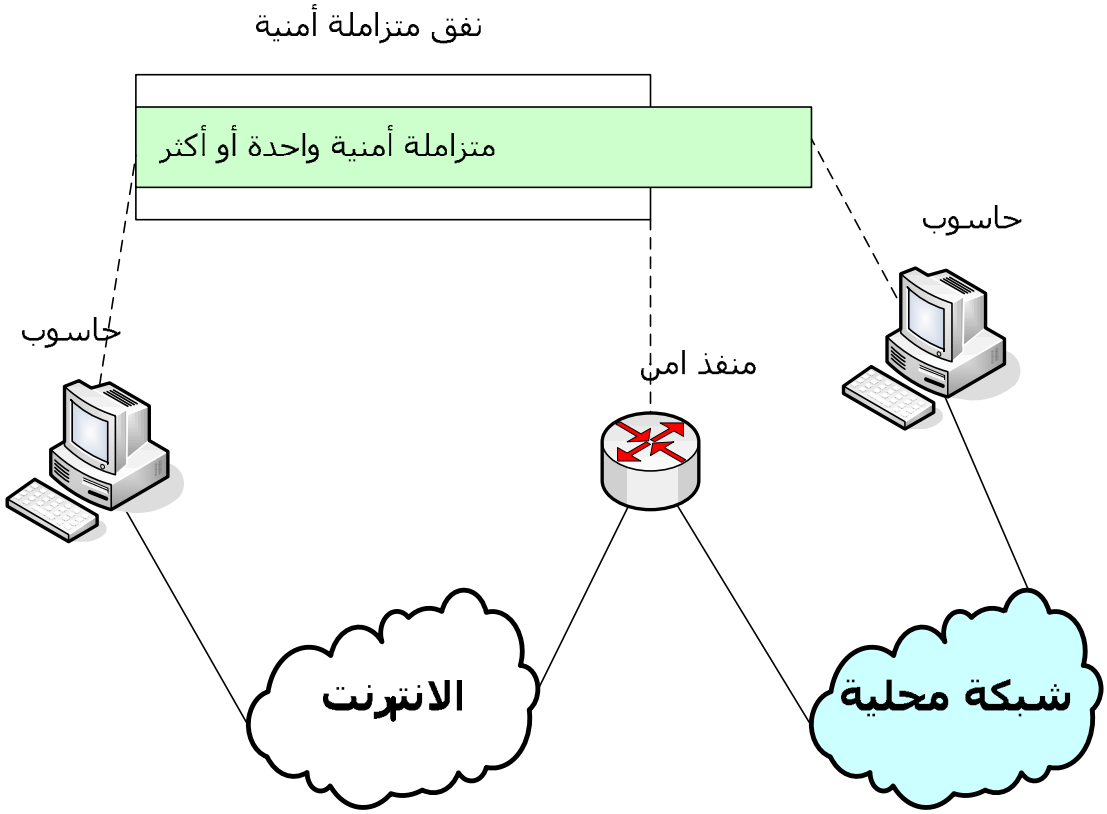
الشكل 12.13، دمج للمتزاملات الأمنية لحماية المنافذ

قد يستخدم الدمج لتوفير المن والحماية بين المنافذ مع استخدام الحواسيب (المضيفين) خدمات امن برتوكول الانترنت إضافية، كما هو موضح في الشكل 12.8.



الشكل 12.14، دمج للمتزاملات الأمنية لحماية الطرفيات والمنافذ

أيضا قد يستخدم الدمج لدعم الحاسوب البعيد والذي يستخدم الانترنت للوصول والنفاذ إلى جدار نار المؤسسة، كما هو موضح في الشكل 12.3. في هذه الحالة نحتاج فقط إلى نفق بين الحاسوب البعيد وجدار النار ومتزاملة أمنية واحدة أو اثنين بين الحاسوب البعيد والحاسوب المحلى.



الشكل 12.15، حمع للمتزاملات الأمنية لحماية النفاذ من الإنترنت

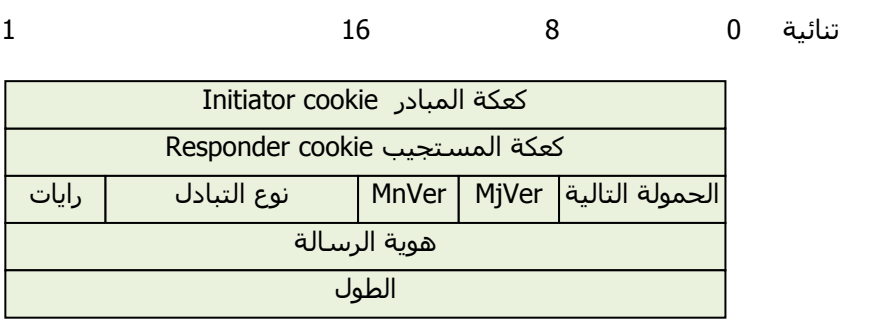
12.8: إدارة المفتاح:

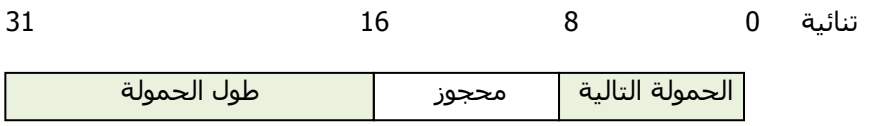
يدعم امن برتوكول الانترنت أيضا توليد المفتاح وتوزيعه. في الحالة النموذجية نحتاج إلى جوزين من المفاتيح، جوز لكل اتجاه وكل برتوكول ترويسة الموثوقية و برتوكول حمولة تغليف الأمن. وقد يدار المفتاح يدويا أو ذاتيا. في حالة الإدارة اليدوية للمفتاح يقوم مدير النظام ترتيب وضبط إي نظام، أما في حالة الإدارة الذاتية يتم إنتاج المفتاح للمتزاملين الآمنين ووفق الحاجة ذاتيا في النظم الكبيرة. برتوكولات الإدارة الذاتية للمفاتيح الأساسية المستخدمة في امن برتوكول الانترنت تتكون من:

- برتوكول أوكلي لتحديد المفتاح Oakley Key Determination Protocol والذي يعتمد على خوارزمية ديفي وهيلمان لتبادل المفتاح (انظر الوحدة رقم ___). يعانى هذا الأسلوب من ضعف يتمثل عدم توفر معلومات لتحديد أطراف لاتصال وإمكانية تعرضه لهجوم المنتصف، والمطلوبات العالية لصد الهجمات.

- وبرتوكول التزامل الأمني في الانترنت وإدارة المفتاح Internet Security Association and Key Management Protocol (ISAKMP). ويحدد هذا البرتوكول إجراءات وانساق حزم لإنشاء وتفاوض وتعديل وحذف المتزاملات الأمنية. كما يعرف حمولة لتبادل توليد المفاتيح وموثقتيها، حيث يوفر اطر لإدارة المفتاح مستقلة عن برتوكول تبادل المفتاح المستخدم وخوارزمية التشفير وأسلوب الموثوقية. تتكون رسالة ISAKMP من ترويسة ISAKMP تتبع بحمولة واحدة أو أكثر . كل حمولة تبدأ بترويسة حمولة، كما يحدد الحقل الثاني في الحمولة نوع الحمولة التالية، وتكون قيمة المحتوي تساوى صفر إذا كانت أخر حمولة في الرسالة. حمولة التزامل الأمنى تستخدم بدء إنشاء التزامل. الشكل 12.5 يوضح بنية ترويسة ISAKMP وترويسات الحمولات.

•





الشكل 12.16، بنية ترويسة ISAKMP وترويسات الحمولات

يوفر برتوكول ISAKMP إطار لتبادل الرسائل، حيث تعمل أنواع الحمولات ككتل بناء. وتشتمل التبادل على الأتي:

- تبادل الأساس *Base exchange* ويشتمل على تبادل المفتاح ومطلوبات الموثوقية وترسا مع بعضها البعض
- حماية الهوية *Identity protection* ، ويمدد تبادل الأساس
- الموثوقية فقط *Authentication only* ، مشاركة الموثوقية دون استخدام مفتاح
- تبادل عدواني *Aggressive exchange* ، والذي يقلل عدد التبادلات ولكن على حساب حماية الهوية
- تبادل معلوماتي *Informational exchange* ، إرسال المعلومات في اتجاه واحد لإدارة التزامل الأمني.

ملخص:

ناقشنا في هذه الوحدة:

- اطر امن آلية امن برتوكول الانترنت
- برتوكول ترويسة الموثوقية
- برتوكول حمولة امن التغليف
- برتوكولات إدارة المفتاح المستخدمة في امن برتوكول الانترنت

أسئلة:

1. افترض استخدام موثوقية وتشفير النهاية إلي النهاية للاتصال بين جهازي حاسوب (مُضيفين). أعطي مخططات لتوضيح التالي:
   أ. تجاور النقل transport adjacency، حين تطبيق التشفير قبل الموثوقية
   ب. تحزيم نقل المتزاملات الأمنية SA داخل نفق المتزاملات الأمنية، حين تطبيق التشفير قبل الموثوقية
   ت. تحزيم نقل المتزاملات الأمنية SA داخل نفق المتزاملات الأمنية، حين تطبيق الموثوقية قبل التشفير