بسم الله الرحمن الرحيم

كلية دراسات الحاسوب والاحصاء

التشفير وأمن المعلومات

الاسم :علي محمد دهب

الدولة :السودان ـ بابنوسه

الجامعة :كردفان ـ كليه دراسات الحاسوب والاحصاء

قسم :علوم الحاسوب

البريد:alidahab52@yahoo.com

المقدمة:ـ

للتشفير (Cryptography) تاريخ طويل وقد استخدمه المصريون القدماء قبل نحو ٤٠٠٠ سنة و له دور فاعل في سنوات القرن العشرين حيث لعب دورا حاسما في نتيجة الحربين العالميتين (الأولى والثانية) وعلى هذا الأساس فان له دور مسيطر في مجالات الجيش (المجالات العسكرية) و الفعاليات الدبلوماسية و مهام الحكومات بشكل عام. استخدم التشفير كأداة من اجل حماية الأسرار الدولية و الاستراتيجيات.

بعد التزايد الواضح في أجهزة الحاسوب و أنظمة الاتصالات و خاصة عام ١٩٦٠ أصبح من الضروري توفير وسائل لحماية المعلومات المتمثلة بأرقام (Digital) و ذلك يجب توفر خدمات أمنية أخرى.تم بذل المزيد من الجهود المؤثرة من قبل شركة IBM في بداية السبعينات لغرض تبني طريقة تشفير للمعلومات

سميت (Data Encryption Standard DES) والتي تعتبر من الطرق التشفيرية المعروفة في تاريخ دراسة التشفير و قد اعتبرت وسيلة فعالة لغرض تأمين أمنية للمعلومات الاقتصادية في مجال الموارد المالية.

في العام ١٩٧٠ حدث تطور له أثـــره الواضـح عندما نشـر كل من ديف وهيلمان (Diffe & Hellman) بحثا تم من خلاله الإعلان عن ميلاد تشـفير المفتاح العام (Public – Key Cryptography) و تم كذلك توفير طريقة جديدة لتبادل المفتاح ، و التي تعني أن الأمنية (Security) تعتمد في الأساس على صفة (صـعوبة الحلIntractability) للمشـكلة اللوغاريثم المنفصـلة (Discrete Logarithm Problem) ، و على هذا الأساس فأن فكرة المفتاح العام أصبحت واضحة و ذات اهتمام واسع في مجال التشفير. في العام ١٩٧٠ تمكن كل من رايفست وشاميـر وادلمـان (Adleman, Shamir, Rivest) من اكتشاف أول طريقة تشـفير معتمـدة على المفتاح العام و كذلك التواقيع الرقمية (Digital Signature) و أطلقوا على هذه الطريقة بـ (RSA) نسبة إلى أسماء مكتشفيها. تعتمد الـ RSA على مسألة رياضية تتميز بالصعوبة أو التعقيد في الخطوات الرياضية و المستخدمة في تحليل العوامل (Factoring) للأرقام الأولية الكبيرة (Prime Integers). و باستخدام مشكلة صعوبة الخطوات الرياضية فقد تم استحداث طرق جديدة و كفوءة معتمدا على تحليل العوامل. (هذا التطبيق للمشكلة الرياضية الصعبة الحل) أعاد الحياة في جهود العثور على طرق أكثر كفاءة لتحليل العوامل. إن الثمانينات قد أظهرت تقدما كبيرا في هذا المجال ولكن أي (من هذه التقدميات) لم يجعل نظام الـ RSA غير أمين (Insecure). في العام ١٩٨٥ أوجد (El-Gamal) صنف من التشفير يتمتع بقوة كبيرة معتمدا في ذلك على فكرة المفتاح العام (Public-Key Scheme) .

احد المظاهر المهمة و الواضحة المعالم في استخدام المفتاح العام هو توفير التواقيع الرقمية. لقد تم إيجاد توقيع رقمي (digital signature) وذلك باستخدام طريقة الـ RSA و كذلك تم إيجاد توقيع رقمي باستخدام طريقة El-Gamal).

أن البحث عن طرق جديد للمفتاح العام، التحسينات لميكانيكيات التشفير المتوفرة حاليا، واثبات السرية استمرت بخطوات سريعة. لقد تم وضع لذلك قياسات (Standards) مختلفة وبنى تحتية والتي تشتمل على التشفير واستخدمت هذه القياسات في التطبيق العملي بشكل فعال.إضافة إلى ذلك، تم تطوير منتجات الأمنية (Security Products) لغرض تطوير وتوفير متطلبات الأمنية المطلوبة في المجتمعات المبنية في تعاملاتها على المعلوماتية بشكل واسع.

١- ٨: أمنية المعلومات والتشفير Information Security and Cryptography):

سوف نتعامل مع المعلومات (Information) بأنها كمية مفهومة (Understood Quantity) لذلك فكل ما يتعلق بها من تأمين سرية هذه المعلومات معتمدا على التشفير يجب أن يكون أيضا مفهوما. أن أمنية المعلومات تعتمد على عدة طرق معتمدة في ذلك على الحالة والمتطلبات (state and requirements). من المهم جداً أن يتضح لكافة المشتركين في أمنية المعلومات الأهداف المتعلقة بأمنية المعلومات.بعض هذه الأهداف ملخصة في الجدول ١.١:

على العموم، فان أمنية كل من أنظمة المشاركة الزمنية وشبكات الحاسوب تتألف من ثلاث مكونات:

- أمنية مركز (أو مراكز) الحاسبات.
- أمنية المحطات الطرفية.
- أمنية قنوات الاتصال.

تحتاج حماية مراكز الحاسبات لعدد مختلف من مقاييس الأمنية (security measurements). المقياس الأول هو أن المراكز يجب حمايتها من أي كوارث طبيعية مثل الفيضانات، الحريق، الزلازل. الخ. كذلك فان البناية يجب أن تحمى ضد النشاطات الخارجية مثل الهجومات الإرهابية، الاستراق (اختلاس السمع Eavesdropping) الخ، كل هذه المقاييس يمكن أن ينظر لها بأنها أمنية خارجية (External Security) . الأمنية الداخلية (Internal)، على كل حال، تشمل مقاييس حماية تستخدم داخل نظام الحاسبة (مثلا ميكانيكية سيطرة وصول أمينة access control mechanism، أنظمة مراقبة لمحاولات الوصول غير الشرعية، ميكانيكية التعرف على المستفيد (Identification)، الخ) ومقاييس أخرى تطبق خارج الحاسبة مثل الاختيار المناسب والصحيح للكادر العامل في الحاسبة، حماية فيزيائية لمكونات الحاسبة، إستراتيجية نسخ إضافية مناسبة (Backup)، الخ). أظهرت التجارب أن المحطات الطرفية هي الأجزاء الأكثر تعرضا للانتهاك من باقي أجزاء الحاسبة. معظم محاولات الوصول غير المشروعة تنشا من المحطات الطرفية. لغرض تقليص فرصة نجاح أي وصول غير شرعي، ويجب وضعها في بنايات أمينة (هذا الأجراء يؤدي إلى تقوية الأمنية الفيزيائية الجزئية)).

يستخدم التشفير لغرض حماية المعلومات التي يمكن أن يتم عليها وصول غير شرعي والتي تكون حالة المقاييس الأخرى للحماية غير كافية. لذلك فان التشفير يمكن تطبيقه لحماية قنوات الاتصال وقواعد البيانات الفيزيائية.

إن العملية الأولية (Primitive) لعلم التشفير هو عملية التشفير (Encryption) وهي عبارة عن عمليات حسابية خاصة تعمل على العبارات (Messages) وتحولها إلى تمثيل لا معنى له لكل الإطراف عدا المستقبل المقصود. إن التحويلات التي تعمل وتؤثر على العبارات هي معقدة الحل (صعبة الحل) بحيث أنها ابعد عن وسائل العدو لإبطال العمل. عملية التشفير (Encryption) هي عملية تحويل البيانات إلى صيغة بحيث تكون اقرب إلى عدم الإمكانية القراءة كلما أمكن ذلك بدون معرفة مناسبة (مثلا، وجود مفتاح). إن الهدف من هذه العملية هو ضمان الخصوصية (privacy) وذلك بالاحتفاظ بالمعلومات بصيغة مخفية من أي شخص أخر والذي هو غير الشخص المقصود، حتى أولئك اللذين يملكون وصول إلى البيانات المشفرة. من جانب أخر فان عملية فتح الشفرة (Decryption)هي عكس عملية التشفير، أي أنها عملية تحويل البيانات المشفرة إلى صيغتها الأصلية.

كل أنظمة التشفير الحديثة (Cryptosystems) في الغالب وبدون استثناء تعتمد على الصعوبة لعكس (Reverse) تحويل التشفير (Encryption) كقاعدة للاتصال الأمين (Secure Communication). إن التشفير الآن هو أكثر من

عملية التشفير وفتح الشفرة. إثبات الشخصية (Authentication) هو جزء أساسي من حياتنا والذي يمثل الخصوصية. نحتاج إلى تقنيات الكترونية لتوفير إثبات الشخصية. يوفر التشفير ميكانيكيات خاصة لمثل هذه الإجراءات. أما التواقيع الرقمية فإنها تقوم بربط وثيقة معينة إلى المعالج بمفتاح معين، بينما ختم الوقت (timestamp) فانه يربط الوثيقة مع منشئها في وقت معين. يمكن استخدام هذه التقنيات التشفيرية للسيطرة على الوصول إلى مشغل قرص مشترك أو أي وسط أخر.

يتم اختيار خوارزمية التشفير من بين مجموعة تحويلات معكوسة Invertible (Transformations) تدعى النظام العام (General System)، نظام التشفير (Cryptosystem) أو للسهولة يعرف نظام (System). إن العامل (Parameter) الذي يختار تحويل محدد من هذه التحويلات يدعى مفتاح التشفير (Enciphering Key) أو للسهولة مفتاح (Key). نعني بنظام التشفير (Cryptosystem) بأنه عبارة عن خوارزمية، زائدا كل النصوص المشفرة الممكنة، والمفاتيح الممكنة.

خلال عدة قرون تم إيجاد عدد من البروتوكولات المحكمة والميكانيكيات والتي تتعامل وتؤمن أمنية المعلومات عند تناقل المعلومات بواسطة وثائق فيزيائية(مادية). غالباً ما تكون أ هداف أمنية المعلو مات لايمكن تحقيقها فقط من

خلال الخوارزميات الرياضية و البروتوكولات لكن تتطلب تقنيات أجرائيه (Procedural Techniques) وكذلك الالتزام بالقواعد و القوانين لغرض الوصول إلى النتيجة المطلوبة. مثلاً، خصوصية الرسائل تكون مزودة بظروف مختومة، وقد يمكن أن تتعرض هذه العملية للإساءة وذلك باستخدام البريد من قبل شخص غير مخول (Not Authorized).

في بعض الأحيان فأن الأمنية يمكن تحقيقها ليس فقط من خلال المعلومات نفسها لكن أيضاً من خلال الوثيقة الفيزيائية المسؤولة عن تسجيل تلك المعلومات. إن طريقة تسجيل البيانات لم تتغير بصورة هامة خلال الفترات الزمنية التي حدثت في تطور البيانات أما من ناحية خزن المعلومات فقد كان يتم على الورق ثم تطور ليصبح الخزن على وسائط مغناطيسية ويمكن إرسالها من خلال أنظمة الاتصالات. إن التغيير الملحوظ الذي حصل هو إمكانية نسخ وتغيير محتويات المعلومات. الآن يستطيع أي مستفيد أن يعمل عدد من النسخ لجزء من المعلومات المخزونة إلكترونياً وان جميع النسخ الناتجة تكون مشابهة الى النسخة الأصلية. إن عملية خزن المعلومات على الورق تعتبر عملية صعبة، بينما خزن أو انتقال هذه المعلومات مع أجهزة إلكترونية يعتبر من العمليات المميزة. وبوجود هذه الحالة الأخيرة فانه يتطلب تأمين أمنية للمعلومات و التي لا تعتمد على الوسط الفيزيائي المستخدم لتسجيل ونقل المعلومات ولكن أهداف الأمنية تتحقق من خلال المعلومات نفسها.

تعتبر التواقيع الرقمية (Digital Signatures) أحد الأدوات الأساسية المستخدمة في أمنية المعلومات. و هذه هي الكتلة التي تبنى عليها العديد من الخدمات والتي منها على سبيل المثال لا الحصر عدم الإنكار، إثبات صحة مصدر البيانات، التعرف (Identification)، والشهادة (Witness). بعد تعلم أساسيات الكتابة، بالامكان التعلم على كيفية عمل توقيع كتابي (Handwritten) لغرض التعرف (Identification). وفي عمر التعاقد مع الاتصال فان التوقيع يتطور لكي يكون جزء متمم للهوية الشخصية (Identity). يرمي هذا التوقيع إلى إن يكون جزء مميز (Unique) للشخص ويخدم وسيلة للتعرف، التخويل (Authorization)، التثبت أو (Validation). باستخدام المعلومات الالكترونية فان فكرة التوقيع تحتاج إلى إعادة تحديد ; وهي إن تكون ببساطة شئ ما مميز للموقع (Signer) وتكون مستقلة عن المعلومات الموقع عليها. يعتبر الاستنساخ الالكتروني (Electronic Replication) للتوقيع هو أمر في منتهى البساطة

بحيث إن إضافة توقيع إلى وثيقة غير موقعة من قبـل منشأ التوقيـع أمر في غايـة التفاهة (Triviality).

يســـتخدم التوقيع الرقمي لغرض التعريف (Identification) بالأجزاء (مثل شـــخص معين، جهاز معين،.....) المطلوب التثبت من صـــحة تخويلها. اعتاد المســتفيدون على اســتخدام التواقيع اليدوية و التي أصــبحت تمثل غرض تعريفي لذلك الشـخص. يجب أن يكون التوقيع الرقمي مميز وفريد للمسـتفيد ويعتبر وسـيلة للتعريف، التخويل وكذلك التحقق (Validation). في المعلومات الرقمية فإن فكرة التوقيع تحتاج إلى إعادة نظر، إنها ليســت ببســاطة عبارة عن شــئ مميز للموقع (Signer) وغير معتمداً على المعلومات الموقعة.

لغرض الوصـــول إلى أمنية المعلومات في الوســـط الإلكتروني فإن ذلك يحتاج لعدد هائل من التقنيات و المهارات القانونية.

١-٩: تعريف: التشفير (Cryptography):

التشفير عبارة عن دراسة التقنيات الرياضية المتعلقة بعدد من مظاهر أمنية المعلومات مثل الوثوقية (Confidentiality)، تكامل البيانات (Data Integrity)، إثبات شخصية الكينونة (Entity Authentication) وإثبات شخصية مصدر البيانات (Data Origin Authentication).إن التشفير ليس عبارة عن وسيلة لتزويد أمنية المعلومات فقط وإنما عبارة عن مجموعة من التقنيات.

فكرة نظام التشفير (Cipher System) هي إخفاء المعلومات الموثوقة بطريقة معينة بحيث يكون معناها غير مفهوما للشخص غير المخول. وان أي شخص يعترض عبارة معينة (أي يحصل عليها) مرسلة من المشفر (Cryptographer) إلى مستقبل العبارة يسمى المعترض (Interceptor). إن هدف التشفير هو الزيادة (maximize) إلى الحد الأقصى لعدم الترتيب لغرض إخفاء المعلومات ،لذلك فان تقليص عدد الاختيارات الممكنة وذلك بمراقبة النماذج الثنائية الغير مقبولة تميل إلى امتلاك نوع من الترتيب .

يمكن إن يعرف التشفير أيضا على انه علم الكتابة السرية وعدم فتح شفرة هذه الكتابة السرية من قبل غير المخولين. بالنسبة لعلم التشفير كدراسة فانه يعود قدمه للاف السنين، وقد تم تطويره من قبل متخصصي الرياضيات، أمثال (Francois Vite 1540-1603) و (John Willias 1616-1703) . من وجهة نظر الرياضيات الحديثة، فانه يرى سمات للإحصاء (William F. Friedman 1920) والجبر (Lester S.Hill 1929) . في الحرب العالمية الثانية أصبح للرياضيات اهتماما كبيرا في هذا المجال، كمثال على ذلك (Hans Rohrbach 1903-1993) في المانيا و (Alan Mathison Turing 1912-1954) في إنكلترا، (A.Adrin Albert 1905-1972) و (Marshall Hall b.1910) كان لهما الاهتمام المتزايد في هذا الحقل في الولايات المتحدة .

القضايا الرياضية التي لعبت دورا مهما في علم التشفير الحالي تشمل نظرية الأعداد (Number Theory)، نظرية المجموعات (Group Theory)، المنطق (Combinatory Logic)، نظرية التعقيد (Complexity Theory)، ونظرية المعلومات (Information Theory). يمكن أن ينظر إلى حقل التشفير عل انه جزء من الرياضيات التطبيقية وعلم الحاسبات. على العكس من ذلك، فان علماء الحاسبات اللذين يعملون على التشفير قد أصبح لهم اهتمام عملي متزايد بما يتعلق بأنظمة التشغيل، قواعد البيانات، وشبكات الحاسبات، مشتملا ذلك تناقل البيانات. إن الجزء الأكبر من عمل الأمنية هو معرض للانتهاك

معتمدا في ذلك على الذكاء الناتج من حل رموز عالية الدرجة وكذلك الشـــفرات. يرتبط علم التشفير أيضا ارتباطا مباشرا مع علم الإجرام (Criminology). هناك العديد من المصادر التي تتطرق إلى علم الإجرام، واعتياديا مرفق معها تقارير تؤكد نجاح عمليات تحليل الشفرة وإدارتها.

أصـبح هناك اهتمام تجاري في التشـفير بعد اكتشـاف التلغراف والمتركز على إنتاج كتب للرموز (Code Books)، وبعد تصـــميم وتركيب ماكنات التشـــفير الميكانيكية والالكترونية. اســـتخدم الحاســـبات الالكترونية بعد ذلك لغرض كســـر الشـــفرات وأصـــبحت هناك محاولات ناجحة لكســـر الشـــفرات في الحرب العالمية الثانية.تعتبر الحاسبـــات المبرمجة أجهزة ملائمة بشكل كامل كماكنة تشفير ، لكن هذه الحالة لم يكن ممكنا انتشارها بسرعة في الاتصالات الخاصة بسبب الأدلة التي تثبت أن التشفير هو علم معلن.

١-١٠ : أهداف التشفير (Cryptographic Objectives):

١- الخصوصية أو السرية (Privacy or Confidentiality): الاحتفاظ بسرية المعلومات عن الجميع باستثناء الذين لديهم صلاحية للاطلاع عليها .

٢- تكاملية البيانات (Data Integrity) : التأكد من أن المعلومات لم تتغير مـــن قبل أشخاص غير مخولين أو بواسطة طرق غير معروفة .

٣- إثبات شخصية الكينونة أو التعرف (entity authentication) : التثبت من هوية الكينونة (شـــخص ما ، محطة حاســـبة طرفية ، بطاقة أتمان (Credit Card)

٤- إثبات شخصية الرسالة (Message Authentication):التثبت من مصدر البيانات وهو أيضا يعرف بإثبات شخصية مصدر البيانات .

٥-التوقيع (Signature): طريقة لربط المعلومات الى كينونة .

٦- الصـــلاحية (Authorization) : نقل الصـــلاحية إلى كينونة أخرى أو قرار معتمد لفعل شئ ما .

٧- مدي الصـــلاحية (Validation) : وســـائل لتوفير ســـقف زمني للصـــلاحيات المخولة لاستخدام او معالجة المعلومات أو مصادرها .

٨- ســـيطرة الوصـــول (Access Control) : حصـــر الوصـــول الى المصـــادر للكينونات المخولة أو ذات الامتياز (Privileged) .

٩- تصـــديق (Certification) : المصـــادقة على المعلومات بواســـطة كينونة موثوقة .

١٠ –إثبات الوقت Timestamping : تسجيل وقت إنشاء المعلومات الموجودة .

١١- الشـهادة (Witness): البرهنة على إنشـاء أو وجود معلومات مامع الكينونة .

١٢- الاستلام (Receipt) - الاعتراف بان المعلومات قد استلمت .

١٣ - التؤكيد Confirmation - الاعتراف بان المعلومات قد أرسلت .

١٤ - الملكيـة Ownership -وســـيلـة لتوفير الحق القـانوني للكينونـة في نقـل المصدر الى الآخرين .

١٥ - إخفاء الشـــخصـــية (Anonymity) : إخفاء هوية الكينونة المشـــتركة في بعض العمليات.

١٦ - عدم الإنكار(Non-Repudiation) : منع الإنكار عن التزامات ســـابقة او أفعال .

١٧ - الإلغاء (Revocation) : سحب التأييد او الصلاحية .

علي العموم امنية كل من انظمة المشـــاركة الزمنية وشـــبكات الحاســـبة تتالف من ثلاث مكونات:

- امنية مركز (او مراكز) الحواسيب .
- امنية المحطات الطرفية .

امنية قنوات الاتصال .

وضع هذه الأهداف بأربعة أطر وهي:

١- الوثوقية (Confidentiality) : هي عبارة عن خدمة معينة تمنع من خلالها معرفة محتويات المعلومات عن جميع المشتركين عدا الأشخاص المخولين بامتلاك هـذه المعلومـات . يعتبر مفهوم الأمنيـة (Secrecy) مرادفـا لكـل من الوثوقيـة والخصوصية (Privacy).

٢- تكامل البيانات (Data Integrity) عبارة عن خدمة موجهة لإغراض احتواء التغييرات الغير مســـموح بها (Unauthorized) للبيانات ولتحقيق هذا الهدف يجب تمتلك الإمكانية لكشـف معالجة البيانات من قبل الأطراف الغير مخولة. تشـــمـــــل معالجـة البيانـات عمليات مثل الحشـــر (Insertion)، الحذف (Deletion) والإحلال (Substitution). يجب أن يكون مستقبل الرسـالة قادرا

على إثبات أن العبارة لم يتم تحويرها أثناء الإرســـال و أن العدو يجب أن لا يكون قادرا على إحلال عبارة كاذبة بدلا من عبارة شرعية.

٣- إثبات الشـــخصـــية (Authentication) :عبارة عن خدمة أو وظيفة تتعلق بتحقيق التعريف (Identification) ،هذه الوظيفة تطبق على كل من المشـتركين في الاتصال (Two Parties) وعلى المعلومات أيضا حيث أن الأطراف المشتركة عند الاتصـــال عليها أن تعرف بعضـــها إلى البعض الأخر . أما ما يخص المعلومات المستلمة فيجب أن تطابق شخصياً المعلومات الأصلية التي أرسلت وكذلـــك تاريخ إرســـــال المعلومات ومحتويات المعلومات ووقت الإرسـال، لهذه الأسـباب يقسـم التشفير اعتماداً على الخاصية أعلاه إلى صنفين رئيسين هما :

أ - إثبات شخصية الكينونة (Entity Authentication) .

ب - إثبات شخصية مصدر البيانات (Data Origin Authentication).

أن طريقة إثبات شخصية مصدر البيانات تزودنا ضمنياً بتكامل البيانات (Data Integrity).

نستنتج من هذا انه في إثبات الشخصية يجب أن يكون ممكنا لمستقبل العبارة أن يتحقق من مصدرها ; وان العدو يجب أن لا يكون قادرا على التنكر بأنه شخص معين أخر.

٤: عدم الإنكار (Non- Repudiation) : عبارة عن خدمة أو وظيفة والتي تمنع أي كينونة (Entity) من أن ينكر أي تعهد أو عمل ســـابق تم أجرائه . لذلك عند حصول مثل هذا النـــزاع (Dispute) بين الأطراف المشتركة في إنكار ما تم اتخاذه من أعمال فيجب توفير وسـيلة معينة لحل هذا النزاع. يتم توفر هذه الوسـيلة من خلال أجراء معين يتضـمن إشـراك طرف ثالث موثوق. يجب على المرسـل أن لا يكون قادرا على الإنكار الكاذب بعد فترة ويدعي انه قد أرسل عبارة.

أن الهدف الأسـاسـي للتشـفير هو تحديد هذه الأهداف في كل من الجانب النظري والعمليات.

الشكل ١.١ يوضح أساسيات التشفير وكيفية ارتباطها :

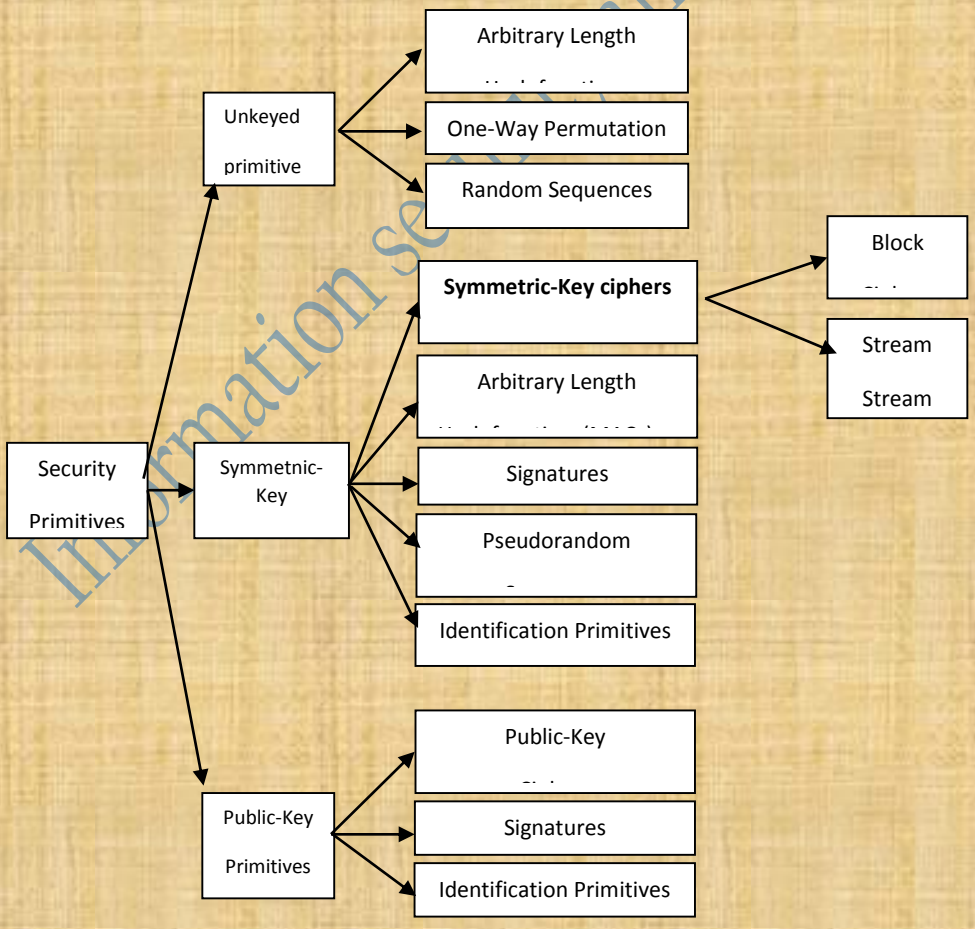
إضافة إلى ذلك فان هدف التشفير هو لجعل الرسالة أو السجل غير قابل للإدراك من قبل الأشـخاص غير المخولين. إن أي محاولة لإعادة تشـفير (re-encipher)، إعادة إر سال نفس الر سالة – بصورة صحيحة ، فانه في هذه الحالة يمثل خطر امني كبير ، لذلك يجب أن يكون هناك تجاه تشفيري متشدد لمنع مثل هذه الحالات .

هناك أدوات تشفير والتي تدعى أحيانا (الأساسيات) أو الأوليات Primitives) والتي تســـتخدم في توفير أمنية المعلومات وان هذه الأدوات يمكن تخمينها (أو تقييمها Evaluated) من خلال عدة مظاهر مثل :

١- مستوى الأمنية (Level of Security) : هذه الخاصية من الصعوبة التعبير كميـــــا عنهـــــا (Quantity) . غالبا ما تعطى بمفردات اومفاهيم عدد العمليات المطلوبة (باستخدام أحسن الطرق المعروفة حاليا) لكي يحبط الأهداف المضادة. يعرف مستوى الأمنية مثاليا من خلال حد أعلى لكمية العمل الضروري لإحبـــــاط الأهداف المضادة وهذا أحيانا يسمى عامل الشغل (Work Factor).

٢- الوظيفية (Functionality) : أن الأوليات (Primitives) تحتاج لان تدمج لغرض مواجهة أو تحقيق عدد من أ هداف الأمنية . ويتم اختيار أي من الأوليات من خلال فعالية تلك الأوليات. ماهو أي من الأســـاســـيات الأكثر فعالية ســـيحدد الخصـائص الأســاسـية للأوليات والأولية التي سـيتم اختيارها هي تلك التي تتميز بفعالية أكثر.

شكل ١.١ : تصنيف أهداف التشفير



٣- طرق العمل (Methods of Operation):عند استعمال الأوليات في طرق متنوعة ومدخلات متنوعة فأنها تظهر لنا خصائص أو ميزات مختلفة. لهذا فأنه قد يكون بامكان احد هذه الأوليات تزويدنا بعدد من الوظائفية معتمداً على أسلوب (Mode) العملية الوظيفية أو الاستعمال.

٤-الأنجازية (Performance): أنها تشير إلى كفاءة واحد من الأوليات في أسلوب تشغيلي أو وظائفي معين (Mode of Operation) ،كمثال على ذلك فأن خوارزمية تشفير قد تقاس (Rated) بعدد البتات(Bits)في الثانية الواحدة والتي يمكن تشفيرها .

٥- سهولة الاستخدام (Ease of Implementation) . هذا يشير إلى صعوبة التحقق من أن الأولية (Primitive) في حالة جاهزية عملية وهذا يشتمل على تعقيد في تنفيذ الأولية أما في صيغة برمجيات أو ماديا (Hardware).

١-١١ :مصطلحات فنية وأفكار أساسية (Basic and Concepts Terminology):

أن المتخصص في موضوع التشفير عليه أن يلم ببعض المصطلحات والأفكار المستخدمة من اجل الوصول إلى فهم لما يتم تنفيذه من خلال خوارزميات التشفير المختلفة.

إن نظام التشفير قد يأخذ صيغة واحدة من بين عدة صيغ، مثلا مجموعة ايعازات، جزء من مكون مادي (Hardware) أو برنامج، واحد هذه الصيغ يتم اختياره بواسطة مفتاح التشفير.

١: مجالات التشفير (Encryption domain and codomains)

١st- تشير إلى مجوعة محددة يطلق عليها أبجدية التعريف (Alphabet of Definition) ، كمثال على ذلك A={0,1} ، تسمى الابجدية الثنائية (Binary Alphabet) . كما هو معروف فأن كل حرف أبجدي يمكن تمثيله بسلسلة من الأرقام الثنائية .

M: تشير إلى مجموعة تسمى مساحة العبارة (Message Space). تتكون M من سلسة من الرموز ضمن مجموعة الحروف الأبجدية وأي عنصر في M يسمى العبارة الواضحة (Plaintext Message) أو باختصار النص الواضح (Plaintext) لذلك فقد تكون M سلسلة من الأرقام الثنائية أو رموز حسابية (Computer Codes).

C: تشير إلى مجموعة تسمى مساحة التشفير (Ciphertext Space) ومتكونة من سلسلة من الرموز المكونة للحروف الأبجدية والتي تختلف صيغتها أو شكلها (Form) عن العبارة الأصلية (M) . أن أي عنصر من Cيسمى النص المشفر (Ciphertext).

١ -١٢: التحويلات التشفيرية (Encryption and Decryption Transformations):

K : يشير إلى مجموعة تسمى مساحة المفتاح (Key Space)، كل عنصر من k يسمى مفتاح (Key) .

كل عنصر e تابع إلى k (e ε k) يحدد لنا عنصر من M إلى C ويطلق عليها E_e حيث تسمى دالة التشفير. يجب أن تعمل E_e في كلا الاتجاهين أي أنها تمكن من تحويل نص وضح إلى مشفر وبالعكس (Bijection).كل عنصر d تابع إلى

k (d ∈k) ، فأن التعبير D_d يشير إلى إمكانية تحويل C ألى M (بمعنى آخر m → C D_d:) ويطلق عليها دالة فتح الشفرة) أو تحويل فتح الشفرة (Decryption Transformation) . أن عملية تطبيق دالة E_e إلى عبارة m (m ε M) عادةً ما تشير إلى تشفير العبارة m أما عملية تطبيق الدالة . D_d إلى عبارة مشفرة c (c ε C) فيشار لها بإعادة فتح التشفير للعبارة c .

طريقة التشفير تتألف من مجموعة تحويلات التشفير (E_e: e ∈ K) وما يقابلها من مجموعة (D_d: d ε K) من تحويلات فتح الشفرة وبخاصية أن كل e ∈k يوجد مفتاح واحد d ∈k بحيث ان $D_d=E^{-1}_e$ وبمعنى أخر :

$$D_d=(E_e(m))=m$$

لكل عنصر m ∈M . يطلق على مفهوم التشفير أحيانا بالشفرة (Cipher) .

المفاتيح e و d يشيران إلى زوج مفتاح ويشار له أحيانا بـ (e ,d) يمكن أن يكون e و d متساويان .

وعلى هذا الأساس ولغرض بناء نظام تشفير فنحتاج إلى مايلي:

١- مساحة العبارة الواضحة M.

٢- مساحة العبارة المشفرة C .

٣- مساحة المفتاح K.

٤- تحويلات التشفير $E_e: c \in K$.

٥- تحويلات فتح الشفرة $D_d. :d \in K$.

كل تحويل تشـــفير $E_{k'}$ يعرف بواســـطة خوارزمية تشـــفير E والتي هي عامة للجميع ومفتاح K' والذي يميزها عن باقي التحويلات (أي أن المفتاح يميز طريقة تشفير عن أخرى) ، بينما تحويل فتح الشفرة هو معكوس تحويل التشفير .

تســـمى خوارزمية التشـــفير أيضـــا شـــفرة (Cipher) ، والتي هي الوظيفة الرياضـــية المســـتخدمة في عملية التشـــفير وفتح الشـــفرة . إذا كانت أمنية أي خوارزمية معتمدة على الحفاظ على أســـلوب أو طريقة تعمل الخوارزمية بســـرية، فإنها تســـمى خوارزمية مقيدة (Restricted Algorithm). أخذت الخوارزميات المقيدة اهتماما تاريخيا، لكنها الآن غير ملائمة لمقاييس الوقت الحاضـــر حيث تتضـــمن الكثير من المســـاوىء، فانه مثلا إذا حدث وان شـــخص ما اكتشـــف صـــدفة أمنية الطريقة، فانه أي شخص يستطيع تغيير الخوارزمية. التشفير الحديث حل هذه المشكلة باستخدام المفتاح (Key) ويشار له بـــ k . هذا المفتاح قد يكون أي عدد كبير من القيم. مدى المفاتيح الممكنة يسمى مساحة المفتاح (Key Space). كل الأمنية المســـتخدمة تعتمد على المفتاح (أو المفاتيح)، ولا تعتمد على تفاصـــيل الخوارزمية. هذا يعني أن الخوارزمية يمكن أن تعلن وتحلل.

أنظمة التشفير يجب أن تحقق ثلاث متطلبات عامة :

١ : تحويلات التشفير وفتح الشفرة يجب أن تكون كفؤة لكل المفاتيح.

٢ : النظام يجب أن يكون سهل الاستعمال.

٣: أمنيـــة النظـــام يجـــب أن تعتمـــد فقط على أمنيـــة المفـــاتيح وليس على أمنيـــة الخوارزمية E ، D .

١-١٣ : المبادئ العملية الأساسية في نظام التشفير المستخدم في الجيوش:

الشـــفرة المســـتخدمة في الجيوش يجب أن تحقق أهدافا عملية طبيعية تتناســـب والواجبات المناطة بها والظروف القائمة أو المحيطة، حيث يتطلب تحقيق مايلي في نظام التشفير المستخدم:

١ : الموثوقية أو التعويل (Reliability)،

٢: الأمنية (Secrecy) ،

٣: السرعة (Rapidity) ،

٤: المرونة (Flexibility) ،

٥: الاقتصاد (Economy) .

تكون أهمية هذه المتطلبات نسبية، ولكن بشكل عام فان ترتيبها يدل على أهميتها. فالموثوقية المطلوبة في نظام التشفير وأجهزته تعني إجراءات التشفير عند تطبيقها على نصوص واضحة ومحولة إلى نصوص مشفرة، يجب أن تتمكن الجهة المستلمة للنص المشفر من حل الشفرة بفترة زمنية مناسبة بشكل صحيح وبدون التباس والحصول على النص الأصلي كاملا. أما الأمنية فإنها تعني حماية المعلومات المرسلة بواسطة نظام التشفير. السرعة تعني سرعة تشفير الرسائل والمعلومات وسرعة حلها والحصول على النص الواضح .

هناك علاقة قوية بين الأمنية والسرعة فتزداد احدهما على حساب الأخرى ووفقا للظروف والمتطلبات الأخرى التي توفق بين الأمنية والسرعة . إن أقصى حد من الأمنية في اغلب الأوقات تكون هي الهدف وخاصة بالنسبة للمعلومات المهمة، لذلك يضحى بالسرعة لإعداد درجة كبيرة من الأمنية.

١ ـ١٤ : تحليل الشفرة (Cryptanalysis):-

إن الجهد الكامل للتشفير هو الحفاظ على النص الواضح (أو المفتاح، أو كلاهما) بصورة سرية من المتنصتين (أو ببساطة يسمون الأعداء). إن الأعداء تم افتراضهم على أنهم يملكون كامل الوصول إلى الاتصالات بين المرسل والمستقبل.

تحليل الشفرة عبارة عن دراسة التقنيات الرياضية لغرض الإستفادة منها في محاولة التعرض أو إحباط (Defeat) التقنيات التشفيرية، أي بمعنى أخر لكسر الشفرات. تكون الشفرة قابلة للكسر إذا كان بالا مكان تحديد النص الواضح آو المفتاح من النص لمشفر، أو تحديد المفتاح من زوج المعلومات النص الواضح – النص المشفر. إن تحليل الشفرة هو علم استرجاع النص الواضح لعبارة معينة بدون الوصول إلى المفتاح. تحليل الشفرة الناتج قد يسترجع النص الواضح أو المفتاح. قد يوجد ضعف في نظام التشفير والذي في الأخير يؤدي إلى نتائج سابقة (فقدان المفتاح خلال وسائل غير تحليلية يسمى التعرض (Compromise) .

يجب ملاحظة أن المفاتيح التشفيرية والنصوص الواضحة التي تملك انتظامات متوقعة تكون ضعيفة بسبب أنها تنتج نصوص مشفرة والتي يمكن تحليلها لكشف أما النص الواضح أو المفتاح .

إن علم التشفير (Cryptography) يتعامل مع التصميم والتحليل للأنظمة التي توفر اتصالات أمينة (Secure) أو عليه مقاومة علم تحليل الشفرة (Cryptanalysis) . إن أي نظام يطلق عليه انه معرض للخطر أو الانتهاك (Compromised) بواسطة علم تحليل الشفرة إذا كان بالامكان استرجاع العبارة الأصلية أو النص الواضح من النص المشفر بدون معرفة المفتاح المستخدم في خوارزمية التشفير . يتعلق علم فتح الشفرة بتخصص عالي للرياضيات التطبيقية حيث يأخذ فرع منها مثل نظرية الاحتمالية ، نظرية الأعداد ، الإحصاء والجبر . يجب على محلل الشفرة (Cryptanalyst) أن يكون ذو قبلية كبيرة جدا في كل هذه الحقول وان لديه القدرة على استيعابها جيدا . كذلك فان على محلل الشفرة أن يحصل على فوائد من المعلومات الثانوية حول النظام مثلا طبيعة خوارزمياته ، لغة الاتصال ، أو محتوى و سياق العبارات والصفات الإحصائية للغة النص الواضح (مثلا ، الحشو Redundancy) .

إذا امتلك المفتاح تسلسل منتظم والذي يمكن استنتاجه من فحص النص الواضح ، فان محتويات على الأقل بعض من النص الواضح يمكن استرجاعه من قبل محلل الشفرة . علاوة على ذلك ، فان محلل الشفرة قد يكون قادرا أيضا على استنتاج الخوارزمية التي أنتجت المفتاح ، والتسلسل المستخدم لبدايتها . مثل هذا المفتاح يعتبر ضعيفا . أمثلة على المفاتيح الضعيفة هي تلك المفاتيح التي تستخدم تنفيذ طويل للواحدات او الاصفار . على كل حال ، فان أي مفتاح يمكن اعتباره ضعيفا إذا امتلك مايلي : الانتظامات الإحصائية ، له هيكل أو تركيب واضح ، يظهر التماثل ، أو يمكن توقعه في وقت متعدد الحدود.

تعتبر مشكلة علم فتح الشفرة هي مشكلة تعريف النظام (System Identification Problem) وان هدف علم التشفير هو بناء أنظمة والتي يصعب التعرف عليها . على نظام التشفير بناء أنظمة تشفيرية بحيث تتصف بالصعوبة من اجل ا التعرف عليها .

من هنا يمكن القول أن التشفير هو عملية تصميم أنظمة التشفير . وتحليل الشفرة (Cryptanalysis) هو الا سم المعطى لعملية ا ستنتاج النص الوا ضح من النص المشفر بدون معرفة المفتاح . في الواقع العملي فان محلل الشفرة غالبا ما يكون مهتما أيضا باستنتاج المفتاح إضافة إلى النص الواضح . يشمل مصطلح الـ

(Cryptology) كلا من علم التشـفير (Cryptography) وعلم تحليل الشـفرة (Cryptanalysis) .

وفقا لما حدده فريندمان (William F. Friendman) ، فان تحليل الشفرة يشتمل على تحديد اللغة المستخدمة ، نظام التشفير العام ، المفتاح المحدد ، والنص الواضح .يحتاج تحليل الشفرة إلى تطبيق الوسائل الصحيحة في الموضع الصحيح . من الشائع لتحليل الشفرة ، فان المسالة المطروحة هي ليست فقط الجهد المبذول ، لكن كذلك الوقت المتوفر .

التشفير وتحليـل الشفرة هما مظهـران مـن مظاهـر دراسـة علم التشفير (Cryptology) ، كل منهما يعتمد على الآخر ويؤثر احدهما في الآخر في تفاعل معين لغرض وضـع تحسينات لتقوية أمنية تحليل الشـفرة من جانب واحد والجهود لجعل هجومات أكثر كفاءة من جانب آخر . يكون من النادر الحصـول على النجاح في هذه المهمة ، حيث أن عملية الفشـل هي الشـائعة في هذا المجال . كل الجهود الرئيسـة التي وضـعت في الحرب العالمية الثانية قد نجحت – على الأقل بين فترة وأخرى – في حل أنظمة تشـفير العدو ، لكن كل هذه المحاولات في بعض الأحيان تواجه دفاعات ، على الأقل جزئيا . إن هذه الأشـياء سـوف لاتكون مختلفة كليا في القرن الحادي والعشرين .

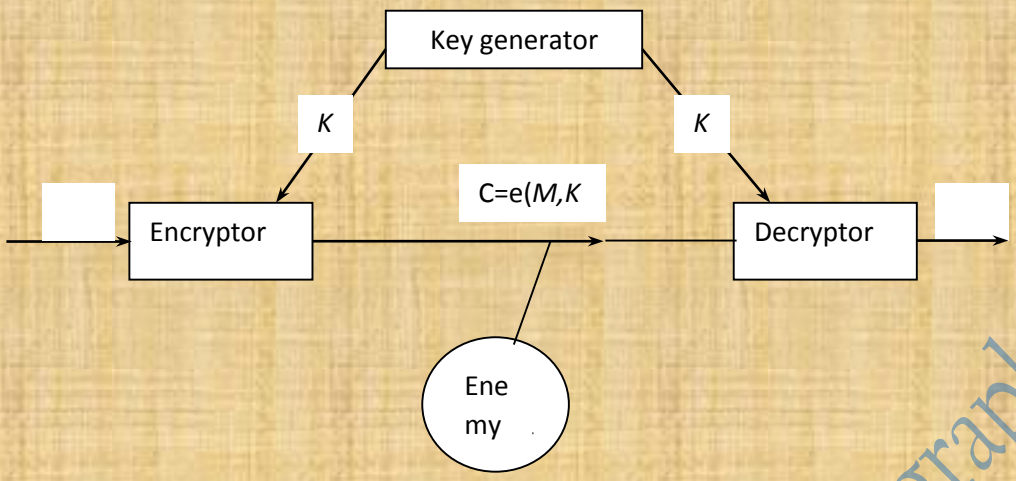
إن لمحلل الشـفرة في بعض الأحيان وقت كافي لإنجاز عمله ، حيث لا توجد شـفرة لايمكن كسـرها ، هذه العبارة يجب طبعا إثباتها بدرجة معقولة . إن قول بول ريفرز المشـهور " اذا كان الرقم واحد يعني البر والرقم اثنان يعني البحر ، لايمكن كسر هذه الشفرة من قبل البريطانيين حتى ولـو استخدمـوا أحدث الحاسبات الالكترونية ، والسبب في ذلك هو عدم توفر المعلومات الكافية " .

تجدر الإشارة إلى أن التقديرات الحسابية بالنسبة لمعدل أو الوقت المطلوب لفك نظام تشفير المعلومات محددة بالوقت الذي يستغرقه جهاز حاسبة الكترونية كبيرة لإيجاد كافة رموز الرقم الأصلية بحجم الكلمة المراد تحويلها .

الآن لنعرف ماذا يعني كسر نظام تشفيري . محلل الشفرة ، أو العدو كما يطلق عليه في المعتاد ، فانه يفترض في هذا العدو أن تكون لديه المعرفة الكاملة بدالة التشفير e ودالة فتح الشفرة d . بالإضافة إلى ذلك ، فان هذا العدو قد يملك العديد من المعلومات الجانبية (الإضـافية) مثلا إحصـائيات اللغة ، معرفة بمحتوى موضوع الرسالة ، الخ .

إن العدو بالتأكيد لديه بعضـا من النص المشـفر ، لكن جميع الأعداء يعوزهم المفتاح والذي منه يسـتطيع أن يسـتخدم d لغرض فتح الشـفرة C بنجاح . هذه الحالة موضحة في الشكل ١ .٢ .

شكل ١. ٢: فعاليات العدو لكسر الشفرة .



١-١٥ : أمنية الخوارزميات (Security of Algorithms):

توفر الخوارزميات المختلفة درجات مختلفة في الأمنية ، إنها تعتمد على مقدار الصعوبة المطلوبة لغرض كسر هذه الخوارزميات ، إذا كانت الكلفة المطلوبة لكسر خوارزمية معينة اكبر من قيمة البيانات المشـــفرة ، عند ذلك فانه من المحتمل أن تكون هذه الخوارزمية أمينة . إذا كان الوقت المطلوب لكسر خوارزمية معينة اكبر من وقت البيانات المشـفرة لبقائها أمينة ، عند ذلك فإنها قد تكون خوارزمية أمينة . إذا كانت البيانات المشـفرة بمفتاح مفرد اقل من كمية البيانات الضـرورية لكسـر الخوارزمية ، فعند ذلك من المحتمل أن تكون أمان . يقال من " المحتمل " بسـبب انه يوجد دائما هجومات جديدة في تحليل الشـــفرة . من ناحية أخرى ، فان قيمة معظم البيانات تتناقص مع الزمن . انه من المهم جدا أن تكون قيمة البيانات دائما اقل من الكلفة المطلوبة لكسر الأمنية المطلوبة لحمايتها .

صـنف العالم كيندسـن (Lars Knudsen) الأنواع التالية من الكسـر لأي خوارزمية :

١) الكسر الكلي (Total Break) : محلل الشفرة يجد المفتاح ، k ، بحيث ان $D_k (C) = P$

٢) الاستنتاج العام (Global Deduction): محلل الشفرة يجد خوارزمية بديلة ، A ، مكافئة إلى D_k (C)، بدون معرفة المفتاح K.

٣) الاستنتاج المحلي (Instance (Local) Deduction): محلل الشفرة يجد النص الواضح لنص مشفر مفترض .

٤) استنتاج المعلومات (Information Deduction) : محلل الشفرة يحصل على بعض المعلومات حول المفتاح أو النص الواضح . هذه المعلومات يمكن أن تكون بتات قليلة من المفتاح ، بعض المعلومات حول صيغة النص الواضح ، والخ .

يقال عن الخوارزمية أنها أمينة غير مشروطة (Unconditional Secure) في حالة مهما تكن كمية النص المشفر الذي يملكه العدو ، كأن لا يوجد معلومات كافية لغرض استرجاع النص الواضح . في الواقع ، فان فقط شفرة الوسادة (One –Time Pad) هي غير قابلة للكسر معطية موارد غير محددة . كل أنظمة التشفير الأخرى هي قابلة للكسر في هجوم النص المشفر فقط ، وذلك ببساطة بمحاولة البحث عن كل المفاتيح الممكنة واحدا بعد الآخر و تدقيق فيما إذا كان النص الواضح الناتج ذو معنى . هذا يطلق عليه هجوم القوة الوحشية (Brute Force Attack) .

يبدي علم التشفير اهتما متميزا وأكثر بأنظمة التشفير التي هي حسابيا متعذرة الكسر . إن الخوارزمية تعتبر أمينة حسابيا (Computationally Secure) (أحيانا يطلق عليها قوية) إذا لم يكن بالامكان كسرها بالموارد المتوفرة ، أما حاليا أو في المستقبل . إن ما تحتويه الموارد المتوفرة يكون مفتوحا للاعتراض .

يمكن قياس التعقيد لأي هجوم بعدة وسائل مختلفة :

١) تعقيد البيانات (Data Complexity) : كمية البيانات المطلوبة كمدخل إلى الهجوم .

٢) تعقيد المعالجة (Processing Complexity) : الوقت المطلوب لتنفيذ الهجوم ، هذا غالبا ما يطلق عليه عامل الشغل (Work Factor) .

٣) متطلبات الخزن (Storage Requirements) : كمية الذاكرة المطلوبة لتنفيذ الهجوم .

١٦-١ : شفرة الوسادة الكاملة (ONE –TIME PADS):

هناك طريقة تشفير تتصف بأنها ذات أمنية تامة ، يطلق عليها شفرة الوسادة (One –Time Pad) تم اكتشافها في ١٩١٧ من قبل (Major Joseph

One – Time Pad اعتياديا ، فان شفرة الوسادة (Gilbert Vernam ، Maubrgne Threshold) هي عبارة عن حالة خاصة من طريقة البداية (Scheme) . من الناحية الكلاسيكية ، فان شفرة الوسادة (One –Time Pad) ليست إلا مجموعة من عدم التكرار كبيرة من حروف المفتاح العشوائية . يستخدم المرسل كل حرف من حروف المفتاح على وسادة (Pad) لغرض تشفير حرف واحد فقط من النص المشفر . يتم التشفير باستخدام أسلوب الجمع بباقي ٢٦ (Module 26) للنص الواضح وحرف المفتاح لشفرة الوسادة ـ (One –Time Pad) .

كل من المفتاح يستخدم بالضبط لمرة واحد ، ولعبارة واحدة فقط . يقوم المرسل بتشفير العبارة وبعد ذلك يرمز الصفحات المستخدمة للوسادة أو يستخدم نفس المقطع في الشريط .

مثال ١ـ١ :

إذا كانت العبارة هي : ONETIMEPAD

وان سلسلة المفتاح من الوسادة هي : TBFRGFARFM

عند ذلك فان النص المشفر هو : IPKLPSFHGQ

بسبب أن :

O + T mod 26 = I

N + B mod 26 = P

E + F mod 26 = K

وهكذا

افرض أن المتنصت (Eavesdropper) لا يستطيع الوصول إلى الـ (One – Time Pad) المستخدمة لتشفير العبارة ، فان هذه الطريقة هي أمينة بالكامل (Perfectly Secure) لعبارة نص مشفر معين فانه متساوي مع أي عبارة نص واضح ممكن مقابل كانتا بنفس الحجم .

بسبب أن كل تسلسل مفتاح هو احتمال متساوي (تذكر ، أن حروف المفتاح تولد عشوائيا) ، فان العدو لا يملك معلومات والتي بواسطتها يستطيع تحليل النص المشفر .

١-١٧ : أفكار رياضية:

١: نظريـة المعلومـات (Information Theory): تم الإعلان عن نظريـة المعلومـات الحـديثـة لأول مرة في العـام ١٩٤٨ من قبـل شـــانون (Claud Elmwood Shannon) وقد تم إعـادة أوراقـه البحثية من قبل IEEE .

٢: الانتروبي وعدم الدقة (Entropy And Uncertainty) : نظرية المعلومات تعرف كمية المعلومات (Amount of Information) في عبارة معينة بأنها العدد الأدنى من البتات المطلوبة لغرض ترميز (Encode) كل المعاني الممكنة لتلك العبارة .

تقاس كمية المعلومات في عبارة معينة M بواسطـة الانتروبي للعبارة ، يرمز لهـا H (M) .

من الناحية التاريخية ،فانه في العام ١٩٤٩ ، فان شـانون أوضـح الترابط بين الانتروبي لنظـام الحركـة الحراريـة ونظريـة الاتصـالات . منـذ ذلـك الوقت فـان الانتروبي اسـتخدمت كمقياس لمحتويات المعلومات . في الأنظمة الفيزيائية ، فان الانتروبي عبارة عن مقياس لعدم توفر الطاقة ، درجة العشـوائية ، وميل النظام الفيزيـائي لان يصبـح معرضـا للانتهـاك . لذلك ، فان الانتروبي تستخدم لقياس محتويات المعلومات ، محتويات المعلومات المرتبطة مع عدم الدقة ، وعدم الدقة التي تصف المظهر الأساسي للعشوائية .

على العموم ، فان الانتروبي لأي عبارة مقاسة في Bits هو $\log_2 n$ ، حيث n هو عـدد المعـاني الممكنـة .الانتروبي لعبـارة معينـة تقيس أيضـا عـدم دقتهـا (Uncertainty) ، وهي عدد بتات النص الواضـح المطلوب اسـترجاعها عندما العبارة تجمع في نص مشفر لغرض معرفة النص الواضح .

٣: معدل اللغة (Rate Of Language) : معدل اللغة هو :

$$r = H(M) / N$$

حيث N هو طول العبارة . معدل اللغة الإنكليزية يأخذ عدة قيم مختلفة بين 1.0 bits /letter و 1.5 bits / letter بالنسبة إلى قيـم كبيرة لـ N . أكد شانون أن الانتروبي تعتمد على طول النص .

المعدل المطلق (Absolute Rate) لأي لغة هو العدد الأقصى لعدد البتات التي يمكن ترميزها في كل حرف . إذا كان هناك L من الحروف في لغة معينة ، فان المعدل المطلق هو :

$$R=\log_2 L$$

هذا هو الانتروبي الأقصى للحروف المستقلة . بالنسبة للغة الإنكليزية فان المعدل المطلق هو $\log_2 26$ ، او حوالي 4.7 bits /letters .

الحشو (Redundancy) لأي لغة ، ويرمز لها D ، تعرف كالآتي :

$$D= R-r$$

إذا كان المعدل في اللغة الإنكليزية هو ١.٣ ، فان الحشو هو 3.4 bits /letters . هذا يعني أن كل حرف في اللغة الإنكليزية يحمل 3.4 من المعلومات المتكررة .

٤: مسافة الوحدة (Unicity Distance) : بالنسبة لأي عبارة بطول n ، فان عدد المفاتيح المختلفة والتي سوف تفتح شفرة عبارة نص مشفر إلى نص واضح ذو معنى بنفس اللغة الأصلية فان هذا العدد (عدد المفاتيح المختلفة) يعطى بالصيغة التالية :

$$2^{H(K) - nD} - 1$$

عرف شانون مساحة الوحدة (Unicity Distance) ، U ، وأطلق عليها كذلك نقطة الوحدة (Unicity Point) ، بأنها التقريب لكمية النص المشفر بحيث أن مجموع المعلومات الحقيقية (Entropy) في النص الواضح المقابل زائدا الانتروبي لمفتاح التشفير يساوي عدد بتات النص المشفر المستخدمة .

في معظم أنظمة التشفير التناظرية (symmetric systems) ، فان مساحة الوحدة تعرف كالآتي :

$$U = H (K) / D$$

تؤدي مسافة الوحدة إلى ضمان عدم الأمنية (Insecurity) إذا كانت صغيرة جدا ، لكن لا تضمن أمنية إذا كانت عالية .

الجدول ١.٢ يعطي مسافات الوحدة لمختلف الأطوال.

٥: نظرية التعقيد (Complexity Theory) : نظرية التعقيد توفر طريقة منهجية لتحليل التعقيد الحسابي لمختلف التقنيات التشفيرية والخوارزميات . انها تقارن الخوارزميات التشفيرية والتقنيات وتحدد امنيتها . نظرية المعلومات تخبرنا ان كل

الخوارزميات التشفيرية (عــدا شفرة الوسادة الواحدة One-Time Pad) يمكن كسرها .

جدول ١.١ : مسافات الوحدة للنصوص الاسكي المشفرة بخوارزميات بمختلف الأطوال .

Key Length (in bits)	Unicity distance (in characters)
40	5.9
56	8.2
64	9.4
80	11.8
128	18.8
256	37.6

٦: تعقيد الخوارزميات (Complexity of Algorithms) : تعقيد أي خوارزمية تحدد بواسطة القوة الحسابية المطلوبة لتنفيذها . التعقيد الحسابي لخوارزمية غالبا ما يقاس بواســـطة متغيرين : T (لتعقيد الوقت Time Complexity) و S (لتعقيد المساحة Space Time ، أو متطلبات الذاكرة) . كلا من T و S في الغالب يعبر عنهما كدوال لـــــــ n ، حيث n هو حجم المدخل (Input) . (هناك مقاييس أخرى للتعقيد : عدد البتات العشوائية ، سعـــــة حزمة الاتصال (Bandwidth) ، كمية البيانات ، وهكذا) .

الفصل الثاني

أمنية وحماية المعلومات

٢-١ عوامل تعريف قيمة الأنظمة:

يعرف النظـام المثـالي بـأنـه ذلـك النظـام الـذي يملـك توزيع منبســـط (Flat Distribution) لكل الخصـــائص الإحصـــائية للشـــفرة ، والتي تعني الخصـــائص

المتكررة للغة الطبيعية . هناك طريقتين رئيسيتين لغرض التوزيع المنتظم للخصائص المتكررة لأي لغة طبيعية . أول هذه الطرق هي الانتشار (Diffusion) ، والتي تنشر العلاقات المتبادلة والاعتماديات (Dependencies) للعبارات المتكونة من سلاسل رمزية (أي تنشر العلاقات المتبادلة والاعتماديات للعبارات إلى سلاسل رمزية فرعية Substring) والتي تكون طويلة إلى حد أقصى لغرض زيادة إلى الحد الأقصى لمسافة الوحدة (Unicity Distance) . الطريقة الثانية هي التشوش أو الإرباك (Confusion) ، حيث فيها ان الاعتماديات الوظيفية (Functional Dependencies) للمتغيرات المرتبطة بعلاقة يجب أن تعمل بتعقيد كلما أمكن ذلك بحيث تزيد الزمن المطلوب لتحليل النظام .

إن مشكلة القناة الفوضوية (Noisy Channel) هي مناظرة لمشكلة أمنية الاتصالات في علم التشفير – إن الفوضى تقابل تحويل التشفير والعبارة المستلمة كنص مشفر . إن دور المرسل هو جعل استرجاع العبارة الأصلية يكون بصعوبة كافية كلما أمكن ذلك . يركز متخصصي علم التشفير أو المشفرون (Cryptographers) بحوثهم لاكتشاف أو استنباط تقنيات تشفيرية والتي تنتج نص مشفر والتي لايمكن تمييزها من سلاسل البتات العشوائية من قبل العدو (Opponent) .

قناة الاتصال الإحصائية لنموذج الترميز وفتح الترميز Coding/Decoding ( ) قد تم التعويض عنها بقناة نظرية اللعبة (Game Theory) .

ليس كافيا ، على كل حال ، أن يكون النظام التشفيري قادرا على إعاقة علم تحليل الشفرة فقط . ولكن نظام التشفير عليه ان يحبط أي محاولة وكل أهداف الإطراف غير المخولة (Unauthorized) والذين يحاولون تدمير تكامل قناة الاتصال الأمينة .

إن الأهداف النموذجية لأي خصم (Opponent) يمكن تلخيصها كما يلي :

١ : تحديد محتويات العبارة M .

٢ : تغيير العبارة M إلى M′ وقبول هذه العبارة من قبل المستلم كعبارة مرسلة من قبل مرسل العبارة M .

٣ : البدء باتصال للمستقبل وجعل المتطفل (Interloper) يتظاهر بانه المرسل المخول .

تقليديا، فان أول هذه الأهداف ، يطلق عليه مشـكلة الخصـوصـية (Privacy Problem)، وقد أخذت الاهتمام الأكبر من جهود علماء علم التشـفير. لكن بعد إحراز تقدم كلي في مجال الاتصال الالكتروني وأصبح مستخدما بكثرة في محيطات الاتصـال سـواء الخاص أو العام منها ، فان إحباط النقطتين الأخيرتين قد أخذت اهتمام ساحق في تصميم النظام . تسمى عملية إحباط هذه الأهداف بمشكلة إثبات الشخصيـة (Authentication Problem) ومشكلـة النـزاع (Dispute Problem) .

ترتبط الأمنية مباشرة بالصعوبة المتعلقة بعكس تحويل أو تحويلات التشفير لأي نظام. يمكن تقييم (evaluate) الحماية الممنوحة بواسطة إجراء تشفير عن طريق عدم الدقة (Uncertainty) التي تواجه العدو (Opponent) لتحديد المفاتيح المسموح بها. عرف العالم شانون نموذجا رياضيا دقيقا عن ماذا نعني بمفهوم إن النظام التشفيري يتصف بالأمنية . إن هدف أي محلل شفرة هو تحديد المفتاح k ، النص الواضح p او كلاهما . على كل حال ، فانه قد يقتنع ببعض المعلومات المحتملة حول p ، هل هي بيانات نص أو (Spreadsheet أو أي شئ آخر) .

في العالم الحقيقي لتحليل الشفرة ، فان محلل الشفرة يملك بعض المعلومات المحتملة حول p قبل حتى أن يبدأ بالتحليل ، ومن المحتمل أن يعرف لغة النص الواضح .

وصف شانون (Shannon) أي نظام انه يملك أمنية تامة (Perfect Security) بحيث يتصف بالخاصية الآتية :

إذا كان هناك عدو(منافس Opponent) يعرف E (تحويل الشفرة) ولديه كمية غير معينة (Arbitrary) من الشفرة ، ولكنه رغم ذلك ترك مع الخيار بين كل الرسائل من مساحة العبارة عند محاولة استرجاع النص الواضح المقابل من بعض النصوص المشفرة .

إذا كانت $P_C(M)$ تمثل احتمالية ن العبارة M قد أرسلت معطية C وقد استلمت بالتعبير C=E(M). عند ذلك فان الأمنية الكاملة تعرف كالآتي :

$$P_C(M)= P(M)$$

حيث P(M) هي احتمالية انه سيتم حدوث العبارة M .

لتكن $P_M(C)$ احتمالية النص المشـــفر المســـتلم C معطية المعلومة أن M قد تم إرســالها . عند ذلك فان $P_M(C)$ هي مجموع الاحتمالات P(K) للمفاتيح التي تشـفر M إلى C .

$$PM = \sum_{Ek(m)=C}^{k} p(K)$$

اعتياديا سوف يكون هناك مفتاح واحد فقط K الذي يحقق التعبير $E_K(M)=C$.

هناك شرط ضروري و ويكفي للوصول إلى ألأمنية الكاملة هو انه لكل C ،

$$P_M(C)=P(C)$$

هذا يعني أن احتمالية النص المشفر المستلم C هي غيرة معتمدة على تشفيرها بنص واضح M . يمكن ضمان الأمنية الكاملة فقط إذا كان طول المفتاح هو بطول العبارة المرسلة ، وان الكاردينالية (Cardinality) لمساحة المفتاح هي نفسها لمساحة العبارة .هذه الشروط تؤدي إلى ضمان أن عدم الدقة (Uncertainty) للمفتاح والنص المشفر قد تم حفظها ووصولها الحد الأقصى.

الشـــفرات (Ciphers) والتي لايمكن أن تظهر بأنها تملك أمنية تامة لكن لا تكشـف أو تظهر معلومات كافية تسـمح بتحديد المفتاح ، فإن شـاتون أطلق عليها الأمنية المثالية (Ideally Secret) . في حالة عدم الكشـف عن معلومات أكثر من مسـاحة الوحدة، فإن هذه الأنظمة غير قابلة للكسـر (Unbreakable) بشـكل فعال . سـيواجه الخصـم على الأقل بكمية من عدم الدقة بالنسـبة للعبارة كما هو الحال مع المفتاح .النظام الوحيد فقط لمثل هذه الحالة هو (One-Time Pad) . المفتاح المستخدم هو عبارة عن سيل من البتات(Bits) العشوائية غير المتكررة ، ويتم إبعادها أو التخلي عنها بعد كل إرسـال . يسـتخدم مفتاح منفصـل لكل إرسـال (Transmission) بسبب أن نصين مشفرين يتم تشفيرهما بنفس المفتاح سوف يكونان مرتبطين بعلاقة أو صـــلة معينة تؤدي إلى كشـــفهما .عند امتلاك النص المشفر C فإن هذا الامتلاك لا يضيف أي معلومات إلى هدف استرجاع $M = D_k$ (C) .

ماذا يمكن أن نقصد بنظام تشفير معين انه نظام أمين ، يمكننا أن نبدأ بالسؤال أولا عن كمية الأمنية التي يوفرها أي نظام قبل أن نعمل هذا الأجراء ، نلاحظ انه من الممكن لأي نظامين مختلفين ان يكونا متكافئان تحليليا Cryptanalytically (Equivalent)، بمنظور أن احد النظامين يمكن أن يكسر وبعد ذلك يمكن كسر النظام الثاني . سوف نطلق على نظامي تشفير R و S أنهما متشابهان (أو نفس النظامين) إذا كان يوجد تحويل عكسي مميز ووحيد f بحيث أن R=f(S) .

من الواضح أن الأمنية التامة هو هدف مرغوب في التشفير . تعني الأمنية التامة انه ، في حالة عدم حصول محلل الشفرة على معلومات إضافية ، فانه سوف لا يحصل على معلومات مهما تكن من النص المشفر المعترض ، بمعنى آخر أن النظام غير قابل للكسر . على كل حال ، فانه يجب أن يكون واضحا انه لغرض ضمان الأمنية الكاملة في أي نظام تشفير عملي ، فان كمية المفتاح والتي يجب توزيعها قد تسبب العديد من مشاكل الإدارة للمفاتيح . رغم ذلك فان هناك مواضع تكون الأمنية التامة ذات أهمية أعلى وأسمى ، عند ذلك ،ومع كل هذه المشاكل الواضحة ، فان مثل هذه الأنظمة تستخدم في الواقع العملي . إذا كانت مساحة العبارة اصغر عند ذلك تكون هذه الأنظمة غير عملية في الاستخدام .

إن الأنظمة التي تعتمد على مبهمات شاتون هي أنظمة أمنية غير مشروطة (Unconditionally Secure) ، يعني ذلك أن النظام سوف يقاوم محاولات علم فتح الشفرة حتى في حالة عدم وجود القوة أو القدرة الحسابية الغير محددة (Computing Power).

يتم اشتقاق أمنية مثل هذه الأنظمة مباشرة من عدم الدقة الإحصائية (Statistical Uncertainty). إذا كانت $H_C(K)$ هي الانتروبي للمفتاح وأنها لايمكن أن تصل إلى الصفر لأي طول للعبارة ، عند ذلك فإن الشفرة تعتبر أمنياً غير مشروطة .

افترض شانون في اختراعه شفراته التامة أن الأعداء يملكون الوصول إلى قدرة حسابية غير محددة .

لا يوجد هناك تأكيد عقلاني يؤدي إلى الاعتقاد إن أي خصم أو تحالف من الأعداء يمتلكون موارد حسابية لا تنضب ، (أو بمعنى آخر ، إنه في المستبعد إدراكه في كل حال، أن يتم الاعتقاد بأن أي عدو مفرد أو تحالف بين الأعداء هو في حالة امتلاك لموارد حسابية لا تنفذ (أي غير محددة) لذلك فان حالة امتلاك العدو لعدد موارد غير محددة هو أمر غير معقول.

مثل هذه المقاييس الأمنية كما قدمت بشكلها المعلن من قبل شانون تبدو أنها مفرطة في تحقيق الهدف الذي تحاول الوصول إليه وهو الحماية ضد تهديد غير محسوس . تنظر أنظمة التشفير إلى ابعد من توفر عدم الدقة ومسافات الوحدة لتأسيس قواعد للأمنية وبشكل خاص،عامل الشغل (Work Factor) ، نسبة إلى التعقيد في تحليل النظام لفتح شفرته، حيث يؤخذ عامل الشغل بمثابة مؤشر قوي لأمنية النظام .

يمكن أن تعرف الأمنية بدلالة عدد السنوات المطلوبة من قبل الشخص/حاسبة (أي الشخص أو الحاسبة) لغرض كسر النظام . بالامكان معرفة الفرق الطفيف بين الأمنية التامة وأمنية التشفير ، الأولى (الأمنية التامة) هي علاقة معايشة معرفة ، بينما الثانية (أمنية التشفير) ترنو إلى فكرة الصعوبة في التعقيد . بالرغم من أن التهديدات التي يجب على نظام التشفير مقاومتها يمكن أن تدرج كما في أعلاه لكن لا توجد إلى الوقت الحالي أي طريقة عامة أو خوارزمية التي تستطيع أن تبرهن أن نظام تشفيري معين يمكن أن يكون هو نظام تشفيري أمين (Cryptosecure) . لقد اعتمد المصممون ا على شهادة أو تصديق (Certification) محللي الشفرة ، والذين من جانبهم يحاولون الاجتهاد في التعرض أو تشويه النظام مستخدمين مقاييس (Ad hoc Heuristic) , كمؤشر لأمنية الذظام . اظهر لنا التاريخ بشكل متكرر أن الأنظمة المبتدعة من قبل مكتشفيها فإنها تكون أنظمة تشفيرية غير قابلة للكسر كما أظهرت بأنها أكثر أمنية من المعتقد بعد أن قدمت إلى البحث والتدقيق المكثف من قبل محللي الشفرة . رغم أن الشهادة أو التصديق (Certification) تعتبر مؤشر غير دقيق وبدون برهان رياضي مميز ، فإنها قد ظلت هي الطريقة المتبعة لإثبات أو تجسيد المطلب أن الذظام التشفيري هو ذظام أمين . تعقد الآ مال الكبيرة على أن نظر ية التعقيد (Complexity Theory) سوف توفر الأدوات النظرية الضرورية لغرض تأسيس أنظمة تشفير أمنية مبرهن علي أمنيتها بشكل دقيق . إذا ما تحقق هذا التمني ، حينئذ فان التشفير سوف يتخلى عن سمعته باعتباره فن وبذلك يفترض خصائص علم دقيق كامل .

إن أي نظام تشفيري والذي يمتلك خطوة التشفير التي يمكن تحديدها بصورة منفردة بواسطة زوج من حروف النص الواضح والمشفر قد يطلق عليها نظام تشفير شانون . هناك العديد من أنظمة التشفير الشائعة تملك هذه الخاصية .

أي نظام تشفيري والذي يمتلك خطوة التشفير وخطوة فتح الشفرة يتصفان بانهما متطابقان ، عند ذلك يمكن وبشكل تناظري تحديد إجراء التشفير حيث يطلق على مثل هذا النظام التشفيري تناظري المفتاح (Keysymmetric) . في هذه الحالة ، فان كل خطوة تشفير تتصف بأنها التفافية (Involuntary) .

هناك عدة معايير (Criteria) ، والتي عادة ما مايطلق عليها الهجومات (Attacks) ، و تستخدم هذه الهجومات لغرض تحديد ملائمة نظام تشفيري مستقبلي او متوقع (Prospective Cryptosystems) . هجوم النص المشفر فقط (Ciphertext –Only Attack) هو ذلك الهجوم الذي يكون فيه النظام معرضا للانتهاك او التشويه وذلك بفحص العبارات المشفرة ، او الشفرات (Ciphers) ، والاشارة الى معلومات ثانوية ذات علاقة بالنظام. أي نظام والذي أمنيته لا تستطيع مواجهة هجوم النص المشفر فقط يعتبر نظام غير ملائم ويكون بالكامل غير أمينا (Insecure) . ينفذ هجوم النص المعروف Known-Plaintext عندما يكون النظام في حالة محاولة التعرض للخطر (Compromised) من قبل محلل الشفرة والذي يملك النص الواضح وما يقابله من نص مشفر. إذا تمكن أي نظام من مقاومة هجوم النص الواضح المعروف ، فانه هذا يؤخذ كمؤشر معقول بان النظام هو أمين (Secure) .(في العام ١٩٧٧ فان NBS قبلت نظام تشفير البيانات القياسي (DES) على أساس مقاومته لنص الهجوم الواضح المعروف) . هناك هجوم ثالث يمنح محلل الشفرة مجموعة من الظروف الملائمة ، والتي تجعل الشفرة معرضة للخطر إلا إن هذه الظروف لا تعتبر أدلة واقعية على أن قدرات النظام المتأصلة فيه تمكنه من مقاومة الكسر. عندما يقع الهجوم فان محلل الشفرة بامكانه تقديم كمية غير محدودة من نصوص واضحة والحصول على النصوص المشفرة المقابلة والتي تسمى هجوم النص الواضح المختار (Chosen-Plaintext Attack) في العالم الحقيقي، فإننا ندرك بأنه من المتعذر منع كل هجوم محتمل. إن الخبرة في كشف الهجومات وإدارة الخطر يمكن أن تساعد أي مصمم لبناء أنظمة والتي توازن الأمنية مع الوظائفية، الكلفة، والوقت.

أي نظام يمنع التشويه أو انتهاك (Compromization) عند تعرضه لهجوم النص الواضح المختار هو بالتأكيد نظام أمين .يجب أن يدرك أن أمنية أي نظام لا تعتمد علي إخفاء تحويل التشفير أو الخوارزمية . عموما هذه الخوارزمية سوف تكون متوفرة وفي متناول الجميع لغرض الفحص والدراسة والتي تعرف بمبدأ كريشوف (Kerckhoff's Principle) : عندما يتم كشف E فانه ستكون عملية أو طريقة صعبة جدا أو غير كفؤة كذلك يتم كشفها لغرض حساب معكوس E . عند إعطاء نص مشفر C ، فان محلل الشفرة يستطيع فحص مساحة العبارة بشكل مكثف حتى يحدد M بحيث E(M)=C ،بينما يتم استخدام مفتاح بطول محدد ، فان المفتاح سيكون دائما نظريا عرضة للخطر وذلك من خلال طرق البحث المباشرة . يعتمد نجاح مثل هذا الهجوم على عامل الشغل (work factor) المرتبط بالشفرة (Cipher) ، بمعنى آخر ، العدد الأدنى من الحسابات المطلوبة لغرض

عكس النظام (Invert) . يجب ملاحظة أن مسافة الوحدة (Unicity Distance) تشـــير إلى عدد الحروف المطلوبة لغرض تحديد المفتاح ، لكن لا تعطي أي ملاحظة حول تعقيد هذا الهدف . أي نظام يستطيع كشف نص مشفر أكثر من مساحة الوحدة التابعة له يعتبر نظاما أمينا (Safe) و لكن قد يبقى نظام تشـــفيري ســـري (Crtptosecure) .

لنأخذ تعريف آخر للأمنية والذي أصبح يجتذب إليه الأنظار ليكون كقاعدة لقبول أنظمة تشفيرية راسخة ومقبولة :

يعتبر أي نظام يعتبر حسابيا نظـــاما أمينا (Computationally Secure) إذا كانت مهمة تحويل او عكس E حســـابيا متعذر أو صـــعب الحل حســـابيـــــا (Computationally Infeasible or Intractability) . (هذا مشـــابه إلى خصائص مشاكل الـ NP) ، وان أكثر تصميمات الأنظمة الحديثة تعتمد على تحويل تشفير حيث فيها أن الخوارزمية المحددة الأفضل (Deterministic Algorithm) المســـئولة عن عكس التحويل تملك تعقيد أســـي (Exponential Complexity) . المشاكل والتي تتصف بصعوبة حسابية تفوق الـــ NP هي غير ملائمة لعلم التشفير بسبب أن خوارزميات التشفير وفتح الشفرة تكون بطيئة جدا.

الأنظمة التي تعتمد على الأمنية الحســابية لعزل المفتاح وإفشــال التعرضــات أو الانتهاكات تفترض بأنه حتى لو أن تحليل الشـــفرة يتم بخطوات محددة العدد ، فان كميـة الموارد المطلوبـة لعكس أي نظـام والمخزون من الموارد (Resources) المتوفرة في متناول يد محللي الشـفرة سـيكون غير مناسـب لكل الإغراض العملية التي صـــمم من اجلها الذظام . بوجود التكنولوجيا الحالية ، فان الحد العملي لعدد العمليات التي يسـتطيع محلل الشـفرة تنفيذها هي بين $٢^{٥٠}$ و $٢^{٦٠}$ .. والحد العملي لعدد خلايا الذاكرة التي يسـتطيع اسـتخدامها هي بين $٢^{٢٥}$ و $٢^{٣٥}$. تتصـف أنظمة شانون بمقاومتها لانتهاك النظام (Compromization) بسبب أن محلل الشفرة لا يملـك معلومـات كـافيـة ، بينمـا في الأنظمـة الأمنيـة حســـابيـا (Computationally Secure) فان محلل الشـــفرة يملك معلومات كافية لغرض حل الغموض للذظام (Equivocation) . هذا يمكن توضـــيحه بمثال من (Lakshivarahan) . ليكن طول المفتاح ١٢٨ بت وان بحث مكثف يتطلب لفتح الشـفرة (Decryption) بمقدار $2^{128}=10^{34}$ · باسـتثناء السـنوات الكبيسـة فانه هناك فقط 10^{7} *3.15 ثانية في السنـــة الواحدة . إذا تم الافتراض أن فتح الشفرة بمفتاح متميز يمكن تنفيذه (أي تنفيذ فتح الشـفرة) في 01^{-1} ثانية ، عند ذلك فانه في الســـنة لواحدة بالامكان اختبار $3.15*10^{16}$ مفتاح متميز (Unique Key) ولغرض معـالجـة كـامـل مســـاحـة العبـارة الكليـة ســـوف يحتـاج على الأقـل

3.17*1021 سـنة . تم تقليل الغموض (Equivocation) للنظام بصـورة مؤثرة إلى الصـفر ، لكن عمليا بقي (الغموض) غير متقلص (Undiminished) بسبب التعقيد الذي يشتمله .

ادخل العالمان ديف وهيلمان فكرة أنظمة التشـفير الأمنية حسـابيا في سـنة ١٩٧٦ وعلى الرغم من أن مثل هذه الأنظمة لها موقع مسـتقبلي أفضـل للتطبيقات التجارية من أنظمة شـانون (بمعنى أن هذه الأنظمة التي افترضـها ديف وهيلمان أفضـل من أنظمة شـانون) ، فان هذه الأنظمة لا توفر على كل حال حل للمشـكلة الأساسية لتصميم أنظمة تشفير ذات أمنية مبرهن عليها (Provable Secure Cryptosystem) إذا كان بالامكان إثبات أن NP = P ، عند ذلك فان الانظمة المعتمدة على مشـاكل تعقيد الحل يمكن كذلك إثبات أنها أنظمة أمينة (Secure) ، استنادا إلى التعريف الحسابي للأمنية في حالة NP = P مع الخلاف الغير محلول فان نظرية التعقيد سـتوفر الحد الأعلى للوقت الذي سـيؤخذ في تحليل شفرة نظام تشفيري أمين حسابيا.

الأنظمة التامة تقاوم العكس (Inversion) وذلك من خلال الإهمال أو الجهل بينما الأنظمة غير التامة (Imperfect) تعتمد على الاعتقاد أن التعرض للخطر (Compromization) يكون اكبر من الوسـائل الاقتصـادية لأي متطفل . هناك فرق جوهري آخر بين النظامين وهو أن النظـام الأول (أي التام) يمكن برهنتـه انه نظام أمين بينما يشـك في إثبات أمنية النظـام الآخر (الغير تام) في أي لحظة من الزمن (لحد الوقت الحالي) . على الرغم من الأمنية التامة ، أنظمة شـانون وضـعت محددات للمفتاح ، طوله وتكرار الإحلال (Frequency of Replacement) ، والتي جعلت مثل هذه الأنظمة غير عملية للاتصالات المتكررة الكثيرة بين عدد كبير من المستفيدين .

لقد حاول مصـمموا أنظمة التشـفير بسـعي حثيث إيجاد إجراءات (Procedures) والتي تكبر أو تعظم عدم الدقة للمفتاح الصـغير ، بحيث يكون كأنه مفتاح ذو طول كبير جدا أكثر من عدم الدقة المرتبطة به . يقال عن المفتاح الحقيقي (True Key) انه تم تحويره إلى مفتاح وهمي (Pseudo Key) بأمنية للنظام تعتمد على الصـعوبة في الحل (Infeasibility) لتحديد المفتاح الحقيقي من المفتاح الوهمي . يجب التأكيد على أن نظرية التعقيد الحالية تنقصـها الإمكانية لإظهار صعوبة حل أي مسألة تشفيرية .

٢-٢ : ملخص عن الأمنية الكاملة:

لغرض وصول أي نظام تشفيري للسرية الكاملة : حيث انه النظام التشفيري الذي فيه النص الواضح المشفر لا ينتج معلومات ممكنة حول النص الواضح (عدا من المحتمل طول النص الوا ضح) . لقد عرف شانون أن هذا يمكن أن يتحقق نظريا فقط في حالة إذا كان عدد المفاتيح الممكنة هو على الأقل كبيرا بعدد العبارات الممكنة . بمعنى آخر ، فان المفتاح يجب أن يكون على الأقل بطول العبارة نفسها ، وانه لا يوجد أي مفتاح يتم إعادة استخدامه . بمعنى آخر ، تبقى شفرة الوسادة (One-Time Pad) هي النظام التشفيري الوحيد الذي يحقق أمنية كاملة.

إن الخوارزمية التشفيرية الجيدة هي التي تبقي المعلومات حول النص الواضح الناتجة من النص المشفر بان تكون اقل ما يمكن ، بينما محلل الشفرة الجيد هو الذي يستثمر هذه المعلومات لتحديد النص الواضح.

يستخدم محللو الشفرة الحشو الطبيعية للغة لغرض تقليص عدد النصوص الواضحة الممكنة . كلما كانت اللغة أكثر تكرارا فإنها تكون اصهل لتحليل شفرتها . هذا هو السبب الذي تكون فيه العديد من الاستخدامات التشفيرية في الواقع العملي تستخدم برنامج ضغط (Compression) لتقليص تكرارية أي عبارة إضافة إلى الجهد المطلوب للتشفير وفتح الشفرة .

إن الانتروبي لأي نظام تشفيري هو مقياس لحجم مساحة المفتاح، K، تعرف كما يلي:

$$H(K) = \log_2 K$$

إن نظام تشفيري بمفتاح بطول ٦٤ بت يملك انتروبي مقدارها ٦٤ بت، والنظام التشفيري بمفتاح بطول ٥٦ بت يملك انتروبي بمقدار ٥٦ بت. على العموم، فانه كلما كانت الانتروبي أكبر، فإنها ستكون هناك صعوبة في كسر نظام.

٢-٣ : أنظمة التشفير العشوائية (Random Cipher):

سنتكلم أولا عن مفهوم الانتروبي والغموض (Equivocation) . فمن خلال ممارسة محلل الأنظمة ودوره في بعض الأمثلة التشفيرية ، فإننا نلاحظ قابليته على التنبأ بتغييرات العبارة الأصلية كلما ازداد طول النص المشفر المعترض (الذي تم الحصول عليه) .

في أي حالة والتي تواجه فيها مجموعة من الإحداث المحتملة ، كل منها له احتمالية مرتبطة بالحدث ، إذا أمكننا تخمين الحدث الفعلي فإننا فقط منطقيا نستطيع اختيار واحد من الاحتمالات العالية . (عندما لا يوجد حدث مميز بهذه الاحتمالية العالية ، فانه علينا أن نعمل اختيار عشوائي بين الأحداث الأكثر احتمالا) . إن الثقة التي بها نستطيع عمل التخمينات تتغير دائما . إنها تعتمد ليس فقط على كيفية زيادة احتمالية الحدث المختار . لذلك أدخلت أفكار الانتروبي والغموض والتي صممت لإعطاء مقياس كمي لهذا المستوى من الوثوقية . دالة الانتروبي لنظام معين هي وسيلة لقياس عدم الدقة (Uncertainty) لذلك النظام (أو ، في حالتنا هذه ، الوثوقية والتي بواسطتها نستطيع التنبأ بان حدث معين قد تم تكراره) . تعكس الانتروبي لأي نظام الوثوقية التي بواسطتها نستطيع التنبأ بأنه سيتم إرسال عبارة معينة . يمكن معرفة انه في موقع كم هي مقدار الموثوقية التي نستطيع بها التنبأ بالعبارة المرسلة ، أو ما هو المفتاح الذي تم استخدامه . هذا يقودنا إلى إدخال فكرة الانتروبي المشروطة ، أو ما أطلق عليه شانون الغموض .

الآن ماذا نعني بالعشوائية ؟ . قبل إعطاء تعريف رسمي ، سوف نحاول أن نقرر ماذا تشير العشوائية . من الواضح انه لا يوجد تسلسل دوري (Periodic Sequence) هو حقيقة عشوائي . في التشفير فان الذي نحتاجه من التسلسل هو عدم التنبأية (Unpredictability) بدلا من العشوائية . ان المطلوب معرفته هنا انه في حالة اعتراض محلل الشفرة لجزء من التسلسل ، فسوف لا يملك معلومات حول كيفية التنبأ بما يأتي لاحقا . مرة آخر فان هذا غير ممكنا لأي تسلسل دوري بسبب ، حال معرفته محلل الشفرة للدورة الكاملة ، فانه سيعرف التسلسل الكلي . بالرغم من ذلك فانه من غير المعقول أن يحاول ضمان فيما إذا كان جزء من النص المشفر والتي هي اقصر من الفترة المعترضة ، فانه لايتم إعلان معلومات إضافية . أي تسلسل محدد يحقق هذه الصفات العامة يطلق عليه في الغالب ما يعرف بالتسلسل الوهمي (Pseudo - Random Sequence) .

احد المتطلبات لأي نظام عشوائي هو ، لأي نص مشفر C فان فتح الشفرة باستخدام كل المفاتيح يؤدي إلى اختيار عشوائي لكل العبارات، بمعنى آخر ، اختيار عشوائي من العبارات ذات المعنى والعبارات التي ليس لها معنى. هذا بوضوح يؤكد أن عدد فتح شفرات ذات معنى هو اقل من الذي نستطيع ضمانه إذا عرفنا أن فتح شفرة نص مشفر، والتي تأتي من عبارة ذات معنى ، يجب أن يعطي عبارة بدون معنى. لكن هذا المطلب الأخير يتطلب أن تكون مساحة النص المشفر يمكن كذلك تقسيمها إلى صنفين ، الصنف الأول من العبارة ذات المعنى، والصنف الثاني من العبارات بدون معنى.

٢-٤: الوصول إلى الوثوقية (Achieving Confidentiality):

تستخدم أي طريقة تشفير لغرض الوصول إلى تحقيق الوثوقية وذلك بان يختار كل من المرسل والمستقبل زوج من المفاتيح السرية (e ,d) ، ثم في لحظة معينة من الزمن فان المرسل يحول كل $m \in M$ إلى ما يقابلها من عبارة مشفرة c ويرسلها إلى المستقبل (الطرف الثاني) بتطبيق $c=E_e(m)$. وعند استلام المستقبل للنص المشفر c فأنه يقوم بتحويلها إلى نص واضح بتطبيق

$D_d(c) = m$ ويسترجع العبارة الأصلية m .

هناك مسألة مهمة الا وهي: لماذا الاهتمام بضرورة المفاتيح المستخدمة ولماذا يعول عليها في تأمين سرية أي خوارزمية تشفير. الجواب على ذلك هو أن طرق التشفير أو خوارزمية التشفير هي معلنة الخطوات ومعروفة للكل ولكي نؤمن سرية الخوارزمية علينا الاعتماد على سرية المفاتيح المستخدمة . والسبب في ذلك انه لو كان الاعتماد في تحقيق السرية يعتمد على الخوارزمية فأنه في حالة كشف الطريقة يتعين إعادة تصميم الخوارزمية من جديد لكي تواجه محاولات الكشف وهذا يعتبر حل غير عملي في حين أن الاعتماد على سرية المفتاح يتطلب فقط تغيير المفتاح بدلاً من تغيير الخوارزمية .وعلى العموم فأنه في الشائع في استخدامات خوارزمية التشفير هو التبديل المستمر للمفتاح بين فترة وأخرى حتى في حالة عدم كشف سرية المفتاح . الشكل ٢ -١ يوضح نموذج بسيط لمشتركين اثنين في الاتصال ويستخدمون احد خوارزمية التشفير .

٢-٥ : المشتركين في الاتصال (Communication Participants):

في الشكل ٢.١، وجود بعض المصطلحات منها:

١:كينونة (Entity) أو مشترك (Party) هي عبارة عن شخص أو إي شيء والذي بإمكانه الإرسال الاستقبال وكذلك المعالجة.

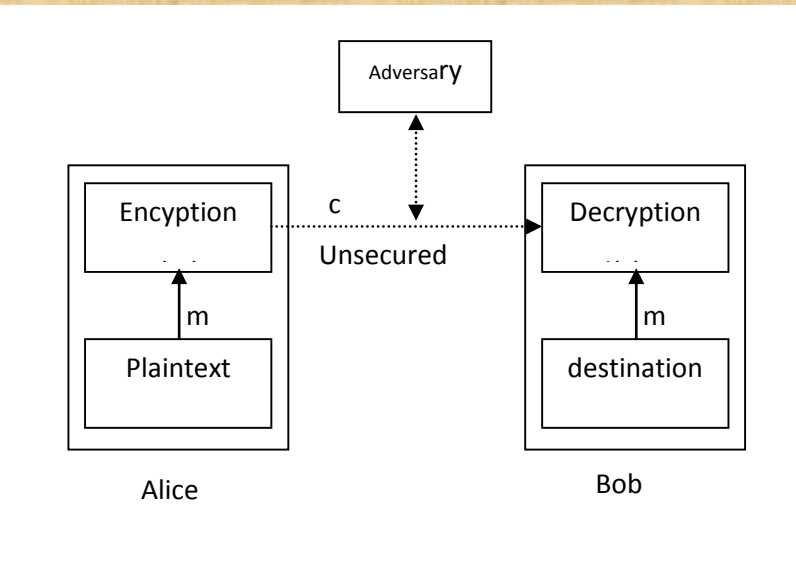
٢: المرسل (Sender) عبارة عن كينونة في وسط اتصال مشترك بين طرفين والذي يعتبر المرسل الشرعي (القانوني) للمعلومات . في الشكل أدناه فأن (Alice) هو المرسل.

٣: المستقبل (Receiver) عبارة عن كينونة في وسط اتصال مشترك بين طرفين والذي يعتبر المستقبل المقصود (المرسل إليه Intended) للمعلومات. في الشكل فأن (Bob) يعتبر المستقبل.

٤:الخصم أو العدو (Adversary):عبارة عن كينونه في وسط اتصال مشترك بين طرفين والذي لا يحمل صفة المرسل أو المستقبل والذي يحاول اختراق (Defeat) أمنية المعلومات التي تم تأمينها أو تحقيقها بين المرسل والمستقبل.

هنـاك عـدة مصـــطلحـات مرادفـة إلى الخصـــم (Adversary) هي العـدو (Enemy) ،المهاجم (Attacker) ، الخصم أو المناوئ (Opponent) ،القناص (Trapper) متنصت أو مسترق السمع (Eavesdropper)، الدخيل (Intruder).

الشكل ٢-١ : رسم تخطيطي للاتصال بين طرفي اتصال يستخدمون التشفير .



٢-٦ : القنوات :(Channels):

تعرف القناة بأنها وســـيلة لنقل المعلومات من كينونه إلى أخرى ، هناك عدة تعاريف تتعلق بمفهوم القناة من حيث توفير الأمنية أو عدم توفيرها وهي :-

١-القناة الأمنة (Physical Secure Channel) : وهي قناة غير قابلة الوصول فيزيائياً من قبل الخصم او العدو.

٢- القناة غير الســـرية (Unsecured Channel) وهي عبارة عن قناة يحاول فيها اى متطفل من غير الأشخاص المخولين الوصول للمعلومات ويحاول إعادة ترتيبها ، يحذف ، يدخل بين المعلومات ، أو يقرأ المعلومات.

القنـــاة الآمنة (Secured Channel) هي القناة التي فيها لا يستطيع المتطفل أن يصل المعلومات ويحاول ترتيبها ، حذف ، يدخل المعلومات ، قراءة المعلومات.

هناك فرق دقيق بين القناة الامينة فيزيائيا (Physical Secure Channel) و القناة الامينة (Secured Channel) هو ان القناة الســـرية قد تؤمن ماديا او باستخدام تقنيات تشفيرية .

٢-٧ : الامنية (Security):

من المعلومات المنطقية أو البديهية (Premise) في التشفير أنه المجموعات:

$M,C,K,\{E_e:eEK\},\{D_d:dEk\}$ تعتبر معلنة للجميع . إن الوســـيلة الوحيدة لتأمين الأمنية هو بأن نحافظ على ســرية كل من (e,d). اثبتت التجارب أن المحافظة على سرية خوارزميات التشفير هو في الواقع عملية صعبة جداً.

تعريف ٢ -١:

تسمى طريقة التشفير التي يمكن كسرها (Breakable) وذلك بوجد مشترك ثالث (Party) و الذي ليس له معرفة سابقه بـــ (e , d) يستطيع أن يكشف أو يسترجع الـنـص الـواضـــح (Plaintext) مـن مـا يـقـابـلـه مـن نـص مشـــفـر (Ciphertext) ضمن إطار زمني مناسب.

يمكن كســر أي طريقة تشــفير وذلك بالعمل على تجريب كل المفاتيح الممكنة التي قد تستخدم في الاتصال بين الأطراف المشتركة، مفترضين أن خطوات طريقة التشفير هي معلنة (Public).

هذه المحاولات تســمى البحث المكثف(Exhaustive Search) في مســاحة المفتاح (Key Space) ، ولذلك لغرض مواجهة هذه المحاولات أو لتأخير عملية البحث المكثف للمفاتيح الممكنة فيجب أن يكون عدد المفاتيح المســتخدمة كبير ، (أي بمعنى مساحة المفتاح تكون كبيرة) حيث انه في هذه الحالة يكون المتطفل أمام مسألة صعبة التحقق أو قد لا يمكن تحقيقها .

هنـــاك قواعد أو قوانين وضعها كيرشوف (Kerckhoff's Desiderata) والتي هي عبارة عن مجموعة من المتطلبات الضـرورية لأي نظام تشـفيري . هذه المبادئ يمكن تلخيصها بمايلي :

١: سيكون نظام التشفير عملياً غير قابل للكشف أو الكسر (Breakable) إذا كان نظرياً لايمكن كشفه .

٢ : الكشف عن تفاصيل النظام يجب ان لايكون غير ملائم للمشتركين (أي يكون ملائم للمشتركين)

٣ : يجب أن يتصف المفتاح بأن يكون سهل تذكره وبدون أي ملاحظات وكذلك سهولة تغييره.

٤ : النص المشفر (Cryptogram) يجب أن يكون قابل للإرسال بواسطة التلغراف (Telegraph).

٥ : الأجهزة المستخدمة في التشفير يجب أن تكون محمولة أو قابلة للحمل (Portable) ويمكن تشغيلها بواسطة شخص واحد.

٦ : يجب أن يكون نظام التشفير سهلاً بحيث لا يحتاج معرفته لقائمة طويلة من القواعد التي توضح عمل نظام التشفير وكذلك لا يتطلب مجهود ذهني.

هذه القائمة من المتطلبات قد وضعت في ١٨٨٣ ، وفي معظم أجزائها ، بقيت مفيدة إلى هذا اليوم .

الفقرة (٢) تسمح أو توضح أن أي صنف أو نوع من التحويلات التشفيرية سيكون معروف علناً وأن أمنية (Security) النظام التشفيري تبقى معتمداً على سرية المفتاح المختار.

هناك ثلاث متطلبات محددة للسرية ، هذه المتطلبات هي :

١ : يجب أن تكون هناك صعوبة في الحل حسابيا لمحلل الشفرة في تحديد تحويل التشفير $D_{K'}$ من نص مشفر معترض (Intercepted) C ، حتى ولو كان النص الواضح المقابل M معروفا.

٢ : يجب أن تكون هناك صعوبة فبي الحل حسابيا لمحلل الشفرة لغرض تحديد النص الواضح M من نص مشفر معترض C.

اقترح شانون خمسة معايير (Criteria) للأنظمة السري في العام ١٩٤٠ ، هذه المعايير هي:

١ : كمية السرية المقدمة (The Amount of Secrecy Afford) .

٢ : حجم المفتاح .

٣ : سهولة عمليات التشفير وفتح التشفير (Ciphering, Deciphering).

٤ : انتشار الأخطاء (The Propagation of Errors).

٥ : امتداد أو توسع العبارة (Extension of the Message) .

إن النقطة (١) أهميتها واضحة .

يحفظ المفتاح بصـــورة ســـرية ، وفي بعض الأحيان قد نحتاج إلى تذكره (او حفظه لدي المســتفيدين) . كنتيجة لذلك فان المفتاح يجب أن يكون اصــغر وأســهل مايمكن . في الشرط (٣) ، فان شانون يؤكد أن عملية التشفير وفتح الشفرة يجب أن تكون ســـهلة كلما أمكن ذلك . إذا تم إنجازها ميكانيكيا ، فان التعقيد يؤدي إلى ماكنات غالية وكبيرة . أخيرا فانه في بعض أنظمة التشـــفير يزداد حجم العبارة بواسطة عملية التشفير . مثلا ، استخدام الفراغات (Nulls) (بمعنى اخر ، اضافة حروف اضـافية بدون معنى لزيادة احصـائيات العبارة) يسـبب نص مشـفر اكبر من العبارة . مـثل هذا التوســـع في العبـارة يكون غير مرغوبـا فيـه في معظم انظمـة الاتصالات .

من مناقشـــة انظمة التشفير ، فانه يتضح بان هناك عدم تطابق (او عــدم توافق) بين متطلبات هذه المعايير الخمسـة عندما تكون عبارة المسـاحة متكونة من اللغة الطبيعية . مـن المحتمل انـه مـن غير الممكن تحقيق كـل المعايير الخمسة لكن ، إذا تم إهمال احـــــدها ، فانه من الممكن تحقيق المعايير الأربعة الأخرى . فمثلا ، لو أهملنا المتطلب الأول ولا يربط بالأمنية ، عند ذلك فان أي نظام تشـــفير أحادي الأحرف (Monoalphabetic) ســـوف يحقق المعـايير الأربعـة الأخرى . في الحقيقة فإننا لا نحتاج لنظام تشـفير على الإطلاق . إذا كان حجم المفتاح غير محدد عند ذلك فإننا نسـتطيع اسـتخدام شـفرة الوسـادة ذات الوقت الواحد (One-Time Pad) والذي ، إذا أهملنا نماذج إدارة المفتاح ، سـوف نعرف بأننا نوفر أمنية تامة . (Perfect Secrecy)

إذا أسـقطنا المعيار (٥) ونسـمح لاتسـاع مسـاحة عبارة غير محددة ، عند ذلك نستطيع تشفير عدة عبارات إضافية واستخدام جزء من المفتاح ليشير إلى العبارة الصـحيحة منها . مثل هذا النظام قد يكون قادرا حتى على تحقيق مسـتوى عالي من الأمنية ، رغم انه غير واضـــح أن هذا النظام يســـتطيع تحقيق المتطلبين الثاني والثالث . بإهمال المعيار (٤) فإننا نسـتطيع تشـفير كتل . لكن مرة أخرى انه من غير الواضـــح إمكانية تحقيق المطلبين الثاني والثالث بهذه الطريقة . رغم أن شـــفرات الكتل قد تؤدي إلى تقادم الخطأ (Error Propagation)، فان هذا ليس سيئا بالضرورة.

ســوف يتم عمدا تجنب مناقشـــة المعيار الثالث لشـــانون ، والمتعلق بالتعقيد. في الوقت الحالي فإننا نملك فوائد الالكترونيات ولا نحتاج لان نقلق بســـبب وجود

الماكنات الميكانيكية . هذا يعني أننا نملك طرق رخيصة معقولة لإنتاج معدات معول عليها ومعقدة لتشفير وفتح الشفرات . لذلك فان معيار شانون الثالث لا يهمنا.

إن تأثير التشفير (Encipherment) على المعلومات السرية يعتمد على الحفاظ على المفتاح بشكل أمين (Secret) . في التطبيقات العسكرية والدبلوماسية للتشفير فانه يتم إقامة مسار أمين لغرض توزيع المفتاح إلى المستفيدين . إن التعابير ، توزيع المفتاح ، وإدارة المفتاح تشير إلى إجراءات (Procedures) في نظام معالجة المعلومات التي تخلق وتوزع المفاتيح إلى المستفيدين .

عند التفكير في الأمنية ، فإنها تعني سلسلة من أمنية البيانات، أمنية الاتصالات، أمنية المعلومات. كل شئ يجب أن يكون سريا، خوارزميات التشفير، البروتوكولات ، إدارة المفتاح ، وأشياء أخرى. إذا كانت الخوارزميات ممتازة العمل لكن هناك أخفاقا في مولد الأرقام العشوائية، فان أي محلل شفرة ذكي يستطيع مهاجمة النظام من خلال توليد الأرقام العشوائية. إذا جمعت كل شئ واتقنت كل الخطوات ونسيت لأغراض الأمنية أن تلغي موقعا في الذاكرة والذي يحتوي على المفتاح، فان محلل الشفرة سوف يكسر نظامك بواسطة الدخول. يجب علينا ان نتذكر كل الوسائل الممكنة للهجوم والحماية ضدها جميعا، لكن محلل الشفرة يحاول إيجاد ثغرة في الأمنية واستثمارها .

علم التشفير (Cryptography)، هو فقط جزء من الأمنية ، وغالبا ما يكون جزء صغير جدا . يستخدم علم التشفير المهارات الرياضية التي تجعل النظام أمينا .

٢-٩ : شرط الحالة الأسوأ (Worst Case Condition):

عند تصميم نظام تشفير، فإننا دائما نفترض انه أي محلل شفرة يملك ما يمكنه من المعرفة الكبيرة والذكاء. إن اهتمامنا الأساسي هو الوقت المطلوب لمحلل الشفرة لكسر النظام.

لغرض تحديد أمنية أي نظام سوف نعمل الافتراضات التالية والتي يشار إليها بشروط الحالة الأسوأ:

الشرط الأول : محلل الشفرة يملك كامل المعرفة حول نظام التشفير .

الشرط الثاني : محلل الشفرة قد حصل على كمية معقولة ومعتبر بها من النص المشفر .

الشرط الثالث: محلل الشفرة يعرف النص الواضح المكافئ لكمية معينة من النص المشفر .

الشـــرط الأول يدل على انه بأننا نعتقد انه لا توجد أمنية في نظام التشـــفير نفســـه ، وان كل الأمنية يجب أن تأتي من المفتاح.

يجب أن يكون واضحا أن الشرط الثاني هو افتراض ضروري يربط مع الشرط الأول ، قد كون الأســـاس للعديد من الهجومات التشـــفيرية الأولى. لقد تم الافتراض انه ، إذا استطلاع محلل الشفرة اعتراض اتصال واحد بين اثنين من المشتركين، فانه من المحتمل أن يكون قادرا على اعتراض اتصـــالات أخرى. علاوة على ذلك، فان عدة اتصالات قد تستخدم نفس المفتاح.

الشـــرط الثالث (بارتباطه مع الشـــرط الأول) هو أســـاس هجوم النص الواضـــح المعروف والذي قد يكون أهم الهجومات على الإطلاق المســـتخدمة في كســـر الشفرات .

٢-١٠: أمنية المعلومات بشكل عام (Information Security in General):

لقد تم التطرق في الفقرات الســـابقة على توضـــيح فكرة الأمنية وذلك بتحديد مفاهيم التشـــفير وفتح التشـــفير مع توفير الخصـــوصـــية (Privacy) . لكن مفهوم أمنية المعلومات هو أكثر أتساعا من المفهوم السابق و يتضمن الكثير من المسائل المتعلقة بـها مـثل إثبات الشـــخصـــية (Authentication) وتكامل البيانات (Data integrity).

أدناه مجموعة من التعاريف التي لها علاقة بالأمنية.

١- خدمة أمنية المعلومات (Information Security Service) عبارة عن طريق لتزويدنا ببعض مظاهر الأمنية ، فمثلاً تعتبر تكامل البيانات المرسلة هو أحد أ هداف الأمنية وإن الطريقة التي تؤيد هذه الظاهرة عبارة خدمة أمنية المعلومات.

٢- كسر (Breaking) خدمة أمنية المعلومات يتضمن إحباط (Defeat) أهداف خدمة أمنية المعلومات.

٣- العدو الخامل (Passive Adversary) عبارة عن عدو أو متطفل و الذي يستطيع قراءة المعلومات من قناة اتصال لا توفر أمنية (Unsecured Channel) .

٤- العدو الفعال (Active Adversary) عبارة عن عدو أو متطفل و الذي له كذلك القابلية لأن يرسل ، يغير أو يحذف المعلومات في قناة اتصال لا توفر أمنية.

٢-١١ : مستقبل التشفير:

إن فوائد التشفير واضحة جدا. يقوم التشفير بحماية المعلومات المرسلة والمخزونة من الوصول غير المأذون أو من الانتهاك . هناك تقنيات تشفيرية أخرى ، مثل طرق إثبات الشخصية والتواقيع الرقمية ، تستطيع الحماية ضد الخداع وتزوير العبارات . إذن لا خلاف أن التشفير هو أداة ضرورية لأمنية المعلومات وكن لسوء الحظ ، فان التشفير لا يوفر هذا النوع من الحماية. التشفير غالبا ما يكون عرضة للبيع بسبب انه المجال الوحيد لحل مشاكل الأمنية أو التهديدات . فمثلا ، البعض يقول أن التشفير يستطيع إيقاف تحطمات الحاسبة.

التشفير ليس إلا حماية ضد العديد من طرق الهجوم المعروفة والشائعة والمتضمنة تلك الهجمات التي تستثمر التجهيزات الافتراضية (Default Settings) أو الانتهاكات في بروتوكولات الشبكات أو البرمجيات – حتى برمجيات التشفير . على العموم فان هناك حاجة إلى طرق غير التشفير يجب أن تبقى خارج متناول الدخلاء. تم اقتراح طرق معينة بدون استخدام أي تشفير.

علاوة على ذلك ، فان الحماية المتوفرة بواسطة التشفير يمكن أن تكون تعطي وهما كبيرا . إذا تم التعرض للنظام الذي يستخدم التشفير ، فان الدخيل قد يكون قادرا على إمكانية الوصول إلى النص الواضح مباشرة من الملفات المخزونة أو من محتويات الذاكرة أو تحوير بروتوكولات الشبكة ، التطبيقات البرمجية ، أو برامج التشفير لغرض الحصول على وصول إلى المفاتيح او بيانات النص الواضح أو تدير عملية التشفير . تم تقديم دراسة حديثة للتطفل او الاختراق لـ ٨٩٣٢ من

الحاســـبات من قبل وكالة أنظمة معلومات الدفاع (Defense Information Systems Agency) أوضـــحت هذه الدراســـة أن 88% من الحاســـبات ممكن مهاجمتها بنجاح . تحتاج أمنية المعلومات إلى وســـائل أكثر بكثير من اســـتخدام التشـــفير فقط – مثلا تحتاج الى توفير إثبات الشـــخصـــية ، إدارة المواصـــفات (Configuration Management)، التصـــميم الجيد ، ســـيطرات وصـــول ، جدران حماية من الحريـــق (Firewalls)، تدقيق سمعي (Auditing) .

من جانب آخر فان للتشـــفير عيوب شـــتى غالبا ما يتم التغاضـــي عنها . تؤدي الإمكانيات الواسـعة للتشـفير المكسـور مع الخدمات المجهولة إلى حالة والتي فيها تكون الاتصالات عمليا حصينة ضد الاعتراضات القانونية كما تجعل الوثائق غير قابلة للبحث والتمحيص القانوني . كذلك يمكن أن يسـتخدم التشـفير من قبل الخونة والعملاء ، وكـذلـك الحـالات التي فيهـا تكون المعـاملات الالكترونيـة غير قـابلـة الوصول لأي تنظيم حكومي أو مراقبة .

التشفير يمتلك تهديـدا علـى المنظمات والأشخاص أيضا . باستخـدام التشفير ، فان مستخدم معين أو موظف ما لشركة معينة يستطيع بيع معلومات الكترونية إلى منافس ما بدون الحاجة إلى استنساخ أو معالجـــة وثيقة فيزيائية . يمكن شـــراء وبيع المعلومات الالكترونيـــة فـــي ما يسمى "الشبكات السوداء " (Black Networks) بأمنية كاملة ومجهولة المصدر بشكل كامل .

عند الأخذ بنظر الاعتبار التهديدات التي يملكها التشفير ، فانه من المهم الإدراك اســـتخدام التشـــفير فقط لأغراض الوثوقية (Confidentiality)، متضـــمنا المجهولية (Anonymity)، له مشـــاكله الأمنية أما اســـتخدام التشـــفير لتكامل البيانات واثبات الشخصية (Authentication)، متضمنا ذلك التواقيع الرقمية ، لا يعتبر تهديدا ويتميز بكفاء أمنية عالية.

٢-١١-١: الانســـياق باتجاه التشـــفير المفوض حكوميا (The Drift Toward Crypto Anarchy):

يوفر التشـــفير حكوميا (Crypto) فوائد حماية الوثوقية لكن لا يعمل شـــيئا حول مضـارها . انه تشـفير مثبت حكوميا والذي ينكر الوصـول إلى الحكومات حتى تحت أمر المحكمـة أو أي أمر قـانوني أخر . انـه لا يمكنـه مراقبـة لغرض حمـايـة المسـتفيدين ومنظماتهم من الأحداث وسـوء الاسـتخدام . انه يشـبه السـيارة بدون مكبحات (بريك).

٢-١١- ٢: ظهور عهد تنفيذ المفتاح (Key Escrow) كبديل:

ان فوائد التشفير القوي يمكن تحقيقها بدون إتباع تشفير الحكومات (Crypto Anarchy). قد يمكن للشخص أن يعطي بديل وهو تشفير تنفيذ عهد المفتاح (Key Escrow). هذه الفكرة هي بربط التشفير القوي مع إمكانيات فتح الشفرة الملحة . هذا يتم إنجازه بربط البيانات المشفرة بمفتاح استرجاع البيانات والذي يسهل عملية فتح الشفرة. لا يتطلب هذا المفتاح ان يكون نفس المفتاح المستخدم في فتح الشفرة العادي ، لكن يجب ان يوفر وصول الى ذلك المفتاح . يمكن حمل مفتاح استرجاع البيانات (Data Recovery Key) بواسطة وكيل موثوق ، والذي يمكن تصوره مثل وكيل حكومي ، محكمة ، منظمة خاصة موثوقة . يجب ان يقسم بين العديد من هذه الوكالات.

في ابريل من عام ١٩٩٣ ، وكاستجابة للحاجة الملحة لاستخدام منتجات التشفير ، فان إدارة كلينتون أعلنت نوع جديد وتمهيدي للتشفير بأسلوب معين بحيث تكون وكالات التحقيق مخولة لاعتراض الاتصالات أو البحث في ملفات الحاسبات . ثم توجهت الوكالات الحكومية الى تطوير سياسة تشفير شاملة تكون ملائمة لاحتياجات الخصوصية والأمنية للمواطنين والأعمال التجارية وتمكين الدوائر الحكومية المخولة للوصول إلى الاتصالات والبيانات تحت محكمة مناسبة أو أي أمر قانوني أخر ، كل ذلك للبدء لاستخدام التكنولوجيا الحديثة لغرض بناء البنية التحتية للمعلومات الدولية (National Information Infrastructure) ، وتهيئة الشركات الأمريكية لصنع وتصدير منتجات تكنولوجية عالية تحت حماية أمنية عالية فطورت الحكومة رقيقة معتمدة على تشفير المفتاح ذو العهد التنفيذي (Escrowed Encryption Chip) أطلق عليه رقيقة Clipper .

تملك كل رقيقة Clipper مفتاحا مميزايبرمج عليها ويستخدم لاسترجاع الببيانات المشفرة بتلك الرقيقة . يقسم هذا المفتاح الى مكونين يحملان من قبل وكالتين حكوميتن منفصلتين . تم تبني المواصفات العامة لرقيقة Clipper في شباط من العام ١٩٩٤ كتشفير متعهد قياسي (Escrowed Encryption Standard (EES) و هو قياس حكومي طوعي للاتصالات الهاتفية، مشتملا الصوت ، الفاكس ، والبيانات.

لقد اقترح العديد من الشركات تصاميما لأنظمة المفتاح التعهدي (Escrow) التجارية حيث فيها عملاء التعهد يستطيعون الوثوق بطرف ثالث والذي يوفر خدمات فتح الشفرة الطارئة لكل من المستفيدين وموظفي الحكومة المخولين . صممت بعضا من هذه الأنظمة المقترحة لتوفير هدفا رئيسيا وهو أن تكون هذه الأنظمة ملائمة للاستخدام الدولي . احد هذه الأمثلة هو الذي تم اقتراحه من قبل (Bankers Trust) للأنظمة التجارية الدولية للاتصالات السرية ، حيث يستخدم

هذا النظام كلا من الكيان المادي والبرمجي ، خوارزميات غير مصـــنفة ، تشـــفير المفتاح العام لغرض تأســـيس المفتاح ووظائف مفتاح التعهد .على العموم فان تشفير الكيان المادي (Hardware Encryption) يوفر أمنية أكثر من التشفير البرمجي .

٢-١١-٣: البدائل لمفتاح التعهد (Alternatives to Key Escrow):

إن مفتاح التعهد هو ليس الوسيلة الوحيدة لغرض تبني وصول حكومي مخول. هناك توجه آخر هو التشـفير الضـعيف (Weak Encryption) الذي تكون فيه مفاتيح تشـــفير البيانات بالحد الذي يمكن فيه تحديد المفتاح عند محاولة كل الاحتمالات. من وجهة نظر المستفيد ، فان تشفير مفتاح التعهد (Escrow) له فوائد أكثر نسبة إلى التشـفير الضـعيف وذلك بالسـماح للمسـتفيد باسـتخدام خوارزميات تشفير قوية غير معرضة للهجوم . على كل حال ، فان التطبيقات التي لا تحتاج مثل هذا المستوى العالي من الأمنية ، فان التشـفير الضـعيف يوفر بديلا اقل كلفة . يكمن العيب في التشـفير الضـعيف (إذا لم يكن ضـعيفا جدا) من وجهة نظر القانون هو أن هذا التشـفير يمكنه أن يعيق فتح تشـــفير الوقت الحقيقي (Real- Time Decryption) في الحالات الطارئة (مثلا ، اختطاف الأشخاص).

هنـاك توجـه ثـالـث هو تشـــفير الربط (Link Encryption) وهو خـاص بالاتصالات التي عادة ما تشفر بين عقد الشبكة ولكن ليس عبر العقد . لهذا ، فان اتصـالات النص الواضـح يمكن الوصـول إليها في عقد تبادل الشـبكة . من الفوائد الأســاســية لتشــفير الربط هو الســماح لشــخص ما يحمل هاتف خلوي بحماية الاتصـــال عبر الهواء في نظام الهاتف بدون الحاجة إلى امتلاك الشـــخص الأخر لجهاز تشفير متوافق ، أو حتى في الواقع بدون الحاجة إلى أي تشفير مطلقا.

الفصل الثالث

مقدمة في طرق التشفير

٣-١ :التشفير(Cryptography):

قبل الحديث عن طرق التشفير هناك بعض التعريفات الهامة نذكر منها:

١: تحليل الشـفرة (Crypt analysis) عبارة عن دراسـة التقنيات الرياضـية لغرض الاستفادة منها في محاولة التعرض أو إحباط التقنيات التشفيرية .

٢: محلل الشـفرة (Cryptanalyst) عبارة عن شـخص ما يرتبط عمله باسـتخدام تقنيات تحليل الشفرة.

٣: علم التشـــفير (Cryptology) ويشـــمـل دراســـــة كـل من التشـــفير (Cryptography) وتحليل الشفرة (Cryptanalysis). الـــ Cryptology (من الكلمة الإغريقية kryptós lógos والتي تعني الكتابة المخفية) .

٤: نظام التشفير (Cryptosystem) عبارة عن مصطلح عام يشير إلى مجموعة من أســاســيات التشــفير و المســتخدمة لتوفير الخدمات الضــرورية لتأمين أمنية المعلومات .

تقسم التقنيات التشفيرية إلى نوعين عاميين:

١: تقنية المفتاح المتناظر (Symmetric Key).

٢: تقنية المفتاح العام (Public Key).

٣-٢ : تشفير المفتاح التناظري (Symmetric- Key Encryption):

هناك نو عان عامان من الخوارزميات المعتمدة على المفتاح : الخوارزميات التناظرية و خوارزميات المفتاح العام . الخوارزميات التناظرية ، في بعض الأحيان تسمى الخوارزميات التقليدية (Conventional Algorithms) ، وهي عبارة عن خوارزميات يكون فيها إمكانية حساب مفتاح التشفير من مفتاح فتح الشفرة وبالعكس . (في معظم الأنظمة التناظرية فان مفتاح التشفير ومفتاح فتح الشفرة هما نفسهما) . يطلق على هذه الخوارزميات كذلك خوارزميات المفتاح السري ، أو خوارزمية المفتاح الواحد ، و تحتاج أن يتفق كل من المرسل والمستقبل على مفتاح معين قبل أن يتصلا بأمان . تعتمد أمنية خوارزمية التناظرية على المفتاح .

تقسم الخوارزميات التناظرية إلى صنفين . خوارزميات تعمل على النص الواضح كثنائية واحدة bit (أو في بعض الأحيان byte واحد) في الوقت الواحد ويطلق عليها خوارزميات التدفق (Stream) .وخوارزميات أخرى تعمل على النص الواضح بشكل مجاميع من الثنائيات يطلق عليها كتل (Blocks) ، وتسمى هذه الطرق خوارزميات الكتلة أو شفرات الكتل (Block Ciphers) . يبلغ حجم الكتلة النموذجي في الحاسبات الحديثة ٦٤ ثنائية وهذا حجم كاف لإعاقة التحليل من غير تبديد . (قبل استخدام الحواسيب كانت الخوارزميات عموما تعمل على نص واضح بشكل حرف واحد في الوقت الواحد ، بهذا يمكن التفكير اعتبارها خوارزمية تدفق تعمل على حزمة (تدفق) من الحروف) .

في الأنظمة التقليدية يتم استخدام نفس المفتاح للتشفير وفتح الشفرة . إن التحدي الأساسي هو جعل المرسل والمستقبل يتفقان على المفتاح السري بدون أن يعرفه أو يجده أي شخص آخر . إذا كان المرسل والمستقبل في أماكن منفصلة ، فان عليهما الوثوق بحامل معين ، نظام الهاتف ، أو أي وسيلة إرسال أخرى لمنع كشف المفتاح السري . إن توليد ، إرسال وخزن المفاتيح تسمى إدارة المفتاح(key management) . كل أنظمة التشفير يجب أن تتعامل مع مسائل إدارة المفتاح . بسبب أن كل المفاتيح في نظام تشفير المفتاح التناظري يجب إن تبقى سرية ، فان هذا النظام يعاني غالبا من إشكالية إدارة مفتاح بصورة أمينة ، خاصة في الأنظمة المفتوحة والتي فيها عدد كبير من المستفيدين .

٣-٣ : نظرة سريعة عن شفرات التدفق والكتل (Overview of Block Ciphers and Stream Ciphers):

تعريف ٣- ١ :

إذا كان لدينا نظام تشـــفيري مكون من تحويلات التشـــفير وفتح التشـــفير بمعنى $\{E_e:e\in K\}$ و $\{D_d : d \in K\}$، حيث K هو مساحة المفتاح ، يكون النظام التشفيري متناظر (Symmetric - key) إذا كان في زوج المفتاح (e,d) فانه من السهولة تحديد d بمعرفة e فقط وكذلك يمكن تحديد e من d فقط .

في معظم الأنظمة التشـــفير التناظرية (Symmetric) فإن d= e ، ويمكن أن تســـتخدم مفردات أخرى للأنظمة التناظرية مثل المفتاح المفرد (Single-Key)، المفتاح الواحد (One-Key)، المفتاح الخاص (Private Key) أو التشـــفير التقليدي (الكلاسيكية)(C conventional Encryption).

ان المفتاح المتفق عليه بين اثنين من المشتركين يحدد في انظمة التشفير الكلاسيكية كل من خطوات التشفير وخطوات فتح الشفرة في اسلوب بسيط والذي ينظر اليه على انه عملية تناظرية تتطلب نفس الجهد المطلوب .
هذه الأنظمة ، تسمى أحيانا طرق المفتاح الخاص (Private Key Methods) لم يتوقف وجودها بحلول عصـــر الالكترونيات ، بحوالى ١٩٥٠ . تعتمد ســـرعة تحليل التشفير على سرية المفتاح . إضافة إلى ذلك ، إذا رغب المستفيد بان يكون مشـــفر غير مخول حتى بمعرفة صـــنف الطريقة المســـتخدمة ســـوف لن يجد هذا المفتاح . إثبات الشخصية ليست مشكلة ، وانـــــه يمكن ضمانها طالما كان هناك للأمنية .

على كل حال ، فانه توجد مساوئ معينة :

١: انه من غير الممكن بالنسبة لمرسل الرسالة أن يبرهن لشريكه أو طرف ثالث بأنه قد أرسل رسالة معينة . هذا يعتبر نقص في الحماية الشرعية .

٢: المفاتيح المطلوبة للاتصـــال أو المحادثة على قناة إرســـال معينة والتي أمنيتها التحليلية للشـــفرة أعلى بكثير عن أمنية القناة المســـتخدمة في تناقل البيانات المضادة . الاتصال الأمني الذاتي قد لا يكون ممكنا .

٣: بوجود عدد كبير من المشتركين واللذين يطلبون اتصال سري ، فان عدد قنوات الاتصال ذات الاتجاهين وبذلك عدد المفاتيح سيصبح كبير جدا . بالنسبة لشبكة معينة فيها ن من المشتركين ، كل واحد منهم يريد تبادل الرسائل بأمان مع كل مشترك ، نحتاج إلى ضرورة وجود ن (ن-١) من المفاتيح التناظرية . إذا كانت ن = ١٠٠٠ فان الرقم سيكون 999000 .

مثال ٣- ١ :

إذا كان لدينا: A={A,B,C,.....,X,Y,Z} ونفرض أن C,M عبارة عن سلسلة ذات طول ٥ من حروف A . يتم اختيار e من المجموعة A . تقسم العبارة إلى كتل مكونة كل منها من خمسة أحرف وإذا كانت العبارة أقل من ٥ أحرف فيتم إكمالها بحيث يصبح طولها ٥ أحرف .

تتم عملية التشفير بواسطة المفتاح e . أما إعادة فتح الشفرة فيكون بموجب d = e-1.

كمثال نفرض أن مفتاح e اختير بحيث يتم تزحيف كل حرف إلى الحرف الذي يليه بثلاث مواقع إلى اليمين ، مثلاً

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

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

لذلك فإن العبارة :

m =THISC IPHER ISCER TAINL YNOTS ECURE

يمكن تشفيرها باستخدام $C=E_e(m)$

C= WKLVF LSKHU LVFHU WDLQO BQRWV HFXUH

هنا يمكن استخدام إزاحة (Shift) بمقدار آخر على (٣) او يكون بموجب معادلة يتفق عليها الطرفان فيزيد بذلك من قوة هذه الطريقة). الشكل ٣ - ١ يوضح كيفية الاتصال بين طرفي الإرسال في نظام المفتاح المتماثل والذي يماثل شكل ٢-١ (في الفصل الثاني) مع إضافة قناة اتصال أمينة لتحقيق الوثوقية والشرعية (Confidential and Authentic) .

من المسائل الرئيسية في أنظمة التشفير المتماثل هو إيجاد وسيلة كفؤة يتم فيها الاتفاق وتبادل المفاتيح بصورة سرية أو أمينة ان هذه المسألة يشار إليها بمسألة توزيع المفاتيح (Key Distribution Problem) .كما تم مناقشته سابقاً فأن أمنية طرق التشفير تعتمد على سرية المفتاح وليس على طريقة التشفير وعلى هذا الأساس فأن أنظمة التشفير المتناظر يجب أن تبقى المفتاح d سري (Secret) وفي هذه الأنظمة يعني ذلك أيضا أن المفتاح e يجب أن يكون سري ولذلك فأنه ينتقل في كينونة إلى أخرى مع التفاهم بأن كل من طرفي الاتصال يمكنه ان يكون المفتاح d .

هناك صنفان رئيسيان في أنظمة التشفير التناظرية هما :

١ : شفرة الكتل (Block Cipher) .

٢ : شفرة التدفق (Stream Cipher) .

٣ - ٤ : تعريف شفرة الكتل (Block Cipher):

شفرة الكتل عبارة عن طريقة تشفير والتي تقسم العبارة الواضحة المرسلة إلى سلاسل (Strings) تسمى كتل (Block) ذات طول ثابت t في مجموعة الأحرف الأبجدية A، ويتم تشفير كتلة واحدة في اللحظة الواحدة . تعمل شفرات الكتل على كتل من النص الواضح والنص المشفر . عادة يكون طول الكتلة ٦٤ بت (ثنائية)لكن في بعض الأحيان تكون الكتلة أطول .

شفرة الكتلة هي نوع من خوارزمية المفتاح التناظري والتي تحول بيانات كتلة من النص الواضح ذات طول ثابت إلى بيانات نص مشفر بنفس الطول . إن التحويل يتم تحت تأثير مفتاح سري متوفر للمستفيدين . إن الطول الثابت للكتلة يسمى حجم الكتلة (Block Size) ، وللكثير من شفرات الكتلة ، فان حجم الكتلة كما ذكرنا سابقا هو ٦٤ بت . في السنين القادمة فان حجم الكتلة سوف يزداد إلى ١٢٨ بت بسبب أن المعالجات تصبح أكثر تعقيدا . يرى الرياضيون أن شفرة الكتلة سوف توفر وبشكل مؤثر تبادلا لمجموعة كل العبارات المحتملة ومن ثم فتح شفرة متميزة ووحيدة . إن التبديل المؤثر خلال أي عملية تشفير معينة هو بالطبع عملية أمينة ، بسبب أنها دالة للمفتاح السري .

معظم تقنيات التشفير المتناظر هي شفرات كتل ويوجد نوعان منها :

١ : شفرة الإحلال (Substitution Cipher) .

٢ : شفرة الإزاحة أو الانتقال (Transposition Cipher) .

يمكن جمع الشفرتين أعلاه معاً لتكوين ما يسمى شفرة الضرب (Product Cipher) .

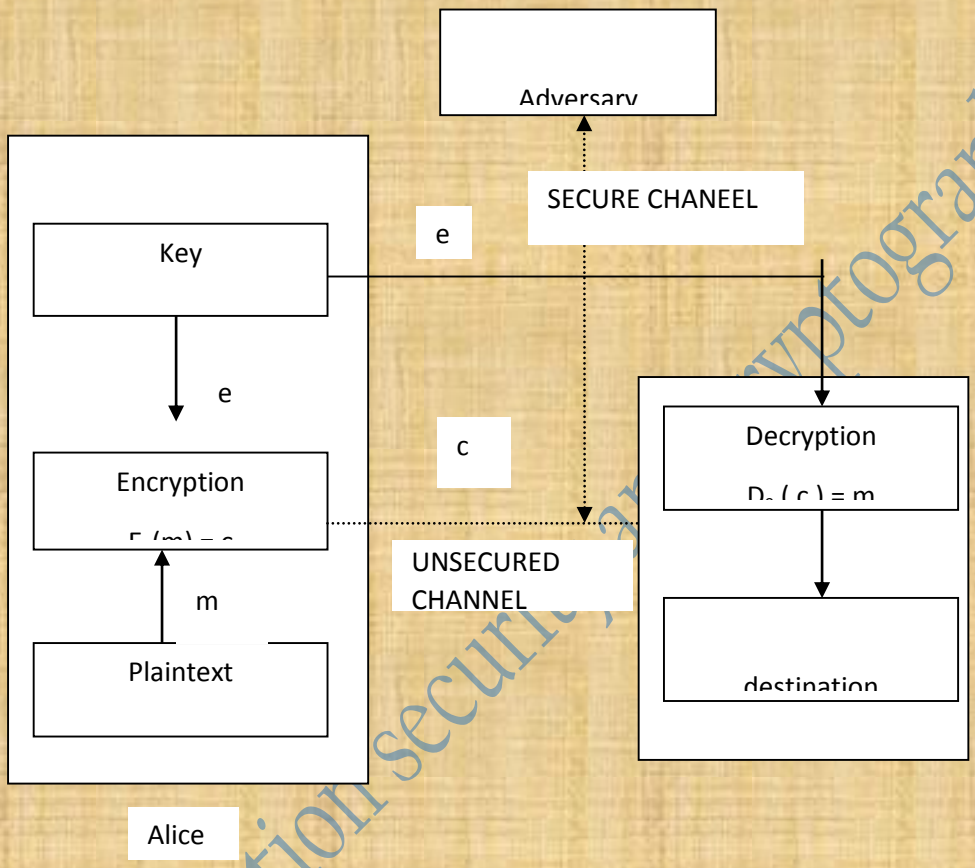
٣- ٥ : شفرات الإحلال وشفرات الانتقال (Substitution Ciphers and Transposition Ciphers):

قبل استخدام الحاسبات ، فان علم التشفير يتكون من خوارزميات معتمدة على الحروف . هناك عدة خوارزميات تشفيرية مختلفة أما تستخدم إحلال الحروف الواحد محل الأخر أو نقل الحروف بحرف أخر . الخوارزمية الأفضل هي التي تستخدم الاثنان معا (الإحلال والانتقال) . الآن مع الحواسيب ظلت الفلسفة كما هي ولكن التغيير الأساسي في الخوارزميات هو عملها على ثنائيات بدلا من حروف .

٣-٥- ١ : الإحلال :

شفرات الإحلال هي احد أنواع شفرة الكتل والذي يتم فيه إحلال رموز (أو مجموعة رموز) برموز أو مجموعة رموز أخرى .

شكل٣-١ : اتصال بين اثنين من المشتركين باستخدام التشفير ، مع قناة أمينة لتبادل المفتاح .



تعريف ٣-٥-٢ : شفرات الإحلال البسيط (Simple Substitution Ciphers)

نفرض أن A هي مجموعة مكون من q من الرموز

M مجموعة من كل السلاسل)بطول t .

K مجموعة من كل التبديلات (Permutation) للمجموعة A .

وباستخدام المفتاح e ($e \in k$) يمكن تعريف E_e كما يلي:

$$(m)=(e(m_1)e(m_2).....e(m_t)=(c_1c_2....c_t)=c$$

حيث أن: $m=(m_1m_2.....m_t) \in M$

لغرض فتح شفرة العبارة c يتم حيث $c=(c_1c_2....c_t)$ فيكون لحساب المفتاح d حيث أن :

$d=e^{-1}$ و تطبيق D_d بالشكل التالي:

$$D_d(c) =(d (c_1)d(c_2).....d(c_t)=(m_1m_2....m_t)=m.$$

E_e تسمى شفرة التبديل البسيط أو تشفير الإحلال الأحادي الأبجدي (Mono-Alphabetic Substitution Cipher) . عدد تشفيرات التبديل هو ! q ولا يعتمد على حجم الكتلة في الشفرة (Cipher).

إن شفرة الإحلال الأحادية عبارة عن شفرة والتي فيها سيستخدم تحويل واحد-إلى-واحد لغرض إحلال كل رمز من النص الواضح بما يقابله من نص مشفر . غالبا ما يستخدم نفس المجموعة من الرموز في كلا من النص الواضح والنص المشفر .

يمكن أن يعرف نظام الإحلال البسيط على انه عبارة عن تبديل (Permutation) π لمجموعة الأحرف الأبجدية وكل حرف من العبارة يتم إحلاله بصورته تحت التبديل π . اعتياديا ، فان المفتاح يمثل بسلسلة حرفية من ٢٦ حرفا ، وبعد ذلك يتم إحلال أي تكرار للحرف A مثلا .....UXEB ، بهذا يتم إحلال كل حرف A بالحرف U ، B بالحرف X وهكذا . عادة ما يتم إهمال الفراغات ويتم تركها في النص المشفر . توصف شفرة الإحلال البسيط بأنها الشفرة أحادية الأحرف (Monoalphabetic Cipher) . مثل هذا النوع من الأنظمة تكون معرضة بشدة إلى الهجوم الذي يستخدم خواص اللغة في تكرار للأحرف ، الأحرف الثنائية (Diagram) ، الخ مثلا الـــــ في العربية و qu في الإنجليزية ، وان

المســـتلزم الأســـاســـي والضـــروري لنظام أمين هو أن يكون متعدد الأحرف (Polyalphabetic) .

عندما يرسـل شـخص معين عبارات سـرية إلى شـخص آخر فانه غالبا ما يجد رمزا وذلك بجعل كل حرف من الحروف الأبجدية تمثل حرفا آخر ، و هذا ما يطلق عليه بالشـفرة الأحادية الأحرف . لغرض الحصـول على هذا الإجراء فان ذلك يتم بكتابة الأحرف الأبجدية و تبديل كل حرف بحرف آخر . هنا سـيتم اسـتخدام مفتاح معين ويجب أن يكون معروفا لكل من المرسـل والمسـتقبل . غالبا ما يشـار إلى الشـفرة أحادية الأحرف بشـفرات الإحلال البسـيط (Simple Substitution Ciphers) .

شـفرات التبديل البسـيط والتي تعمل على حجوم كتلة صـغيرة لا توفر أمنية مناسبة حتى ولو كانت مساحة المفتاح كبيراً جداً .فإذا كانت لدينا مجموعة الأحرف المكونة لأحرف اللغة الإنكليزية ستكون مساحة المفتاح $4*10^{26} = 26!$ ، إلا أن المفتاح المستخدم يمكن تحديده بسهولة وذلك باختبار كمية بسيطة من النص المشفر على ضوء تكرارية أو تردد الحروف (Letter Frequencies) والموجودة في النص المشفر . كمثال على ذلك فأن الحرف E يكون أكثر تكراراً في باقي حروف اللغة الإنكليزية . لذلك فأن الأكثر تكرار في النص المشفر يقابل الحرف E في النص الواضح ، ومن ثم بملاحظة كمية بسيطة في النص المشفر يتمكن محلل الشفرة في تحديد المفتاح .

٣-٥-٣ : أنواع شفرات الإحلال:

في التشفير الكلاسيكي ، يوجد أربعة أنواع من شفرات الإحلال :

١ : الشـفرة أحادية الحرف او البسـيطة (Monoalphbetic Cipher): هي الشـفرة التي فيها كل حرف من النص الواضـح يعوض بحرف مقابل في النص المشفر.

٢ : شفرات الإحلال المتجانس (Homophonic Substitution Ciphers) : تشبه هذه الشفرة نظام شفرة الإحلال البسيط ، عدا أن كل حرف مفرد من النص الواضح يمكن أن يحول إلى نص مكون من عدة أحرف مكـونة النص المشفر . كمثـال ، فان الحرف " A " يمكن أن يقابل إمـا ٥٦ ،أو ، ٢٥ ، ١٣ ، ٥ ، " B " يمكـن أن يقابـل أما ٤٢ أو ، ٣١ ، ١٩ ، ٧ وهكذا.

٣: شفرات الإحلال المتعدد (A Polygram Substitution Ciphers) : هي الشـفرة التي فيها كتل من الحروف تشـفر في مجموعات . مثلا ، " ABA " يمكن أن تقابل " RTQ " ، " ABB " يمكن أن تقابل " SLL " وهكذا .

٤: شفرة متعددة الأحرف(A polyalphabetic ciphers) : مكونة من عدة شفرات إحلال بسيطة كمثال ، قد تستخدم خمسة شفرات إحلال بسيطة نزاراتيم عبد المطلب في وقت واحد ، بمعنى أخر، فإنها تستخدم أكثر من تحويل (Mapping) . من الناحية التاريخية فقد تم تطوير شفرة الإحلال متعدد الأحرف من قبل (Alberti) في العام ١٤٦٦ .

الشفرة القيصرية تعتبر شفرة مشهورة.

ROT 13 هي عبارة عن برنامج تشفير بسيط غالبا ما يستخدم في أنظمة UNIX ، إنها أيضا شفرة إحلال بسيط . في هذه الشفرة ، " A " يعوض بالحرف " N " ، " B " يعوض بالحرف " O " وهكذا . كل حرف يدور ١٣ خانة . إن تشفير ملف معين مرتين باستخدام ROT 13 فانه سيعيد الملف الأصلي : (P = ROT 13 ROT 13 (P))

يمكن بسهولة كسر شفرات الإحلال البسيط بسبب أن الشفرة لا تخفي الترددات الأساسية للحروف المختلفة من النص الواضح . كل ما تستخدمه هذه الشفرات هو ٢٥ حرفا في اللغة الإنكليزية قبل أن يستطيع محلل شفرة جيد أن يعيد ترتيب النص الواضح . تم تصميم خوارزمية لحل هذه الأنواع من الشفرات .

استخدمت شفرات الإحلال المتجانس (Homophonic) في بداية العام ١٤٠١ . تتميز هذه الشفرات بأنها أكثر تعقيدا لان تكسر من شفرات الحلال البسيط ، لكن ما زالت لا تخفي كل الخصائص الإحصائية للغة النص الواضح . باستخدام هجوم النص الواضح المعروف ، فان هذه الشفرات تكون سهلة الكسر جدا . الهجوم الأصعب هو هجوم النص المشفر فقط ، لكنه يستغرق ثواني قليلة فقط في الحاسب .

شفرات إحلال (Polygram) هي الشفرات التي فيها مجموعة من الأحرف تشفر سوية . اكتشفت شفرة (Playfair) في ١٨٥٤ و قد تم استخدامها من قبل الإنكليز خلال الحرب العالمية الأولى . هذه الشفرة تقوم بتشفير زوج من الأحرف معا . مثال أخر لهذا النوع من الشفرات هو شفرة(Hill) . في بعض الأحيان يمكن ان ينظر غلى ترميز هوفمان (Huffman Coding) انه يستخدم كشفرة ويعتبر شفرة إحلال (Polygram) غير أمينة .

تم اكتشاف شفرات الإحلال المتعدد الأحرف (Polyalphabetic) من قبل (Lean Battista) في العام ١٥٦٨ . لقد استخدمت من قبل الجيش الاتحادي خلال الحرب الأمريكية الأهلية . بالرغم من إن هذه الشفرات يمكن بسهولة كسرها (خاصة بمساعدة الحواسيب) ، فان العديد من منتجات أمنية الحاسبات

التجارية تستخدم شفرات من هذا النوع . شفرة فايجنر التي تم الإعلان عنها لأول مرة في ١٥٨٦ وشفرة (Beaufort) يعتبران أيضا مثالين لشفرات الإحلال متعددة الأحرف.

تملك شفرات الإحلال متعددة الأحرف مفاتيحا متكونة من عدة حروف ، ويستخدم كل حرف من المفتاح لتشفير حرف واضح من النص الواضح . لذلك فان كل حرف يمثل مفتاح . المفتاح الأول يشفر الحرف الأول من النص الواضح ، المفتاح الثاني يشفر الحرف الثاني وهكذا . بعد أن يتم اكتمال كل المفاتيح المستخدمة ، فان المفاتيح (الأحرف) يعاد تكرارها . في حالة وجود مفتاح مكون من ٢٠ حرفا فانه سيتم تشفير كل ٢٠ حرفا بنفس المفتاح . هذا يطلق عليه فترة (Period) الشفرة . في علم التشفير الكلاسيكي فان الشفرات التي تملك فترات أطول كانت تواجه صعوبة في كسرها تكثر مما تواجهه تلك الشفرات التي تملك فترات اقصر . هناك تقنيات في الحاسب والتي يمكنها بسهولة كسر شفرات الإحلال التي تملك فترات طويلة .

شفرة المفتاح التنفيذي (Running - Key Cipher) والتي أحيانا يطلق عليه شفرة الكتاب (Book Cipher) حيث تستخدم نص واحد لتشفير نص آخر ، هو مثال لهذا النوع من الشفرة . بالرغم من هذه الشفرة تملك فترة (Period) بطول النص ، فانه يمكن كسرها بسهولة.

٣-٥-٤ :الشفرات الجمعية: (Additive Ciphers):

احد الأمثلة الأولى للشفرات أحادية الحرف كانت شفرة قيصر (Caesar Cipher) . في هذه الشفرة كل حرف من a إلى w تمثل بإزاحة ٣ مواقع بعد الحروف في موقع الحروف الأبجدية ، يتم تمثيل الأحرف x,y,z بالأحرف A,B,C على التوالي . لذلك فان شفرة قيصر تمثل كالأتي :

plaintext: 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

ciphertext: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

مثال٣. ٢ :

Plaintext	:	Caesar	was	a	Great	Solider
Ciphertext	:	FDHVDU	ZDV	D	JUHDW	VROGLHM

٣-٥-٥ : احلال N-GRAM:

بدلا من إحلال الأحرف ، فانه يمكن اســتخدام إحلال مجموعة من الرموز ، مثلا تقســم بمجموعات ثنائية (Diagrams) ، أو ثلاثية (Triagrams) ، الخ . في الإحلال متعدد الأحرف العام ، مثلا ، فانه سـوف يحتاج إلى مفتاح متكون من تبديل لـــ $٢٦^{٢}$ من المجموعات الثنائية المختلفة ، وانه من المفضـل تمثيله بمصـفوفة قياسية ذات 26 x 26 والتي الأسطر فيها تقابل الحرف الأول من المجموعة الثنائي والأعمدة تقابل الحرف الثاني .

لأي رقم صـحيح موجب d ، فان العبارة M تقسـم إلى كتل بطول d . بعد ذلك ياخذ التبديل л من 1,2,....,d وتطبق л لكل كتلة .

مثال ٣- ٣ :

إذا كانت d=5 و (4 1 3 2 5) = л فان عبارة مثل

M = JOHN IS A GOOD SKIER سوف تتحول إلى

C=ONHJ SA I ODOG KEISR

مثلا الكتلة JOHN تتحول الى ONHJ وهكذا

ينفذ التشفير باستخدام معكوس $л^{-1}$.

٣-٥-٦ : شفرات عبارة المفتاح (Key Phrase Ciphers):

في هذه الشفرات فان المفتاح يأخذ صورة عبارة (Phrase) مع حرف إضافي خاص . بما انه نسـتطيع اسـتخدام أي عبارة ، فسـوف نعرف كم هو العدد الكبير المتزايد للمفاتيح المستخدمـــة . في هذه الشفـــرات يكتب النص الواضح أولا ، ثم تكتـب عبـارة المفتـاح تحتـه مبتـدأ بحرف خـاص ، لكن لايمكن تكرار أي حرف في

حروف العبارة . كمثال ، إذا تكررت METTLE في عبارة المفتاح فإننا نكتب فقط METL . بعد ذلك تكتب حروف النص المشفر بعد عبارة المفتاح .

مثال ٣- ٤ :

لنأخذ عبارة المفتاح MY LITTLEFINGER مع حرف خاص d . أولا سنكتب العبارة أعلاه بعد حذف الأحرف المتكررة لنحصل على MYLITEFNGR . بع ذلك نكتب أحرف النص الواضح وتكتب M تحت d لنحصل على :

plaintext : 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

ciphertext : M Y L I T E F N G R

الآن تم اكتمال الإحلال الحرفي وذلك بكتابة ما تبقى من أحرف النص المشفر مبتدأ بالحرف A تحت n ثم B. تحت O ثم C تحت P وهكذا حتى الوصول إلى الحرف Z الذي سيكون تحت C . هذا يعطينا الأتي :

plaintext : 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

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

بما أن أي عبارة مفتاح قد يمكن اختيارها ، لذلك فإننا سنكون قد نجحنا في الحصول على شفرة يكون فيها المفتاح قد تم اختياره بحيث يمكن تذكرة بسهولة . كذلك فانه من الواضح أن محلل الشفرة ليس بامكانه فتح هذه الشفرة وذلك باستخدام أسلوب محاولة كل عبارات المفتاح الممكنة . وهذا يعتبر أسلوبا غير عملي كثرة عبارات المفتاح

إذا حاولنا تبديل ٢٦ حرفا من مجموعة الأحرف الأبجدية في أي ترتيب ويكتبها تحت حروف النص الواضح ، فسوف يكون لدينا شفرة أحادية الأحرف (Monoalphabetic) . يوجد !26 تقريبا وهذه تساوي تقريبا $4x10^{26}$ ، إذن حتى مع سرعة الحواسيب الحالية ، فانه من غير الممكن لأي محلل شفرة أن يضمن فتح شفرة أي نص مشفر وذلك بتجريبه لكل الاحتمالات .

لايمكن لمحلل الشفرة تجريب كل الاحتمالات ، لذلك قد يعتقد المشفر هذا النظام يوفر أمنية معقولة . لكن هناك العديد من المقترحات الرياضية والإحصائية والتي تمكن محلل الشفرة من التخلص من ملايين المفاتيح في وقت واحد ، انه ق لا يحتاج لتجريب كل المفاتيح .

مثال ٣ - ٥ :

نفرض لدينا العبارة m ممثلة بالشكل التالي $m=m_1m_2m_3$..... . تقوم خوارزمية التشفير الأحادي بتعويض كل حرف بإحلال وحيد ، حيث سيكون لدينا كما هو معروف !26 من المفاتيح . حالما يتم اختيار مفتاح معين k مع التحويل المرتبط به t ، عند ذلك فانه لأي m في مساحة العبارة M ، سيتم التشفير بالشكل c=t(m) .

أولا سنقوم بكتابة النص الواضح وتحت كل حرف نكتب ما يقابله من النص المشفر . لذلك سنحصل على :

plaintext : a b c d .....

ciphertext: t(a) t(b) t (c) t(d) .....

تعريف ٣- ٢ : شفرات الإحلال المتجانس (Homophonic Substitution Ciphers):

في هذه الطريقة التشفيرية يتم إحلال كل رمز a في كتلة من النص الواضح بسلسلة مختارة عشوائياً من H(a) . ولغرض فتح الشفرة c والمتكونة من t من الرموز ، فيجب علينا أن تحدد a εA بحيث أن C∈ H(a) – أن المفتاح هنا مكون من المجموعات في H(a) .

مثال ٣-٦ :.

افرض أن :

A={a,b}

H(a)={00,10}

H(b)={01,11}

يمكن تشفير النص الواضح ab الى واحد من آلاتي :

١٠١١,١٠٠١,٠٠١١,٠٠٠١

لذلك يمكننا تحديد شفرات العبارات الواضحة التالية كما يلي :

aa → { 0000, 0010, 1000, 1010 }

ab → { 0001, 0011, 1001, 1011 }

ba ⟶ { 0100, 0110, 1100, 1110 }

bb ⟶ { 0101, 0111, 1101, 1111 }

يمكن بنفس الطريقة اختيار احد مكونات العناصر أعلاه لتحديد النص الواضح .

أي سلسلة أربعة بت (4-bitstring) متميزة تحدد عنصر Coodomain ، وعليه يحدد بذلك عبارة نص مشفر .

في الغالب فان الرموز لا تحدث بتردد متساوي في النص الواضح . في الإحلال البسيط (Simple Substitution) فان تشفير خاصية التردد الغير منتظم قد عكست في النص المشفر . يمكن استخدام شفرة التجانس (Homophonic) استخدامها لجعل التكرار (Occurrence) لرموز النص المشفر أكثر انتظاما على حساب توسيع البيانات (Data Expansion) . لايمكن تنفيذ فتح التشفير (Decryption) بسهولة كما هو الحال في لشفرات الإحلال البسيط .

إن ابسط طريقة تشفير عشوائية هي التي نطلق عليها شفرة الإحلال المتجانس . تحتوي العبارة M على سلسلة من مجموعة الأحرف الأبجدية Σ_1 يتم تشفيرها إلى نص مشفر عشوائي C من الرموز من مجموعة الأحرف الأبجدية Σ_2 ، بحيث أن $\Sigma_2 \geq \Sigma_1$.

٣-٥-٦ : شفرات الإحلال متعدد الأحرف (Polyalphabetic Substitution Ciphers):

يعرف هذا النوع في التشفير بأنه عبارة عن كتلة مشفرة وبطول t في مجموعة الأحرف الأبجدية A ولـه الصفات التالية :

١ : تتكون مساحة المفتاح K من كافة المجاميع المرتبة والتي يتم إعادة ترتيبها بعدد معين هو t (t Permutations) وهذه المجموعة المعادة الترتيب هي ($P_1, P_2, \ldots P_t$) حيث كل واحد في p_i هو ضمن مجموعة الحرف الأبجدية .

٢- لغرض تشفير العبارة $m=(m_1 m_2 \ldots\ldots m_t)$

باستخدام المفتاح $e = (p_1, p_2, \ldots\ldots p_t)$ تكون طريقة التشفير بالصيغة التالية :

$$E_e(m)=(p_1(m_1)p_2(m_2)\ldots\ldots pt(m_t))$$

٣-مفتاح فتح التشفير (Decryption Key) يمكن إيجاده في المفتاح $e=(p_1, p_2 \ldots\ldots, p_t)$ فيكون بذلك

$$d = (p_1^{-1}, p_2^{-1}, \ldots\ldots, p_t^{-1})$$

مثال ٣-٧ : شفرة فايجنر (Vigenere cipher):

نفرض ان A=(A,B,C, ……..,X,Y,Z) وان t=3 ، نختار المفتاح e = (p_1,p_2,p_3) حيث ان:

p_1 تشفر كل حرف وذلك بتبديله بالحرف الذي موقعه ٣ إلى يمين الحرف الأصلي .

p_2 تبدل الحرف الأصلي بـــ ٧ مواقع إلى يمينه .

p_3 تبدل الحرف الأصلي بـــ ١٠مواقع إلى يمينه .

m = THI SCI PHE RIS CER TAI NLY NOT SEC URE

عند ذلك فان :

c = Ee(m) = WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO

تملك شـــفرات الإحلال المتعدد الأحرف فائدة أكثر من شـــفرات الإحلال البســـيط وذلك لان تردد الرمز لا يحفظ .في الأمثلة أعلاه مثلا فان الحرف E قد شـــفر إلى حرفين O ، L . لمحلل الشفرة قد لا يواجه صعوبة بارزة في عملية تحليل الشفرة لهذا النوع من التشفير .

مثال ٣- ٨:

إن شفرة فايجنر تعتبر مثال للتشفير المتعدد الأحرف . رغم أن مساحتي العبارة والنص المشفر همـــا نفسهما ، فان عـــدد المفاتيح سوف يزداد بشكـــل كبير . كل كلمة مفتـاح (Keyword) هـي عبـارة عن مفتـاح وتحـدد تحويل t: M → C . اذا كانت t هي التحويل حيث يحدد التسلسل $t_1t_2t_3t_4$..... للاحلال البسيط من M الى C وان $m=m_1m_2m_3m_4$..... ، عند ذلك فان t(m) = $t(m_1)t(m_2)t(m_3)t(m_4)$..... – كمثـــال على ذلك إذا كانت كلمـــة المفتاح هـــي "may" واذا كانت t_1,t_2,t_3 هـي تتويلات مـن C → M المحدد بالشفرات التجميعيـة مع ازاحـات 12,0,24 على التوالي، فعنـد ذلـك t هي التســلســـل $t_1t_2t_3t_1t_2t_3t_1$..... .

٣ -٥ -٧ : شفرة المفتاح الذاتي (The Autokey C ipher):

في هذا النظام ، فانه يوجد مفتاح أولي ، والذي عادة ما يكون قصيرا ويستخدم في بداية عملية التشفير .عملية التشفير تستمر بعد ذلك ، مستخدمة أما العبارة نفسها أو النص المشفر المنفذ حاليا (Running Cryptogram) .

مثال ٣-٩ :

افرض أن المفتاح هو COMET وان العبارة هي SEND SUPPLIES ، عند ذلك باستخدام العبارة كمفتاح ، سوف نقوم بالترميز للحصول على الجمع بباقي ٢٦ .

M : S E N D S U P P L I E S

K : C O M E T S E N D S U P

Cryptogram U S Z H L M T C O A Y H

باستخدام النص المشفر كمفتاح ، ونفس المفتاح الرئيسي سوف نحصل على :

M : S E N D S U P P L I E S

K : C O M E T U S Z H L O H

Cryptogram U S Z H L O H O S T S Z

٣ ـ٥ ـ٨ : طريقة سريعة لتحليل شفرات الإحلال:

بالامكان إنجاز عملية تحليل شـــفرات الإحلال (كلا من الأحادية والمتعددة الأحرف) باســتخدام خوارزمية ســريعة معتمدة على عملية معينة يتم فيها تخمين مفتاح أولي يتم تنقيته خلال عدد من التكرارات . في كل خطوة فان النص الواضـــح المقابل للمفتاح الحالي يتم تخمينه وان النتيجة تســـتخدم كمقياس لكيفية قرب اكتشاف المفتاح الصحيح .

إن الفكرة من وراء الخوارزمية يمكن اســـتخدامها عموما لهجومات النص المشـفر على شـفرات بسـيطة أخرى . تبدأ الخوارزمية بعمل تخمين أولي حول ماهو المفتاح . هذا التخمين (Guess) يمكن إنجازه على أســاس التحليل البســيط للنص المشـــفر و يمكن أن تعتمد على المعرفة الجزئية للمفتاح أو قد تكون فقط عشـوائية . كلما كانت هناك رموز صـحيحة في المفتاح المفترض ، كلما كان أكثر سرعة للخوارزمية أن تقترب من الحل الصحيح . بعد ذلك تستخدم الخوارزمية هذا التخمين كمفتاح لفتـــح شفـــرة النص المشفر . يكون النص الناتج أكثر احتمالا انه نص غير مقروء ، لكن محتوياته ســـوف تملك بعض التشـــابه إلى اللغة المتوقعة للنص المشـــفر معتمدا على كم هو عدد الرموز الصـــحيحة التي كانت موجودة في التخمين في الحالة الأولى .

في الدورة التكرارية والتي تتبع هذه العملية فسوف يتم تغيير المفتاح الحالي كل مرة بكمية ثنائيات قليلة ، ثم بعد ذلك فان هذا المفتاح ســوف يســتخدم لفتح شـفرة النص المشـــفر مرة أخرى وأخيرا يتم تدقيق فيما إذا كانت محتويات النص الجديد الناتج اقرب إلى اللغة الطبيعية المتوقعة من تلك المســـتخدمة في النص المشـــفر الســـابق . إذا كان الحال كذلك (أي اقرب إلى اللغة الطبيعية) ، فانه يتم الاحتفاظ بالمفتاح الجديدة إلى الدورة التكرارية القادمة ، وان لم يكن كذلك ، فان المفتاح القديم يســـتخدم لكن يتم تحويره للاســـتخدام في طريقة أخرى في الدورة القادمة المنفذة وهكذا . إذا تم بناء دالة والتي تعكس حالة " كم هو القرب " لمحتو يات نص معين من اللغة المتوقعة ســـتكون هناك خوارزمية عاملة تســـتطيع بالتعاقب كشف الكثير من الرموز الصحيحة .

٣ـ٥ـ ٩ : تحويرات لشفرات الإحلال:

لقد تم تصـــميم العديد من التحويرات في آلية الإحلال ، حيث تم على ســـبيل المثال استخدام جدول ترجمة (Translation Table) لغرض إحلال رموز النص الواضح برموز النص المشـفر ، يتضـمن التحوير تغييرا لمحتويات جدول الترجمة مع كل إحلال . جدول الترجمة الحركي (Dynamic) يعمل تشـويش لإحصـائيات تردد الأحرف وبذلك يحبط الهجومات محللي الشفرة العادية .

نفس الميكانيكيـــة يمكـــن أن ينظر إليها كذلك كرابط تشفيري (Combiner) ، وتستطيع إحـــلال دالـــة XOR المستخدمة في شفرات فيرنام . إن جدول الترجمة الحركي يعمل كدالة ذات اتجاه واحد لغرض حماية التسلسل العشوائي الوهمي ، وكنتيجة لذلك سوف تساعد في منع تحليل الشفرة .

تـــم تحوير ميكانيكية جديدة والتي يمكن وصفها كإحلال حركي (Dynamic) . رغم أنها هيكليا أو تركيبيا مشابهة إلى الإحلال البسيط ، فان الإحلال الحركي يملك مدخل بيانات ثاني والذي يعمل لإعادة ترتيب محتويات جدول الإحـــلال . إن هـــذه الميكانيكية تربط مصدرين للبيانات لتكون أكثر تعقيدا .

رابط الإحلال الحركي يمكنه مباشرة إحلال رابط XOR المستخدم في شفرات فيرنام التدفقية .

قد تؤشر شفرة فيرنام وبصورة جيدة بداية التشفير الحديث . تربط شفرة فيرنام تدفق النص الواضح بتدفق تشويس بصورة عشوائية وهمية مستخدمة ما نطلق عليه الآن الجمع بباقي ٢ (mod 2 addition) . تعرف هذه الدالة الرابطة نفسها أيضا باستخدام العملية البوليانية المنطقية XOR ، وأنها متوفرة بصورة واسعة في الدوائر المتكاملة الرقمية وكذلك كإيعاز في معظم الحواسيب وخاصة والحاسبات الصغيرة . بما أن كل عنصر من عناصر رابط فيرنام هو عبارة عن الجمع بباقي ٢ لقيمتين غير معروفتين ، فان بيانات النص الواضح تبدو بأنها مخفية بصورة جيدة .

كوسيلة بديلة لتصميم شفرة تدفق أمينة هو البحث عن دوال رابطة والتي تقاوم الهجوم ، مثل هذه الدوال سوف تعمل على إخفاء التسلسل العشوائي الوهمي من التحليل وان مثل هذه الدوال التشفيرية الرابطة (Cryptographic Combining Functions) يمكن استخدامها لغرض إحلال رابط XOR لفيرنام ، أو تربط فقط التسلسلات العشوائية الوهمية لغرض إنتاج تسلسل أكثر تعقيدا والتي هي أكثر صعوبة للتحليل . لا ينوي الرابط التشفيري إلى تكوين شفرة مطلقة .

٣- ٦ : شفرات الانتقال (Transposition Ciphers):

يتميز هذا النوع بأنه يعيد ترتيب (Permutation) الرموز في كتلة معين .

يمكن تعريف هذا النوع في التشفير بما يلي :

إذا كان t هو طول الكتلة ، K هو مجموعة إعادة الترتيب (Permutations) في المجموعة {1,2,.....,t} .لذلك فأن لكل e بحيث $e \in K$ يمكن تعريف دالة التشفير بما يلي :

$$E_e(m)=(m_{e(1)}m_{e(2)}.....m_{e(t)})$$

حيث أن $m=(m_1m_2.....m_t) \in m$

أما في دالة فتح الشفرة (Decrypt) فانه يتم ذلك بإعادة الترتيب العكسي للرموز أي $d= e^{-1}$

لغرض فتح شفرة العبارة C حيث $c=(c_1c_2.....c_t)$ يكون الصيغة التالية :

$$D_d(c_{d(1)}c_{d(2)}.....c_{d(t)})$$.

تحفظ شفرات الانتقال البسيط (Transposition) عدد الرموز لنوع معين ضمن كتلة واحدة (Block) ، وعليه يكون من السهولة تحليل شفرتها .

في شفرة الانتقال فان النص الواضح يبقى نفسه ، لكن ترتيب الحروف يتم خلطها بغير انتظام وبشكل التفافي . في شفرة الانتقال العمودي البسيط (Simple Columnar Transposition Cipher) ، فان النص الواضح يكتب أفقيا على قطعة من ورق التخطيط بعرض ثابت (عرض الورقة) وان النص المشفر يقرأ عموديا ، كما في المثال التالي :

مثال ٣-١٠:

plaintext : COMPUTER GRAPHICS MAY BE SLOW BUT AT LEAST IT`S EXPENSIVE

COMPUTERGB

APHICSMAYB

ESLOWBUTAT

LEASTITSEX

PENSIVE

Ciphertext : CAELP OPSEE MHLAN PLOSS UCWTI TSBTV EMUTE RATSG YAERB TX

أي أن اسطر المصفوفة تمثل النص الواضح وأعمدة المصفوفة هي النص المشفر .

٣-٦ : عمليات XOR البسيطة:

عمليات XOR تمثل بالشكل التالي :

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

كذلك نلاحظ :

إن خوارزمية XOR البسيطة هي في الواقع ضعيفة ، إنها ليست بشيء سوى أنها

$$a \oplus a = 0$$
$$a \oplus b \oplus b = a$$

عبارة عن شفرة فايجنر متعدد الأحرف . تم الاهتمام بها بسبب انتشارها في حزم البرمجيات التجارية ، على الأقل تلك البرمجيات المستخدمة في MS – DOS وعالم الماكنتوش بسبب ان إجراء عملية XOR مرتين يستعيد الأصل ، فان التشفير وفتح الشفرة يستخدم نفس الإجراء :

$$p \oplus k = c$$
$$c \oplus k = p$$

لا توجد أمنية حقيقية في هذا النوع من التشفير ويمكن أن يكسر ببساطة ، حتى بدون استخدام الحواسيب و يستغرق وقت كسرها ثواني قليلة في الحاسب .

الانتقال له فائدة تميزه عن الإحلال حيث انه رغم أن الإحلال يحفظ توزيع التكرار للأحرف المنفردة ، فإنها تدمر المجموعات الثنائية الأحرف (Diagrams) ، الثلاثية الأحرف (Triagrams) ، وإحصائيات عالية الدرجة للغة ، لهذا السبب فان الانتقال يعتبر أكثر أمنا لتشفير اللغة الطبيعية من الإحلال البسيط .

٣-٧ : تركيب التشفير (Composition of Ciphers):

لغرض توضيح فكرة شفرة الضرب (Product Cipher) يجب علينا التعرف على دمج (تركيب) الدالات . يعتبر مفهوم الدمج (Composition) طريقة ملائمة لبناء دوال أكثر تعقيداً من الدوال البسيطة .

إن الطريقة الاعتيادية لمحاولة زيادة الأمنية هو اختيار مجموعة من أنظمة التشفير وربطها أو تركيبها بعدة أساليب . تم اقتراح طريقتين من هذه الطرق من قبل شانون في العام ١٩٤٩ ، والتي لا تزال من أسس التشفير العملي ، الطريقتين هما :

١: المجموع الموزون (The weighted Sums) .

٢: الضرب (Product) .

٣-٧- ١ : المجموع الموزون:

إذا كان S1 و S2 عبارة عن نظامي تشفيري بنفس مساحة العبارة (المدى) ، ولدينا $0 < P < 1$ ، عند ذلك فان المجموع الموزون $pS1 + (1-p) S2$ هو النظام التشفيري المحدد وذلك بجعل اختيار أساسي :

استخدام S1 باحتمالية p أو S2 باحتمالية 1-p . يمكن توسيع هذا الأسلوب وذلك بتطبيقه على أكثر من نظامي تشفير .

مثال ٣- ١١:

إذا كان لدينا نظامي تشفير T و R عند ذلك فانه توجد ظروف معينة والتي بموجبها يمكننا دمجهما للحصول على نظام ثالث S .قبل مناقشة بعض هذه الطرق ، سنوضح ماذا نعني بالعبارة " نظامان متساويان " أو " نظامان مختلفان " . يطلق على نظامي التتشفير أنهما متساويان (او نفسهما) اذا كانا يملكان نفس مساحتي العبارة والنص المشفر زائدا التحويلات . (إذا تجاهلنا الافتراض أن كل مفتاح متساوي ، عند ذلك ، فانه لكي يكون النظامان متساويان ، فيجب ان يملك كل تحويل نفس الاحتمالية في كل نظام) . في هذه الطريقة لدمج الأنظمة ، وكذلك في أنظمة أخرى عديدة ، حتى إذا تم البدء بنظامين واللذان يملكان مفاتيح متساوية فانه لا توجد ضمانة أن النظام الناتج سوف لن يكون متغيرا . لذلك سيتم التركيز على طريقة دمج نظامين متغيرين أو مختلفين (Variant) .

إذا كان T و R هما نظاما تشفير متغيرين بنفس مساحة العبارة M وإذا كان p و q رقمان حقيقيان موجبان وبالخاصية p+q=1 ، عند ذلك فانه باستطاعتنا دمج التحويلين لـــ R و T لغرض الحصول على نظام تشفير مختلف S ، ويطلق عليه المجموع الموزون لكل من R وT ويكتب S= pR+qT بمساحة عبارة M . لغرض التشفير باستخدام S فانه يجب علينا أو الاختيار بين النظامين R و T (احتمالية اختيار R سيكون p) . عند اختيار احد النظامين فنكون بذلك اخترنا النظام المستخدم للتشفير . لذلك اذا كانت التحويلات لـــ R هي $r_1,r_2,r_3,.....r_m$ باحتمالات $p_1,p_2,p_2,....p_m$ على التوالي ، وان التحويلات لـ T هي $t_1,t_2,.....,t_n$ بالاحتمالات $q_1,q_2,.....,q_n$ على التوالي، عند ذلك فان تحويلات S هي :

$t_1,t_2,.....,t_n$ ، $r_1,r_2,r_3,.....r_m$ بالاحتمالات $p_1,p_2,p_2,.....,p_m$, $q_1,q_2,.....,q_n$ على التوالي .

٣-٧-٢ : تركيب الدوال (Composition of Functions):

تعريف ٣- ٤ :

إذا كان S,T,U عبارة عن مجموعات محددة (Finite) ،

وان $f:s\rightarrow T$

وان $g:T\rightarrow m$

إن تركيب (دمج Composition) للـــــ g مع p يعرف بالشكل التالي dof (للسهولة تكتب gf) عبارة عن دالة من S إلىU ويمكن توضيحها بالشكل التالي المعرف بـ $(gof)(x)=g(f(x))$ لكل x بحيث $x \in S$.

يمكن توسيع فكرة التركيب ليشمل استخدام كثر من دالة .

٣-٧-٣ :التركيب والالتفاف (Compositions & Involutions):

أن الالتفاف(Involution) عبارة عن صنف بسيط من الدوال وبخاصيته أن E_K ($E_K(x)=x$

لكل قيم x في مجال E_k (Domain of E_k) ، بمعنى آخر أن E_k oE_k هو دالة هوية (Identity Function) .

ملاحظة ٣-١ :

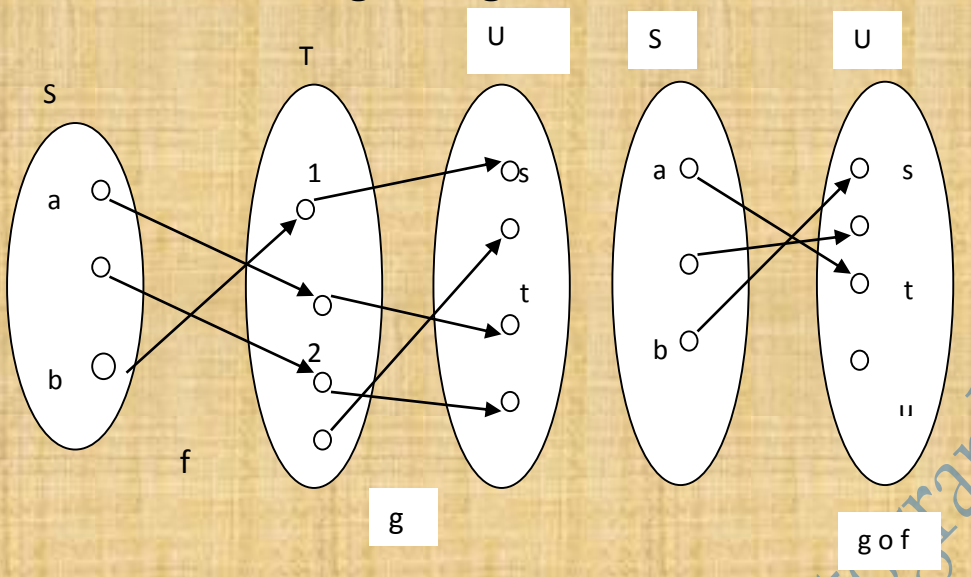
أن تركيب التفافين (Two Involutions) ليس بالضرورة أن يكون التفاف . وعلى العموم فان ألالتفافات يمكن أن تدمج لتكون دوال أكثر تعقيداً بحيث أن معكوس هذه الدالات يمكن إيجاده بسهولة ، وتعتبر هذه خاصية مهمة في التشفير (Decryption) . كمثال إذا كان :

$E_{k1}.,E_{k2},\ldots\ldots\ldots\ldots,E_{Kt}$ عبارة عن التفافات فأن معكوس (Inverse) لـ $E_K=E_{K1}E_{K2}\ldots\ldots\ldots E_{Kt}$ هو :

$$E^{-1}{}_K=E^{-1}{}_{K1}E^{-1}{}_{K2}\ldots\ldots\ldots E^{-1}{}_{Kt}$$

حيث يعتبر تركيبا (Composition) للالتفافات و بترتيب معكوس .

شكل ٣. ٢ : تركيب g o f لدالتين g و f.



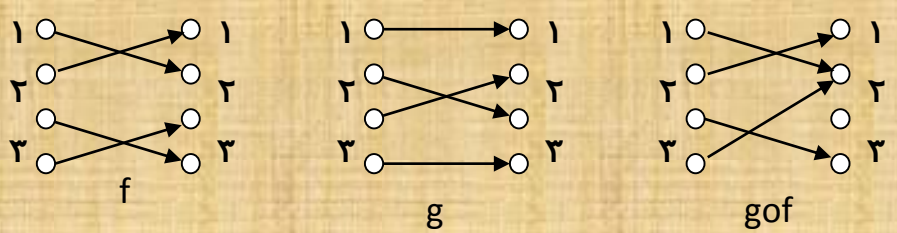
٣-٨ : شفرة الضرب (Product Cipher):

إن الإحلال والانتقال البسيط (Simple Substitutions and Transposition) كل بمفرده لا يوفر درجة عالية من الأمنية لذلك فأن دمج هذين التحويلين يؤدي إلى الحصول على طريقة تشفير كفوءة وقوية .

كمثال على شفرة الضرب (Product Cipher) هو التركيب لـــ 2 ≤ t من التحويلات

حيث كل E_{Ki} , (1 <I < t) إما أن يكون انتقال أو إحلال . سوف يطلق على دمج التعويض والإحلال اسم دورة (Round).

شكل٣. ٣ : التركيب لـ g o f بالتفافين g و f هو ناتج غير التفافي .



مثال ٣-: شفرة الضرب (Product Cipher):

اذا كـــان M=C= K عبـــارة عن مجموعة لجمع السلاسل الثنائية Binary (String) وبطول ٦ . ان عدد العناصر في M هو 2^6=64.

لتكن $m=(m_1m_2.....m_6)$. يمكن تعريف الاتي :

$E^{(1)}{}_k(m) = m \oplus k$ حيث أن $k \in K$

$E^{(2)}{}_{(m)} = (m_4m_5m_6m_1m_2m_3)$

ان $E^{(1)}$ هي طريقة تشفير من النوع إحلال متعدد الأحرف (Polyalphabetic Substitution) وان $E^{(2)}$ هي طريقة تشفير من النوع انتقال (Transposition) . إن هذه الطريقة $E^{(2)}$ لا تشمل استخدام المفتاح .

إن ناتج ضرب (Product) $E_k^{(1)}$ $E_{k(2)}$ هو دورة (Round) .

يمكن لطرق التشـــفير ان تجمع بناء على طريقة تشـــفير ، مثلا تجميع كل الاحلالات الخطية (Linear Substitution) لطول معين n ، تجميع كل الاحلالات متعددة الأحرف (أو أحادية الأحرف) لفترة معينة (Period) d ، أو تجميع كـــل تناقلات الكتل (Block Transposition) لطول معين n .

إن تركيب طريقتـــــي تشفير (تشفيرات الضرب Product Encryptions) يؤدي الى تكوين طريقة تشـــفير جديدة . تركيب طريقتي تشـــفير متعددة الاحرف خطيا بفترات d1 ,d2 هو بصورة عامة طريقة تشفير متعددة الاحرف خطيا بفترة lcm (d1, d2) ، بالمثل ينطبق هذا الإجراء نسبة إلى تناقل الكتل بسعة n1 , n2 .

التشـــفير العالي (Superencryption) هي حالة شـــائعة للتشـــفير الضـــربي: الرموز الحرفية والرقمية يتم تشـــفيرها مرة ثانية. إن شـــفرة فايجنر بحدود Z10 ، بمعنى أن N=10 . تستخدم للرموز الرقمية.

ملاحظة ٣-٢ :الأمنية العملية (Practical Security):

لقد تم الافتراض بان محلل الشفرة يملك كل من الوقت ، التسهيلات . والتخصيصات المالية غير المحدودة لكل منهما . عندما يكون أي نظام أمين تحت هذه الافتراضات ، يطلق على مثل هذا النظام بأنه أمين نظريا (Theoretically Secure) .

في الواقع العملي ، فان محلل الشفرة قد يواجه حالات مختلفة كليا و سيبذل جهدا لامتلاك الافتراضات أعلاه ، إلا انه في حالات عديدة فان الوقت المستغرق لحل شفرة معينة ستكون له أهمية بالغة بالنسبة لمحلل النظام ومن ثم يصبح بامكان النظام الغير أمين نظريا (Theoretically Insecure) توفير أمنية عملية مناسبة . كذلك ، فانه من الممكن للنظام الأمين نظريا إن يكون معرضا للهجوم عند استخدامه في بعض الحالات العملية . كمثال على ذلك نظام شفرة الوسادة One-Time Pad) الذي هو نظريا نظام غير قابل للكسر ولكنه يملك بعض الثغرات العملية .

هناك توضيح آخر نحتاجه لغرض التمييز بين الأمنية العملية والنظرية ، سوف نأخذ لهذه الحالة الأنظمة المثالية (Ideal System) . إن احد الأمثلة للنظام المثالي هو مجموعة شفرات أحادية الأحرف (Monoalphabetic Ciphers) للغات حيث إن كل الأحرف ذات احتمالية متساوية وان الحروف المتتالية يتم اختيارها بصورة مستقلة . هذا النظام المقترح يوفر مستوى عالي من الأمنية . لكن مثلا ، إذا تم استخدام النظام فعليا وان محلل الشفرة حصل على جزء من النص المشفر والنص الواضح ، فان النظام يكون معرضا للانتهاك والهجوم . وبالفعل إذا كانت عينة النص المشفر والنص الواضح كافية ، فان محلل الشفرة يستطيع إعادة كامل الإحلال الأبجدي ، بمعنى آخر ، المفتاح بأكمله ، ويستطيع عند ذلك فتح شفرة النص المشفر الباقي زائدا أي نصوص مشفرة أخرى والتي تم تشفيرها باستخدام نفس المفتاح .

ملاحظة ٣-٣: الانتشار والتشويش (Confusion and Diffusion:

هناك تقنيتيان أساسيتان لإخفاء (Obscuring) الزوائد (الحشو Redundancies) في أي عبارة نص مشفر ،واستنادا على أفكار شانون ، هما الانتشار والتشويش .

يقال على الإحلال (Substitution) في دورة (Round) بانها أضاف تشويش (Confusion) إلى عملية التشفير بينما الانتقال (Transposition) يقال عنه أضاف انتشار (Diffusion) .

أن المغزى والهدف من استخدام التشويش هو العمل على جعل العلاقة بين المفتاح والنص المشفر أكثر ما يمكن من التعقيد . يستطيع التشويش إخفاء العلاقة بين نماذج النص الواضح والنص المشفر . إن أسهل طريقة لعمل التشويش هو بواسطة الإحلال ، مثلا استخدام طريقة قيصر أو أي طريقة إحلال كتل بكتل أخرى .

إن الانتشار يشير إلى إعادة ترتيب أو انتشار البتات (الثنائيات) في العبارة بحيث أن أي حشو في النص الواضح ينتشر في النص المشفر . يقوم الانتشار بتشتيت حشو النص الواضح وذلك بنشرها على النص المشفر. محلل الشفرة الذي يبحث عن هذا الحشو سوف يضيع وقتا كثيرا في البحث عن هذا الحشو . الطريقة الأسهل للحصول على انتشار هو بوا سطة الانتقال Transposition) (يطلق عليه كذلك التبديل Permutation). شفرة الانتقال البسيطة، مثل الانتقال العمودي، تعيد ترتيب أحرف النص الوا ضح. الشفرات الحديثة تعمل هذا النوع من التبديل، لكن هذه الشفرات تستخدم صيغ أخرى للانتشار والتي تستطيع نشر أجزاء العبارة خلال العبارة الكلية.

عند ذلك يمكن القول انه تمت إضافة التشويش والانتشار إلى طريقة التشفير. معظم شفرات الكتل الحديثة تستخدم عدد من الدورات (Rounds) بالتعاقب لغرض تشفير النص الواضح . تعتمد شفرات التدفق على التشويش وحده ، وبعض طرق التغذية الخلفية تضيف الانتشار. تستخدم خوارزميات الكتل كلا من التشويش والانتشار معا .

إن فكرة الانتشار والتشويش هي المبادئ المعتمدة في تصميم معظم أنظمة تشفير الكتل . في شفرة الكتل ولغرض تشفير عبارة معينة $m=m_1m_2m_3.....m_sm_{s+1},.....m_{2s},m_{2s+1}.....$ فانه أولا نختار عدد صحيح S . بعد ذلك نحتاج المفتاح K و S من التحويلات (اعتياديا تكون مختلفة) $f_1,f_2,.....,f_s$ لغرض الحصول على النص المشفر $c_1c_2.....c_s$. باستخدام نفس المفتاح والدوال ، نستطيع تشفير الكتلة القادمة المتكونة من s من الحروف ، النص المشفر الناتج في كتل بطول s وكل بت من النص المشفر في كتلة معينة اعتياديا تعتمد على كامل كتلة النص الواضح المقابلة . إن العيب الرئيسي لمثل هذا النظام هو ملازمته لتقادم الخطأ .

ملاحظة ٣- ٤:

هناك ضعف آخر في شفرة أحادية الأحرف والتي هي يجب ان يتنبه لها المشفر لغرض تجنب هذا الضعف في أنظمة تشفير أخرى . عند استخدام شفرة متعددة الأحرف ، فان عملية تشفير أي حرف مفرد يشتمل على استخدام جزء صغير من

المفتاح . في هذه الحالة ، فانه هناك حرف واحد فقط تم استخدامه للإحلال . لذلك سيتم تحديد المفتاح وذلك بإيجاد مجموعات صغيرة منه ، وبعد ذلك يستخدم جزء المفتاح الذي تم إيجاده حاليا لغرض تحديد الباقي . ولغرض جعل النظام أمينا ، فيبدو أن الأسلوب الأفضل هو أن يتم استخدام كمية معينة من المفتاح لغرض تشفير كل حرف من العبارة . من المحتمل أيضا أن يكون مفيدا انتشار الهيكل الإحصائي للنص المشفر وذلك بتشفير عدد من حروف العبارة في وقت واحد . كمثال على الانتشار (Diffusion) . بعد تغيير كل حرف كعدد صحيح بباقي ٢٦ (modulo 26) في الأسلوب المعتاد ، هو تنفيذ معدل عملية على كل عبارة . لذلك ، فإذا كانت $m=m_1m_2.....$ فعند ذلك نختار عدد صحيح s ويتم إحلال m بالتسلسل $y_1y_2....$ حيث ان :

لقيم n =1,2,3,..... . بتنفيذ هذا العمل سنحصل على مساحة عبارة لها نفس الحشو للعبارة الأصلية M ، لكن ترددات الحرف لمساحة العبارة الجديدة y سوف تكون أكثر مساواة من الموجودة M . تأثير كل هذا هو أن محلل الشفرة يتطلب

$$y_n = \sum_{i=0}^{s=1} m_{n+1} \pmod{260}$$

عليه اعتراض نص مشفر أكثر طولا قبل محاولتة فتح الشفرة الإحصائي . في الواقع العملي هذا يعني أننا نشفر عدد من حروف العبارة في وقت واحد وبصورة مستقلة . احد عيوب هذا النوع من الأنظمة يبدو واضحا عند جهة المرسل . كل جزء من العبارة يعتمد على عدد حروف النص المشفر . لذلك ، إذا تم إرسال حرف واحد من النص المشفر بصورة خاطئة ، هذا قد يسبب أخطاء في العبارة المستلمة . هذا التأثير ألانتشاري لخطا واحد في الإرسال مسببا أخطاء كثيرة في عملية فتح الشفرة عادة ما يطلق عليه تقادم الخطأ (Error Propagation) .

لغرض التكيف مع هاتين النقطتين و بالتالي تقليص تأثير الهجمات الإحصائية على النصوص المشفرة ، فان شانون اقترح أن يستخدم المشفر تقنيتين هما الانتشار والتشويش (Confusion and Diffusion) . إن فكرة الانتشار هي نشر الإحصائيات لمساحة العبارة إلى هيكل إحصائي والذي يشتمل على تراكيب طويلة للأحرف في النص المشفر . إن فكرة التشويش هي لجعل العلاقة بين النص المشفر والمفتاح المقابل علاقة معقدة . هذا يؤدي إلى جعل هناك صعوبة للإحصائيات اللازمة لتحديد المفتاح بدقة والتي تأتي من جزء معين من مساحة المفتاح . إن كل حرف من حروف العبارة المشفرة سوف يعتمد على المفتاح الكلي وهذا يؤدي بمحلل الشفرة إلى محاولة إيجاد المفتاح الكلي وكذلك علي حل معادلات

أكثر تعقيدا من محاولة لإيجاد جزء من المفتاح وهذا يعتبر شئ مهم لغرض مقاومة نوايا محلل الشفرة .

٣- ٩: شفرات التدفق (Stream Ciphers):

تعتبر شفرة التدفق نوع من طرق التشفير التناظرية ، وهي عبارة عن شفرة كتلة بسيطة تتصف بان يكون طول الكتلة فيها مساوياً إلى واحد . ما يجعل هذا النوع من التشفير مفيداً هو أن تحويل التشفير يمكن أن يتغير لكل رمز في النص الواضح المطلوب تشفيره . في الحالات التي تؤدي إلى احتمال كبير في حصول أخطاء في انتقال المعلومات (Transmission Errors) فأن شفرات التدفق يعتبر مفيدة جداً بسبب عدم امتلاكها خاصية تقادم الخطأ (Error Propagation) . بالإمكان استخدام هذا النوع من التشفير عندما تكون هناك حاجة لمعالجة البيانات برمز واحد في الوقت الواحد . (فمثلاً عندما لا يملك الجهاز ذاكرة أو أن الذاكرة الوسطية (Buffer) للبيانات تكون محددة الحجم). تعمل شفرات التدفق على تدفقات (Streams) من النص الواضح والنص المشفر ثنائية واحدة bit واحد أو حرف وفي بعض الأحيان تتعامل مع عدة حروف (مثلا كلمة بطول ٣٢ بت) في الوقت الواحد. في شفرة الكتل فانه يتم تشفير نفس كتلة النص الواضح إلى نفس كتلة النص المشفر ، باستخدام نفس المفتاح . باستخدام تشفير التدفق ، فان الثنائية أو الحرف من النص الواضح سيتم تشفيره إلى ثنائية أو حرف مختلف في كل مرة .

يمكن تصميم شفرات التدفق لكي تكون اسرع بشكل استثنائي من شفرة الكتل . تعمل شفرات الكتل على كتل كبيرة من البيانات و بشكل نموذجي على وحدات اصغر من النص الواضح عادة منكون ثنائيات. سوف ينتج التشفير لاي نص واضح معين في شفرات الكتل نفس النص المشفر عند استخدام نفس المفتاح. باستخدام شفرة التدفق ، فان تحويل النصوص الواضحة الصغيرة سيكون متغيرا ، معتمدا على اين سيتم معالجتها خلال عملية التشفير .

تنتج شفرة التدفق ما يطلق عليه مفتاح التدفق (keystream) (وهو عبارة عن سلسلة من الثنائيات والتي تستخدم كمفتاح تشفيري) . يتم إنجاز التشفير بربط مفتاح التدفق مع النص الواضح ، عادة باستخدام بعملية XOR . توليد مفتاح التدفق يمكن أن يكون مستقلا عن (غير معتمدا) النص الواضح والنص المشفر ، منتجا ما يطلق عليه شفرة التدفق التزامنية (synchronous) ، أو قد يكون معتمدا على البيانات وشفرتها ، وفي هذه الحالة فان شفرة التدفق يقال عنها أنها متزامنة ذاتيا (self-synchronizing) . معظم تصميمات شفرة التدفق هي لشفرات تدفق تزامنية .

الاستخدام الأبسط لشفرة التدفق موضحة في الشكل ٣-٤ . مولد التدفق (Stream Generator) (في بعض الأحيان يطلق عليه مولد المفتاح المنفذ Running-Key Generator)) يخرج تدفق من البيانات :

$$K_1 , K_2 , K_3 , ... , K_i$$

يعمل مفتاح التدفق (Key Stream) باســـتخدام XOR مع ثنائيات تدفق النص الواضح ، P_i , ... , P_3 , P_2 , P_1 لغرض إنتاج تدفق من ثنائيات النص المشفر :

$$C_i = P_i + K_i$$

في جهة فتح الشـفرة ، فان بتات النص المشـفر يعمل لها XOR مع مفتاح التدفق المماثل لاسترجاع ثنائيات النص الواضح :

$$P_i = C_i + K_i$$

إذ أن :

$$P_i + K_i + K_i = P_i$$

تعتمد أمنية النظام كليا على مولد مفتاح التدفق .

تعريف ٣ـ ٥:

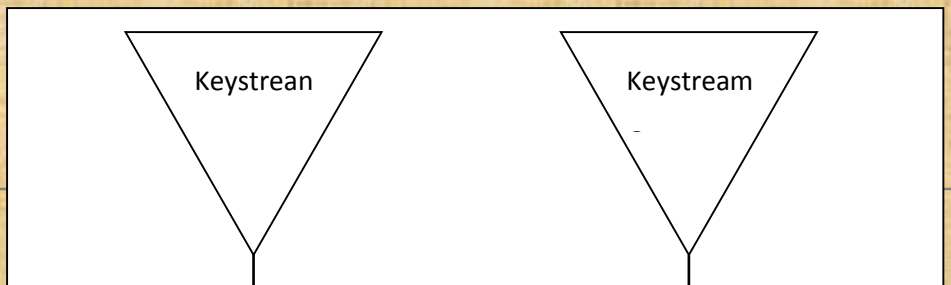
إذا كان K هو مســاحـــــة المفتاح لمجموعة من تحويلات التشـفير، فأن سـلسـلة الرموز $e_1e_2e_3...e_i \in k$ يطلق عليها مفتاح التدفق (Keystream).

تعريف ٣ـ ٦:

لتكــن A مجموعة الحروف الأبجدية (Alphabet) تحتوي على q من الرموز ، ولتكن E_e عبـــارة عن طريقة تشفير إحلال وتستخدم كتلة بطول ١ ، وان $e \in k$. نفترض أن $m_1m_2m_3.....$ سلسلة رموز النص الواضح وان $e_1e_2e_3.....$ هو مفتاح تدفق في المجموعة k . ان شفرة التدفق سوف تشفر سلسلـــة رموز النص الواضح المشفر $c_1c_2c_3.....$ حيث $c_i=E_{ei}(m_i)$. وإذا كان d_i يمثل معكوس e_i فعند ذلك $D_{di}(C_i)=m_i$ يمكنها أن تفتح شفرة (Decrypt) النص المشفر .

تستخدم شفرة التدفق تحويلات تشفيرية بسيطة طبقاً لمفتاح التدفق المستخدم في هذه الطريقة .

شكل ٣ـ ٤



شكل ٣-٣ : شفرة التدفق .

يمكن توليد مفتاح تدفق عشـوائياً او بواسـطة خوارزمية تكون مفتاح التدفق من مفتاح تدفق ابتدائي بسـيط [يقصـد به جزء محدد في مفتاح التدفق]، ويطلق على هذا التدفق الابتدائي (Initial) اســـم البادئة (Seed) ،أو يمكن توليده من بادئة (Seed) رموز نص مشفر سابق . مثل هذه الخوارزمية تسمى مولد مفتاح التدفق .

لقد زاد الاهتمام بشــفرات التدفق بســبب أنها تظهر خصــائص نظرية لشــفرة الوسادة (one-time pad) .والتي يطلق عليه أحيانا شفرة فيرنام حيث يتم توليد سلسلة من الثنائيات بصورة عشوائية . يملك مفتاح التدفق نفس طول عبارة النص الواضح وان السلسلة العشوائية تربط باستخدام عملية XOR مع

النص الواضح لإنتاج النص المشفر . لان مفتاح التدفق هو عشوائي فان أي عدو مهما امتلك من موارد حسابية يستطيع فقط أن يخمن النص الواضح إذا حصل على النص المشفر . يقال عن مثل هذه الشفرة أنها توفر أمنية تامة (Perfect Secrecy) ، وان تحليل شفرة الوسادة ينظر إليه بأنه احد الأركان الأساسية لتحليل الشفرة الحديث . رغم أن شفرة الوسادة أظهرت استخداما مؤثرا خلال الحرب عبر القنوات الدبلوماسية التي تحتاج إلى أمنية عالية استثنائية ، فان الحقيقة التي تؤكد أن المفتاح السري (والذي يمكن استخدامه لمرة واحدة فقط) هو بطول العبارة ، هذا سيؤدي إلى مشاكل في توفير خدمات صارمة لإدارة مفتاح .على الرغم من أن شفرة الوسادة توفر لنا أمنية تامة ، لكنها على العموم تعتبر شفرة غير عملية .لا يوجد **لحد الآن شفرة تدفق أظهرت خصائص عالية تزودنا بمقياس حقيقي أو واقعي . شفرة التدفق الأكثر شهرة وا ستخداما هي RC4** .

ملاحظة ٣ـ ٥ :

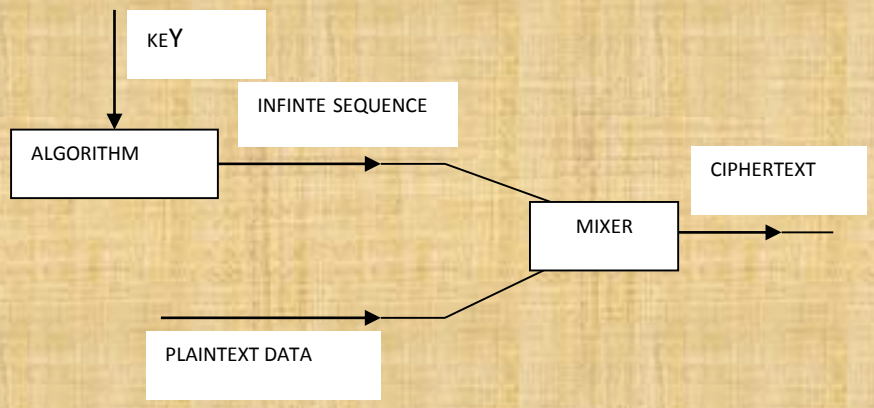
كل نظام تشفير تمت مناقشته يمكن أن يستخدم لوقت قصير معقول ، إما يدويا أو ميكانيكيا . إن من أهم العوا مل ذات الأهمية المميزة هو تطور أنظمة التشفير وذلك بعد انتشار الحاسبات . هذا يعني أن هناك مدى جديد من هذه الوظائف تم توفيرها إلى المشفر . يمنك التعبير عن العديد من هذه الوظائف الجديدة فقط بلغة الرياضيات التي تطورت مفاهيمها .

تأثر تطور نظام التشفير تأثرا كبيرا بالحقيقة التي أثبتها شانون أن شفرة الو سادة One-Time Pad غير قابلة للكسر . شعر العديد من المشفرين انه إذا كان بامكانهم محاكاة نظام شفرة الوسادة بطريقة ما ، فإنها تعتبر نظاما بمستوى امني عالي ومضمون . لقد تشجع المشفرون أيضا باستخدام المفهوم الذي ظهر في العام ١٩٢٠ حيث العديد من الماكنات الميكانيكية الالكترونية بدأت تعمل بطريقة تشبه شفرة الو سادة ، حيث ان هذه الماكنات تنتج تسلسلات طويلة من الازاحات والتي تطبق ، حرف بحرف ، على النص الواضح . على كل حال ، فان هناك اختلاف أ ساسي واحد . عدا حالة شفرة الو سادة ، فان التسلسل المتولد من احد هذه الماكنات هو غير عشوائي ، في الحقيقة ان هذا التسلسل يتم تحديده كليا بواسطة المفتاح . بالرغم من ذلك ، الاختيار الجيد للخوارزمية ، فانه بالامكان إنتاج تسلسل يبدو انه عشوائي ، بمعنى آخر ، تسلسل معين والذي لا توجد علاقة واضحة بين عناصره . لقد اتفق بين معظم المشتركين انه مثل هذا النظام سيكون عالي الأمنية .

قد تؤدي الأفكار أعلاه التعريف بشفرة التدفق (Stream Cipher) كما موضح في الشكل ٣ـ ٥ .

إذن فان شفرة التدفق عبارة عن نظام يتم فيه إعطاء المفتاح إلى الخوارزمية والتي تستخدم هذا المفتاح لتوليد تسلسل غير محدد . (الخوارزمية عادة ما يشار لها بمولد التسلسل (Sequence Generator) او مولد مفتاح التدفق (Keystream Generator) .

شكل ٣-٥



يجب ملاحظة مسألة مهمة بادراك عالي وهو أن شفرة التدفق تحاول استثمار التشويش (Confusion) وليس الانتشار (Diffusion) و هذا يعطيها فائدة أساسية على شفرة الكتل ، أي أن شفرة التدفق ليست تقادم خطأ (Error Propagating) . لهذا السبب ، فان شفرة التدفق توفر على الأرجح الطريقة الأكثر أهمية للتشفير الحديث .

٣-٩- ١ : شفرات التدفق ذاتية التزامن (Self-Synchronizing Stream Ciphers) :

في هذه الشفرات فان كل ثنائية bit من مفتاح التدفق عبارة عن دالة لرقم ثابت من ثنائيات النص المشفر السابق .

يطلق على هذا الأسلوب المفتاح الذاتي للنص المشفر (Ciphertext Autokey CTAK) . لقد قدمت الفكرة الأساسية لهذا المفتاح في العام ١٩٤٦ .

٣-٩- ٢ : شفرات التدفق التزامنية (Synchronous Ciphers) :

في هذه الشفرة فان مفتاح التدفق (Key Stream) يتولد بصورة مستقلة عن تدفق العبارة . يطلق العاملون في الشؤون العسكرية عليه المفتاح الذاتي المفتاح (Key Auto - Key KAK) . يقوم مولد مفتاح التدفق عند التشفير بتجزئة مفتاح التدفق إلى ثنائيات يتم تدفقها الثنائية تلو الأخرى . وعند فك التشفير يقوم مولد مفتاح تدفق آخر بتجزئة ثنائيات مفتاح التدفق المتماثلة ، الثنائية تلو الأخرى

. هـــذا الإجـــراء يمكنه من تنفيذ هذا العمل ، طالما أن هناك مولدي مفتاح تدفق متزامنين . إذا حدث وان احد المولدين قفز دورة أو فقدت ثنائية بين النص المشفر الإرسال ،عند ذلك فان كل حرف من النص المشفر بعد حدوث الخطأ سوف تفتح شفرته بصوره صحيحة . إذا حدث هذا الشئ ، فان المرسل والمستقبل يجب أن يعيدا التزامن لمولداتهما قبل استمرار العمل .

يجب أن تكون فترة مولد مفتاح التدفق اكبر (Long Period) التي سيخرجها المولد بين تغييرات المفتاح . إذا كانت الفترة (Period) اقل من النص الواضح ، فان الأجزاء المختلفة من النص الواضح سوف تشفر بنفس الطريقة – وهذا ضعف شديد – فإذا عرف محلل الشفرة جزء من النص الواضح ، فانه يستطيع استرجاع جزء من مفتاح التدفق ويستخدمه لاسترجاع العديد من النصوص الواضحة .تستطيع شفرات التدفق المتزامنة توفير الحماية ضد أي محاولة ادخالات (Insertions) وعمليات حذف (Deletions) من النص المشفر ، بسبب أن هذه العمليات(إدخال والحذف) تؤدي إلى فقدان التزامن وسيتم كشفها مباشرة .

٣-٩-٣ : هجوم الإدخال (Insertion Attack):

تكون شفرات التدفق التزامنية معرضة لهجوم الإدخال (Insertion Attack). قد يسجل المهاجم الفعال المخادع تدفق نص مشفر ، لكن لا يعرف النص الواضح أو مفتاح التدفق المستخدم في تشفير النص الواضح :

Original plaintext : p_1 p_2 p_3 p_4 .....

Original keystrean : k_1 k_2 k_3 k_4 .....

Original ciphertext : c_1 c_2 c_3 c_4 .....

يقوم المهاجم الفعال الماكر يحشر (Insert) ثنائية معروفة واحدة ، p’ ، في النص الواضح بعد p_1 وبعد ذلك يحاول تحليل الشفرة للحصول على نص واضح محور مشفر بنفس مفتاح الدفق . سوف يسجل النص المشفر الجديد الناتج من هذه العملية :

New plaintext :		p_1	p’	p_2	p_3	p_4	Original
keystream :	k_1	k_2	k_3	k_4	k_5		
Updated ciphertext :	c_1	$c’_2$	$c’_3$	$c’_4$	$c’_5$		

بما أن المخترق يعرف قيمة p’ ، فانه يستطيع تحديد النص الكلي بعد ذلك البت من النص المشفر الأصلي والنص المشفر الجديد :

$k2 = c'2 \oplus p'$ ثم بعد ذلك $p2 = c2 \oplus k2$

$k3 = c'3 \oplus p3$ ثم بعد ذلك $p3 = c3 \oplus k3$

$k4 = c'4 \oplus p3$ ثم بعد ذلك $p4 = c4 \oplus k4$

قد لا يحتاج المهاجم حتى لمعرفة الموقع الدقيق والتي تم فيها إدخال الثنائية ، بل يمكنه فقط مقارنة النص المشفر المبدل مع النص المشفر الأصلي وبعد ذلك يشاهد في أي موقع يختلفان . لغرض الحماية ضد هذا الهجوم ، فان المرسل لا يستخدم نفس مفتاح التدفق لتشفير عبارتين مختلفتين .

٣-٩-٤ : شفرة فيرنام (The Vernam Cipher):

أن ميزات شفرة فيرنام هما هو البساطة والسهولة في استخدامها .

تعريف ٣- ٧ :

شفرة فيرنام عبارة عن شفرة تدفق معرف بمجموعة الرموز $A=\{0,1\}$. سوف تستخدم سلسلة المفاتيح الثنائية (Binary) وهي $k_1k_2...k_t$ لغرض تشفير العبارة الثنائية $m_1m_2...m_t$ حيث يكون كل من k,m بنفس الطول ويتم تكوين النص المشفر $c_1c_2...c_t$ حيث أن:

$$c_i = m_i \oplus k_i, 1 \le i \le t$$

إذا تم اختيار مفتاح التدفق بصورة عشوائية ولايمكن استخدامه مرة ثانية فأن شفرة فيرنام يطلق عليها (One-Time-System) أو شفرة الوسادة (One – Time-Pad) .

لغرض معرفة أن شفرة فيرنام تحقق مواصفات شفرات التدفق ،نلاحظ وجود شفرتين كل منهما تستخدم الإحلال (Substitution) ضمن المجموعة A .أحد هاتين الشفرتين E_0 والتي تقوم بإرسال ٠ إلى ٠ و ١ إلى ١ ، الشفرة الأخرى E_1 ترسل ٠ إلى ١و ١ إلى ٠ . فعندما يحتوي مفتاح التدفق على ٠ تطبق E_0 على ما يقابله من رمز في النص الواضح ، وبعكسه تطبق E_1 .

إذاً تمت إعادة استخدام سلسلة المفتاح فسيكون هناك طرق لمهاجمة النظام التشفير ي .فمثلاً إذا كان $c_t \ldots c_2 \ c_1$ و $c'_t \ldots c'_2 c'_1$عبارة عن سلسلتين مشفرتين والمتكونان بواسطة نفس مفتاح التدفق فعند ذلك :

وان :

$$c_i = m_i \oplus k_i , c'_i = m'_i \oplus k_i$$

لذلك فان الحشو (Redundancy) تسمح باستخدام تحليل الشفرة .

$$c_i \oplus c'_i = m_i \oplus m'_i .$$

يمكن أن يكون نظام شفرة الوسادة (One-Time Pad) نظرياً غير قابل للانتهاك .أي انه إذا امتلك محلل الشفرة نصا مشفرا $c_1 c_2 \ldots\ldots c_t$ قد تمت تشفيره باستخدام سلسلة مفتاح عشوائية والمستخدم لمرة واحدة فقط فأن محلل الشفرة في هذه الحالة لا يستطيع أن يفهم سلسلة الرموز الثنائية المقابلة للنص الواضح. لقد ثبت أن أي نظام تشفيره لايمكن كسره أو انتهاكه إذا تم اختيار مفتاح عشوائي بطول مساوي إلى طول العبارة . لهذا يستخدم هذا النظام في حالات أو تطبيقات متخصصة .

تقريريا إلى وقت حديث فان امن وسلامة خط الاتصال بين موسكو وواشنطن تم باستخدام شفرة الوسادة (One-Time Pad) .تم نقل المفتاح باستخدام حامل موثوق فيه (Trusted Courier) .

٣-١٠ : مساحة المفتاح (The Key Space):

إن حجم مساحة المفتاح هو عدد أزواج مفتاح التشفير وفتح الشفرة والمتوفرة أو الموجودة ضمن النظام التشفيري .

من الناحية المثالية فان المفتاح يعتبر طريقة محكمة لتحديد تحويل التشفير (من كل مجموعة تحويلات التشفير) والتي سيتم استخدامها .

كمثال

على ذلك فانه في شفرة الانتقال (Transposition Cipher) وبطول كتلة مقدار t يكون هناك !t من دالات التشفير (Encryption Functions) وكل منها يمكن أن يستخدم المفتاح . أن في الحقائق المهمة هو ارتبط ألا منية لأي طريقة تشفير مع حجم مساحة المفتاح . أن الحقيقة التالية من الأهمية بحيث يجب أن تأخذ ينتظر الاعتبار .

حقيقة ٣- ١ :

لغرض توفير شـــرط الأمنية لأي نظام تشـــفيري فانه يجب ان تكون مســـاحة عمليات البحث المكثف المفتاح كبيرة بما فيها الكفاية لغرض إعاقة أو منع (Exhaustive Search) ، فمثلاً في طريقة الإحلال والتي تشـــفر كل حرف بإزاحة مقدارها ٣ إلى اليمين من الحرف المطلوب في النص الواضح، نقول أن هذا النظام يملك مساحة مفتاح قدرها $4X*10^{26}$≈26! . أما في المثال الذي يستخدم طريقة الإحلال متعدد الأحرف (Polyalphabetic Substitution) حيث تم استخدم ثلاثة انو أع في الازاحات هي على التوالي ٣،٧،١٠ أحرف عن الحروف الثلاثة الأولى في النص الواضح فيكون حجم مساحة المفتاح $7*10^{79}$≈ (26!).

البحث المكثف لمســـاحة هو كليا غير مجدي (Infeasible) ، لكن تظل كلا الشفرتين ضعيفتين ويقدمان أمنية قليلة نسبيا .

الفصل الرابع

تقنيات التشفير

٤-١ : التواقيع الرقمية (Digital Signatures):

إن أحد أساسيات (BASICS) التشفير و الذي يغير في المتطلبات الأساسية في كل من إثبات الشخصية (Authentication) ، التخويل (Authorization)، وعدم التبرأ أو الإنكار (Non –Repudiation) هو التوقيع الرقمي (بمعنى آخر أن أحد أساسيات التشفير المهمة هو التوقيع الرقمي). إن الغرض من التوقيع الرقمي هو توفير وسيلة لكينونة (Entity) وذلك بربطها بتعريف تلك الكينونة مع جزء من المعلومات . تستلزم عملية التوقيع العبارات وبعض المعلومات السرية و المرتبطة بالكينونة في حزمة معلومات (Tag) يطلق عليها التوقيع . لقد استخدمت التواقيع اليدوية ة زمنية طويلة لإثبات ملكية او مرجعية محتويات أي وثيقة . لكن ماذا عن توقيع والذي يفرض بقوة ؟

أدناه مجموعة من المصطلحات المستخدمة في التوقيع الرقمي:

١: M عبارة عن مجموعة العبارات و التي يمكن توقيعها.

٢: S هو مجموعة العناصر يطلق عليها التواقيع ، حيث يمكن أن تكون سلسلة أرقام ثنائية وبطول ثابت .

٣: S_A عبارة عن عملية تحويل من مجموعة العبارة M إلى مجموعة التوقيع S ويطلق عليها تحويل التوقيع للكينونة A (يقصد به المرسل). يجب ان تبقى S_A سرا وسوف تستخدم لغرض تكوين التواقيع للعبارات ضمن M .

٤: V_A هو عبارة عن عملية تحويل من المجموعة MXS إلى المجموعة {True , False} . تتكون MXS من كل الأزواج (m ,s) حيث أن $m \in M$ و $s \in S$ ويطلق عليها الضرب الكارديناليي (Cartesian Product) لـ SوM . يطلق على V_A عملية تحويل التحقق (Verification Transformation) من تواقيع A، تكون V_A معروفة علناً (Public) ويمكن استخدامها من قبل كينونات أخرى وتستخدم أيضا للتحقق من التواقيع التي تنشأ من قبل A.

تعريف ٤-١:

تزودنا التحويلات S_A، V_A بطريقة التوقيع الرقمي ويطلق عليها أحياناً آلية التوقيع الرقمي .

مثال ٤ -١ : (طريقة التوقيع الرقمي):

لتكن ($M = \{ m_1 , m_2, m_3 \}$ و $S= \{s_1, s_2 , s_3 \}$

إن الجزء الأيسر من الشكل ٢. ٥ يبين دالة التوقيع S_A من المجموعة M ، بينما الجزء الأيمن ، يمثل دالة التحقق V_A .

٤-١- ١ : إجراء التوقيع (Signing Procedure):

تقوم الكينونة A (يطلق عيها الموقع Signer) بتكوين توقيع للعبارة $m \in M$ بتنفيذ الخطوات التالية:-

١ : تحسب A التوقيع $s = S_A(m)$

٢ : ترسل الزوج (m, s) . يدعى s توقيع للعبارة m .

٤-١- ٢ : إجراء التحقق (Verification Procedure):

التحقق من التوقيع s للعبارة m والمتكون من قبل A يتم بواسطة كينونة B (يطلق عليها المحقق Verifier) بتطبيق الخطوات التالية :

١ : الحصول على دالة التحقيق V_A للكينونة A

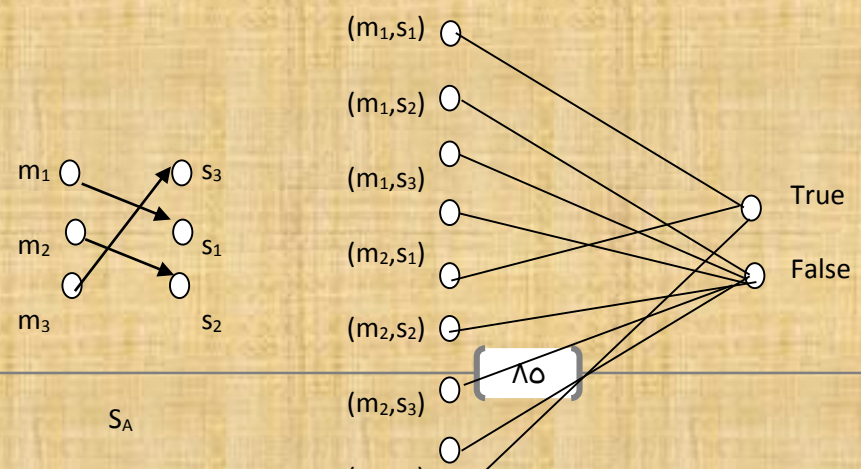
٢ : حساب $u = V_A(m, s)$.

٣ : يتم قبول التوقيع المتكون من قبل A إذا كان u=true وبعكسه يرفض التوقيع إذا كان u =false.

ملاحظة ٤-١ : التمثيل المختصر (Concise Representation):

يتم تمييز التحويلات S_A و V_A بواسطة المفتاح ، بمعنى إن أي نوع من عملية التوقيع وخوارزميات التحقق (Verification) معروفة ومعلنة و كل خوارزمية يمكن أن تعرف بواسطة مفتاح .لذلك فان خوارزمية التوقع S_A المكونة (المتولدة) من قبل المرسل A تحدد بواسطة المفتاح K_A وان المرسل A يحتفظ بـ k_A بصورة سرية (Secret). وبنفس المفهوم فان خوارزمية التحقق (Verification) لتوقيع المرسل A تحدد بواسطة المفتاح المعلن l_A .

شكل ٤ -١ : دالة التوقيع والتدقيق لطريقة توقيع رقمي .



ملاحظة ٤-٢ : التواقيع اليدوية (Handwritten Signatures):

يمكن ترجمة التواقيع كصنف خاص من التواقيع الرقمية . لتحقيق هذا الغرض نأخذ مجموعة التواقيع S التي تحتوى على عنصر واحد فقط والذي هو توقيع يدوى للمرسل A ويشار له بـ S_A . ستقوم دالة التحقيق بتدقيق إذا كان التوقيع للعبارة الذي تم فعلاً من قبل A هو S_A . تقوم دالة التحقق بتدقيق فيما إذا كان التوقيع لعبارة معينة موقعة فعليا من قبل A هو التوقيع S_A .

نلاحظ هنا إشكالية وهي أن التوقيع لا يعتمد على العبارة لذلك يجب وضع محددات أخرى تفرض في آلية التوقيع الرقمي .

٤-١-٣ : الخصائص المطلوبة لدوال التوقيع والتحقق:

هناك عدة خصائص يجب على تحويلات التوقيع والتحقق أهما .

١: s يعتبر التوقيع صحيحا (Valid) من الراسل A للعبارة m إذا كان $V_A(m.s)=true$

٢: كل الكينونات من غير A سوف تواجه خطوات حسابية في غاية التعقيد والتي تحاول كل كينونة عدا A إيجاد لكل $m \in M$ التوقيع $s \in S$ بحيث أن $V_A(m,s)=true$. (بمعنى آخر لا يتمكن أي مستفيد عدا A أن يكتشف التوقيع الرقمي s للعبارة m) .

٤-٢ : إثبات الشخصية والتعرف (Authentication and Identification):

يستخدم مفهوم إثبات الشخصية استخداما واسعا ومخلا في بعض الأحيان في أمنية المعلومات . ولكن يمكن القول بالتحديد أن أهداف إثبات الشخصية هو التحقق من أن الكينونة هي في الواقع مخولة لذلك النوع من المعالجة . أمثلة لتلك الأهداف تشمل سيطرة الوصول (Access Control) ،موثوقية الكينونة (Entity Authentication)، موثوقية العبارة (Message Authentication)، تكامل البيانات (Data Integrity) ، عدم الإنكار (Non - Repudiation) ، وموثوقية المفتاح (Key Authentication) .تعتبر الموثوقية (Authentication) الأكثر أهمية بين جميع أهداف أمنية المعلومات.

حتى منتصف عام ١٩٧٠ كان يعتقد بأن الأمنية (Secrecy) و الوثوقية (Authentication) تعطيان نفس المعنى. ولكن باكتشاف الدالة الهاشية (Hash Function) و التواقيع الرقمية فقد تم إدراك أو التحقق بأن الأمنية و الوثوقية شيئين منفصلين عن بعضها وكل منهما يحقق هدف أمنية المعلومات بصورة مستقلة . هناك بعض الحالات تستدعي ضرورة التمييز بينهما (أي بين الأمنية و الوثوقية). كمثال على ذلك فإنه إذا كان هناك إتصال بين طرفين كل منهما في بلد معين ، وكانت الحاسبة المركزية في البلد المضيف لا تؤمن ضمان أمنية قناة الإتصال فانه يستوجب حينئذ على كل منهما إثبات هوية أو شخصية (Identity) وكذلك تكامل ومصدر المعلومات التي يرسلونها أو يستقبلونها .

نستنتج من ما تقدم أن هناك عدة مظاهر للوثوقية فادا كان طرفي الاتصال يحاولان التثبت من هوية كل منهما فيجب أن يراعي وجود احتمالين :

١: إن كـــلا طرفي الاتصال على اتصـــال نشط (active) وفي الوقت الحقيقي (Real Time) .

٢: يستطيع طرفي الإرسـال تبادل العبارات مع بعض التأخير (Delay) في تبادل المعلومات ، بمعنى آخر أن العبارات قد تسـير أو ترسـل (Routed) من خلال عدة شبكـات اتصال يمكن أن تخزن ويتـم بعد دلك إرسالها في وقت لاحق .

في الحالة الأولى ، فأن كلا من طرفي الاتصال يرغب في إثبات هوية الآخر في الوقت الحقيقي . يتم دلك بواسطة المرسل وذلك بأن يرسل معلومة الغرض منها هو قيام المستقبل بإعطاء الاستجابة الصحيحة لتلك المعلومة وبذلك يمكن التحقق من هوية المرسـل . (أي أن كلا طرفي الإرسـال يسـتطيع كل منهما أن يتحقق من هوية الطرف الآخر). هذا النـــوع مـــن الوثوقية يطلق عليه وثوقية الكينونية (entity Authentication) أو ببساطة يمكن ان يسمى التعرف (Identification) . أما في الحالة الثانية فانه من غير الملائم أن ترســـل معلومة التحقق إلى الطرف الآخر وتنتظر الاستجابة (Response) , في هده الحالة فان مسار الاتصال قد يكون في اتجاه واحد فقط بمعنى آخر فان المطلوب هو التحقيق من وثوقية مصدر العبارة، وهناك عدة تقنيات تتطلب هذا النوع من الوثوقية . إن هـذا النـــوع مـــن الوثوقية يطلـــــق عليـــــه وثـــــوقية مصـــدر البيانات (Data Origin Authentication) .

٤-٢-١ : التعريف (Identification):

تعريف ٤ -٢ : تقنيـة التعرف او اثبـات الكينونـة (Identification or Entity Authentication) :

تقنية التعرف هي كل طرف لادلة تثبت هوية الطرف الثاني المشـــترك وبان هذا الطرف كان نشطا (Active) في الوقت الذي نشأت فيه او اكتبست فيه هذه الادلة . مثاليا فان البيانات المرسلة فقط هي التي ستكون ضرورية للتعرف على الاطراف المتصلة او المترا سلـــــة . ستكون كلا الكينونتين (المرسل والمستقبل) نشطا خلال الاتصال ، مع توفير موثوقية السقف الزمني .

مثال ٤-٢ : التعرف (Identification)

عندما يتصل الطرق A مع الطرق B عبر الهاتف فإنه إذا كان بامكان كل من A, B تعريف احدهما إلى الآخر عند ذلك يمكن توفير وثوقية الكينونة من خلال تمييز الصـــوت لكل منهما (Voice Recognition). رغم أن هذه العملية غير مضمونه لكن هذه الطريقة لها تأثيرها الواضح في الواقع العملي .

مثال ٤-٣ : التعرف (Identification):

إذا ادخل الشـــخص A إلى آلة المصـــرف (Banking Machine) رقمه التعريفي (Personal Identification Number - PIN) بواســـطة بطاقة مغناطيسية (Magnetic Stripe Card) تحتوي على معلومات عن A ، فأن الة المصـــرف تســـتخدم المعلومات في البطاقة ومعلومات PIN لغرض التحقيق في شـــخصـــية حامل البطاقة. فإذا تم التحقق بنجاح فإن المســـتفيد A يعطي إمكانية الوصول إلى الخدمات المتنوعة التي توفرها .

مثال ٤-٢ هو نموذج لإثبات الشخصية التبادلي (Mutual Authentication) ، بينمـا مثـال ٤ -٣ يوفر إثبـات شـــخصـــيـة أحـادي (Unilateral Authentication) . هنـاك العديـد من الميكـانيكيـات والبروتوكولات التي توفر عمل هذين المثالين .

٤-٢- ٢ : وثوثيقة مصدر البيانات (Data Origin Authentication):

تعريف ٤ -٣ :

وثوقية مصـــدر البيانات أو وثوقية العبارة (Message Authentication) توفر دليلا مؤكدا عن هوية(Identity) للمشترك الذي انشأ العبارة .

عادة عندما نرسـل عبارة معينة إلى B تكون معها معلومات إضـافية تمكن الطرف B من تحديد هوية الكينونة التي أرسلت العبارة (أي مصدر إرسال العبارة) . هذه المعلو مات الإضـــافية هي في الواقع عبارة عن دالة بالغة التعقيد ولايمكن للعدو اختراقها . هذا النوع من الوثوقية يكون مناسـبا فقط في الحالات التي يكون فيها احد المشتركين قد تغير أثناء الإرسال .

مثال ٤-٤ : عن وثوقية مصدر البيانات (Data Origin Authentication)

إذا أرسل Aعبارة إلى B عن طريق البريد الالكتروني (E- Mail) فان العبارة تنتقل خلال عدة أنظمة شـــبكات اتصـــال ثم تخزن لصـــالح الطرف B لغرض استرجاعها متى مـا رغب فـي وقت لاحق . لا يـوجد عـادة اتصال مباشر بين A وB . يـرغب الطـرف B بان يمتلك بعض الوسائـل لغرض التحقق (Verify) من أن العبارة المســـتلمة والمتكونة من قبل الطرف A هي فعلاً قد صـــدرت من B. توفر وثوقية مصدر البيانات ضمنياً تكامل البيانات (Data Integrity) والسبب في دلك انه لو تم تحوير أو تغيير العبارة خلال الإرسال ، فان الطرف A لا يعتبر مصدرا للعبارة .

٤-٣ : تشفير المفتاح العام (Public – Key Cryptoyraphy):

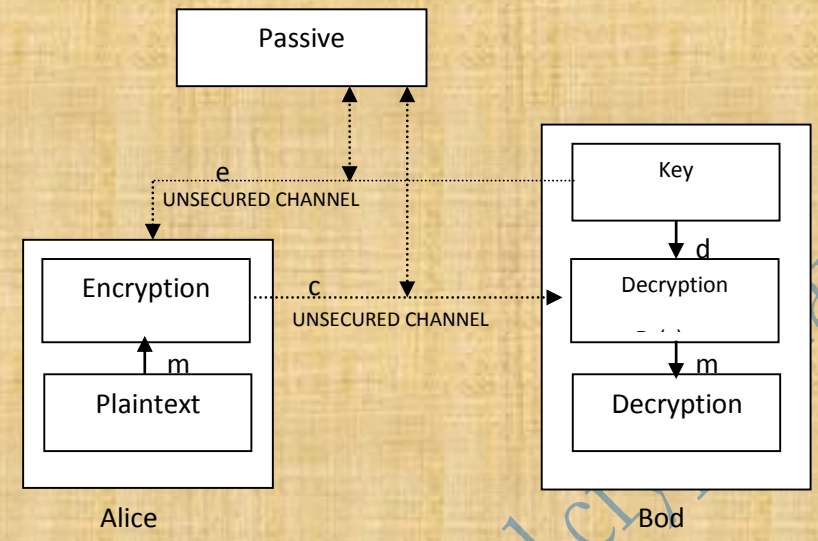
تعتبر فكرة المفتاح العام من المباديء البسيطة والراقية الاستخدام .

إذا كان $\{E_e : e \in K\}$ هو مجموعة تحويلات التشفير وان $\{D_d : d \in K\}$ هو مجموعة تحويلات فتح الشـفرة (Decryption) حيث أن K يمثـــل مسـاحة المفتـــاح .إذا فرضنـــا أن زوج تحويـــلات التشفير وفتـــح التشفيـــر هو (E_e , D_d) وتفترض أن كل زوج يملك خاصية انه بمعرفة E_e وبوجود نص مشفر عشوائي $c \in C$ ستكون هناك صعوبة في حساب العبارة $m \in M$ بحيث ان $C= E_e(m)$. (يعني صعوبة إيجاد m من c عشوائية من خلال المعادلة $(Ee(m)=c$. تدل هده الخاصية ضمنياً انه لقيمة معينة لـــ e فانه من الصعوبة جداً تحديد مفتاح فتح الشفرة d المقابل للمفتاح e . إن المفتاحين d,e يمثلان دالة التشفير ودالة فتح

الشـفرة علي التوالي . إن الخاصـية الرئيسـية في أنظمة المفتاح العام هو انه يمكن حســـاب المفتاح الآخر بمعرفة معلومات المفتاح الأول (أي آن دالة التشـــفير هي معكوس دالة فتح الشـــفرة) ، و هده الخاصـــية لا تتميز بها أنظمة التشـــفير المتناظرة (Symmetric-Key) حيث أن e و d يكونان متساويتان .

الشكل ٤-٢ يمثل طريقة التشفير باستخدام تقنية المفتاح العام .

شكل ٤-٢ : التشفير باستخدام تقنيات المفتاح العام.



نفترض وجود مرسل ومستقبل(Bob ,Alice). يقوم الطرف Bob بأختيار زوج المفتاح (e ,d) . يرسل Bob مفتاح التشفير e (والذي يسمى المفتاح العام) إلى Alice عبر قناة الاتصـــال لكنه يحتفظ بالمفتاح (d) (يطلق عليه المفتاح الخاص private key) بصورة سرية وأمينة (أي أن المفتاح الخاص هو سري وغير معلن) . عند إرسال Aliceعبارة m بواسطة طريقة التشفير والتي تستخدم المفتاح العام الذي حدده Bob فانه سيتم الحصول علي النص المشفر $c = E_e(m)$. يقوم الطرف Bob بفتح شـــفرة c بتطبيق التحويل المعاكس D_d والمعرف بواسطة المفتاح d.

فـــي أنظمة المفتاح العام فان مفتاح التشفير يرسل إلى Alice عبر قناة غير أمينة . هذه القناة غير الأمينة هي نفس القناة التي يرســـل من خلالها النص المشفر. بما أن e هو مفتاح معلن وليس من الضروري أن يكون سري ، فان أي

كينونة تستطيع أن ترسل عبارات مشفرة إلى Bob والذي فيه يستطيع Bob فقط أن يفتح الشفرة (decrypt) .

ملاحظة ٤-٣ :

لغرض تأمين السرية لطريقة المفتاح العام فيجب أن تكون هناك صعوبة واضحة في حساب d من e .

ملاحظة ٤-٤ : المفتاح الخاص ومايناظره من المفتاح السري

لغرض إزالة الغموض ، فانه من الشائع استخدام التعبير المفتاح الخاص (Private Key) كي يرتبط استخدامه مع أنظمة تشفير المفتاح العام ، وان المفتاح السري (Secret Key) مع أنظمة التشفير التناظرية . وهذا يعزى إلى أن المفتاح السري المتاح لاثنين أو أكثر من المشتركين وكلهم مسؤولون عن أمنيته وسريته لكن المفتاح هو حقيقة خاص (Private) حيث أن هذا الطرف هو الذي فقط يعرف المفتاح .

توجد العديد من الطرق والتي يعتقد بصورة واسعة أنها طرق تشفير مفتاح عام أمينة ، ولكن لا توجد أي طريقة منها تم إثباتها رياضيا أنها أمينة مستقلة عن الافتراضات المؤهلة (Qualifying Assumptions) . هذه الواقع غير موجودة في أنظمة المفتاح التناظري حيث أن نظام شفرة الوسادة (one-time pad) تمت برهنته انه أمين .

٤-٣-١ : ضرورة تامين الوثوقية في أنظمة المفتاح العام The Necessity of Authentication in Public –Key Systems):

سوف يتبن لنا أن علم تشفير المفتاح العام هو نظام مثالي (Ideal System) ولا يحتاج إلى قناة امينه في نقل مفتاح التشفير . هذا ربما يعطي الانطباع بان كلا الكينونتين تستطيعان الاتصال من خلال قنوات غير أمينة بدون الحاجة لتبادل المفاتيح . للأسف الشديد ، إن هذا هو غير الواقع . الشكل ٤-٣ يوضح لنا كيف يستطيع عدو فعال اختراق النظام ويفتح شفرة العبارة المرسلة إلى الكينونة الأخرى من غير أن يكسر نظام التشفير . هدا نوع من انتحال الصفة أو الشخصية (Impersonation) وهو مثال لفشل البروتوكول (Protocol Failure) . في هذا السيناريو فان الخصم ينتحل شخصية الكينونة B (المستقبل) وذلك بواسطة إرسال الكينونة A لمفتاح عام هو e والذي يفترضه A (وهو غير صحيح) انه المفتاح العام لـ B . إن العدو أو الخصم يعترض العبارات

المشفرة المرسلة من A إلى B ويفتح شفرتها بمفتاحه الخاص ' d'(أي مفتاح الخاص للخصم) ، ثم يعيد تشفير (re –encrypts) العبارة بواسطة المفتاح العام e للكينونة B ويرسل العبارة الأخيرة إلى B . إذن لابد من توفير وثوقية (Authenticate) المفاتيح العامة لغرض تامين وثوقية مصدر البيانات للمفاتيح العامة نفسها (بمعني آخر وجود وسيلة لتأمين صحة وموثوقية المفاتيح العامة).
ان الكينونة A يجب أن تتأكد من تشفير البيانات بأستخدام المفتاح العام الشرعي لكينونة B و هذا متاح من خلال تقنيات المفتاح العام والتي تعطي حلا رائعاً لهذه المشكلة .

٤-٣-٢ : التواقيع الرقمية النابعة من تشفير المفتاح العام العكسي (From Reversible Public –Key Encryption):

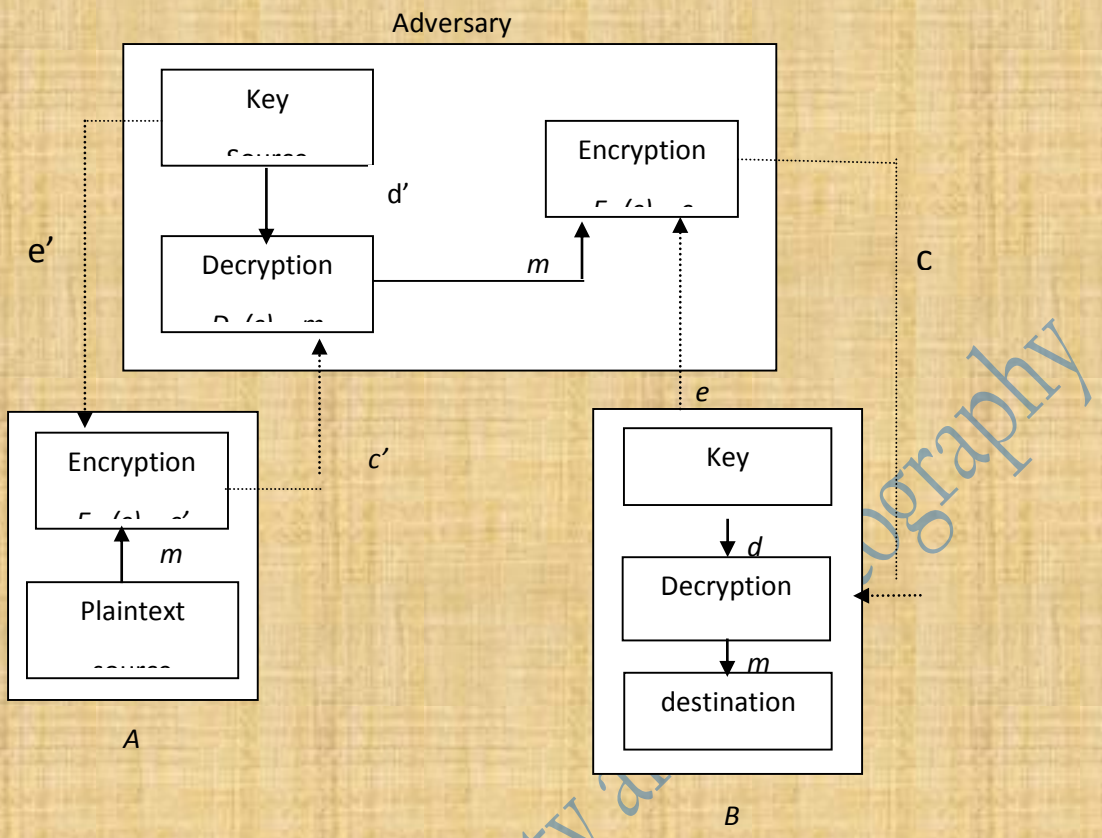
إن التوقيع الرقمي الذي سيتم مناقشته هنا يعتمد علي أنظمة تشفير المفتاح العام .

نفرض أن E_e هو عبارة عن تحويل تشفيري لنظام المفتاح العام وان هناك مساحة عبارة M ومساحة نص مشفر C. نفرض أن M=C فإذا كان D_d هو طريقة تحويل فتح الشفرة المقابل لـ E_e وبما أن كل من D_d , E_e عبارة عن عمليات تبديل عنصر مكان عنصر (Permutation) فانه يمكن تطبيق مايلي :

$$D_d (E_e (m))=E_e(D_d(m))=m$$

لكل عبارة M $m\in$. ان طريقة تشفير المفتاح العام في هدا النوع يطلق عليها المعكوس (Reversible) .

شكل ٤ ـ ٣ : هجوم انتحال الشخصية في اتصال لمشتركين اثنين .



٤-٣-٣ : بنـاء طريقـة التوقيع الرقمي (Construction for a Digital Signature Scheme):

١: لتكن M هي مساحة العبارة المطلوب توقيعها .

٢: لتكن C=M هو مساحة التوقيع S .

٣: ليكن زوج المفتاح (e ,d) هو المفاتيح المستخدمة في طرق تشفير المفتاح العام .

٤:: تعرف دالة التوقيع S_A بأن تكون D_d بمعني آخر فأن التوقيع للعبارة $M \in m$ هو $s=D_d(m)$

٥: تعرف دالة الإثبات أو التحقيق V_A (Verification Function) كما يلي :

$$V_A(m,s) \begin{cases} \text{True, if } E_e(s)=m \end{cases},$$

يمكن أن يبسط مفهوم التوقيع بأنه إذا كان A يوقع فقط العبارات التي تملك هيكل خاص وان هذا الهيكل هو معروف علنا . فإذا كانت M' هي مجموعة جزئية (Subset) لـ M وان عناصر M' تملك هيكل خاص ومعرف مسبقاً بحيث أن M تحتوي علي جزء غير مهم من عبارات المجموعة . كمثال على ذلك نفرض أن M'تتكون من سلاسل ثنائية بطول t ٢ ، حيث t عدد صحيح موجب ، وتفرض أن M' هي مجموعة جزئية من M متكونة من السلاسل بحيث أن أول t ثنائي سيتم تكرارها في آخر مواقع لـ t في الـ bits (مثلاً 101101 سوف تكون هذه السلسلة الثنائية في M' ولقيمة t=3). إذا كان A هو فقط الذي يوقع العبارات ضمن المجموعة الجزئية M' ، فانه يمكن بسهولة إدراكها بواسطة الطرف المحقق (Verifier) لذلك سوف تعيد تعريف دالة التحقق V_A كما يلي :

$$V_A(s) = \begin{cases} \text{true; if } E_e(s) \in M' \\ \text{False , otherwise} \end{cases},$$

بموجب هدا السيناريو الجديد فأن A يحتاج فقط أن يرسل التوقيع s لان العبارة $m = E_e(s)$ يمكن استعادتها (recover) وذلك بتطبيق دالة التحقق . مثل هذه الطريقة يطلق عليها طريقة التوقيع الرقمي باسترجاع العبارة . إن ميزة اختيار العبارات بهيكل خاص (Special Structure) يشار له بأنه اختيار العبارات بحشو (بمعني آخر أن العبارة يتم اختيارها بهيكل معين بحيث تحشى معها عبارة إضافية ملتصقة بها)

٤-٣- ٤: التواقيع الرقميــة في الواقع العملي (Digital Signatures in Practice):

يجب ان يتميز التوقيع الرقمي بما يلي :

١- أن يكون التوقيع سهل حسابه من قبل الموقع (Signer) (بمعني آخر يجب أن تكون دالة التوقيع سهلة التطبيق) .

٢-يجب أن يتميز التوقيع الرقمي بســـهولة التحقق منه (Verify) من قبل أي شخص (بمعني آخر يجب أن تكون دالة التحقق Verification Function سهلة التطبيق) .

٣-يستغرق التوقيع الرقمي زمن مناسب ، متى ما كانت هناك ضرورة لمواجهة أي تزوير (Forgery) .

٤-٣- ٥ : حل النزاعات (Resolution of Disputes):

إن الغرض من التوقيع الرقمي (أو أي طريقة توقيع) هو قابليته في حل النزاعات . كمثال علي ذلك فأن الكينونة A من المحتمل في حالة معينة أن ينكر توقيعه لعبارة معينة أو أن الكينونة B تدعي الكذب بان توقيع العبارة قد تم صدوره من الكينونة A . لغرض معالجة مثل هده المشكلة فان يتطلب وجود كينونة أو طرف ثالث موثوق فيه (Trusted Third Party TTP) أو يسمي الحكم (Judge). يجب أن يكون TTP عبارة عن كينونة بحيث أن جميع الإطراف المشتركة تتفق مقدماً أو سلفاً على وثوقيته .

إذا أنكر A ت توقيعه للعبارة m المرسلة إلى B ، فان B يجب أن يكون قادرا على تقديم التوقيع S_A للعبارة M إلى الطرف الثالث TTP .عند ذلك فان الطرف الثالث TTP يحكم لصالح B إذا كان $V_A(m, S_A) = true$ وفي غير ذلك يحكم لصالح A . إن الطرف B سوف يقبل هذا القرار إذا كان B على ثقة بان الحكم TTP يملك نفس تحويل التحقق V_A الذي قام بعمله A . أما الطرف A فانه سيقبل قرار الحكم TTP إذا كان A كان واثقا من أن الحكم TTPاستعمل الـ- V_A وان S_A لم يتم تشويهه او اعتراضه . لذلك فانه لتوفير حل عادل للنزاعات فان ذلك يتطلب عدد من المعايير (Criteria) التالية والمدرجة في الفقرة التالية:

٤-٣-٦ : المتطلبات الضرورية لحل التواقيع المتنازع عليها:

١: V_A ,S_A لهما خواص التواقيع الرقمية ودالة التحقق التي تم الإشارة إليها سابقا .

٢: يملك الحكم نسخة موثوق فيها (Authentic) من V_A .

٣: يجب أن يحفظ تحويل التوقيع S_A بســـرية ويبقى غير معرض للإنتهاك (أي يبقى مؤمنا).

٤-٤ : أنظمة التشـفير التناظرية ومايقابلها من المفتاح العام (Symmetric – Key vs. Public-Key Cryptography):

من هو الأفضـل تشـفير المفتاح العام أم التشـفير التناظري ؟ أشـار نيدمان واشـرودور (Needman و Schrooder) إلى أن عدد وطول العبارات هي اكبر بكثير في خوارزميات المفتاح العام من الخوارزميات التناظرية . ومنها استنتجا أن الخوارزمية التناظرية هي أكثر كفائة من خوارزمية المفتاح العام .

إن تشـفير المفتاح العام والتناظري هما نوعان مختلفان ولهما القدرة الكبيرة لحل أنواع مختلفة من المشاكل . طرق التشفير التناظري هو أفضل لتشفير البيانات وهي أسرع وغير معرضة إلى هجومات النص المشفر المختار . من ناحية أخرى فان تشفير المفتاح العام يستطيع إنجاز الأشياء التي لا يستطيع التشفير التناظري أداؤها ، تعتبر طرق تشفير المفتاح العام الأسلوب الأفضل لإدارة المفتاح .

لكل من أنظمة تشـفير المفتاح العام وأنظمة التشـفير المتناظرة عدة فوائد و مساوئ بعضها مشترك بينهما. في هذه الفقرة سيتم إلقاء الضوء على عدد من هذه الخصائص المبينة أدناه :

١: فوائد أنظمة التشفير التناظري:

أ : يمكن تصـميم شـفرات المفتاح التناظري بحيث تعطي معدلات عالية من الإنتاجية البيانية (Data Throughput) . بعض الاسـتخدامات المادية (Hardware) يمكنها ان تعطي معدلات تشـفير تصـل لمئات من الميكابايت لكل ثانية ، بينما الاسـتخدامات البرمجية قد تعطي معدلات إنتاجية في حدود الميكابايت في الثانية كمعدل .

ب : المفاتيح المستخدمة في أنظمة التشفير التناظري نسبياً قصيرة.

ج : يمكن توظيف أنظمة التشفير التناظرية كأساسيات (Primitives) لتكوين آليات تشفير متعددة تشمل مولدات الأرقام العشوائية (Pseudorandom Number Generators)، الدوال الهاشية (Hash Functions)، وطرق تواقيع رقمية كفوءة .

د : أنظمة التشفير التناظرية يمكن أن تدمج أو تجمع (Composed) بهدف تكوين نظام تشفيري قوي وكفوء وان التحويلات التشفير البسيطة هي معرضة لعمليات تحليل الشفرة وتكون سهلة التعرض لهذه العمليات التحليلية، ولكن رغم ضعفها في توفير الأمنية ، فأنه يمكن أن تكون لنا نظاما مشفر جديد يتميز بأنه أكثر قوة.

هـ : لأنظمة التشفير التناظرية تاريخ واسع ولكنها تطورت لاحقا بصورة سريعة ونالت اهتماما خاصة عند طريقة تشفير البيانات القياسية (DES) .

٢ : مساوئ التشفير في أنظمة المفتاح المتماثل:

أ : عند أتصال طرفين في شبكة أتصال فيجب أن يبقى المفتاح سري في كلا نهايتي الإتصال (طرفي الاتصال) .

ب : في شبكات الإتصال الكبيرة يوجد عدد كبير من أزواج المفاتيح التي يجب أدارتها وتحتاج إستخدام طرف موثوق فيه غير مشروط .

ج : في الإتصال بين كينونتين A , B فأن عملية التشفير الكفوءة تتطلب تغيير المفتاح بصورة متكررة وربما في كل دورة إتصال (Communication Session) .

د : آليات التوقيع الرقمية المعتمدة علي أنظمة تشفير المفتاح التناظري تحتاج أما استخدام مفاتيح كبيرة لغرض تكوين دالة التحقق العامة (Verification Function) أو استخدام طرف ثالث حكم (TTP) .

٣: فوائد انظمة تشفير المفتاح العام :

أ: تلتزم هذه الأنظمة أن يحفظ المفتاح الخاص بصورة سرية (يجب التثبت أو التحقق (Authenticity) في المفاتيح العامة) .

ب : إدارة المفاتيح في شبكة الاتصال يتطلب وجود فقط حكم موثوق منه وليس TTP موثوق وغير مشروط .

ج : معتمداً علي طريقة (طور) الاستخدام (Mode of Usage) فان زوج المفاتيح العامة والخاصة تظل غير متغيرة (ثابتة) لفترة زمنية مقبولة قد تكون لعدد من دورات الاتصال (أو لعدة سنوات) .

د : هناك العديد من طرق المفتاح العام تنتج طرق توقيع رقمي ً أكثر كفائة نسبيا . يكون المفتاح المستخدم لغرض وصف دالة التحقق او التثبت اصغر بكثير من المفتاح المستخدم بما يقابلها في أنظمة المفتاح التناظرية .

ه : في شبكة الاتصال الواسعة آو الكبيرة (Large Network) فان عدد المفاتيح الضرورية أو المطلوبة اقل بكثير من تلك المستخدمة في أنظمة المفتاح التناظرية .

٤: مساويْ أنظمة تشفير المفتاح العام :

أ : معدلات الإنتاجية (Throughput Rates) لمعظم طرق التشفير الشائعة أبطا بعدة مرات من أحسن طرق المفتاح التناظري المعروفة .

ب : حجوم المفتاح (Key –Sizes) تكون اعتيادياً اكبر بكثير من تلك التي نحتاجها في أنظمة تشفير المفتاح التناظرية ،وان حجم تواقيع المفتاح العام اكبر من تلك المستخدمة في التقنيات التي توفر وثوقية مصدر البيانات في أنظمة تشفير المفتاح التناظرية .

ج : لم يتم التحقق من أن أنظمة المفتاح العام هي أنظمة سرية (Secure) ، (نفس الشي يقال بالنسبة لشفرة الكتل). إن معظم أنظمة تشفير المفتاح العام الأكثر فعالية والمستخدمة حتى هذا التاريخ أمنيتها تعتمد علي الصعوبة المفترضة لمجموعة صغيرة من مسائل رياضية نظرية .

د : أنظمة تشفير المفتاح العام ليس لها تاريخ واسع مثل ما تتميز به انظمة تشفير المفتاح التناظرية ، حيث ثم اكتشاف طرق المفتاح العام فقط في منتصف السبعينات ١٩٧٠ .

٤-٤- ١ : ملخص للمقارنة بين أنظمة المفتاح العام وأنظمة التشفير المتناظر:

تبين أن أنظمة المفتاح العام وأنظمة التشفير التناظرية تملك عددا من الفوائد المتممة . لهذا فان أنظمة التشفير الحالية تستثمر إمكانيات القوة لكل منها. يمكن لتقنيات أنظمة تشفير المفتاح العام أن تستخدم بحيث تنشئْ مفتاحا لأنظمة تشفير المفتاح التناظرية والذي يمكن ا ستخدامه للاتصال بين الطرفين A , B . في هذا السيناريو فانه يستطيع كل من A , B أن يستفادا من خاصية طول المفاتيح المطبقة للمفتاح العام والمفتاح الخاص في أنظمة تشفير المفتاح العام وكذلك يمكن لكل من A , B ان يستخدم قدرات التنفيذ لأنظمة تشفير المفتاح التناظرية . بما أن تشفير البيانات هو غالباً ما يا خد أو يستهلك معظم الوقت المخصص لعملية التشفير ، فان استخدام أنظمة المفتاح العام في إنشاء المفتاح يأْخد جزءا بسيطا من العملية الكلية للتشفير المنفذة بين A , B .

حتى هذا التاريخ فان الأداء (الإنجاز) الحسابي لأنظمة تشفير المفتاح العام هو اقل مستوى من أنظمة التشفير التناظرية ولكن لا يوجد إثبات لهده الحالة .

١: توفر أنظمة تشفير المفتاح العام تواقيع رقمية كفوءة (خاصة في توفير عدم الإنكار Non –Repudiation) وكذلك كفوءة في إدارة المفتاح (Key Management) .

٢- تعتبر أنظمة تشفير المفتاح التناظرية ذات كفاءة عالية في تطبيقات التشفير وبعض تكامل البيانات (Data Integrity) .

ملاحظة ٤-٥ : أحجام المفاتيح - المفتاح التناظري وما يقابله من المفتاح الخاص:

يجب أن تكون المفاتيح الخاصة في أنظمة تشفير المفتاح العام كبيرة (مثلاً 1024 bits في الـ RSA) واكبر في العادة من المفاتيح السرية في أنظمة تشفير المفتاح التناظرية (مثلاً ٦٤ أو ١٢٨ بت) ،والسبب في ذلك انه عند تامين سرية الخوارزمية في أنظمة التشفير التناظرية فان أكثر الطرق كفاءة لمهاجمة هذه الأنظمة يتطلب بحثا مكثفا عن المفتاح، بينما جميع أنظمة تشفير المفتاح العام تعتمد في دحض هذه الهجومات على تعقيد تحليل العوامل (Factoring) وهو أكثر كفائة من عمليات البحث المكثف . وكنتيجة لذلك فانه لتامين السرية في كلا النظامين فان مفاتيح أنظمة التشفير التناظرية تكون بطول (عدد من bits) اصغر من المفاتيح الخاصة المستخدمة في أنظمة تشفير المفتاح العام (مثلاً بمعامل ١٠ أو أكثر).

ملاحظة ٤-٦ :

بالنسبة إلى أنظمة التشفير التناظرية ، فان مفتاح الشفرة ، يجب أن يكون طبعا محميا حماية بالغة ، لكن في أنظمة التشفير غير التناظرية فان مفتاح التشفير يكون غير محميا وأحيانا معلنا (مفتاح عام) . في قناة اتصال باتجاهين وبوجود مشتركين A و B ، يوجد الآن أربعة مفاتيح ، مفتاح تشفير مفتوح للمشترك B مع ما يقابله من مفتاح خاص لـ A ، ومفتاح تشفير مفتوح للمشترك A مع ما يقابله من مفتاح خاص لـ B . إن المشترك A يريد الآن استلام رسائل من عدد آخر من المشتركين ، وجميعهم يعرفون المفتاح العام للمشترك A والثقة بان المستقبل الوحيد المخول لفتح شفرة الرسائل هو المشترك A . لذلك ، فان كل مشترك له مفتاح عام ومفتاح خاص ، وان العدد الكلي للمفاتيح لشبكة مكون من ١٠٠٠ مشترك تتقلص من حوالي مليون إلى ألفين .إن فكرة المفتاح المفتوح (العام) أعلنت من قبل ديف وهيلمان في العام ١٩٧٦ .

٤- ٥ : ضغط البيانات ، الترميز ، والتشفير (Compression, Encoding , and Encryption):

ان استخدام خوارزمية ضغط البيانات مع خوارزمية تشفير له عدة فوائد اهمها :

١ : يعتمد محلل الشفرة على استثمار الحشو (Redundancies) في النص الواضح ، إن عملية ضغط ملف معين قبل تشفيره يقلص هذا الحشو .

٢ : إن ضغط البيانات يقلص من الحشو في النص الواضح الذي كان يمكن أن يستثمره محلل الشفرة .

٢ : إن عملية التشفير تكون عادة مستهلكة للوقت (Time-Consuming) و ضغط ملف معين قبل تشفيره يسرع هذه العملية .

الشئ المهم المطلوب هو إجراء عملية الضغط قبل عملية التشفير . إذا كانت خوارزمية التشفير تتصف بأنها خوارزمية جيدة ، فان النص المشفر سوف لا يحتاج لضغطه .

عند إضافة أي نوع من ترميز الإرسال (Encoding) ، أو معالجة وكشف الخطأ (Error Detection and Recovery) ، فانه يجب أن يتم إضافة ذلك بعد التشفير .

٤-٦ : الدوال الهاشية (Hash Functions):

إحدى أوليات (primitives) طرق التشفير الحديث هو استخدام الدالة الهاشية التشفيرية ، التي تسمى عادة الدالة الهاشية ذات الاتجاه الواحد (One –Way Hash Function) .

تعريف ٤-٤:

الدالة الهاشية H عبارة عن دالة حسابية كفوءة تستخدم لتحويل (Mapping) سلاسل من الأرقام الثنائية بطول اختياري إلى سلاسل من الأرقام الثنائية بأطوال ثابتة معين يطلق عليها القيم الهاشية (Hash –Values) ، H (M) = h لأي متغير M .

بالنسبة إلى الدالة الهاشية والتي تنتج قيم هاشية بمقدار n-bit (مثلاً n=128 او n=160) ولها خصائص مقبولة ، فان احتمالية تحويل سلسلة مختارة عشوائياً

الى قيم هاشـــية بمقدار n (Image) هو 2^{-n} (2^{-n} هي الاحتمالية) . الفكرة الأساسية لهذا الاجراء هو أن القيمة الهاشية تؤدي كتمثيل مكدس أو مدمج لأي سلسلة مدخلة . في حالة استخدام هذه الدالة للتشفير، فان الدالة الهاشية h يجب اختيارها بحيث تؤمن صـــعوبة في عمليات الحســـاب والتي تمنع أن يأخذ مدخلين محددين نفس القيمة (بمعنى حدوث تصادم (Collision) بين قيم x، y ، وهذا يعني أن (h(x) =h (y) ، أيضا فان أي قيمة هاشية معينة مثل y فيجب أن تكون هناك أيضا صعوبة في الحساب والتي تؤدي أن يكـــون هنـــاك مدخل معين x مثلاً بحيث ان h(x)=y (أي يجب منع هده الحالة).

عندما تستخدم الدالة الهاشية في التشفير تكون لها الخواص التالية :

١: المدخل (Input) يمكن أن يكون بأي طول .

٢: المخرج (Output) طوله ثابت .

٣: H(x) تكون سهلة الحساب نسبيا لأي قيمة لـ x .

٤: H(x) هي دالة ذات اتجاه واحد .

٥: تكون خالية من التصادم (collision-free) .

يطلق على الدالة الهاشـية H أنها دالة ذات اتجاه واحد إذا كانت تتميز بصـعوبة العكس (hard to invert) ، أي انه من المتعذر حســـابيا إيجاد مدخل معين x بحيث أن H(x) = h . إذا كانت هناك عبـــارة معينـــة x ، فانـــه يكـــون من الصعب حسابيـــا إيجـــاد عبـــارة y لا تساوي x بحيث أن H(x) = H(y) ، عند ذلك فان H يطلق عليها بأنها دالة هاشية ضعيفة التحرر من التصادم (weakly collision-free) . تكون الدالة الهاشية قوية التحرر من التصادم H إذا كان من المتعذر حسابيا إيجاد أي عبارتين x و y بحيث أن H(x) = H(y) .

القيمة الهاشـية تمثل مختصـرا للعبارات الطويلة او الوثائق التي قد تم حسـابها منها لذا أحيانا يطلق عليها مختصر العبارة (message digest) . يمكن التفكير بمختصر العبارة أنها تشـــبه طبع الأصـــابع الرقمي (digital fingerprint) لوثيقة الطويلة . أمثلة للدوال الهاشية المعروفة بشكل جيد هي MD2 و MD5 .

ربما يكون الدور الرئيسي لدالة الهاشية التشفيرية هو في توفير تدقيقات تكامل العبارة والتواقيع الرقمية لان الدوال الهاشية عموما أسرع من خوارزميات التشفير أو التوقيع الرقمي ، فان من الامثل حســـاب التوقيع الرقمي أو تدقيق التكامل لوثيقة معينة وذلك بتطبيق المعالجة التشـــفيرية على القيمة الهاشـــية للوثيقة وهذه القيمة تكون صغيرة مقارنة بالوثيقة نفسها . إضافة إلى ذلك ، فان المختصر (Digest)

يمكن أن يعمل بشـــكل معلن (Public) بدون إظهار أو كشـــف محتويات الوثيقة التي اشتق منها .

اثر العـالمـان دامكـارد وميركلي (Damgård و Merkle) بشـــكـل كبير في تـصميم الدوال الها شية التـشفيرية وذلك بتعريف دالة ها شية بمفهوم ما يطلق عليه دالة الضغط (compression function) . تأخذ دالة الضغط مدخلا ثابت الطول وترجعه الى مخرج اقصر وثابت الطول . باسـتخدام دالة الضـغط ، فان الدالة الهاشـية يمكن تعريفها بواسـطة تطبيقات متكررة لدالة الضـغط إلى أن يتم معالجة العبارة بأكملها . في هذه الطريقة ، فان العبارة بطول اختياري يمكن تجزئتهـا إلى كتل بحيث تعتمد أطوالها على دالـة الضغـط ، ثـم تحشى(تضاف Pad) (لأسباب أمنية) حتى يكـون حجم العبارة مضاعف (multiple) لحجم الكتلة .

أكثر الاستخدامات التشفيرية المعروفة للدوال الها شية هو تطبيقها في التواقيع الرقمية وفي تكا مل البيا نات . وفي التواقيع الرقمية، فان اي عبارة طويلة يتم معاملتها بدالة هاشـية مناسـبة ومعلنة ثم فقط توقيع القيمة الهاشـية . إن الطرف الذي يستقبل العبـــارة يقـــوم بتطبيق الدالـــة الهاشيـــة علـــى العبارة المستلمة ، ويستطيع التحقق (Verifies) ان التوقيع المستلم هو صحيح لهذه القيمـــة الهاشـــية . يؤدي هذا العمل الي توفير كلا من الوقت والمســـاحة مقارنة بالتوقيع الذي يتم على العبارة مباشـــرة ، والذي فيه يتطلب تجزئة العبارة إلى عدة كتل بحجم منا سب لكل كتلة ويتم توقيع كل كتلة بصورة منفصلة (هذا الإجراء يطبق في التوقيع الذي يتم على العبارة نفسها وليس مع القيمة الهاشية) .

يجب علينا ملاحظة أن عدم القدرة على إيجاد عبارتين بنفس القيمة الهاشـــية (أي لهما نفس القيمة الها شية) هو احد متطلبات توفير الأمنية ، لان ه في الو ضع المعاكس لهذه الحالة (أي بوجود قيمتين متســـاويتين) ســـيكون التوقيع لعبارة معينة هو نفســـه لعبارة أخرى ، وهذا ما يســـمح لأي موقع (Signer) بتوقيع عبارة معينة ثم في و قت لاحق من الزمن يدعي (Claim) بأنه قد وقع عبارة أخرى وليس العبـارة الأولى . لاحظ هنـا أن عـدم القـدرة لإيجـاد عبـارتين بنفس القيمة الهاشـــية هو مطلب امني حيث انه عدا ذلك فان التوقيع لعبارة معينة بقيمة هاشـية سـوف يكون نفسـه للعبارة الأخرى ، وبذلك يسـمح للموقع بالتوقيع على عبارة واحدة وفي وقت لاحق من الزمن يدعي انه قد وقع العبارة الأولى .

قد تستخدم الدوال الهاشية في تكامل البيانات وكما يلي:

يتم حســاب القيمة الهاشــية المقابلة لمدخل معين في لحظة معينة من الوقت . تتم حماية تكامل هذه القيمة الهاشية بصيغة معينـة . في لحظـة لاحقـة مـن الزمن ، ولغرض التحقق من أن البيانات المدخلة لم يتم تغييرها فانه يعاد حســـاب القيمة الهاشـــية باســـتخدام المدخل المتوفر ثم يتم مقارنة هذه القيمة مع القيمة الأصـــلية

للتأكد من أنها تساوي القيمة الهاشية الأصلية . هذا التطبيق مفيد بالتحديد في الحماية من الفيروسات وتوزيع البرمجيات .

التطبيق الثالث للدوال الهاشية هو استخدامها في البروتوكولات مشتملا ارتباط سابق ، ومتضمنا بعض طرق التواقيع الرقمية وبروتوكولات وبروتوكولات التعرف (Identification) .

الدوال الهاشية التي تمت مناقشتها أعلاه هي معروفة علناً ولا تتضمن مفاتيح سرية . عندما تستخدم هده الدوال لكشف أو إظهار فيما ان العبارة المدخلة قد تم تغييرها، ففي هذه الحالة تسمي هذه الدوال (شفرات كشف التحوير (MDCs) Modification Detection Codes) . هناك بعض الدوال الهاشية تتضمن مفتاح سري وتوفر وثوقية مصدر البيانات بالإضافة إلى تكامل البيانات وتسمي هذه الدوال في هذه الحالة (شفرات وثوقية العبارة

. (Message Authentication Codes (MACs)

٧-٤ : مقدمة الى البروتوكولات:

إن الاهتمام الأساسي لعلم التشفير هو حل المشاكل المشتملة على الأمنية ، إثبات الشخصية ، التكامل ، والأشخاص غير الأمينين . البروتوكول(protocol) عبارة عن سلسلة من الخطوات يشترك فيها اثنين أو أكثر من المشتركين و مصممة لتحقيق هدف معين . هذا تعريف مهم . إن " سلسلة الخطوات " تعني أن البروتوكول له تسلسل ، من البداية إلى النهاية . يجب تنفيذ كل خطوة بالتتابع ، وليس بالامكان ا ستعمال أي خطوة قبل انتهاء الخطوة السابقة لها . شرط وجود " اثنين من المشتركين أو أكثر " تعني أننا نحتاج على الأقل إلى شخصين لإكمال البروتوكول ، حيث أن وجود شخص واحد بمفرده لا يستطيع عمل البروتوكول . أخيرا فان التعبير " يحقق هدفا معين " يعني أن البروتوكول يجب أن يحقق شيئا ما . سلسلة الإجراءات التي تشبه البروتوكول كلها لا تؤدي هدف معين فهي ليست بروتوكول .

البروتوكولات لها خصائص أخرى إضافة إلى مذكر أعلاه وهي الأتي :

١: كل شخص مشمول في البرتوكول يجب أن يعرف البروتوكول وكل الخطوات المطلوبة فيه وكيفية تتابعها .

٢: كل شخص مشمول في البروتوكول يجب أن يتفق على إتباع ذلك البروتوكول .

٣: البروتوكول يجب أن يكون غير غامض و كل خطوة فيه يجب أن تعرف بصورة جيدة ولا مجال لعدم الفهم (ولسوء الفهم) .

٤: يجب أن يكون البروتوكول قادرا على إكمال عمله .

تشـــتمل كل خطوة من خطوات البروتوكول على حســـابات تجري من قبل مشترك واحد أو أكثر من المشتركين أو عبارات ترسل بين المشتركين أو الاثنين معا .

٤-٧-١: البروتوكولات والاليات (Protocols and Mechanisms):

تعريف ٤- ٥ :

بروتوكول التشفير عبارة عن خوارزمية موزعة معرفة بسلسلة من الخطوات التي تحدد بدقة الفعاليات المطلوبة لكينونتين أو أكثر لغرض الو صول إلى هدف امنـــي محـــدد . إذن البروتوكول التشفيري (Cryptographic Protocol) هو عن بروتوكول يستخدم التشفير . يمكن للمشتركين أن يكونوا أصدقاء وكل واحد منهم يثق بالآخر أو قد يكونوا أعداء ولا يثق احدهم بالآخر . يشتمل البروتوكول التشـــفيري على خوارزمية معينة لغرض تحقيق الأمنية البســـيطة . إن الأطراف المشـــتركة التي تتشـــارك في البروتوكول قد تطلب مشـــاركة في جزء من أمنية البروتوكـــول لغـــرض حســـاب قيمـــة معينة ، تسلسل عشوائي مولد لغرض الارتباط ، إقناع المشترك بهوية المشترك الآخر ، أو توقيع عقد أو اتفاق في وقت واحد . الهدف الأساسي من استخدام التشفير في البروتـوكول هـو لمنـع أو كشف التنصت أو الغش أو الخداع (Cheating) .

ملاحظـة ٤-٧ : البروتوكول ومـا يقـابلـه من ميكـانيكيـة (Protocol vs. Mechanism):

ما يقابل البروتوكول ،هو مفهوم الآلية وهو تعبير أكثر عمومية ويشـــتمل على بروتوكولات وخوارزميات (والتي تســـتخدم لغرض تحديد الخطوات المتبعة في كينونة واحدة) وتقنيات غير تشـــفيرية مثل حماية الأجهزة المادية وإجراءات سيطرة (Procedural Control) لغرض الوصول إلى أهداف أمنية محددة .

تلعب البروتوكولات دوراً أســاســيا في عمليات التشــفير وتعتبر ضــرورية جداً لغرض تحقيق أهداف التشـــفير. يمكن اســـتثمار كل من طرق التشـــفير ، التواقيع الرقمية ،الدوال الهاشـــية ، ومولد الأرقام العشـــوائية في بناء البروتوكول .(يعني طرق التشـــفير والتواقيع الرقميـة ومولـدات الأرقـام العشـــوائيـة هي الأوليـات المستخدمة في بناء البروتوكول) .

٤-٧-٢ : مولدات الأرقام العشـــوائية (Random Number Generators RNG):

إن مولدات الأرقام العشوائية (RNG's) لها موقع مركزي في بعض تصميمات أنظمة التشـــفير . مثلا ، شـــفرات التدفق تســـتخدم مولد أرقام عشـــوائي (RNG) لغرض توفير تســـلســـل تشـــويش (Confusion) يعمل على إخفاء بيانات النص الواضـــح . يعتبر اســـتخدام مولدات الأرقام العشـــوائية من الأســـس المركزية في

شفرات التدفق [مثلا 26, 54]. تتألف شفرة فيرنام مثلا من رابط (على العموم أما بوابة XOR أو إيعاز) ومولد تسلسل تشويش .

من مظاهر البيانات أنها غالبا ما تكون متكررة ، ولذلك يتم ضـغطها وينتج عن ذلك حجم اصغر وأكثر تشابها بتسلسل عشوائي .

مثال ٤- ٥ : البروتوكول المسؤول عن الاتفاق علي مفتاح بسيط (A Simple Key Agreement Protocol):

إذا كان هناك طرفي اتصال هما أليس وبوب (Alice , Bob) وقد اختارا طريقة تشفير المفتاح المتماثل لغرض الاتصال بينهما عبر قناة اتصال غير سرية ولغرض تشفير المعلومات فان ذلك يحتاج إلى استخدام مفتاح . ستكون خطوات البروتوكول لتنفيذ هذا الاتصال كما يلي :

١: ينشي بوب(Bob) طريقة تشفير المفتاح العام ويرسل مفتاحه العام إلى أليس (Alice) عبر قناة الاتصال .

٢: تقوم أليس (Alice) بإنشاء المفتاح المطلوب لطريقة تشفير المفتاح التناظري .

٣: تقوم أليس (Alice) بتشفير المفتاح مستخدمة المفتاح العام لبوب(Bob) وترسل المفتاح المشفر إلى بوب .

٤: يقوم بوب بفتح التشفير (decrypt) باستخدام مفتاحه الخاص وبذلك يمكنه استرجاع المفتاح التناظري (المفتاح الخاص السري) .

٥: يستطيع أليس وبوب Alice, Bob الاتصال مع بعضهما باستخدام طريقة التشفير التناظري ومفتاح سري مشترك بينهما .

يستخدم هذا البروتوكول وظائفا أساسية لغرض توضيح خصوصية (Privacy) الاتصال من خلال قناة اتصال غير سرية . إن المبادئ الأولية التي يستخدمها هذا البروتوكول هو طريقتي تشفير المفتاح التناظري والمفتاح العام . هذا البروتوكول له بعض نقاط الضعف تشمل مثلاً الهجوم لغرض انتحال الشخصية (Impersonation Attack) ، لكنه يحمل الفكرة الأساسية للبروتوكول .

ماذا يستطيع متنصت يدعى ايف (Eve) ، موجودا بين اليس وبوب (Alice ، Bob) ، ان يتعلمه من التنصت في هذا البروتوكول ؟ انه يحاول تحليل النص المشفر . هذا الهجوم الخامل (Passive) هو هجوم نص مشفر فقط هذا باستخدام الخطوة (٣) ويمكن أن يحاول أيضا معرفة الخوارزمية والمفتاح .

النظام التشفيري الجيد هو الذي يكون فيه كل الأمنية متأصلة في معرفة المفتاح وليس في معرفة الخوارزمية . (هذا هو السبب الحقيقي في التركيز على الأهمية الكبر لإدارة المفتاح في التشفير) . باستخدام خوارزمية متناظرة ، فان

اليس وبوب يستطيعان تنفيذ خطوة (١) بشكل معلن ، لكن عليها تنفيذ الخطوة (٢) بسرية . يجب أن يبقى المفتاح سريا قبل و خلال وبعد البروتوكول .

كملخص ، فان أنظمة التشفير المتناظر : لها المشاكل التالية :

١: يجب توزيع المفاتيح بسرية تامة . إذ أن معرفة المفتاح تؤدي إلى معرفة كل العبارات .

٢: إذا تم انتهاك المفتاح (مثلا يسرق أو يخمن أو يغتصب أو يرشى) ، فان المتنصت يستطيع فتح شفرة كل العبارات المشفرة بذلك المفتاح . كما يمكن أن يتظاهر بأنه احد المشتركين وينتج عبارات كاذبة لغرض إيهام الطرف الآخر .

٣: إذا تم افتراض استخدام مفتاح منفصل لكل زوج من المستفيدين في الشبكة ، فان عدد المفاتيح الكلية تزداد بشكل كبير كلما ازداد عدد المستفيدين . في شبكة مكونة من n من المستفيدين تحتاج n (n - 1) / 2 من المفاتيح ، مثلا ١٠ مستفيدين تحتاج إلى ٤٥ مفتاح مختلف لغرض اتصال طرف مع الآخر و ١٠٠ مستفيد يحتاج ٤٤٥٠ مفتاح . يمكن تقليص المشكلة ا وذلك بجعل عدد المستفيدين صغيرا لكن هذا الأمر ليس دائما ممكنا .

غالباً ما يحدد دور تشفير المفتاح العام في الاتصالات الخاصة (Privacy Communications) مثلا هذا الدور هو نفسه الذي اقترح في البروتوكول أعلاه حيث تم استخدام المفتاح العام كوسيلة لغرض تبادل المفاتيح لاستخدام لاحق في تشفير المفتاح التناظري وذلك للميزة الانجازية (Performance) التي تتصف بها أنظمة التشفير المفتاح العام نسبة إلى تشفير المفتاح التناظري .

٤-٧-٣ : قصور البروتوكول والآلية Protocol and Mechanism Failure ( ) :

يحدث قصور البروتوكول أو الآلية عندما تفشل الميكانيكية في تلبية الأهداف المطلوب من البروتوكول تحقيقها ، وذلك بان يتمكن الخصم (Adversary) بالحصول على فوائد ليس فقط من كسر مباشرة خوارزمية التشفير ، لكن من المعالجة (Manipulate) البروتوكول أو الآلية نفسها ، بمعنى آخر يستطيع العدو أن يغير أو يتعامل مع البروتوكول نفسه وليس التلاعب بخوارزمية التشفير .

مثال٤ -٦ : فشل الميكانيكية (Mechanism Failure):

إذا فرضنا أن بوب واليس يتصلان مع بعضهما مستخدمين شفرة التدفق والذي تكون فيه العبارات المطلوب تشفيرها لها صيغة خاصة ومعروفة

(Special Form) فمثلاً الثنائيات العشرون الأولى تحمل معلومات تمثل كمية العملة (Monetary Amount) يستطيع العدو أو الخصم ببساطة أن يعامل الدالة المنطقية (XOR) مع سلسلة مناسبة من الأرقام الثنائية في العشرين ثنائية الأولى من النص المشفر و أن يغير الكمية . بهذا الأسلوب استطاع العدو أن يغير أو يؤثر في إرسال المعلومات رغم عدم تمكنه من الحصول أو قراءة العبارة الكلية . يعنى ذلك أن طريقة التشفير لم يتم اختراقها وإنما قد فشل البروتوكول من أداء عمله بصورة ملائمة ; نستنتج من هذا أن الافتراض الأساسي بان التشفير يزودنا أو يوفر لنا تكامل البيانات هو غير صحيح (لان البيانات قد تم تغير ها و هذا معارض لتعريف تكامل البيانات) .

٤-٧-٤ : الهجومات ضد البروتوكولات:

يمكن أن توجه الهجومات التشفيرية ضد الخوارزميات التشفيرية المستخدمة في البروتوكولات ، وضد التقنيات التشفيرية المستخدمة لتطبيق الخوارزميات والبروتوكولات ، أو ضد البروتوكولات نفسها . من هذه الفقرة سوف نفترض أن الخوارزميات التشفيرية والتقنيات هي أمينة ، وسيتم التركيز على الهجومات ضد البروتوكولات .

هناك عدة وسائل لغرض الهجوم على بروتوكول معين . حيث يستطيع بعض الأشخاص غير المشمولين في البروتوكول التنصت على بعض أو كل البروتوكول . هذا ما يطلق عليه الهجوم الخامل (Passive Attack) بسبب أن المهاجم لا يؤثر في عمل البروتوكول ، حيث أن كل ما يستطيع عمله هو مراقبة البروتوكول في هجوم النص المشفر فقط بسبب أن الهجومات الخاملة تكون صعبة الاكتشاف ومن ثم تحاول البروتوكولات منع الهجومات الخاملة بدلا من اكتشافها .

كبديل آخر ، فان المهاجم يستطيع محاولة تغيير البروتوكول لفائدته (لصالحه) . فهو يستطيع أن يزعم (Pretend) بأنه شخص آخر ويدخل عبارات جديدة في البروتوكول ويحذف العبارات الموجودة ويحل عبارة محل الأخرى وسترجع (Replay) العبارات القديمة ويقطع قنوات الاتصال و تغيير المعلومات المخزونة في الحاسبة . هذا يطلق عليه الهجومات الفعالة (Active Attacks) ، لأنها تحتاج إلى اعتراض فعال . تعتمد صيغة هذه الهجومات على شبكة الاتصال .

يحاول المهاجمون الخاملون الحصول على معلومات حول الأطراف المشمولة في البروتوكول ، حيث أنهم يجمعون العبارات باختراق عدة أطراف مشتركة متنوعة لمحاولة تحليلها . المهاجمون الفعالين من جهة أخرى يملكون

العديد من الأهداف المتنوعة . قد يكون المهاجم مهتما في الحصـــول على معلومات ،أو التقليل من انجازية النظام أو تحريف المعلومات الموجودة أو الحصول على وصول غير مخول للموارد . تكون الهجومات الفعالة أكثر خطورة على وجه الخصوص في البروتـــوكولات التي لا تثق فيها الأطراف المختلفة ببعضها البعض . قد يكون المهاجم شخص خارجي بالكامل أو قد يكون مستخدم نظام شـــرعي وقد يكون مدير النظام وقد يكون المهاجمون مجموعة من المهاجمين الفعالين يعملون سوية .

انه من الممكن أيضـــا أن المهاجم قد يكون احد المشـــتركين المشـــمولين في البروتوكول و قد يكذب أثناء البروتوكول . هذا النوع من المهاجمين يطلق عليه المخادع (Cheater) . المخادعون الخاملون (Passive Cheater) يتبعون البروتوكول لكنهم يحاولون الحصول على معلومات أكثر من المشتركين اللذين يقصدهم البروتوكول . يستطيع المخادعون الفعالون (Active Cheater) تعطيل البروتوكول في محاولة للغش والفشل .

مثال ٤ -٧ : هجوم البحث الامامي (Forward Search Attack):

افـــرض انـــه لدينـــا فعاليات مصرف يؤدى أعماله الكترونيا (Electronic Bank Transaction) وان هناك حقل بطول ٣٢ ثنائية يستخدم لتسجيل قيمة الحركات (Transactions) والتي تشفر باستخدام طريقة المفتاح العام . هدف هذا البروتوكول البسيط هو توفير الخصوصية (Privacy) لقيمة هذا الحقل ، ولكن هل بإمكان القيام بذلك ؟. يستطيع أي خصم بسهولة الحصول على كل المدخلات الممكنة وهي 2^{32} في هذا الحقل(الذي يحتوي النصوص الواضحة) ويشفر هذه النصوص الواضحة باستخدام دالة تشفير عامة . (تذكر انه بسبب طبيعة تشـــفير المفتاح العام فان هذه الدالة تكون في متناول العدو). وبمقارنة كلاً من 2^{32} من النصوص المشفرة بالنص الموجود أصلا في حقل المتغيرات ، فان العدو يستطيع أن يحدد النص الواضح . في هذا الأسلوب فانه لم يتم اختـــراق (Compromised) دالة لتشفير المفتاح العام (أي لم يكن استخراج النص الواضح كان بسبب كشف الدالة) وإنما تم اختراق الأسلوب الذي استخدمت به الدالة . هناك هجوم يشبه هجوم البحث الأمامي يستخدم بصورة مباشرة إثبات الشـــخصـــية (Authentication) لإغراض ســـيطرة الوصـــول ويســـمى هجوم القاموس (Dictionary Attack) .

ملاحظة ٤-٨ : أسباب فشل البروتوكول (Causes of Protocol Failure) :

قد تفشل البروتوكولات أو الآليات لأسباب عديدة منها:

١: ضعـــف في أولية (Primitive) التشفير الخاص قد يضخم (Amplifie) من قبل البروتوكول أو الآلية ثم يؤدي إلى الفشل .

٢: الافتراض بضـمان (Guarantees) الأمنية بصـورة مبالغا فيها قد يؤدي إلى فشل البروتوكول أو الآلية .

٣: إغفـال بعض القواعـد التي تعود إلى صـــنف من الأوليـات مثـل التشـــفير Encryption) يؤدي إلى الفشل .

ملاحظة ٤-٩ : تصميم البروتوكول (Protocol Design) :

عنـد تصميـم أي بروتوكول تشفيري أو الآلية ، يجب إتباع الخطوتين التاليتين :

١: تعريف أو تحديد كل الافتراضـــات (Assumptions) المطلوبة في تصـــميم البروتوكول أو الآلية .

٢: يجب تحديد التأثير الذي تتعرض له أهداف الأمنية في حالة انتهاك أي افتراض من هذه الافتراضات .

٤-٨ : إنشـــاء المفتـاح ،الإدارة ، التصـــديق (Key Certification, Establishment ,Management):

في هذه الفقرة سـتعطى مقدمة مختصـرة للطرق والوسـائل التي تحقق أغراض التشفير .

تعريف ٤-٦ : إنشاء المفتاح (Key Establishment) :

إنشاء المفتاح هو أي عملية توفر مفتاحا سريا يمكن استخدامه باثنين أو أكثر من المشتركين في عملية تشفير لاحقة .

تعريف ٤-٧ : إدارة المفتاح (Key Management) :

عبارة عن مجموعة من العمليات والآليات التي تدعم إنشـاء المفاتيح وصـيانة علاقات المفاتيح المسـتقبلية (Ongoing) بين الأطراف المشـتركة ، متضـمناً ذلك استبدال المفاتيح القديمة بمفاتيح جديدة كلما كانت هناك ضرورة لذلك .

يمكن تقسيم إنشاء المفتاح إلى اتفاق المفتاح (Key Agreement) ونقل المفتاح (Key Transport) . لقد تم اقتراح العديد من البروتوكولات لغرض توفير إنشاء المفتاح .

إن المبدأ الأساسي عند استخدام تقنيات المفتاح التناظري هو إنشاء زوجين من المفاتيح السرية .هذه الظاهرة تصبح أكثر وضوحاً أو أثباتا عند وجود شبكة اتصال لمجموعة من الأطراف ويرغب أي طرفين منها في أن يتصلا مع بعضهما . فإذا كان هناك شبكة اتصال متكونة من ٦ كينونات و كل زوج من الأطراف يرغب في الاتصال (طرفين) فان هذه الشبكة الصغيرة تحتاج لتبادل سري (أمين) بمقدار زوج من المفاتيح هو كالآتي :

$$15 = \binom{6}{2}$$

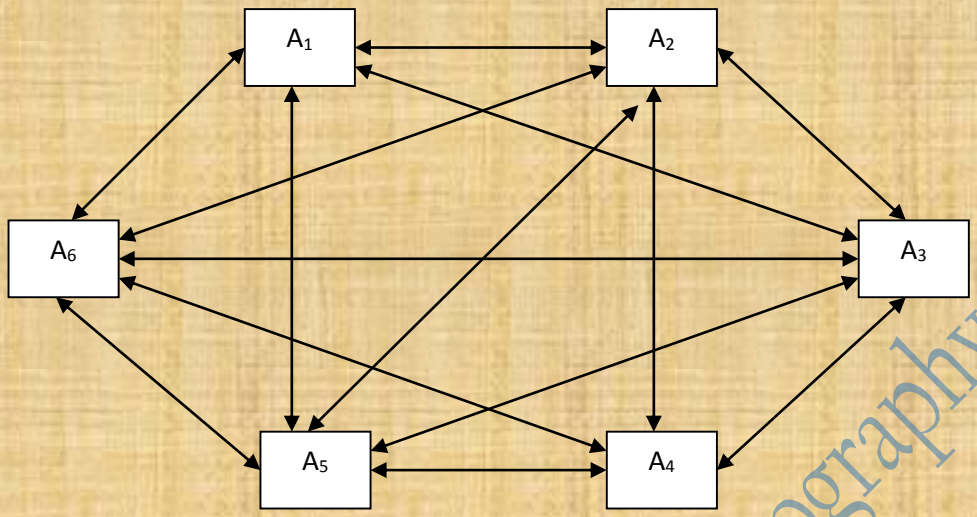
في أي شبكة اتصال بعدد n من الكينونات فان عدد تبادل المفاتيح السرية المطلوب هو :

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

الشبكة الموضحة في الشكل ٤-٤ هي ببساطة عبارة عن دمج لـ ١٥ من الاتصالات بين زوجين من الأطراف كما موضحة في الشكل ٤-

٥ . في الواقع العملي فان شبكات الاتصال تكون كبيرة جداً (أي وجود عدد كبير من الأطراف المشتركة) ،وان مشكلة إدارة المفتاح تعتبر من المسائل المهمة والحاسمة جداً . هناك عدد من الوسائل لمعالجة هذه المشكلة . هنا سيتم مناقشة ابسط طريقتين . احدهما تعتمد على تقنية المفتاح التناظري والأخرى معتمدة على تقنية المفتاح العام .

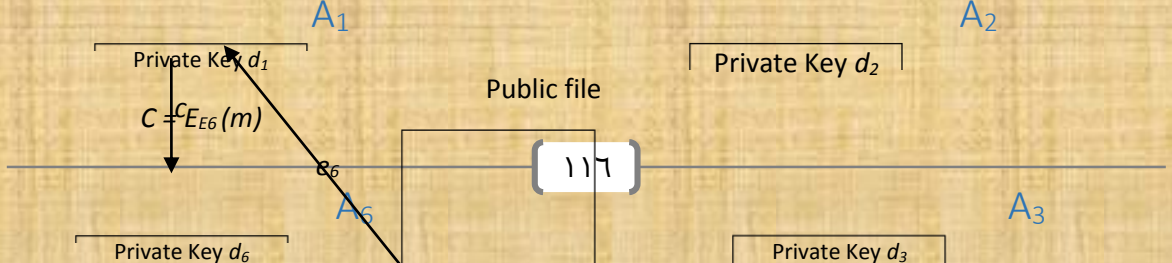
الشكل ٤-٤ : علاقة المفاتيح في شبكة مكونة من ٦ مشتركين



٤-٩ : إدارة المفتاح بواسطة تقنيات المفتاح التناظري:

احـــد الحلول التي تستخدم تقنيات المفتاح التناظري هو ضرورة وجود كينونة (Entity) في شـــبكة الاتصـــال والتي تتصـــف بأنها موضـــع ثقة من قبل جميع الكينونات الأخرى . وكما تم توضـــيحه ســـابقا فان هذه الكينونة أطلق عليها اســـم الحكم أو الطرف الثالث الموثوق (TTP) . تشارك كل كينونة A_i بمفتاح متماثل مميز K_i مع الـــ TTP وقد تم افتراض أن توزيع هذه المفاتيح يتم من خلال قنـــاة اتصـــال ســـرية .إذا رغب أي طرفين (كينونتين) ان يتصـــلا في وقت لاحق ، فان الحكم يولد مفتاح K (يدعي احياناً مفتاح حصـــة الاتصـــال (Session Key) ويرسـله مشـفراً بواسـطة احد المفاتيح الثابتة مثلا بين الكينونات A_1 ، A_5 كما موضح في الشكل ٤-٦ :

شكل ٤-٥ : إدارة المفتاح باستخدام تقنيات المفتاح العام .



شكل ٤-٦ : إدارة المفتاح باستخدام طرف ثالث موثوق (TTP) .

٤-٩-١ : فوائد هذا الأسلوب (الاقتراح) (Advantages of This Approach):

١: من السهولة إضافة أو حذف كينونات من الشبكة .

٢: كل كينونة تحتاج أن تخزن مفتاحا طويل سريا وطويل الفترة – (Long Term Secret Key)

٤-٩-٢ : مساوئ هذا الاقتراح (Disadvantages):

١: تحتاج كل الاتصالات إلى تفاعل ابتدائي مع الحكم .

٢: يجب على الحكم أن يخزن n من المفاتيح السرية الطويلة الفترة .

٣: الـ TTP له القابلية في قراءة كل العبارات .

٤: إذا تم انتهاك الحكم فان جميع الاتصالات تصبح غير سرية .

٤-١٠ : إدارة المفتاح باستخدام تقنيات المفتاح العام :

هناك عدد من الطرق لإدارة المفتاح باستخدام تقنيات المفتاح العام . سوف نصف نموذج بسيط لهذه التقنية . كل كينونة في شبكة الاتصال لها زوج من المفاتيح التشفيرية احدهما عام والآخر خاص ، يخزن المفتاح العام المعرف لكل كينونة في مستودع أو مخزن مركزي (Central Repository) يطلق عليه الملف العام (Public File) ، بمعنى آخر يخزن المفتاح العام مع الرمز التعريفي(Identity) لتلك الكينونة . فإذا رغبت كينونة معينة مثل A_1 أن ترسل عبارة مشفرة إلى A_6 فان A_1 تسترجع المفتاح العام e_6 للكينونة A_6 من ملف المفاتيح العامة ، وتشفر العبارة المطلوبة باستخدام هذا المفتاح e_6، ثم ترسل النص المشفر إلى A_6 . الشكل ٤-٤ يمثل هذا النوع من الشبكة .

٤-١٠-١ : فوائد هذه الطريقة (الاقتراح):

١: لا تحتاج لوجود طرف ثالث موثوق أو الحكم .

٢: ملف المفتاح العام يستطيع البقاء (أو يقيم Reside) مع كل كينونة.

٣: نحتاج فقط n من المفاتيح العامة المطلوب تخزينها لغرض السماح بالاتصالات السرية بين أي زوج من الكينونات . إن الهجوم الوحيد الذي يمكن أن يحدث هو بواسطة عدو خامل (Passive Adversary) .

إن مشكلة إدارة المفاتيح تصبح أكثر صعوبة عندما نأخذ في الحسبان أن يكون العدو فعالا (أي عدو بامكانه أن يغير ملف المفتاح العام الذي يحتوي على المفاتيح العامة) . يستطيع العدو تغيير الملف العام وذلك بإحلال المفتاح العام لكينونة معينة مثلا A_6 بقيمة المفتاح العام للعدو مثلا بقيمة e^x . أي عبارة تشفر إلى الكينونة A_6 باستخدام المفتاح العام المستحصلة من الملف العام يمكن إعادة فتح تشفيرها من قبل العدو فقط . بعد إعادة وقراءة العبارة الأصلية ، فان العدو يستطيع أن يشفر هذه العبارة مستخدما المفتاح العام للكينونة A_6 ويوجه النص المشفر إلى الكينونة A_6 . ستعتقد الكينونة مثلا A_1 أن الكينونة A_6 فقط هي التي تستطيع إعادة فتح الشفرة للنص المشفر C .

لغرض منع أو حجب هذا النوع من الهجوم ، فان على الكينونات استخدام الحكم لغرض إثبات صحة (أو التصديق Certify) المفتاح العام لكل كينونة . يمتلك الحكم خوارزمية توقيع S_T وخوارزمية تحقق (V_T (Verification Algorithm والمفترض أن تكون معروفة من قبل جميع الكينو نات . يقوم الحكم بالتحقق من هوية كل كينونة ويوقع أي عبارة يكون مصدرها معرف (Identifier) والتحقق من المفتاح العام للكينونة موثوق فيه (أو مخول Authentic) . هذا مثال بسيط للشهادة (أو التصديق Certificate) التي تربط هوية الكينونة مع مفتاحها العام . إن فوائد استخدام الحكم هو لغرض المحافظة على تكامل المفتاح العام وتشمل :

١ : تمنع العدو الفعال من انتحال شخصية في شبكة الاتصالات .

٢ : لا يستطيع الحكم مراقبة الاتصالات . تحتاج الكينونات إلى ثقة الحكم فقط لغرض ربط الهويات التعريفية مع المفاتيح العامة بصورة صحيحة .

٣ : يمكن إزالة التفاعل قبل الاتصال مع ملف العام إذا استطاعت الكينونات خزن الشهادة محليا (Locally) .

رغم وجود الحكم فانه مازال هناك بعض القلق او المشاكل ومنها :

١ : إذا تعرض مفتاح التوقيع الحكم إلى الخطر أو الانتهاك ، فان كل الاتصالات ستكون غير أمينة .

٢ : توضع كل الثقة في كينونة واحدة وهذا له خطورته البالغة .

٤-١٠-٢ : الطرف الثالث الموثوق وشهادات المفتاح العام:

إن الثقة الموضوعة في ألحكم تتغير تبعا للطريقة التي تستخدم فيها هذه الثقة ، وعلى هذا الأساس يمكن أن يكون لدينا الأصناف التالية :

تعريف ٤-٨ :

الصنف الأول : يقال عن الحكم انه موثوق غير مشروط (Unconditionally) إذا كان يوفر الثقة في جميع المسائل (الحالات)، كمثال على ذلك ، إن الحكم قد تكون له الإمكانية في الوصول إلى المفاتيح العامة أو الخاصة للمستفيدين ، بالإضافة إلى انه يكون مسؤولا عن علاقة الربط للمفاتيح العامة مع الهويات أو الأشخاص المعرفين (Identifiers) .

تعريف ٤-٩ :

الصنف الثاني : يقال عن الحكم انه موثوق وظيفيا (Functionally) إذا افترضت الكينونة بأنها أمينة (Honest) وعادلة لكن ليس لها إمكانية الوصول إلى المفاتيح الخاصة أو السرية للمستفيدين .

إن الحكم الموثوق وظيفيا يمكن أن يستخدم لغرض التصديق على صحة (Certify) هويات المستفيدين ومحتويات الوثائق (أو يؤكد ويثبت هوية المستفيدين ومحتويات المعلومات) .

٤-١٠-٣ : الشهادات المتحققة بواسطة المفتاح العام (Public –Key Certificates):

إن توزيع المفاتيح العامة هو بصورة عامة أسهل من توزيع المفاتيح التناظرية ، لعدم الحاجة إلى الأمنية . ولكن في كل الأحوال ، فان تكامل (التحقق Authenticity) للمفاتيح العامة تعتبر عملية حرجة . تتكون شهادة المفتاح العام من جزء من البيانات وجزء من التوقيع . يتكون جزء البيانات من اسم الكينونة ، المفتاح العام لتلك الكينونة، وقد تكون هناك معلومات إضافية ذات صلة بالكينونة (مثل عنوان الشبكة ، فترة صحة أو سريان المفعول التدقق (Validity Period) وبعض الصفات الأخرى Attributes) . أما جزء التوقيع فيتكون من توقيع الحكم المطبق على جزء البيانات . من اجل أن تتحقق الكينونة B من التثبت من صحة (Authenticity) المفتاح العام للكينونة A ، فان على B أن تملك نسخة موثوقة (Authentic Copy) لدالة تحقق التوقيع العام للحكمTP . وعادة تزود ثبوتية هذه الدالة B بواسطة وسيلة غير مشفرة ، مثلا بان يحصل B على هذه الدالة من الحكم شخصيا . عند ذلك يستطيع B تنفيذ الخطوات التالية :

١ : يحصل على شهادة المفتاح العام للكينونة A بأي قناة اتصال حتى إن كانت غير أمينة ،أو من قاعدة بيانات مخزن فيها الشهادات أو من A مباشرة ، أو بطريقة أخرى .

٢ : يستخدم دالة تحقق الحكم للتحقق من صحة توقيعه لشهادة الكينونة A .

٣: إذا تحقق التوقيع بصورة صحيحة فانه يقبل المفتاح العام في الشهادة كمفتاح عام موثوق فيه للكينونة A ، عدا ذلك فان المفتاح العام سيكون غير قانوني أو غير صحيح (Invalid) .

قبل عملية تكوين شـــهادة (Certificate) للمفتاح العام إلى الكينونة A فان على الـــحكم أن يأخذ عددا من المقاييس المناسبة لغرض للتثبت من صحة هوية A ومن حقيقة أن المفتاح العام المطلوب التصـــديق عليه هو فعليا تابع إلى A . احد الطرق أن يقابل الحكم شخصيا مع وثيقة مناسبة لإثبات للهوية ليسلمه المفتاح العام ويؤكد انه يعرف المفتاح الخاص المقابل .

الفصل الخامس

استخدامات السلاسل العشوائية في التشفير

٥-١ : توليد السلاسل العشوائية والعشوائية الوهمية (Random And Pseudo-Random Sequence Generation):

لا بد من الإشارة هنا الى أنه يوجد حاليا مولد رقمي عشوائي في أي مترجم تقريبا(Compilers) ، وتقوم دالة معينة باستدعائه . إن السبب في عدم استخدام هذه المولدات هو أن هذه المولدات على الأغلب غير أمينة بما فيها الكفاية لأغراض التشفير ، ومن المحتمل أن لا تكون حتى عشوائية بشكل جيد يراعي حساسية التشفير لكنها ربما تكون مفيدة في التطبيقات البسيطة مثل ألعاب الحواسيب . يكون علم التشفير حساسا جدا إلى خصائص مولدات الأرقام العشوائية .عند استخدام مولد أرقام عشوائي رديء سنلاحظ الحصول على روابط تكهنية ونتائج غريبة .

إن المشكلة الأساسية هي أن مولد الأرقام العشوائية في الحاسوب لا يمكنه إنتاج تسلسل عشوائي حقيقي . لكنه ينتج بما يعرف بالتسلسل العشوائي الوهمي (Pseudo) وهو تسلسل يحقق في ظاهره كل الاختبارات الإحصائية للعشوائية .

٥-١-١ : الأرقام العشـوائية الوهمية والسـلاسـل المتعاقبة Pseudorandom Numbers and Sequences) :

يعتبر عملية توليد الأرقام العشوائية من المبادئ الأساسية المهمة في عدد كبير من آليات التشـفير . مثلا ، المفاتيح المطلوبة لتحويلات التشـفير يجب أن تتولد بأسـلوب يجعل من الصـعب التنبؤ بها من قبل أي عدو . يشـتمل توليد أي مفتاح عشوائي اختيار أرقام عشوائية أو سلسلة متعاقبة من الأرقام الثنائية.

الغالب في تطبيقات التشفير ، فان احد الخطوات التالية يجب تنفيذها :

١ : من مجموعة n من العناصـر (مثلا { 1,2,.....,n}) ، نختار منها احد هذه العناصر عشوائيا .

٢ : مـن مجموعة كل السلاسل المتعاقبة (Sequences) (او سلسلة String) وبطول m من مجموعـة الحروف الابجـديـة A والمكونـة من n من الرموز ، نختار واحد من هذه السلاسل عشوائيا .

٣ : توليد سلسلة متعاقبة عشوائية أو سلاسل عشوائية من الرموز بطول m من مجموعة n من الرموز .

ليس من الواضـح تحديدا ماذا يعني الاختيار عشـوائيا أو التوليد عشـوائيا . اسـتدعاء رقم عشـوائي بدون محتوى يوفر القليل من العقلانية . وهل يمكن القول بان الرقم ٢٣ تم توليده عشـوائيا من خلال توزيع منتظم ؟ إن احتمالية إخراج الرقم ٢٣ هي 1/ 49 .

إذا كان رقم الكرة التي يتم إخراجها من الحاوية يتم تسـجيله وان هذه العملية تكرر ٦ مرات ، فان تسـلسـلا عشـوائيا طوله ٦ أرقام يتم توليده من المجموعة A={1,2,...,49] .

ماهي فرصـة حدوث التسـلسـل 17,45,1,7,23,35 ؟ بما أن كل عنصـر في التسـلسـل له احتمالية حدوث 1/ 49 ، فان احتمالية حدوث التسـلسـل 17,45,1,7,23,35 هو

1/49*1/49*1/49*1/49*1/49*1/49= 1/13841287201

لهذا سـوف يكون لدينا بالضـبط 13841287201 من التسـلسـلات بطول ٦ في مجموعة A . إن عملية إيجاد طرق جيدة لتوليد سلاسل أرقام عشوائية تعتبر عملية صعبة .

مثال ٥-١: مولد السلاسل العشوائية (Random Sequence Generator):

لغرض توليد سلسلة عشوائية من أصفار وواحدات (1,0) ، قد تستخدم عملة نقدية يتم قذفها بالإصبع ويسجل واحدا (١) للوجه وصفر للذيل ، يفترض في القطعة النقدي أن تكون غير متحيزة (Unbiased) والتي نعني بها أن احتمالية الحصول على ١ في قذفه (رمية إصبع) واحدة هي بالضبط (½ هذه الاحتمالية لحدوث الرقم ١) . هذا يعتمد على كيفية عمل أو تصميم القطعة النقدية (Coin) وكيفية تنفيذ عملية القذف للقطعة النقدية . هذه الطريقة لها اهمية قليلة وخاصة في نظام يحتاج فيه توليد السلاسل العشوائية بسرعة وباستمرار وان هذه الطريقة تعتبر غير عملية عدا أنها توفر وسيلة لمثال عن فكرة توليد الأرقام العشوائية .

مثال ٥-٢ : مولد سلسلة الأرقام العشوائية Random Sequence Generator):-

يمكن استخدام قطب ثنائي فوضوي (Noise Diode) لتوليد سلسلة من الأرقام الثنائي العشوائية . تعتبر هذه الحالة مقبولة إذا كانت احتمالية توليد ١ في أي محاولة هي ½ . هذا الافتراض سيكون صحيحا إذا كان توليد السلسلة لا يتم اختيارها من توزيع منتظم وبذلك سوف لاتكون كل السلاسل بطول معين متساوية . (أي أن التوزيع غير منظم لتوليد الأرقام العشوائية) . إن الوسيلة الوحيدة للتعويل (Reliability) على هذا النوع من التوليد هو إجراء اختبارات إحصائية على ناتج (output) كل مصدر عشوائي . إذا كان القطب هو مصدر التوزيع المنتظم لمجموعة كل التسلسلات الثنائية (Binary Sequences) وبطول معين ، فانه سيوفر طريقة مؤثرة لغرض توليد التسلسلات العشوائية .

بما أن معظم المصادر الحقيقية للتسلسلات العشوائية تأتي من وسائل فيزيائية ، فإنها عادة إما تكون مكلفة أو تتميز بالبطئ في التوليد . لغرض معالجة هذه المشاكل ، تم إيجاد عدة طرق لغرض تكوين تسلسلات عشوائية وهمية (Pseudorandom) من سلسلة عشوائية قصيرة تسمى المنشأ (أو البادئة Seed) . غالبا ماتكون خوارزمية التوليد معروفة للجميع ، لكن البادئة (seed) غير معروفة إلا للكينونة التي تكون هذه التسلسلات (البادئة تكون معروفة فقط لهذه الكينونة وليس للجميع) . هناك العديد من هذه الخوارزميات لتوليد تسلسلات ثنائية وأكثرها تكون ملائمة بصورة كاملة لأغراض التشفير .

٥-٢ : أصناف الهجومات (Classes of Attacks):-

لفترة طويلة فان هناك أنواع مختلفة من الهجومات على أوليات او أساسيات التشفير (Primitives) والبروتوكولات ، و قد تم تحديد هذه الهجو مات . إن النقاش في هذه الفقرة محدد بالهجومات على التشفير والبروتوكولات . هناك أنواع أخرى تهاجم أوليات التشفير الأخرى .

تم في الفقرات السابقة توضيح الدور الذي يلعبه العدو المتعدي والعدو الفعال و أن هجمات هؤلاء الأعداء يمكن تصنيفها إلى ما يلي :

١ : الهجوم الخامل (Passive) هو ذلك النوع الذي يستطيع فيه المهاجم أن يراقب فقط قناة الاتصال . يستطيع المهاجم الخامل فقط تهديد وثوقية البيانات (Confidentiality) .

٢ : الهجوم الفعال (Active) هو ذلك النوع الذي فيه يحاول العدو أن يحذف ، يضيف ، أو بطريقة معينة يستطيع أن يغير الإرسال أو الانتقال عبر قناة الاتصال . يهدد المهاجم الفعال تكامل البيانات والتحقق من الوثوقية (Authentication) إضافة إلى وثوقية البيانات . يمكن تقسيم الهجوم الخامل هجومات أكثر تخصصا لغرض استنتاج النص الواضح من النص المشفر .

٥-٢-١ : الهجومات على طرق التشفير Attacks on Encryption (Schemes):-

أي محاولة لتحليل الشفرة يطلق عليها الهجوم (Attack) . أول افتراض اساسي في تحليل الشفرة ، تم من قبل كيرشوف (Dutchman A – kerchoffs) في القرن التاسع عشر ، وهذه الافتراض هو أن الأمنية تكمن بشكل كامل في المفتاح . افترض كيرشوف ان محلل الشفرة يملك التفاصيل الكاملة لخوارزمية التشفير وكيفية استخدامها .

إن الهدف من الهجومات أدناه هو استرداد (Recovery) النص الواضح من النص المشفر ، وربما أكثر من ذلك استخراج (Deduce) مفتاح التشفير . تفترض هذه الهجومات التالية أن محلل الشفرة يملك المعرفة الكاملة لخوارزمية التشفير المستخدمة .

١ : الهجوم على النص المشفر فقط (Ciphertext –Only Attack) :

هو ذلك النوع من الهجومات الذي فيه يحاول محلل الشـــفرة اســـتخراج مفتاح التشـفير او النص الواضـح وذلك فقط بمراقبة النص المشـفر . أي طريقة تشـفير معرضـــة للهجوم لهذا النوع من الهجومات تعتبر غير أمينة بالكامل . يملك محلل الشـفرة النص المشـفر لعدة عبارات تم تشـفيرها باسـتخدام نفس الخوارزمية ، ثم يسعى الى استرجاع النص الواضح لأي عدد ممكن من العبارات ، أو بشكل أفضل استنتاج المفتاح (المفاتيح) المستخدم لتشفير العبارات لغرض فتح شفرة عبارات مشفرة أخرى بنفس المفاتيح .

إذا كان لدينا :

$$C_1 = E_k (P_1) , C_2 = E_k (P_2) , C_i = E_k (P_i)$$

فان محلل الشفرة يستنتج أما :

$$P_1 , P_2 , \ldots , P_i , k$$

أو خوارزمية لاستنتاج P_{i+1} من $C_{i+1} = E_K (P_{i+1})$.

٢ : هجوم على نص واضح معروف (Known –Plaintext Attack) :

في هذا النوع من الهجومات يمتلك العدو كمية من النص الواضـــح وما يقابلها من النص المشـفر .هذا النوع من الهجوم هو مثالي وهامشـي إذ ليس من السـهولة أن يصـل محلل الشـفرة ليس فقط إلى النص المشـفر لعدد من العبارات ، لكن كذلك إلى النص الواضح لهذه العبارة . يكون حينئذ عمـــل محلل الشفرة هـــو استنتاج المفتاح (المفاتيح) المستخدمة لتشفير العبارة أو خوارزمية لفتح شفرة أي عبارة مشفرة بنص المفتاح (المفاتيح) .

إذا أعطي : $C_1 = E_k (P_1) , C_2 = E_k (P_2) , . , P_i, C_i = E_k (P_i)$

فانه يستطيع استنتاج أما المفتاح k أو الخوارزمية لاسترجاع P_{i+1} من $C_{i+1} = E_k (P_{i+1})$.

٣: هجوم النص الواضح المختار (Chosen- Plaintext Attack) :

هو الهجوم الذي يختار فيه العدو نصا واضحا ثم يتوصل إلى ما يقابله من النص المشفر . وفي مرحلة لاحقة ، فان العدو يستخدم أي معلومات مستخلصة لكي يسترجع النص الواضح المقابل لنص مشفر سابقا غير منظور . في هذا الهجوم فان محلل الشفرة لا يملك فقط الوصول إلى النص المشفر وما يقابله من نص واضح لعدة عبارات ، وإنما يملك كذلك اختيارات النص الواضح التي تم تشفيرها. يعتبر هذا الهجوم أكثر قوة من هجوم النص الواضح المعروف ، بسبب أن محلل الشفرة يستطيع اختيار كتل نص واضح محددة لغرض التشفير ، والتي ينتج معلومات أكثر حول المفتاح . إن وظيفة محلل الشفرة (هذا الهجوم) هو استنتاج المفتاح (المفاتيح) المستخدمة في تشفير العبارات أو خوارزمية لفتح شفرة أي عبارات مشفرة بنفس المفتاح (المفاتيح) .

إذا أعطي :

$P_1 , C_1 = E_k (P_1), P_2 , C_2 = E_k (P_2) , ... , P_i , C_i = E_k (P_i)$

حيث أن محلل الشفرة حصل على اختيار Pi , ... , P1 , P2 . يستنتج منه إما المفتاح k أو الخوارزمية للحصول أو تخمين P_{i+1} من $C_{i+1}= E_k (P_{i+1})$.

٤: هجوم النص الواضح المختار القابل للتكييف (Adaptive Chosen- Plaintext) :-

هو عبارة عن هجوم نص واضح مختار يكون فيه اختيار النص الواضح معتمدا على نص مشفر تم استلامه من طلبات سابقة . إذن هذا الهجوم هو حالة خاصة من هجوم النص المختار ، إن محلل الشفرة ليس فقط بامكانه اختيار النص الواضح الذي تم تشفيره ، لكن كذلك يستطيع تحوير اختياره المعتمد على النتائج من التشفير السابق . في هجوم النص الواضح المختار ، فان محلل الشفرة قد يكون فقط قادرا على اختيار كتلة كبيرة واحدة من النص الواضح المطلوب تشفيرها ، بينما في هذا الهجوم فان محلل الشفرة يستطيع اختيار كتلة صغيرة من النص الواضح وبعد ذلك يختار كتلة أخرى معتمدة على نتائج الكتلة الأولى ، وهكذا .

٥: هجوم النص المشفر المختار (Chosen –Ciphertext Attack) :

هو ذلك النوع من الهجومات والذي يستطيع فيه العدو أن يختار النص المشفر ويعطي ما يقابله من النص الواضح . احد الوسائل لتنفيذ هذا الهجوم أن العدو

يتمكن من الوصول إلى المعدات المستخدمة للتشفير (لكن ليس الوصول إلى مفتاح التشـفير ، والذي يدمج بسـرية كجزء لا يتجزأ من المعدات) . إذن الهدف هو عدم التمكن من الوصول إلى مثل هذه المعدات لغرض استنتاج النص الواضح من نص مشـفر أو عدد من النصـوص المشـفرة المختلفة . يطبق هذا الهجوم أساسـا على خوارزميات المفتاح العام . يكون هجوم النص المشـفر المختار في بعض الأحيان مؤثرا على الخوارزميات التناظرية أيضـا . يطلق على كل من هجوم النص الواضـح المختار وهجوم النص المشـفر المختار بأسـم هجوم النص المختار (– Chosen Text Attack) .

٦: هجوم النص المشـفر المختـار القـابـل للتكييف(Adaptive Chosen-Ciphertext Attack) :

هو عبارة عن هجوم نص مختار والذي فيه اختيار النص المشفر قد يعتمد على نص واضح تم استلامه من طلبات سابقة .

٧:هجوم المفتاح المختار (Chosen –Key Attack) :

هذا الهجوم لا يعني أن محلل الشـفرة يسـتطيع اختيار المفتاح لكنه يملك بعض المعرفة حول العلاقة بين مختلف المفاتيح . إن هذا الهجوم غريب وغامض وليس عمليا .

٨ : تحليـل شـفرة بطريقـة الخرطوم المطـاطي (Rubber –Hose Cryptonalysis) : -

في هذه الطريقة فان محلل الشـفرة يهاجم ، او يعذب شـخصـا ما حتى يعطوه المفتاح .

من هذا نستخلص أن هجومات النص الوا ضح المعروف وهجومات النص الوا ضح المختار هما أكثر شيوعا مما هو متوقع .

تملك معظم العبارات بدايات ونهايات مناسـبة والتي تكون معروفة إلى محلل الشـفرة مثلا رموز برنامج المصـدر (Source Code) هي بالأخص معرضـة

للانتهـــاك بسبب الظهور المنظـــم لكلمـــات المفتاح , struct , else , return
: #define . الرموز التشـفيرية المشـفرة لها نفس المشـاكل : loop
structures , functions ، الخ . تم استخدام كل من هجومات النص الواضح المعروف (وحتى هجومات النص الواضح المختار) بنجاح ضد الألمـــان واليابان في الحرب العالمية الثانية . كتب ديفيـــد كاهان (David kahn) أمثلة تاريخية لهذه الأنواع من الهجومـات .ولكن في كـل الأحوال لا يســـتطيع محللو الشـــفرة الوصول إلى الخوارزمية ، كما فعلت الولايات المتحدة في كسر الرموز الدبلوماسية لليابان خلال الحرب العالمية الثانية .

معظم هذه الهجومـات التي ذكرنـاهـا تطبق كـذلـك على طرق التواقيع الرقميـة وشفرات ثبوت صحة العبارة حيث يقوم المهاجم يقوم تزوير العبارات .

٥-٢-٢ : الهجومات على البروتوكولات (Attacks on Protocols) :-

ندرج أدناه قائمة من الهجومات المؤثرة حتى على البروتوكولات التي ثبت أنها توفر الخدمات المطلوبة بكفاءة :

١ : هجوم المفتاح المعروف (Know-Key) :

في هذا الهجوم يحصـــل العدو على بعض المفاتيح المســـتخدمة ســـابقا ثم يستخدمها لتحديد المفاتيح الجديدة .

٢ : الإعادة (Replay) :

في هذا الهجوم فان العدو يســجل حصــص (Sessions) اتصــال ثم يعيد كامل الحصة ، أو جزء منها ، في وقت لاحق من الزمن .

٣ : انتحال الشخصية (Impersonation) :

في هذا الهجوم يتظاهر العدو أو يفترض هوية احد الأطراف الشـــرعيين في الشبكة .

٤ : القاموس (Dictionary) :

هذا الهجوم في العادة يكون ضـد كلمات المرور . من المعروف أن كلمة المرور تخزن في ملف حاسـوب بشـكل صـورة (Image) لدالة هاشـية بدون مفتاـــح (Unkeyed Has Function) عند دخـول المستفيـد (Log On) إلى الحاسوب وإدخاله كلمة مرور ، فان كلمة المرور تعامل كدالة هاشـــية والصـــورة المتكونة تقارن مع القيمة المخزونة . يســـتطيع العدو أن يأخذ قائمة من كلمات المرور المحتملة ويعاملها بدالة hash لكل المدخلات في القائمة ، ويقارنها مع قائمة كلمات المرور المشـفـــــرة على أمل منه أن يجد مطابقات(matches) لكلمات المرور هذه .

٥: البحث المتقدم أو الأمامي (Forward Search) :

هذا الهجوم هو مشـــابه لمحتوى هجوم القاموس ويســـتخدم لغرض فتح شـــفرة العبارات .

٦: الهجوم المتداخل (Interleaving Attack):

هذا الهجوم يتضـــمن بعض انتحال الشـــخصـــية في بروتوكول ثبوت صـــحة الشخصية .

٣-٥ : نماذج تخمين (تقييم) الأمنية (Models of Evaluating Security) :-

إن أمنية أساسيات التشفير والبروتوكولات يمكن أن تقيم بعدد من النماذج والمقاييس أهمها :

١ : الأمنية غير المشروطة (Unconditional Security) :

إذا كان العدو يملك مواردا حسابية غير محدودة ، والسؤال هنا هو توجد أو لا توجد معلومات كافية متوفرة لغرض التعرض (Defeat) للنظام التشفيري . إذا كانت الإجابة لا فأننا نقول أن النظام التشفيري يملك أمنية غير مشروطة ويطلق عليها الأمنية التامة (Perfect Security) . إذن الأمنية التامة تعني أن الشكوك (Uncertainty) حول النص الواضح بعد مراقبة النص المشفر تظل كما هي وبمعنى آخر أن مراقبة النص المشفر لا تزود العدو بمعلومات مهما قلت عن النص الواضح .

هناك شرط ضروري لان تكون طرق التشفير التناظرية ذات أمنية غير مشروطة وهو أن يكون المفتاح على الأقل بطول العبارة . شفرة الوسادة (one-time pad) هي مثال لخوارزمية تشفير ذات أمنية غير مشروطة . على العموم ، فان كل طرق التشفير لا توفر أمنية كاملة ، وان كل حرف مشفر تتم مراقبته يقلل الشك (uncertainty) النظري في النص الواضح ومفتاح التشفير ولو بنسبة غير معتبرة . إن طرق تشفير المفتاح العام لايمكن أن تكون ذات أمنية غير مشروطة إذا انه من أي نص مشفر c ، يمكن استرجاع النص الواضح p وذلك بتشفير كل النصوص الواضحة الممكنة حتى يمكن الحصول على c . إذن إذا أعطي العدو المال الكافي والوقت الكافي يمكنه انتهاك أي مفتاح عام .

هناك أنواع أخرى من الأمنية ندرجها أدناه :

٢ : أمنية التعقيد النظري (Complexity –Theoretic Security)

٣ : الأمنية المبرهنة (Provable Security)

٤ : الأمنية الحسابية (Computational Security)

٥-٣-١ : وجهة نظر عن الأمنية الحسابية (Perspective for Computational Security):-

لغرض تقييم(Evaluate) سرية طرق التشفير فانه يجب الأخذ بنظر الاعتبار عدد من الكميات .

٥-٣-٢ : تعريف (عامل الأداء work factor Wd):-

عامل الأداء W_d هو الحد الأدنى من عدد العمليات الحسابية الأولية (Elementary Operations) أو دورات الوقت (Clock Cycles) المطلوبة لحساب المفتاح الخاص d بمعرفة المفتاح العام k (بإعطاء المفتاح العام k) أو بتحديد المفتاح السري k في أنظمة التشفير التناظري . (بمعنى آخر W_d هو اصغر كمية مطلوبة لحساب المفتاح الخاص d بمعرفة المفتاح العام k أما في حالة أنظمة التشفير التناظرية يستخدم الـ W_d لحساب المفتاح السري k) . إذا أخذنا في الاعتبار العمل المطلوب في حالة هجوم النص المشفر فقط والمتوفر فيه n من النصوص المشفرة ، فان عامل الأداء يشار له بـ (n) W_d .

إذا كان W_d يساوي t من السنين وكانت t كبيرة بما فيه الكفاية نقول أن طريقة التشفير ستكون أمينة لكل الأغراض العملية . غلى الوقت الحاضر لا يوجد نظام للمفتاح العام ثبت انه أمين من الناحية العلمية أي آن عامل الغداء W_d اكبر من الوقت الكافي لغرض الأمنية .

٥-٣-٣ : تعريف (عامل الأداء التاريخي (W_d Historical Work Factor) :

عامل الأداء التاريخي هو الحد الأدنى من الوقت المطلوب لحساب المفتاح العام e باستخدام خوارزميات معروفة بجودتها في فترة زمنية محددة . عامل الأداء التاريخي W_d يتغير مع الزمن الذي فيه تتطور الخوارزميات والتقنيات . تقابل w_d تقابل الأمنية الحسابية ، بينما w_d تقابل مستوى الأمنية الحقيقي .

٥-٣-٤ : ماهو حجم المفتاح المطلوب ؟

يجب أن تكون مساحة المفتاح (Key Space) كبيرة بما فيه الكفاية التي تجعل عملية البحث المكثف غير ممكنة التحقيق بصورة تامة . السؤال المهم هو كم

مقـــدار الكبر المطلوب ؟ . لكي نحصل على بعض الانطباعات ، فان الجـــدول ٥-١ يوضح الكثير من العناصر مع قيمها المقابلة .

بعض القوى (Powers) يشـــار لها بالتعيين مقدما (Prefix) . كمثال ، فان الحواسيب الحديثة عالية السرعة تقاس معدلاتها (Rated) بـــ (teraflops) حيث أن teraflop يعادل 10^{12} عملية لكل ثانية .

جدول ٥-١ : بعض الأرقام مقارنة بقيمها النسبية .

Reference	Magnitude
Seconds in a year	$\approx 3 \times 10^7$
Age of our solar system (years)	$\approx 6 \times 10^9$
Seconds since creation of solar system	$\approx 2 \times 10^{17}$
Clock cycles per year, 50MHz computer	$\approx 1.6 \times 10^{15}$
Binary strings of length 64	$2^{64} \approx 1.8 \times 10^{19}$
Binary strings of length 128	$2^{128} \approx 3.4 \times 10^{38}$
Binary strings of length 256	$2^{256} \approx 1.2 \times 10^{77}$
Number of 75-digit prime numbers	

Electrons in the universe	**$\approx 5.2 \times 10^{72}$** **$\approx 8.37 \times 10^{77}$**

الجدول ٥-٢ يزودنا بقائمة الـ(Prefixes) الشائعة الاستعمال .

٥-٣-٥ : طول المفتاح التناظري (Symmetric Key Length):

امنية أي نظام تشفيري متناظر هو عبارة عن دالة من شيئين : قوة الخوارزمية وطول المفتاح .
افرض أن قوة الخوارزمية هي تامة . هذا يعني استحالة الوصول إلى المفتاح في الواقع العملي ، تعني بالتامة ، لا توجد طريقة أفضل لكسر أي نظام تشفيري ذي قوة خوارزمية تامة من محاولة كل المفاتيح الممكنة في هجوم القوة الوحشية (Brute –Force Attack) .

جدول ٥-٢ : بعض الـ Prefixes المستخدمة لمختلف القوى من ١٠ .

Prefix	Symbol	magnitude
Exa	E	10^{18}
Peta	P	10^{15}
Tera	T	10^{12}
Giga	G	10^{9}
Mega	M	10^{6}
Kilo	K	10^{3}
Hecto	H	10^{2}
Deca	Da	10

Prefix	Symbol	magnitude
Deci	D	10^{-1}
Centi	C	10^{-2}
Milli	M	10^{-3}
Micro	U	10^{-6}
Nano	N	10^{-9}
Pico	P	10^{-12}
Femto	F	10^{-15}
Atto	A	10^{-18}

في هذا الهجوم فان محلل الشفرة يحتاج إلى كمية صغيرة من النص المشفر وما يقابلها من النص الواضح ، إذن هجوم القوة الوحشية هو عبارة عن هجوم نص واضح معروف . بالنسبة لشفرة الكتلة ، فان محلل الشفرة يحتاج كتلة من النص المشفر وما يقابلها من النص الواضح : عادة فان الكتلة ٦٤ ثنائية . إن الحصول على هذا النص الواضح والنص المشفر هو أسهل مما يتخيل الكثيرون . يستطيع محلل الشفرة أن يحصل على نسخة من عبارة النص الواضح ببعض الوسائل ثم

يعترض النص المشـــفر المقابل في الإرســـال . قد يعلم محلل الشـــفرة صـــيغة (Format) النص المشفر : كمثـــال على ذلك هل هو ملف wordperfect ، أو ملف UNIX ، أو قيـــد قياسي في ملـــف قاعدة البيانات ،وكل هذه الصيغ لها بعض البيانات المعرفة سابقا . إن محلل الشفرة لا يحتاج أكثر من نص واضح يستهل به هذا الهجوم .

حساب تعقيد هجوم القوة الوحشية تعتبر عملية سهلة . إذا كان المفتاح بطول ٨ بت ، فانه يوجد $٢^{٨}$ ، أو ٢٥٦ من المفاتيح الممكنة . لذلك ، فانه سيأخذ ٢٥٦ محاولة لإيجاد المفتاح الصحيح ، مع فرصة بنسبة ٥٠% لإيجاد المفتاح بعد نصف المحاولات . إذا كان المفتاح بطول ٥٦ بت ، فانه يوجد $٢^{٥٦}$ مفتاح ممكن أو بافتراض أن حاسوب فائق (Super Computer) يستطيع محاولة كل مليون مفتاح في الثانية ، فإنها تأخذ ٢٢٨٥ ســـنة لإيجاد المفتاح الصـــحيح . إذا كان المفتاح بطول ٦٤ بت ، فإنها تستغرق حوالي ٠٠٠ ، ٥٨٥ سنة لإيجاد المفاتيح الصـــحيحة من بين $٢^{٦٤}$ المفاتيح الممكنة . إذا كان المفتاح بطول ١٢٨ بت ، فإنها ستأخذ $١٠^{٢٥}$ سنة . إن عمر الكون هو $١٠^{١٠}$ ، لذلك فان $١٠^{٢٥}$ زمن طـــويل جدا . أما المفتاح بطول ٢٠٤٨ بت بمحاولات مليون مليون لكل ثانية لحســـابات تعمل بالتوازي سوف تحتاج إلى $١٠^{٥٩٧}$ سنة لغرض إيجاد المفتاح .

قبل أن يكـــون هنـــاك اندفـــاع لاختراع نظام تشفير بمفتاح بطول ٨ كيلوبايت ، يجب أن نتذكر الجانب الآخر لمسألة القوة : يجب أن تكون الخوارزمية أمينة بحيث لاتكون هناك وسيلة لكسرها إلا بهجوم القوة الوحشية . إن أنظمة التشفير التي تبدو تامة (Perfect) غالبا ماتكون ضـــعيفة جدا جدا .أنظمة التشـــفير القوية ، بزوج من التغييرات الأساسية ، يمكن أن تصبح ضعيفة .

٦ : تقديرات الوقت والكلفة لهجوم القوة الوحشية (Time and Cost Estimates for Brute-Force Attack):

يجب ان نتذكر ان هجوم القوة الوحشية نموذج هجوم نص واضح معروف . تعتمد امنية الخوارزمية على ان يكون المفتاح كبيرا بما فيه الكفاية ، لكن ماهو هذا الطول ؟

هناك عاملان يحددان سرعة هجوم القوة الوحشية هما : عدد المفاتيح المطلوبة للاختبار وســـرعة كل اختبار . معظم الخوارزميات التناظرية تقبل أي نموذج بت لطول ثابت لاستخدامه كمفتاح . طـــول المفتاح لطريقة دي أي أس (ديس DES) ٥٦ ثنائية ومن ثم تملك $٢^{٥٦}$ من المفاتيح الممكنة . بعض الخوارزميات تســـتخدم مفتاح بطول ٦٤ ثنائية ، أي لديها $٢^{٦٤}$ من المفاتيح الممكنة ، بعض الخوارزميات الأخرى تســـتخدم مفتاح بطول ١٢٨ ثنائية . الســـرعة التي يســـتتغرقها كل مفتاح للاختبار هي أيضـــا عامل هام ، لكن اقل أهمية من العوامل الســـابقة . لغرض الســـهولة ســـوف نفترض أن كل الخوارزميات يمكن اختبارها بنفس الفترات الزمنية

. يمكن أن يتم اختيار احد الخوارزميات مرتين أو ثلاث أو حتى عشر مرات وتكون أسرع من الأخرى .

معظم النقاشات والمنازعات حول كفاءة هجوم القوة الوحشية تركزت على خوارزمية دي أي أس (DES). في العام ١٠٧٧ ، اقترح كل من ديف وهيلمان ماكنة دي أس (DES) خاصة الأغراض . الماكنة مصممة من مليون رقيقة (Chip) ، كل رقيقة قادرة على اختبار مليون مفتاح لكل ثانية . مثل هذه الماكنة تستطيع اختبار $٢^{٥٦}$ مفتاح في ٢٠ ساعة . إذا صممت هذه الماكنة لمهاجمة خوارزمية تستخدم مفتاح بطول ٦٤ بت ، فإنها تستطيع اختبار كل $٢^{٦٤}$ في ٢١٤ يوم .

يمكن استخدام المعالجات المتوازية مع هجوم القوة الوحشية . كل معالج يستطيع اختبار مجموعة جزئية من مساحة المفتاح لا يتطلب أن تتصل هذه المعالجات مع بعضها ، الاتصال الوحيد المطلوب على الإطلاق هو عبارة واحدة تشير إلى نجاح العمل . لا توجد متطلبات لذاكرة مشتركة . انه من السهولة تصميم ماكنة تتكون من مليون من المعالجات المتوازية ، كل معالج يعمل بصورة مستقلة عن المعالجات الأخرى .

لقد تم بناء ماكنة من قبل بحوث التشفير (Cryptography Research, Advanced Wireless Technologies) ، والـ EFF قد صممت بحثا للمفتاح سريع للدي أي اس (DES) . تستخدم الدي أي اس مفتاح تشفير بطول ٥٦ بت ، بمعنى انه يوجد (72,057,594,037,927,936) من المفاتيح المحتملة . تم تطوير هذا المشروع لبحث مفتاح دي أي أس خصيصا لتصميم كيان مادي وبرمجي ليقوم بالبحث عن ٩٠ بليون مفتاح في كل ثانية ، محددا المفتاح وقد ربح المكافأة المقدمة للتحدي والبالغة 10,000 دولار . تصميم الكيان المادي والبرمجي ومحاكاة الرقائق (chip simulators) تم تطويرها من قبل كوفر (Paul Kocher) بمساعدة من جيف (Joshua Jaffe) و باحثين آخرين في معهد بحوث التشفير .

حديثا فقد صمم (Michael Winer) ماكنة معينة ، حيث صمم لهذا الغرض شرائح خاصة ولوحات خاصة (board) . الجدول ٥-٣ يعطي أرقام معينة لمختلف أطوال المفاتيح .