"الحاسبات الالكترونية"
العدد ١٧ السنة ١١
١٤٠٧ هـ - ١٩٨٧ م

مبادىء وأساسيات تشفير البيانات في نظم الحاسبات الالكترونية

د . سامي زهران/ خبير الحاسبات الالكترونية - مكتب الامم المتحدة
سعد عبد العزيز/ محلل انظمة اقدم - وزارة التعليم العالي والبحث العلمي - بغداد

خلاصـــة :

يهدف هذا البحث الى جذب الانتباه لضرورة واهمية تأمين البيانات المنقولة عبر شبكات الاتصال والمتداولة بواسطة نظم الحاسبات الالية . والى خطورة النتائج المترتبة على اختراق تلك النظم .. ثم يتعرض لاحد الاساليب الاساسية المتبعة في تأمين البيانات وهو اسلوب تشفير البيانات حيث يقدم تعريفاً لهذا الاسلوب وطرق تطبيقه باستخدام « خوارزمية تشفير » بالاضافة الى مفتاح شفري لتصعيب مهمة مخترقي النظام ، ومنها على سبيل المثال استخدام خوارزمية تشفير معقدة وتشفير المفاتيح الشفرية وتغيير قيمتها من حين الى اخر ... الخ واخيراً يناقش البحث الحاجة الى نمطيات موحدة متفق عليها لنظم تشفير البيانات مع ضرب مثال لنظام نمطي . ثم عرض امثلة لبعض التطبيقات التي تستخدم فيها نظم تشفير البيانات .

١ ـ مقدمـــة :

بعد ظهور شبكات الاتصال وتكنولوجيا الحاسبات الالكترونية والتطور الكبير فيهما سلاحاً ذي حدين فمن ناحية ، ادى ذلك الى تسهيل تبادل المعلومات بين اطراف بعيدة متباعدة من ارجاء المعمورة في زمن يسير ، مما ييسر على رجال الاعمال اعمالهم وعلى السياسيين والاقتصاديين اتخاذ القرارات السليمة في الوقت المطلوب وفي المكان المطلوب .. ومن ناحية اخرى ادى ظهور هذه التقنيات الحديثة الى زيادة احتمالية تسرب المعلومات والبيانات الهامة والحساسة الى المجرمين وسيء النية والى جهات معادية قد تسيء استخدامها بشكل يضر في مصالح الدولة او المؤسسة المعنية .. لذلك فإن تصميم اي نظام لتبادل المعلومات عبر شبكات الاتصال لابد ان تصحبه عملية دراسة وتصميم دقيقة لوسائل واجراءات تأمين البيانات المتداولة في ذلك النظام وخاصة المنقولة منها عبر الشبكات وخطوط الاتصال ويكون الهدف الرئيسي لتلك الوسائل هو منع تسرب البيانات المنقولة حتى لا تقع في ايد خارجية غير امينة مما قد يؤدي بالتالي الى ايقاع ضرر بالغ بالجهات او المنظمات او الدول الناقلة او المستقبلة للبيانات .

وقد ظهرت حتى الان عدة اساليب متنوعة لتأمين البيانات المنقولة عبر الشبكات فعلى سبيل المثال توجد وسائل حماية خاصة بقواعد البيانات وملفاتها ، ووسائل حماية خاصة بتأمين المنشأة والاجهزة ، ووسائل حماية خاصة بضوابط واجراءات استخدام النظام ، وهناك ايضاً عمليات تشفير البيانات **Data Encryption** المتبادلة بين المواقع المختلفة للنظام وهذا ما يتناوله هذا البحث .

ترجع اصول عملية تشفير المعلومات والرسائل الى زمن بعيد قبل ظهور الحاسبات الالكترونية ، بل اننا نستطيع ان نتقصى لها جذوراً في الصين القديمة حيث كانت تستخدم بواسطة الجواسيس والعشاق والمتآمرين . وقد ازدادت اهميتها في العصر الحديث نظراً لشيوع استخدامها في التطبيقات العسكرية ودوائر الاستخبارات .. ولعل في بعض قصص واحداث الحرب العالمية الثانية الخاصة باختراق نظم تشفير الاعداء ما يدل على زيادة خطورة عملية التشفير وليس هناك اكثر دلالة من القصة المتداولة حول ان خطة تدمير ميناء « بيرل هاربور » في الحرب العالمية الثانية قد تم فك شفراتها في حينها ولكن بدون اتخاذ اي اجراء بصدد ذلك ..

وببساطة يمكن ان نصف عملية التشفير بانها تمثل معركة بين الشخص الذي يقوم بتشفير البيانات .

والشخص الذي يحاول فك واختراق نظام التشفير قد تغيرت طبيعة هذه المعركة بشكل جذري بظهور الحاسبات الالكترونية وذلك لان مخترقي الشبكة غالباً ما يحاولون استخدام الحاسبات الالكترونية لفك الشفرات وذلك باستخدام برامج تقوم بالبحث بسرعات خارقة خلال عدد كبير جداً من التحويلات الممكنة .. مما يزيد من احتمالية فك الشفرات عما اذا

كانت هذه العملية ستتم يدوياً .. ولكن على الجانب الاخر يمكن ايضاً استخدام الحاسب الالكتروني في تصميم وتعقيد عملية التشفير بدرجة تزيد من صعوبة عملية فك الشفرة .. وبشكل عام يمكن القول بانه اذا استخدم كلا الطرفين تقنية الحاسبات بشكل جيد فإن مهمة مشفري البيانات تعتبر اقل صعوبة من مهمة مخترقي نظام التشفير وسوف نستعرض فيما يلي بعض طرق واساليب نظم تشفير البيانات مع ذكر بعض الامثلة لنمطيات وتطبيقات هذه النظم .

٢ – تعريف اسلوب تشفير البيانات :

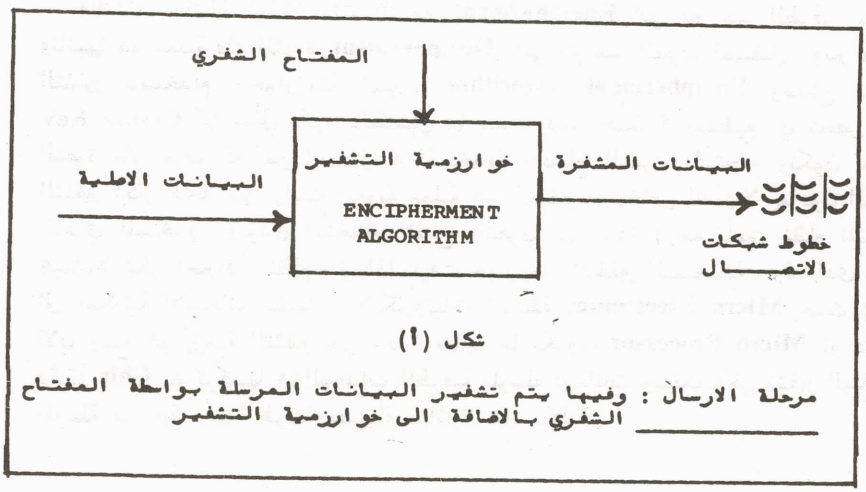
يمكن تعريف مصطلح تشفير البيانات **Data encryption** بأنه يشير الى الاساليب والوسائل الفنية التي يمكن بواسطتها اخفاء المعنى الحقيقي للرسائل المرسلة بحيث لا يمكن لاحد من الاعداء التلاعب بمحتويات الرسالة او الكشف عن معناها او تعديلها او اضافة اجزاء لها .. الخ ويعد اسلوب تشفير البيانات من اكثر الطرق امانا لضمان عدم تسرب البيانات المنقولة عبر الشبكات الى جهات خارجية وذلك لانه اذا تمت عملية التشفير باتقان فانه حتى اذا نجح شخص ما في اختراق الشبكة والحصول على البيانات المنقولة فانها لن تتمثل له اي معنى او فائدة مالم يستطع معرفة الاسلوب المستخدم في تشفيرها حتى يمكنه التوصل الى الصورة الاصلية للبيانات قبل التشفير فعلى سبيل المثال لتكن البيانات الاصلية المرسلة هي جملة ((اتصل فوراً بسفارتنا في بروكسل)) فقد تظهر بعد التشفير بصورة ارقام ورموز لا معنى لها مثلا ((*/ A O * ; 5 0 , /)) والتي لن تعني اي شيء للمصطلح على الرسالة المشفرة فلا يمكنه معرفة مصدرها او مستقرها او معناها .

وللتشفير جانبان اولهما عملية التشفير **Encipherment** التي تتم عند الطرف المرسل وثانيهما هو عملية فك الشفرة **Decipherment** التي تتم عند الطرف المستقبل . وتتم عملية التشفير باستخدام « خوارزمية تشفير » **Encipherment Algorithm** ومفتاح شفري **Crypto Key** كما سيأتي ذكره بالتفصيل فيما بعد ، وذلك بحيث لا يستطيع اي شخص فك الشفرة مالم يعرف كلا من الخوارزمية المستخدمة والمفتاح الشفري المستخدم وتكون عملية التشفير اكثر نجاحاً كلما زادت صعوبة عملية فك التشفير للاشخاص الذين لا يعرفون المفتاح الشفري المستخدم . ويؤدي استخدام المفتاح الشفري الى زيادة درجة تأمين نظام التشفير بحيث لا يمكن اختراق النظام حتى اذا عرفت خوارزمية التشفير المستخدمة . وقد ادى ذلك الى امكانية الاستعانة بتقنيات الالكترونيات الدقيقة **Micro Electronics** حيث يمكن الان وضع خوارزمية التشفير على وحدة معالجة ما يكروية **Micro Processor** او دائرة دقيقة **Chip** يتم تركيبها في الوحدات الطرفية المرسلة للبيانات وبذلك يمكن تشفير البيانات المرسلة من اية وحدة طرفية بطريقة مباشرة غير مكلفة .

وفي حالة شبكات الاتصال التي يكون مطلوباً فيها بشكل عام توفير الاتصال بين حاسبات ووحدات متعددة من شركات مختلفة ، يجب أن تستخدم خوارزمية التشفير نفسها بواسطة جميع الوحدات والحاسبات المتخاطبة مع بعضها البعض وغالباً ما يحدث أن تستخدم طريقة التشفير نفسها بواسطة جميع أطراف الشبكة خاصة اذا كان كل طرف يحتاج الى ارسال واستقبال بيانات عن أي من الاطراف الاخرى . ويمكن في مثل تلك الحالات تنفيذ ذلك باستخدام الدائرة الدقيقة نفسها بشكل متكرر وبعدد كبير مما يجعل عملية انتاجها واستخدامها أقل تكلفة . ولكن هل يؤدي مثل ذلك الحل الى الوصول الى درجة الأمانة المطلوبة؟ ان استخدام مثل تلك الدائرة الدقيقة ا نتجة بكميات كبيرة في عملية التشفير قد يقود الى احتمال أن يستخدمها مخترقو الشفرة أنفسهم في محاولاتهم لفك الشفرة ... ولمعالجة مثل هذا الاحتمال يمكن لمصممي نظام التشفير استخدام ما يسمى بالمفتاح الشفري **Crypto Key** .

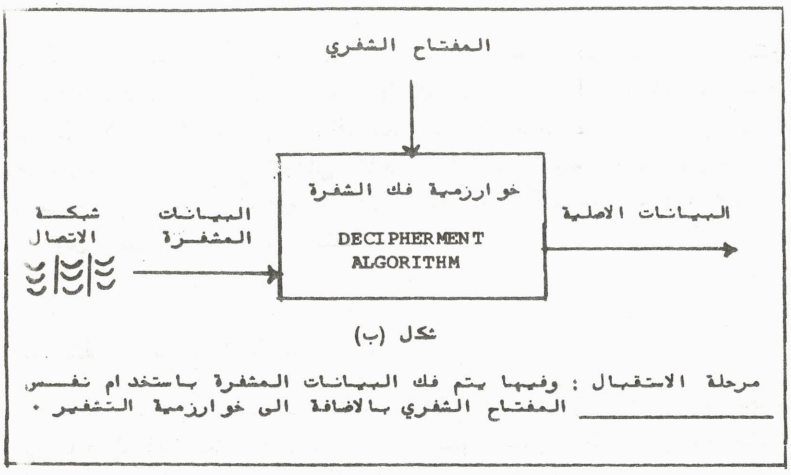
٣ ـ استخدام المفتاح الشفري في عملية تشفير البيانات :

في هذه الحالة يقوم الطرف المرسل للبيانات باستخدام مفتاح شفري **Crypto Key** بالاضافة الى خوارزمية التشفير ... وبذلك تزيد درجة تأمين النظام لانه اذا عرف مخترق النظام خوارزمية التشفير بدون معرفة المفتاح الشفري فسوف يتضاعف الوقت المطلوب منه لفك الشفرة أضعافاً كثيرة ويوضح الشكلان رقم (أ) ، (ب) أسلوب استخدام خوارزمية التشفير مع المفتاح الشفري في كل من مرحلتي الارسال والاستقبال .



شكل (أ)

مرحلة الارسال : وفيها يتم تشفير البيانات المرسلة بواسطة المفتاح الشفري بالاضافة الى خوارزمية التشفير



شكل (ب)

مرحلة الاستقبال : وفيها يتم فك البيانات المشفرة باستخدام نفس المفتاح الشفري بالاضافة الى خوارزمية التشفير .

وحتى يمكننا تصور درجة التعقيد التي يضيفها استخدام المفتاح الشفري أمام محاولات إختراق الشفرة . دعونا ننظر الى نظام التشفير التي تستخدم مفتاح شفري يتكون من (٦٤) بت . اذا حاول مخترق الشفرة أن يفك شفرة رسالة معينة باستخدام حاسب الكتروني فعليه محاولة جميع قيم المفاتيح الشفرية الممكنة والتي يبلغ عددها (٢)^{٦٤} احتمالاً وحتى اذا كان لديه جهاز حاسب خارق السرعة يستخدم فقط في عملية فك الشفرة بحيث يمكنه تجربة مفتاح شفري واحد كل مايكرو ثانية (جزء من مليون من الثانية) فإن متوسط الوقت اللازم لتجربه جميع القيم الممكنة للمفتاح الشفري يكون كما يأتي :

$$\text{الزمن المطلوب} = \frac{(٢)^{٦٤}}{٢} \text{ مايكرو ثانية} = \frac{(٢)^{٦٤}}{٣٦٥ \times ٢٤ \times ٣٦٠٠ \times ١٠٠٠٠٠٠ \times ٢}$$

= ٢٧١ ، ٢٩٢ سنة

وعلى سبيل الطرافة دعونا ننظر الى الوقت اللازم لفك شفرة تستخدم مفتاح شفري يتكون من (١٢٨) بت بطريقة المحاولة والخطأ **Trial and Error** باستخدام جهاز حاسب الكتروني (كما سبق ذكره) يختبر قيم المفاتيح بمعدل مفتاح شفري واحد كل مايكرو ثانية .. يكون الوقت اللازم لتحديد قيمة المفتاح السليم كما يلي :

$$\text{الزمن المطلوب} = \frac{(٢)^{١٢٨}}{٢} = \frac{(٢)^{١٢٧}}{٣٦٥ \times ٢٤ \times ٣٦٠٠ \times ١٠٠٠٠٠٠}$$

= ٥،٤ × ٢٢١٠ قرنا من الزمن .

أي ما يساوي عشرة ملايين مرة قدر عمر كرتنا الارضية وهو وقت أطول بكثير من عمر الكون بأكمله . والواضح من تلك الأمثلة أنه باستخدام اسلوب المحاولة والخطأ وحده لايمكن على الاطلاق النجاح في اختراق تلك الشفرات لذلك قد يلجأ مخترقو الشفرات الى استخدام وسائل أقصر وأسرع لتحاشي الحاجة الى اسلوب المحاولة والخطأ . وفي جميع الاحوال يجب على مشفري البيانات اللجوء الى كافة الأساليب الممكنة لتصعيب مهمة مخترقي الشفرة وذلك بجعل التشفير معقداً قدر المستطاع .

٤ ـ تشفير المفاتيح الشفرية :

يتضح من المناقشة السابقة ان استخدام المفاتيح الشفرية يؤدي الى زيادة تصعيب مهمة مخترقي نظام التشفير ويمكن القول بأن اختيار المفاتيح الشفرية وطريقة توليدها وتأمينها يعد من اهم العوامل التي تضمن تأمين البيانات المنقولة والمتداولة عبر النظام . فمعرفة المفتاح الشفري سوف تؤدي حتماً الى اختراق نظم التشفير . ويلجأ مخترقو نظم التشفير احياناً الى اسلوب بسيط لمعرفة نظام التشفير المستخدم في شبكة اتصالات معينة باتباع الخطوات الاتية : ـ

١) يقوم مخترق نظام التشفير في شبكة معينة بقطع خطوط الاتصالات وملاحظة طريقة واسلوب اعادة الربط والتخاطب **Recovery** .

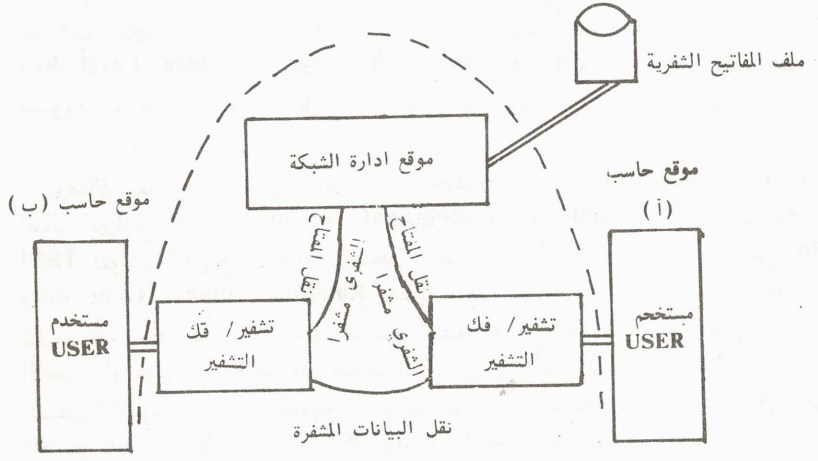
٢) بعد ذلك يقوم مخترق النظام بملاحظة وتسجيل الرسالة المشفرة قبل قطع الاتصال وتسجيل الرسالة المشفرة بعد اعادة الربط والتخاطب .

٣) في معظم النظم عند حدوث قطع اتصال ثم اعادة ربطه يتم اعادة ارسال اخر رسالة تم ارسالها قبل حدوث الانقطاع . فاذا تم اعادة الارسال باستخدام مفتاح شفري مخالف لذلك الذي استخدم في تشفير الرسالة الاصلية فيمكن عندئذ لمخترق النظام المقارنة بين الرسالتين بعملية تحليل شفري **Crypto Analysis** بسيطة يمكنه فك الشفرة خصوصاً اذا امكنه تكرار تلك العملية عدة مرات .

ويمكن منع حدوث ذلك باسلوب بسيط وهو استخدام نفس المفتاح الشفري عند اعادة ارسال الرسائل المعاد ارسالها بعد حدوث عطل (انقطاع في الاتصالات بالشبكة) . وهناك أمر آخر هام يتعلق بالمفاتيح الشفرية وهو انه عند اختيار او تحديد مفتاح شفري جديد عند احد اطراف الاتصال يلزم اخبار الطرف الاخر بقيمة ذلك المفتاح الجديد . وقد يتم ذلك عن طريق ارسال المفتاح الجديد عبر خط اتصال . وفي تلك الحالة يكون من الضروري جداً والهام جداً تأمين عملية ارسال هذا المفتاح او بمعنى اخر يجب تشفير المفتاح الشفري عند ارساله وعندئذ يطرأ السؤال الطريف التالي : ـ

« أي مفتاح شفري يمكن أن تستخدمه لتشفير المفتاح الشفري »؟

وتظهر احياناً اجابة بسيطة لذلك باستخدام اخر مفتاح شفري يتم ارساله عبر الشبكة ، ولكن يمكن استخدام ذلك الاسلوب فقط في حالة ما اذا كان التخاطب يتم بين حاسبين فقط (حاسب أ ، حاسب ب) اما اذا كان الحاسب (أ) يتخاطب مع حاسب (ب) ثم مع حاسب (جـ) فعند ذلك لن يستطيع الحاسب (جـ) معرفة آخر مفتاح تم استخدامه في الشبكة لذا ففي بعض الشبكات يتم تخصيص وحدات طرفية معينة للتخاطب المستديم مع الحاسب نفسه ، اما في حالة ما اذا كان ممكناً للوحدة الطرفية الواحدة التخاطب مع عدة حاسبات في اوقات مختلفة فيمكن عندئذ تخصيص موقع لادارة الشبكة **Network ManagementNode** تلجأ اليه جميع الوحدات الطرفية العاملة في الشبكة عند بدء جلسة اتصال معينة **Session** للحصول على اخر قيم للمفاتيح الشفرية . وهذا يعني ان جميع هذه الوحدات تكون على اتصال مستمر بذلك الموقع ويتم تشفير اي اتصالات منه واليه ... ويوضح الشكل (جـ) مثالا لتلك الحالة والتي يظهر فيها موقعان مختلفان على الشبكة يتبادلان البيانات مباشرة ولكنهما يحصلان على مفاتيح التشفير عن طريق موقع ادارة الشبكة الذي به ملف المفاتيح الشفرية **Key File Crypto** .



شكل (جـ)

دور موقع ادارة الشبكة كمصدر رئيسي لارسال المفاتيح الشفرية الى مواقع مستخدمي النظام، بعد تشفيرها

وفي الشكل الموضح يتم العمل كما يلي : ـ

١) يقوم الحاسب (أ) بالاتصال بموقع ادارة الشبكة طالباً بالبدء بجلسة اتصال مع الحاسب (ب)

٢) يقوم موقع ادارة الشبكة بتحضير جلسة الاتصال واخطار كلا من الحاسبين المعنيين (أ) ، (ب) وارسال مفتاح التشفير الخاص بالجلسة الى كل منهما . ويتم ذلك الارسال مشفراً بواسطة مفتاحي تشفير أولهما مخزن في كل من موقع الحاسب (أ) وموقع ادارة الشبكة وثانيهما مخزن في كل من موقع الحاسب (ب) وموقع ادارة الشبكة ومن شأن ذلك ان يزيد من درجة حماية وأمن المفاتيح الشفرية عند ارسالها عبر الشبكة .

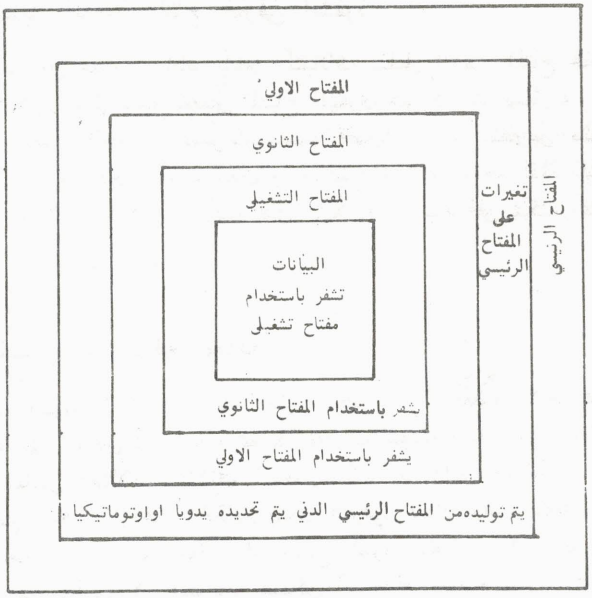
٥ ـ طبقات تشفير المفاتيح الشفرية : ـ

عادة مايسمى المفتاح الشفري المستخدم لتشفير البيانات بالمفتاح التشغيلي **Operational Key** ويسمى المفتاح الشفري الذي يستخدم لتشفير عملية ارسال المفاتيح التشغيلية بالمفتاح الثانوي **Secondary key** او مفتاح المستوى الثاني **Second level key** ومن الطريف ان موقع ادارة الشبكة سوف يقوم بتخزين كل من المفاتيح التشغيلية والمفاتيح الثانوية على ملف المفاتيح الشفرية **Crypto key File** وهذا الملف نفسه يكون من الاهمية بمكان بحيث انه يجب تشفيره هو الاخر باستخدام مفتاح شفري يسمى مفتاح شفري من المستوى الثالث **Third Level Key** او المفتاح الأولي **Primary Key** . وبذلك تكون هناك عدة مستويات للمفاتيح الشفرية تمثل عدة طبقات من عملية تشفير المفاتيح الشفرية .

وهناك بعض النظم التي توفر برامج جاهزة للتعامل مع المفاتيح الشفرية على سبيل المثال البرنامج المسمى **Programmed Cryptographic Facility** والذي توفره شركة **IBM** لتوليد المفاتيح الشفرية بأستخدام مولدات للارقام العشوائية من نوع **Psuedo Random Number Generators** حيث تقوم بتوليد مفاتيح شفرية تشغيلية ومفاتيح شفرية ثانوية وأولية . وتستخدم المفاتيح التشغيلية في تشفير البيانات المرسلة عبر خطوط الاتصال او البيانات المخزنة على ملفات الاقراص او الأشرطة الممغنطة بينما تستخدم مفاتيح التشفير الثانوية في تشفير المفاتيح التشغيلية وتستخدم مفاتيح التشفير الاولية في تشفير جميع المفاتيح عند تخزينها ويوضح الشكل رقم (د) هذه الطبقات في التشفير والحماية .

واخيراً يجب ملاحظة انه يمكن توليد جميع المفاتيح اوتوماتيكياً من مفتاح رئيسي واحد **Single Master Key** يمكن تحديده للنظام يدوياً . ويعني ذلك انه يمكن تغيير جميع المفاتيح الشفرية بالنظام على كل المستويات كلما دعت الحاجة بمجرد إدخال مفتاح رئيسي جديد . كما يجب ملاحظة وجود ثلاثة انواع من المفاتيح الثانوية كما يأتي : ـ

١) المفاتيح الثانوية المستخدمة لتشفير الاتصالات بين حاسب ووحدة طرفية .
٢) المفاتيح المستخدمة لتشفير الاتصالات بين حاسبين .
٣) المفاتيح المستخدمة لتشفير البيانات المخزنة على ملفات أشرطة أو أقراص ممغنطة .



شكل (د)

الطبقات المختلفة من مفاتيح التشفير والتي تستخدم في تشفير مفاتيح تشفير اخرى

ويجب الانتباه الى أن كل نظم التشفير يجب ان تكون مصحوبة بنظم جيدة لتأمين المنشأة والاجهزة **Physical Security** وذلك لمنع إحتمال سرقة او نسخ الملفات المخزن عليها مفاتيح التشفير نفسها أو احتمال تسرب المعلومات الخاصة بالمفتاح الرئيس المستخدم في توليد المفاتيح الشفرية الاخرى .

٦ ـ طرق تصعيب مهمة مخترقي نظم التشفير : ـ

تسهل مهمة مخترقي نظم التشفير **Code Breakers** إذا توفر لهم أي من الشرطين الآتيين : ـ

اولاً : ـ اذا كان متاحاً لهم الحصول على البيانات المشفرة لفترة طويلة بحيث يمكنهم تجريب مختلف وسائل الاختراق . وكلما زادت تلك الفترة زاد إحتمال نجاحهم في اختراق نظام التشفير .

ثانياً : ـ إذا كان متاحا لهم الحصول على كمية كبيرة من البيانات المشفرة تيسر لهم تجريب طرق متعددة للكشف عن نظام التشفير المستخدم . لذلك فهناك عدة اساليب مختلفة يمكن اتباعها لتقليل إحتمالية حدوث اي من هاتين الحالتين كما يأتي : ـ

٦ ـ ١ تقليل الوقت المتاح لمخترقي الشفرة

فمثلاً يجب على مصممي نظم تأمين البيانات تقليل الوقت المتاح لمخترقي الشفرة قدر الامكان . ويمكن تحقيق ذلك بتغيير المفتاح الشفري على فترات متقاربة ... أو بمعنى اخر تقليل الوقت المتاح لاختراق الشفرات ليصبح قصيراً جداً . فلنفترض مثلاً ان شخصاً ما يحاول اختراق نظام تأمين حاسب معين وانه يحتاج الى يوم واحد لفك الشفرة المستخدمة . فإذا تم تغيير المفتاح الشفري المستخدم قبل نهاية ذلك اليوم فلن يمكنه إتمام عملية اختراق النظام .

٦ ـ ٢ تصميم نظم تشفير معقدة

قد تكون الطريقة السابقة مناسبة لبعض النظم بينما في بعضها الآخر قد توجد البيانات السرية مخزنة على أقراص أو أشرطة ممغنطة لفترات طويلة جداً . على سبيل المثال البيانات الدالة على مناطق احتمالات اكتشاف النفط أو المعادن والتي قد تكون ذات قيمة كبرى لمخترقي النظام . وفي مثل هذه الحالات يتوفر لمخترقي النظام وقت طويل وكاف ، لذا يجب اللجوء الى خوارزمية تشفير معقدة أو مفتاح شفري طويل . وفي حالة ماذا استخدمت خوارزمية تشفير نمطية لكل البيانات فيمكن استخدام مفاتيح شفرية مختلفة لتشفير أقسام مختلفة من البيانات أو يمكن اعادة تشفير البيانات المشفرة أكثر من مرة . وبشكل عام فهناك طريقتان لتصميم شفرات لايمكن تحطيمها .

أولاً : استخدام مفتاح شفري معقد .
ثانياً : استخدام خوارزمية تشفير معقدة بدرجة كافية .

وقبل ظهور الحاسبات كانت أكثر نظم التشفير أماناً تلجأ الى استخدام مفاتيح شفرية يتم استخدام كل منها مرة واحدة فقط لا أكثر ، وفي بعض الحالات يتم اللجوء في النظم المستخدمة بواسطة بعض الوحدات العسكرية الى استخدام مفتاح شفري طويل يخزن على شريط ورقي على شكل لفة قطرها (٨) بوصة بأكملها .

أما في هذا العصر وبظهور اتصالات حاسب مع حاسب فيمكن وضع المفاتيح الشفرية على أقراص ممغنطة تبلغ سعتها عدة ملايين من الأرقام الثنائية العشوائية **(Random Bits)** وفي تلك الحالة يجب أن يكون القرص الممغنط المخزن عليه المفتاح الشفري متوفراً في كل من موقعي الحاسب المرسل والحاسب المستقبل وعندها تكون عملية إختراق الشفرة شبه مستحلية خصوصاً اذا تم تغيير محتويات ملف المفتاح الشفري **Crypto key File** بين حين وآخر .

٦ ـ ٣ تغيير المفتاح الشفري

يمكن أحياناً اللجوء الى تغيير المفتاح الشفري كل فترة معينة لتضليل مخترقي الشبكة . وتوجد ثلاث طرق لتغيير المفتاح الشفري أثناء ارسال البيانات كما يأتي : ـ

١ ـ تغيير المفتاح الشفري يدوياً : بأستخدام بعض أجهزة التشفير الملحق بها لوحة مفاتيح تستخدم لتغيير المفتاح الشفري يدوياً على فترات .

٢ ـ تغيير المفتاح الشفري أوتوماتيكياً : بأستخدام جهاز حاسب الكتروني يقوم بأرسال القيم الجديدة للمفتاح الشفري الى مستخدمي النظام بطريقة أوتوماتيكية .

٣ ـ تحديد المفتاح الشفري أوتوماتيكياً عند بداية كل جلسة عمل **Session** على الحاسبة ، وفي تلك الحالة يكون تحميل المفتاح الشفري واختباره هو جزء من إجراءات تحضير الجلسة .

وفي كل تلك الحالات الثلاث يتم ارسال واستقبال القيم الجديدة للمفاتيح الشفرية عبر الشبكة بين المواقع المتخاطبة . ويجب تشفير ذلك الارسال نفسه حتى لا يتم تسرب قيمة المفتاح الجديد . ويتوقف اختيار احدى تلك الطرق الثلاث على طبيعة النظام التطبيقي **Application System** وعلى خواص برامج الشبكة . ونذكر فيما يلي مثالين لنظم التطبيقات المطلوب تأمينها وكيفية توليد المفاتيح الشفرية بها .

أ ـ نظم تحويل النقود الكترونياً : وفيها تكون الوحدات الطرفية في حالة عمل وإتصال مستمرة لذا يمكن اللجوء الى تغيير المفاتيح الشفرية اوتوماتيكياً .

ب ـ النظم المصرفية : وفيها يمكن تحديد مفتاح شفري جديد يدوياً عند بداية تشغيل النظام صباح كل يوم .. وأيضاً عند الحاجة الى ارسال بيانات حساسة لمرة واحدة فقط يمكن تحديد المفتاح يدوياً قبل الارسال .
وبالنسبة لمعظم الشبكات فأن أكثر النظم شيوعاً هو تحديد مفتاح التشفير اتوماتيكياً عند بداية الجلسات حيث تصبح تلك العملية جزءاً من اجراءات بداية جلسة الاتصال . ولا يتم تحديد المفتاح الشفري الا للجلسات المطلوب فيها السرية فقط ويمكن أن تتم تلك العملية بواسطة النظام وبدون أن يشعر بها مستخدمو النظام . هذا ويجب ملاحظة أنه يمكن توليد جميع مفاتيح التشفير بأستخدام مفتاح تشفير رئيسي **Master key** واحد باستخدام حاسب الكتروني مركزي يقوم بتوليدها وإخطار باقي مراكز الشبكة بقيم المفاتيح الشفرية المخصصة لها .

٦ ـ ٤ العنونة غير المباشرة Indirect Addressing

في بعض الشبكات الكبيرة يمكن تضليل مخترقي الشبكة بشكل أكثر تعقيداً بحيث أنه حتى اذا استطاع شخص ما الحصول على بعض البيانات غير المشفرة فلن يمكنه معرفة الجهة المرسلة أو الجهة المستقبلة لتلك البيانات ويمكن تحقيق ذلك باستخدام الاسلوب المسمى بـ « العنونة غير المباشرة » . ويتم في ظل هذا الاسلوب تحديد عناوين مميزة لاطراف الشبكة تختلف في كل جلسة إتصال عن سابقها . وتكون تلك العناوين معروفة فقط للاطراف المتخاطبة أثناء تلك الجلسة بالذات . وتتغير تلك العناوين المميزة من جلسة الى إخرى .

٦ ـ ٥ تأمين المنشآت والاجهزة Physical Security

يجب أن تشمل طرق الحماية والتأمين وسائل تأمين المنشآت والاجهزة في المناطق الحساسة من الشبكة بالاضافة الى عملية التشفير وذلك لكي نضمن أنه حتى اذا نجح أحد مخترقي الشبكة في الاتصال بالنظام والحصول على بياناته فأنه سيواجه بعائق هو ضرورة فك الشفرة .

٦ ـ نمطيات نظم تشفير البيانات Data Encryption Standards

من الطبيعي ان تقوم مختلف الشركات العالمية المهتمة بتشفير البيانات بتطوير وتبني نظم مختلفة ومتباينة للتشفير .. لذا فلسنا في حاجة الى التأكيد على ضرورة وضع وتبني نظم نمطية على المستوى القومي National والعالمي International بحيث تتبنى جميع الشركات المنتجة للحاسبات تلك النظم النمطية بشكل ييسر توصيل حاسبات من انواع مختلفة على شبكة واحدة وبطريقة تمكنها من التخاطب مع بعضها البعض . وتكون مثل تلك النظم النمطية مؤمنة وعملية اذا توفرت فيها الشروط الاتية :

١ ـ ان تقوم بعملية تشفير البيانات بشكل دقيق ومعقد بدرجة كافية .
٢ ـ ان تستخدم مفتاحاً شفريا ذا طول كاف لتصعيب او منع اختراق الشفرة بطريق المحاولة والخطأ .
٣ ـ الا تضيف عبئاً اضافيا كبيرا على عملية ارسال البيانات عبر الشبكة .
٤ ـ أن يكون من الممكن تنفيذها بواسطة دائرة مايكروية مصغرة (Microchip) منتجة على نطاق كبير وقليلة الكلفة .

ونورد فيما يأتي مثالاً لهذه النمطيات وهو النظام المعروف باسم نمطية تشفير البيانات Data Encryption Standard (DES) والذي تم تطويره بواسطة المكتب الوطني للنمطيات بالولايات المتحدة U.S National Bureau of Standards عام ١٩٧٧ وقد تم

تنفيذه الان على دائرة الكترونية مايكروية مصغرة تبلغ كلفتها اقل من ٥٠ دولارا وهناك اسلوبان لتطبيق هذا النظام النمطي .

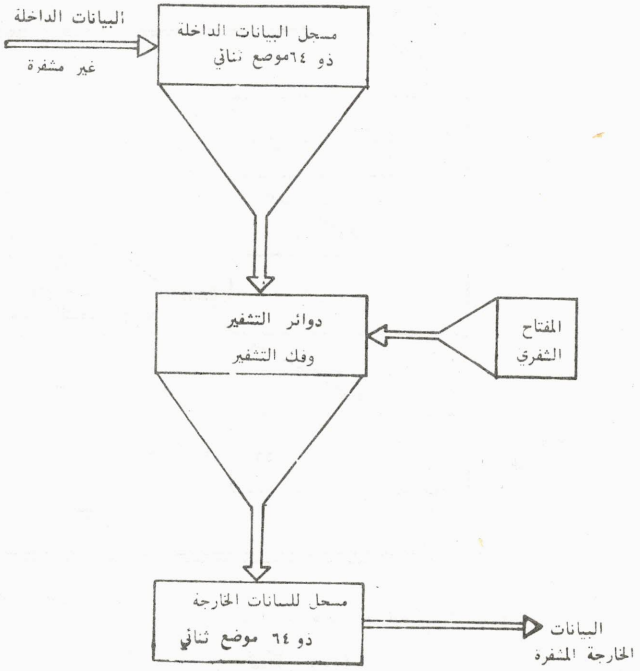
١) الاسلوب المعروف بإسم (Key Auto Key - KAK) .

٢) الاسلوب المعروف باسم (Cipher Text Auto Key - CTAK) .

وفيما يأتي نبذة مختصرة عن كل من هذين الاسلوبين : ـ

اولاً : الأسلوب المعروف بأسم (KAK)

في ظل هذا الاسلوب تتم قراءة البيانات الداخلة في ذاكرة مرحلية (Buffer) على دفعات طول كل منها (٦٤) بت ثم يتم اعادة ترتيبها عشوائياً Scrambling وارسالها على شكل (٦٤) بت من البيانات المخرجة .. وتبدأ عملية التشفير هذه بأمر يسمى « إبدأ التشفير » Start Encipher وتستمر حتى تنتهي البيانات جميعها ويكون الحاسب المستقبل للبيانات على علم ببداية البيانات . واذا فقد أي موضع ثنائي (بت) أثناء الارسال يتم طلب إعادة الارسال مرة أخرى ويوضح الشكل (هـ) تمثيلا لتنفيذ اسلوب (KAK) في تشفير البيانات .

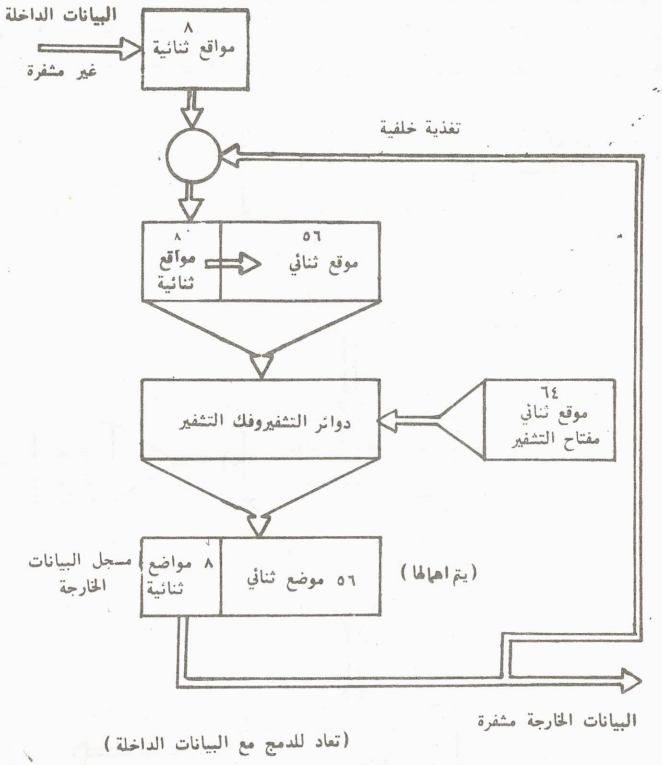


شكل (هـ)

الأسلوب المعروف باسم (KAK) لتنفيذ النظام الامريكي النمطي لتشفير البيانات (DES)

ثانياً : الاسلوب المعروف باسم (CTAK)

وهذه الطريقة هي اكثر تعقيداً من قرينتها السابقة ويتم فيها ادخال البيانات الداخلة الى سجل ذي (٦٤) بت على شكل مجموعات طول كل منها (٨) مواضع ثنائية الى حين امتلاء السجل ، ثم تبدأ عملية التشفير باستخدام مفتاح شفري طوله (٦٤) بت وينتج منها بيانات خارجة طولها (٦٤) بت ، ومنها يتم فقط استخدام الثمانية بتات الاخيرة التي يعاد ادخالها الى سجل البيانات الداخلة ودمجها مع جزء من البيانات الداخلة طوله ثمانية بت من جديد ، وهكذا دواليك كما هو موضح في شكل رقم (و) ويسمى هذا الاسلوب بأسلوب التغذية الخلفية لسياق الشفرة **Cipher-Text Feed Back** ويزيد هذا الاسلوب من صعوبة عملية اختراق الشفرة ولكنه يسبب زيادة في طول الرسائل المرسلة قدرها (٦٤) بت ، يجب إرسالها عبر الشبكة قبل البدء في ارسال البيانات الحقيقية .



شكل (و)

الأسلوب المعروف بأسم (CTAK) لتنفيذ النظام الامريكي النمطي لتشفيل البيانات (DES)

٨ ـ أمثلة للتطبيقات التي تستخدم نظم تشفير البيانات :

تتوقف درجة التأمين المطلوبة لنظام ما على طبيعة البيانات المتداولة والمخزنة في ذلك النظام . وعلى ذلك فان درجات التأمين المطلوبة تتفاوت بشكل كبير من نظام الى اخر فقد يوجد نظام لا يتطلب أي نوع من أنواع التأمين على سبيل المثال نظام إستعلامات عامة لتوفير معلومات معينة للجمهور أو لموظفي دائرة معينة للرد على الاستفسارات ، مثلا الاستفسار عن مواعيد رحلات القطارات أو وصول الطائرات ... الخ ومثل هذه النظم تكون إستعلامية بحتة وبياناتها من النوع الخدمي الذي لايخص منشأة بعينها .

وعلى النقيض من ذلك نجد النظم البالغة في السرية **Top Security** والتي تتداول معلومات ورسائل حساسة إذا وقعت في آيد غير أمينة أو آيد معادية فأنها قد تسبب ضرراً بالغاً للهيئة أو الدولة صاحبة البيانات وكمثال لتلك النظم ، لنعتبر مثلا المخابرات أو الاتصالات العسكرية التي قد تتضمن موعد البدء بعملية عسكرية معينة .

وفيما بين هذين النقيضين يمكن تحديد الموقع المناسب لدرجة التأمين المطلوب توفيرها لنظام ما . والآن دعونا نتصور شبكة إتصالات ولنحاول أن نعدد بعض نظم التطبيقات المطلوب إستخدام نظم تشفير البيانات لها .

نظم تحويل النقود الكترونياً

تتم في هذه النظم تحويل مبالغ تصل الى ملايين الدولارات من بنك الى آخر عبر شبكات الاتصالات بشكل الكتروني . لذلك تكون درجة التأمين المطلوبة لهذه النظم عالية حتى لايتم أي تلاعب من خارج الشبكة أو من خارج النظام يغير من قيمة المبالغ المحولة أو الحسابات المحوّل اليها .

نظم الاستخبارات والاتصالات العسكرية

يتم في هذه النظم تبادل رسائل ومعلومات في غاية من الاهمية وغالباً ما تكون على درجة كبيرة من الخطورة إذا وقعت في يد الاعداء وتكون درجة السرية المطلوبة في مثل هذه النظم عالية للغاية .

المراسلات الدبلوماسية

يتم في هذه النظم إرسال رسائل دبلوماسية حساسة الى بعثات القطر الدبلوماسية في أنحاء العالم وقد يؤدي الكشف عن هذه الرسائل الى حرج كبير لدولة ما أو قد يؤدي ذلك لحدوث أزمة دبلوماسية بين الدول لذلك فأن درجة التأمين المطلوبة لمثل هذه النظم تكون عالية .

نظم المعلومات التجارية والصناعية ذات الاهمية الخاصة

مثل نظم توقعات إستكشافات النفط الخام أو المعادن الثمينة الاخرى والتي قد يؤدي تسرب بياناتها الى الشركات المنافسة الى ضياع فرص إستثمارية كبيرة على الشركة صاحبة الاكتشاف الاصلي لذا تحتاج مثل تلك النظم الى درجة كبيرة من التأمين .

نظم البيانات الخاصة بالمنافسة بين الشركات الصناعية والتجارية

مثلاً قوائم عملاء شركة معينة أو قوائم مبيعاتها أو خطط التطوير المستقبلية أو تفاصيل المنتجات الجديدة التي لم يتم الاعلان عنها بعد .. أو معلومات حول بحوث سرية ... الخ فمثل هذه المعلومات إذا وقعت في أيدي الشركات المنافسة قد تؤدي الى ضياع وفقدان عائدات كبيرة من الشركة المعنية وتحتاج مثل هذه النظم الى درجة عالية من التأمين .

نظم معلومات الافراد والمعلومات الامنية

على سبيل المثال نظم رواتب الموظفين وأجور العمال وتفاصيل البيانات الشخصية للافراد والتي قد يكون تسربها ضاراً للشخص ذي العلاقة . وتحتاج عادة الى درجة معقولة من التأمين .

٩ ـ تفاوت درجات التأمين المطلوبة في أجزاء النظام الواحد :

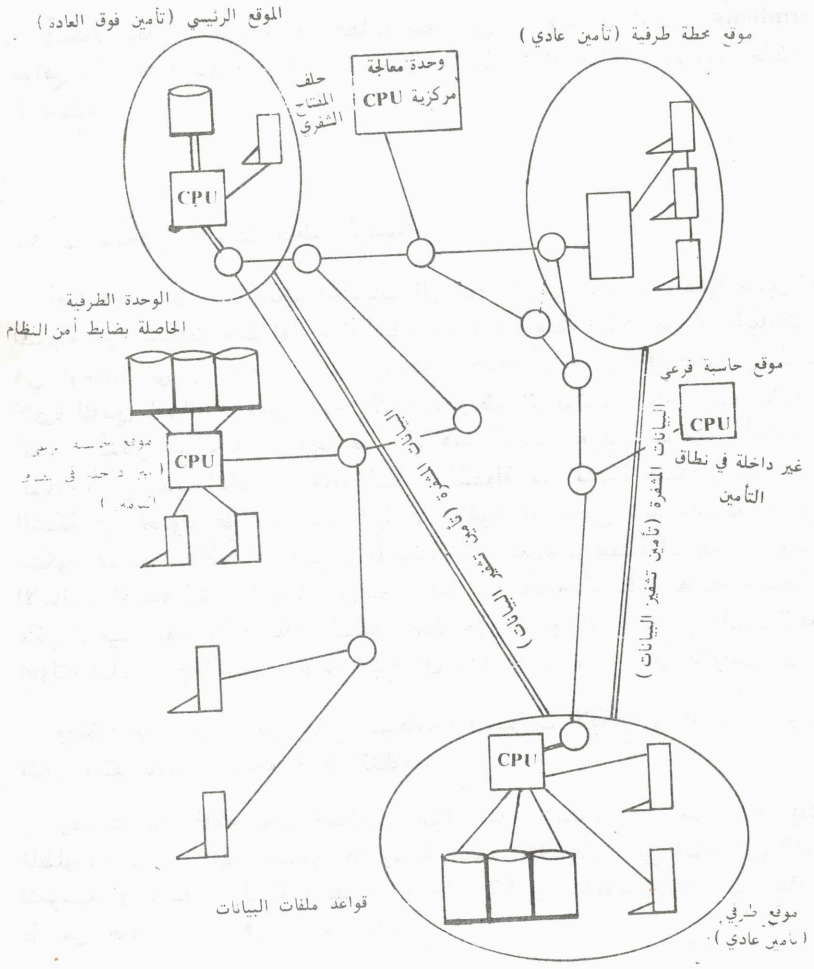
في أحيان كثيرة تتفاوت درجة التأمين المطلوبة في أجزاء النظام المختلفة كما هو مبين في شكل (ز) الذي يوضح أجزاء شبكة إتصالات تربط بين مواقع حاسبات متعددة .
ويوضح الشكل (ز) درجات التأمين الاتية : ـ

تأمين فوق العادة :

ويكون ذلك مطلوباً لموقع الحاسب الذي يكون مخزناً فيه ملف المفتاح الشفرى أو أي بيانات أخرى ذات خطورة وأهمية . مثلاً البيانات الخاصة بإجراءات تأمين النظام نفسه .

التأمين بتشفير البيانات :

ويكون ذلك مطلوباً عادة على خطوط الاتصال التي تربط بين المواقع المختلفة . ويعد تشفير البيانات الطريقة الرئيسة لتأمين البيانات في مرحلة الارسال عبر الشبكة حيث لا يمكن تنفيذ إجراءات أخرى إضافية مثل تأمين الموقع أو فرض إجراءات إدارية أو أمنية على خطوط الاتصال التي قد تمتد لمسافات بعيدة .



شكل (ز)

مثال على اختلاف مستويات التأمين للاجزاء المختلفة فى النظام الموحد

التأمين العادي :

ويكون ذلك مطلوباً لموقع المحطات مثلا التي بها وحدات إتصال **Terminals** أو مواقع حاسبات فرعية قد يكون بها ملفات البيانات أو قواعد البيانات الخاصة بالنظم التطبيقية .

١٠ ـ ملخص الاستنتاجات الرئيسة :

أدى ظهور الشبكات ونظم الحاسبات الى زيادة الوعي بضرورة وأهمية تأمين البيانات المنقولة عبر الشبكات والمتداولة بهذه النظم وضرورة وأهمية التأكد من أن البيانات المنقولة هي الرسائل التي تم إرسالها من دون إضافة أو حذف أو تغيير . وقد ظهرت أساليب ونظم كثيرة لتأمين البيانات المنقولة عبر الشبكات ونظم الاتصالات . وأحد هذه الاساليب هو أسلوب تشفير البيانات ... وقد قمنا في هذا البحث بعرض مبادىء وأساليب تشفير البيانات التي تهدف أساساً الى حماية البيانات المنقولة عبر الشبكة بحيث إذا نجح احد مخترقي الشبكة في الحصول على جزء من البيانات المنقولة فلن تعني شيئاً بالنسبة له حيث أنها ستكون قد تغيرت تماماً عن صورتها الاصلية حيث تعرضت لعملية التشفير ... وقد عرضنا الاساليب المختلفة لتشفير البيانات ووضحنا كيف أنه باستخدام نظم المفاتيح الشفرية المناسبة يمكن تصعيب مهمة مخترق نظام التشفير بحيث حتى اذا لجأ الى استخدام حاسب الكتروني في محاولته لفك نظام التشفير فسوف يحتاج الى عدد خيالي من السنين للتوصل الى ذلك .

وهكذا يجب على مصممي نظم الشبكات والإتصالات الالكترونية إختيار أسلوب ونظام تشفير معقد لتصعيب مهمة مخترق النظام .

وضربنا بعد ذلك مثالاً لنمطيات طرق تشفير البيانات وعدَّدنا أمثلة للتطبيقات المطلوب استخدام نظم التشفير لها وتشمل تلك التطبيقات التي تتناول بيانات حساسة للمؤسسة أو الهيئة أو الدولة وكيف أن درجات التأمين المطلوبة تتفاوت من نظام الى آخر بل من جزء الى آخر في النظام الواحد .

إن عدم استخدام نظم التشفير يجعل البيانات سواء المخزنة على ملفات الحاسب أو التي ترسل عبر شبكات الاتصالات ، عرضة للسرقة أو العبث أو التغيير من جانب جهات معادية أو أشخاص سيء النية ومن هنا تكتسب عملية تشفير البيانات أهمية خاصة لجميع البيانات المتداولة في نظم المعلومات ذات الطبيعة الحساسة .

وأخيراً نأمل أن نكون من خلال هذا البحث قد جذبنا الإنتباه الى دور أساليب تشفير البيانات ووضعنا الخطوات الاولى على طريق تطبيقها في العالم العربي .

والله الموفق

References for Reading

1) Brown, W.F. (ed)
"Computer and Software Security"
AMR International Inc., N.Y., 1971

2) Carrol, J.M. and Mcielland, P.M.
"Fast Infinite Key Privacy transformation for Resource Sharing Systems"
Proceedings AFIPS 1970 Fall Joint Computer Conference, vol. 26, AFIPS Press, N.J. USA.

3) Data Encryption Standard (DES),
Federal Information Processing Standard 46,
National Bureau of Standards, 1977, USA.

4) Diffe, W. and Hellman, M.E. "New Directions in Cryptography",
IEEE Transactions on Information Theory, Nov. 1976.

5) Girsdansky, M.B. "Cryptology, The Computer and Data Privacy", Computers and Automation, April 1972.

6) Healy, R.J., "Design for Security", John wiley & Sons, New York, 1968.

7) Kahn, D., "The Codebreakers", Macmillan, N.Y., 1967.

8) Martin, James, "Security, Accuracy, and Privacy in Computer Systems", Prentice-Hall, Englewood Cliffs, N.J., U.S.A., 1973.

9) Martin, James, "Computer Networks and Distributed Processing: Software, Techniques and Architceture', Prentice-Hall, Engewood Cliffs, N.J., U.S.A., 1981.

10) Morgan, B.D., and Smith, W.E., "Data Encryption", Data Communication, Feb. 1977.

11) Needham, R.M. and Schoeder M.D. "Using Encryption for Authentication in Large Networks of Computers", Communications of the ACM, No.21, 1978.

12) IBM, "Programmed Cryptographic Facility", General Information Manual, IBM Manual No. GC28-0942, IBM.

13) Skatrud, R.O., "The applications of cryptographic techniques to data Processing", Proceedings AFIDS 1969 Fall Joint Computer Conference, Vol. 34, AFIPS Press, N.J., U.S.A. 1969.

14) Titus, J.P. "Washington Commaentary-Security and Privacy", Communication of the ACM, Vol.10 No.6, June 1967.

15) Ware, W.H. 'Security and privacy in computer systems" proceedings of the spring Joint Computer Conference, Vol. 30, 1967.