

INFORMATION SECURITY



أمن المعلومات

مقدمة

Damascus University

في عصر المعلومات الذي يشهد نمواً سريعاً في المعلومات والمعارف، حيث تتضاعف كمية المعلومات كل خمس سنوات، وتتضاعف قوة الحاسب الآلي كل سنتين، وفي هذا العصر نشهد ثورة في المعلومات الذي يقوم فيها الحاسب الآلي بالدور الأول، حيث أصبح العلم قرية صغيرة تربطها شبكات المعلومات.

في هذا العصر اعتمدت المؤسسات في تسيير أعمالها على تقنية المعلومات التي أثبتت أنها تسهم في إنجاز الأعمال بسرعة عالية وبدقة متناهية، وحيث أن البيانات والمعلومات تخزن في قواعد بيانات ومعلومات مربوطة مع حاسبات المؤسسة من خلال شبكة الاتصال، وغالباً ما تكون متاحة عبر شبكة الانترنت تسهياً لإجراءات العمل واختصاراً للوقت.

ولهذا تطورت طرق معالجة البيانات للتوافق مع بيئة الحاسبات من طرق يدوية إلى طرق آلية منتجة نظم سير العمل الإلكترونية لتصل إلى مفهوم الحكومة الإلكترونية، وبذلك نجد أن تقنية المعلومات قد ساهمت في تسهيل الأعمال الطبية والهندسية والصناعية والمصرفية وأنظمة المكاتب وأعمال المؤسسات التعليمية بل إنها أصبحت سلاحاً في المؤسسات العسكرية يستخدم في الأعمال الحربية.



يخزن الحاسوب كثيراً من المعلومات الحساسة عن الأفراد والمؤسسات، ويجري تبادل أجزاء من هذه المعلومات بين المستخدمين من خلال الشبكات أو وسائط الاتصال المتنوعة، فكان لابد من حماية هذه المعلومات، بمنع الوصول إليها لمن لا يملك الحق في ذلك، وكذلك المحافظة على سريتها أثناء نقلها عبر وسائط الاتصال المختلفة.

أماكن الخطر في النظام المعلوماتي تكمن بـ: المكونات المادية، المكونات البرمجية، الشبكات أو وسائط الاتصال، البيانات، الإجراءات، العنصر البشري، موقع منظومة التجهيزات وتوابعها.



Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects

إن استخدام مصطلح أمن المعلومات ليس جديداً، فهو موجود قبل ظهور وسائل تكنولوجيا المعلومات والاتصالات، إلا أنه أصبح شائعاً ومتداولاً بكثرة بعد ولادة تلك الوسائل واستخدامها في معالجة ونقل و تخزين البيانات وتداولها.

- اعتبر أمن المعلومات والمحافظة عليها من أن تكشف لغير المخولين بالاطلاع عليها واحد من أقدم وأهم المجالات سواءً على مستوى الدول أو المؤسسات أو الأفراد.

- ومع انطلاق أجهزة الحاسب الآلي وتكنولوجيا المعلومات والاتصالات، فقد أصبحت المعلومات تنتقل بين الأجهزة بكميات هائلة، وأصبح من السهل الوصول للمعلومات من أي مكان، وقد تطور هذا المجال حتى بات من أهم مجالات علوم الحاسب.

- يشمل حماية المعلومات والأجهزة المادية والأنظمة من فقد البيانات أو تعديلها أو الدخول غير المشروع عليها أو حجب خدماتها.

أمية القرن الحادي والعشرين هي أمية المعلومات.

من الأمور التي تعتبر في غاية الأهمية هو التصنيف الأمني للمعلومات، فلا بد من تحديد القيمة الفعلية للمعلومات، والتعريف بدرجات سريتها وحساسيتها، ومن ثم تعريف إجراءات الحماية المناسبة لكل معلومة بحسب أهميتها، فليس كل البيانات بنفس القدر من الأهمية، ولهذا يجب التفاضل أيضاً بينها في درجة الحماية.

أصبحت سرية المعلومات وأمنها موضوعاً يورق الإدارة العليا لأي مؤسسة في عصر المعلوماتية إذ أصبح من المحتم على هذه المؤسسة توفير حماية ورقابة النظام المعلوماتي، وتختلف أساليب الحماية باختلاف التهديدات ومصادرها.

• وجود حرب مستمرة بين مدرستين تدور رحاها حول أمن المعلومات، والتحقق من هوية الأطراف المتصلة، حيث تعمل المدرسة الأولى على تطوير آليات أمن المعلومات والتوثيق والتحقق من هوية أطراف الاتصال، بينما تمثل المدرسة الثانية وجهة نظر الأطراف غير المشروعة والمتطفلة، والتي ترغب في كسر واختراق آليات التشفير والتحقق والتوثيق.

Computers Security في مرحلة الستينيات ظهر مفهوم أمن الحواسيب والذي يعني حماية الحواسيب وقواعد المعطيات.

Data Security في مرحلة السبعينات ظهر مفهوم أمن المعطيات أو البيانات حيث تم استخدام كلمات السر البسيطة للسيطرة على الوصول إلى البيانات، إضافة إلى وضع إجراءات الحماية لمكان الحواسيب من الكوارث، واعتماد خطط لخرن نسخ إضافية من البيانات والبرمجيات بعيداً عن مكان الحاسوب.

في مرحلة الثمانينات والتسعينات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم بالمشاركة في قواعد البيانات كل هذا أدى إلى الانتقال من مفهوم أمن البيانات إلى مفهوم أمن المعلومات **Information Security**، وأصبح من الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة وثوقيتها.

وكانت شركة **IBM** الأمريكية أول من وضع تعريف لأمن المعلومات، وكانت تركز على حماية البيانات من التزوير والتدمير أو الدخول غير المشروع لها.

والسؤال الذي يطرح نفسه هو ماذا

سيكون بعد أمن المعلومات؟

كل التوقعات تشير إلى ظهور

مصطلح أمن المعرفة

Knowledge Security

وذلك لانتشار أنظمة الذكاء

الاصطناعي وازدياد معدلات نقل

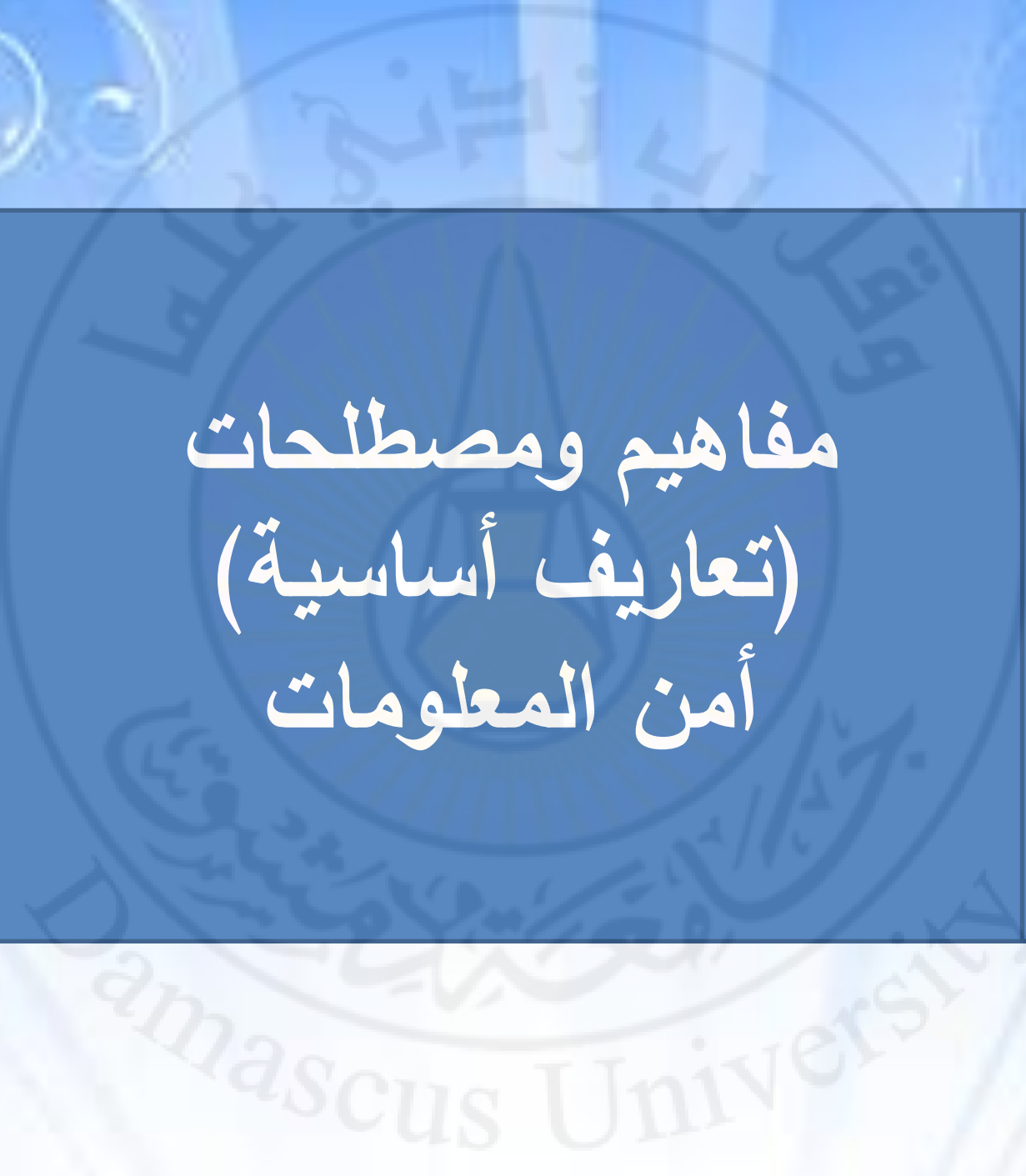
البيانات والتفاعل بين المنظومات

والشبكات وصغر حجم أجهزة

الحاسب الشخصي، ... إلخ.

وربما نيجةً للتطورات المتسارعة
في مجال تكنولوجيا المعلومات
والاتصالات وما يطرأ من تغيرات
في علم الحاسب وفروعه وخاصةً
الذكاء الصناعي سنسمع عن
مصطلح جديد آخر يعرف بـ:
أمن الحكمة

Wisdom Security

The background of the slide features a large, faint watermark of the Damascus University logo. The logo is circular, containing a five-pointed star in the center, surrounded by Arabic calligraphy. The words "Damascus University" are written in English at the bottom of the logo.

مفاهيم ومصطلحات (تعريف أساسية) أمن المعلومات

البيانات: هي رموز لغوية أو رياضية أو معنوية متفق عليها رسمياً لتمثيل الأفراد أو الأشياء أو الحوادث أو المصطلحات.

أو هي حقائق تم تسجيلها بشأن أحداث معينة تمت أو ستتم مستقبلاً وهذه الحقائق قد تكون مستقلة وغير مرتبطة ببعضها البعض وغير محدودة العدد.

المعلومات: هي ما تحصل عليه من تمثيل أو تأطير أو تنظيم أو تحرير البيانات بطريقة تزيد مستوى المعرفة للأشخاص الذين يحصلون عليها.

أو هي بيانات قد تم معالجتها بشكل أعطى لها معنى بالنسبة لمستقبلها أو استخدامها وأضاف إليها قيمة حقيقة بالنسبة لعمليات صنع القرارات الحالية والمستقبلية ويمكن التعبير عن العلاقة بينهما كالعلاقة بين المادة الخام والمنتج النهائي، أي أن مدخلات الجهاز تسمى بيانات أما مخرجات الجهاز بعد المعالجة والتخزين تسمى معلومات.

الحِمْيَةُ لُغَةً: حَمَى الشَّيْءَ يَحْمِيهِ حَمِيًّا وَحِمَايَةً، مَنَعَهُ، وَقَدْ حَمَاهُ حَمِيًّا وَحَمِيَّةً وَحِمَايَةً وَحَمَوَةً. وَحَمَى الْمَرِيضَ مَا يَضُرُّهُ: مَنَعَهُ إِيَّاهُ، فَالْحِمَايَةُ لُغَةً الْمَنْعُ.

الحماية اصطلاحاً (Protection): بالنسبة لحماية طريق السفر يعني الأفعال والاحتياطات التي تؤدي لضمان مرور ووصول المسافرين بأمان، وبالنسبة لحماية المنتجين في بلد ما، فهي مجموعة النظم والإجراءات التي تحمي المنتجين المحليين من المنافسين الأجانب.

الحماية الأمنية للمعلومات: هي العملية التي يتم فيها حماية الأصول المعلوماتية الرقمية وهدفها هو حماية الخصوصية وصيانة التكامل وضمان الاستمرارية، وبهذه الأهداف تتم الحماية من جميع التهديدات والثغرات الأمنية للوصول إلى تحقيق أهداف المؤسسة، ويُقصد بالتهديد الدخول غير المخول ويُقصد بالثغرات الأمنية نقاط الضعف الناتجة عن سوء إعداد البرمجيات ومكونات الأجهزة وضعف التصميم أو إهمال المستفيد وسوء استخدامه.

• مصطلح الأمن (Security)
يعني ضمناً

الحماية (Protection).

وفيمايلي مجموعة من التعاريف لأمن المعلومات والتي أطلقت من قبل مختصي وفني وخبراء هذا المجال:

• أمن المعلومات: هي مجموعة من السياسات والإجراءات الفنية المتخذة من أجل منع الاشخاص غير المخولين من الدخول الى الشبكات وتغيير معلوماتها، أو سرقتها أو تدمير نظم المعلومات.

الأمن المعلوماتي: هو ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزنة في أجهزة الحاسب إضافة إلى الأجهزة الملحقة وشبكات الاتصال والتصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك التي ترمي إلى نقل الخزين المعلوماتي لهذه القواعد أو تغييره أو تخريبه.

أمن المعلومات: "حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المؤسسة نفسها والأفراد العاملين فيها وأجهزة الحاسوب المستخدمة فيها ووسائل المعلومات التي تحتوي على بيانات المنظمة، ويتم ذلك عن طريق إتباع إجراءات ووسائل حماية عدة تضمن في النهاية سلامة المعلومات".

كما عرفه آخر بأنه:

"علم يدعو لوضع إجراءات كافية لضمان أمن المعلومات المركزية وقواعد البيانات الموزعة"
أما أحدهم، فقد عرفه من عدة زوايا:

أكاديمياً: هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

تقنياً: هي الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

قانونياً: هي محل الدراسات والتدابير اللازمة لضمان سرية وسلامة محتوى المعلومات وتوفرها ومكافحة أنشطة الاعتداء عليها أو استغلالها في ارتكاب جرائم المعلوماتية.

وعليه، فأمن المعلومات هو مجموعة من الوسائل والأدوات والإجراءات المطلوب توفرها لحماية وتأمين كافة الموارد أو المصادر المستخدمة في جميع مراحل تواجد المعلومة (تخزين، نقل، معالجة).

أو هو العلم الذي يهتم بدراسة النظريات والاستراتيجيات والقوانين التي تهتم بتوفير الحماية للمعلومات من المخاطر التي تواجهها والعمل على تطبيق الوسائل والإجراءات اللازمة لتوفير تلك الحماية وسن القوانين الصارمة لمنع حدوث المخاطر مستقبلاً ومعاقبة مرتكبيها.

اختراق المعلومات Hacking: وهو الوصول غير المسموح به لنظام المعلومات بهدف تبديل البيانات والمعلومات أو سرقتها أو تدميرها.

المخترقون: هم أشخاص يتمتعون بموهبة وبراعة وقدرة عالية على كتابة وتصميم البرامج وفهم عميق لكيفية عمل الحاسوب الآلي وإدارة نظامه مما يسهل عليهم اختراق أنظمتها وتغييرها أو سرقة معلوماتها أو تدميرها.

المتسللون والمهاجمون Hackers and Attackers: هما مصطلحان مترابطان للأفراد الذين يمتلكون المهارات اللازمة للوصول إلى نظام الحاسب من خلال وسائل غير مصرح بها، أو غير موافق عليها. التسلل إلى النظام هو إشارة إلى مهارة فنية خلاقة تدريجياً ارتبطت مع تطفل الأنظمة المؤذي وغير الأخلاقي. المهاجم: هو مصطلح يعبر دائماً عن تسلل للنظام مؤذٍ.

مصطلح Cracker: يعود للأفراد الذين يكسرون تشفير الكود، ويزيلوا الحماية عن نسخ البرمجيات، أو متخصصين في كسر الأنظمة. cracker أحياناً يستخدم لوصف hacker or attacker.

القبعات البيضاء White Hats:

أشخاص فائقوا الذكاء ويسيطرون بشكل كامل على الحاسب ويجعلون البرامج تقوم بأشياء أبعد بكثير مما صممت له أصلاً، وهم الذين يكتشفون العيوب الأمنية في التطبيقات ونظم التشغيل ويفضحوها لتمكين المصنعين قبل أن تصبح مشكلة واسعة الانتشار. هم يفعلوا ذلك من خلال أساس احترافي، ويعملون في المنظمات الأمنية أو لدى مصنعي الأنظمة.

القبعات السوداء Black Hats:

هم أشخاص يسخرون ذكائهم بطريقة شريرة ويهتمون بدراسة الحاسب والبرمجة ليتمكنوا من سرقة المعلومات أو كسر أنظمة الحماية أو يقومون بأعمال تخريبية أخرى، وهم الذين يكتشفون العيوب الأمنية ونقاط الضعف لمكاسب مالية أو بهدف الإيذاء، ومن الممكن أن لا يعمل القبعات السوداء على كسر الأنظمة مباشرة مثل المهاجمين، إلا أنهم قد يقوموا بنشر الثغرات الأمنية مما يسبب خسارة مادية كبيرة ودمار للمنظمة.

القبعات الرمادية: هم من يكون في الأصل من ذوي القبعات البيضاء ثم في أوقات معينة ولأي سبب كان يتحولون إلى ذوي القبعات السوداء.

الأدوات التي يستخدمها الهاكرز

- الخداع الالكتروني Spoofing: والمتمثل بإرسال بريد الكتروني "ايميل" مزيف، أو التمثيل بأنه ايميل لشخص آخر، وتوجيه شبكة الانترنت لإرسال معلومات إلى جهات أخرى غير المخصصة.
- برامج التجسس Sniffer: هي برامج حاسوبية خاصة بالتجسس ومراقبة المعلومات المرسلة عبر الشبكة دون علم المستثمر، وغالباً ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتبديل برمجيات أو ملفات مجانية من شبكة الانترنت.
- انكار الخدمة: يقوم بإرسال كم هائل من الرسائل الالكترونية إلى حاسب معين عبر الشبكة، والذي لا يستطيع التعامل معها وبالتالي تعطيل النظام.

الهندسة الاجتماعية Social Engineering: وتعني تحضير مستخدم الحاسوب على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع المعلومات دون إثارة أي شبهة أو انتباه.

يعتمد هذا الأسلوب على عدة أدوات أو تقنيات بغية تحقيق أهدافها نذكر منها:

١ - التوأمة الشريرة: أي إدعاء جهة معينة بأنها جهة موثوقة فيها من قبل المستخدم وتطلب منه استخدام ملف مرفق يكون ضاراً به.

٢ - سرقة الهوية: أي إدعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر.

٣ - التصيد: ويقصد منها وصول رسالة مزيفة من جهة (غالباً مالية ومعروفة) لطلب معلومات أو التحقق منها وقد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة.

البرمجيات الضارة Malware: وهي مجموعة البرامج المتخصصة بتسهيل التسلل إلى النظام المعلوماتي أو الشبكة الحاسوبية بهدف التدمير، وما أن يتم تثبيت هذه البرمجيات فمن الصعوبة جداً إزالتها.

ومن الأدوات أو التقنيات التي تستخدمها بغية تحقيق أهدافها نذكر منها:

آ- الفيروس: هو برنامج تنفيذي يهدف الى تحقيق اهداف محددة او إحداث خلل في نظام الحاسب.



ب- الدودة (worm): هي برامج حاسوبية مستقلة تقوم بنسخ نفسها من حاسب إلى آخر عبر الشبكة، وسميت بذلك لأنها قادرة على نسخ نفسها والانتشار سريعاً عبر وسائل الاتصال كالبريد الإلكتروني.



ج- حصان طروادة (Trojan Horse): ((سمي بذلك لأنه يذكر بالقصة الشهيرة لحصان طروادة، حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها))، وبالتالي فهذا الفايروس يكون مرفقاً مع برنامج دون علم المستخدم، ويهدف لسرقة البيانات، وكشف كلمات المرور والحسابات المصرفية.

أو هو برنامج في ظاهرة يبدو أنه سينفذ شيء معين، ولكن عند البدء يقوم بعمل شيء آخر مضر بنظم المعلومات.



التهديد (Threat): يشير إلى أي حدث معادي مقصود أو أي حدث غير مقصود يمكن أن يتسبب في أضرار لنظام المعلومات.

أثر التهديد (Impact or Exposure): ويعني الخسائر المادية التي تحدث نتيجة حصول التهديد.

هجوم السيطرة الكاملة:
في هذا النوع يقوم القرصان بالسيطرة الكاملة على جهاز الضحية والتحكم في جميع ملفاته كما لو كانت في جهازه هو، ويمكن للقرصان مراقبة الضحية بصورة كاملة، ويتم الهجوم بعد أن يضع القرصان ملف صغير على جهاز الضحية (عن طريق البريد الإلكتروني، أو عن طريق استغلال نقاط الضعف في أنظمة التشغيل، أو أي وسيلة أخرى.

هجوم التضليل:

وفيه يقوم القرصان بانتحال شخصية موقع عام، كما يمكن للقرصان أن ينتحل شخصية مستخدم موثوق به للحصول على معلومات غير مصرّحة له.

الوصول المباشر لكوابل التوصيل:

يقوم المهاجم بالوصول المباشر لأسلاك التوصيل والتجسس على المعلومات المارة، ولكنه هجوم صعب ويتطلب عتاد خاص.

التشفير هو عملية الحفاظ على سرية المعلومات (ثابتة أو متحركة) باستخدام خوارزميات لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة.

فك التشفير: تحويل النص المشفر إلى النص الأصلي الصريح والواضح والمفهوم.

المقاطعة Interruption: وتعني تأخير أو رفض خدمة ليصبح النظام المعلوماتي خارج الاستخدام.

مثال: شخص مهمته فقط التأثير على وصول المعطيات أو تبادلها سواءً بتأخير وصولها أو منع وصولها أصلاً عن سوء أو حسن نية مثل قطع أحد وصلات المبدلة Switch.

الاعتراض Interception: قراءة معلومات بطريقة غير شرعية وأن الأشخاص الذين يصلون لهذه المعلومات غير مخولين بذلك، أي الوصول إلى البيانات بطريقة غير قانونية.

التعديل Modification: تعديل المعلومات بطريقة غير شرعية مثل شخص يعمل على ملف مخزن على الحاسب دون علم صاحب الملف وهي ممكنة حتى عن طريق استغلال المكونات المادية حيث من المعروف أن النبضة الكهرومغناطسية كفيلة بتغيير البت من الصفر إلى الواحد.

انتحال الشخصية Masquerade: وتعني إدخال أو تخزين معلومات إلى النظام المعلوماتي أو الشبكة الحاسوبية لتظهر وكأنها قادمة من مستخدم مخول، كمعرفة كلمة المرور لشخص ما والدخول بها والعمل على تغيير العنوان (IP) الخاص بالحاسب.

النكران Repudiation: ادعاء عدم القيام بإرسال أي شيء، كأن ترسل رسالة إلى زميلك ثم تقول لاحقاً بأنك لم ترسل هذه الرسالة.

تحليل المرور Traffic Analysis: مراقبة الاتصال الشبكي بهدف استخلاص معلومات عن الاتصال بغض النظر عن المحتوى مثل معرفة مكان وعنوان أطراف الاتصال وحجمه وتكراره.

إعادة الإرسال Replay: إعادة إرسال رسالة تم اعتراضها سابقاً على الشبكة ومن ثم إرسالها لاحقاً لإنتاج تأثير غير مخول.

الجريمة الالكترونية

الجرائم المعلوماتية: هي تعبير شامل يشير إلى جريمة تتعلق باستعمال احدى وسائل تقنية المعلومات لغرض خداع الآخرين وتضليلهم أو من أجل تحقيق هدف معين لجهة معينة.

- هي أي فعل يخالف الأنظمة والقوانين ويستخدم لارتكابه أجهزة الحاسب الآلي وشبكات وتقنيات الحاسب الآلي المختلفة، ويتضمن ذلك اختراق الأنظمة ومواقع الانترنت، صناعة البرامج الخبيثة ونشرها، تسريب المعلومات السرية للمنظمات أو الأشخاص، التهديدات الالكترونية تحميل ونشر الملفات المحتوية على ممنوعات كالملفات الإباحية والإرهابية والكثير غيرها.

- وتختلف العقوبات في الجرائم الالكترونية بحسب القوانين في كل دولة، ومن المهم لكل مستخدم في أي بلد الاطلاع على نظام الجرائم المعلوماتية الخاص بهذا البلد وقراءته وفهمه لكي لا يقع في فخ الجرائم المعلوماتية سواء بقصد أو بدون قصد.

العناصر الضرورية لشن الهجمات الالكترونية على المعلومات

١ - وجود الدافع (مال، انتقام، تخريب، ... إلخ).

٢ - وجود طريقة لتنفيذ الهجوم، حيث أن المهاجم لن يتمكن من شن هجوم ناجح ما لم يكن لديه تصور وخطة واضحة.

٣ - وجود الثغرات ونقاط الضعف في تصميم أو إعدادات البرامج والأنظمة.

عناصر أمن المعلومات

Damascus University

منذ أكثر من عشرين عاماً مضت، وأمن المعلومات قد حددت بالسرية وتكامل سلامة البيانات والتوافر (المعروفة باسم الثلاث CIA: CIA: Confidentiality Integrity Availability)، ويشار إليها بالتبادل في الأدبيات على أنها، سمات أمان، خصائص وأهداف أمنية، جوانب أساسية، معايير معلومات، خصائص معلومات هامة، واللبنات الأساسية والمبادئ الأساسية لأمن المعلومات.

في عام ٢٠٠٢، اقترح دون باركر نموذجاً بديلاً للثلاث التقليدي (CIA)، حيث يتكون نموذج باركر من ستة عناصر من أمن المعلومات، وهذه العناصر هي السرية، الحيابة، السلامة، الأصالة، التوفر والأداة، وإن سداسي باركر هو موضع نقاش بين المتخصصين في مجال الأمن، وحتى تاريخه لم يعتمد بشكل معياري.

(integrity)

تعني أن تكون المعلومة صحيحة عند ادخالها، وأثناء نقلها بين الأجهزة في الشبكة وذلك باستخدام مجموعة من الأساليب والأنظمة.

يجب توفر ثلاث عناصر للمحافظة على أمن البيانات والمعلومات في البرنامج أو النظام الذي نتعامل معه وهي كالتالي:

(confidentiality)

وهي منع الوصول إلى المعلومات الا من خلال الأشخاص المصرح لهم فقط، سواء عند تخزينها، أو عند نقلها عبر وسائل الاتصال، وكذلك تحديد صلاحية التعديل والحذف والاضافة.

(Availability)

تعني بقاء المعلومة متوفرة للمستخدم وإمكانية الوصول اليها، وعدم تعطل ذلك نتيجة لخلل في أنظمة ادارة قواعد المعلومات والبيانات أو وسائل الاتصال.



السرية هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالإطلاع عليها أو الكشف عنها. على سبيل المثال، استعمال بطاقة الائتمان في المعاملات التجارية على شبكة يتطلب إدخال رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة. يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الوصول إلى أماكن تخزين أو ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها، أما إذا كان الطرف غير المصرح له قد حصل على رقم البطاقة بأي شكل من الأشكال فإن ذلك يعد انتهاكا لمبدأ السرية في حفظ وتخزين البيانات.

خرق السرية يتخذ أشكالاً عديدة. تجسس شخص ما على شاشة الحاسوب لسرقة كلمات سر الدخول ،أو رؤية بيانات سرية بدون علم مالكيها، يمكن أن يكون خرقاً للسرية. إذا كان الحاسوب المحمول يحتوي على معلومات حساسة عن موظفي الشركة، فإن سرقة أو بيعه يمكن أن يسفر عن انتهاك لمبدأ السرية. إعطاء معلومات سرية عبر اتصال هاتفي هو انتهاك لمبدأ السرية إذا كان طالب الاتصال غير مخول بأن يحصل على المعلومات.

السرية أمر ضروري (لكنها غير كافية) للحفاظ على خصوصية الناس الذين تحتوي الأنظمة معلوماتهم الشخصية.

التكامل (السلامة): في مجال أمن المعلومات، التكامل (السلامة) يعني الحفاظ على البيانات من التغيير أو التعديل من الأشخاص غير المخولين بالوصول إليها. عندما يقوم شخص، بقصد أو بغير قصد، بحذف أو انتهاك سلامة ملفات البيانات الهامة أو الإضرار بها، وهو غير مخول بذلك، يعد هذا انتهاكاً لسلامة البيانات. وعندما يصيب فيروس حاسوباً، ويقوم بتعديل بياناته أو يتلفها يعد هذا انتهاكاً لسلامة البيانات، وكذلك عندما يكون الموظف (غير المخول) قادراً على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم (غير مصرح له) بتخريب موقع على شبكة الإنترنت ، كل ذلك يعد انتهاكاً لسلامة البيانات. و تعني سلامة البيانات كذلك، أن تكون التغيرات في البيانات مطردة، فعندما يقوم عميل البنك بسحب أو إيداع، ينبغي أن ينعكس ذلك على رصيده في البنك.

إن الإخلال بسلامة البيانات ليس بالضرورة نتيجة عمل تخريبي، فمثلاً، الانقطاع في النظام قد ينشئ عنه تغيرات غير مقصودة أو لا تحفظ تغيرات قد تمت فعلاً.

استمرارية توفر المعلومات أو الخدمة **AVAILABILITY**: التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وإن مستخدم المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها.

توفر البيانات: يهدف أي نظام للمعلومات لخدمة غرضه، وأن تكون المعلومات متوفرة عند الحاجة إليها، وهذا يعني أن تعمل عناصر النظام الآتية بشكل صحيح ومستمر:

- الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات.
- الضوابط الأمنية المستخدمة لحماية النظام.
- قنوات الاتصال المستخدمة للوصول.
- نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات.
- منع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، اونظام الترقية والتحديث.
- ضمان منع هجمات الحرمان من الخدمة.

مثال على السرية:

مستند لا يحق لأي موظف الاطلاع عليه إلا المدير.

مثال على سلامة المحتوى:

تعميم لا يحق لأي شخص التعديل عليه.

مثال على استمرارية توفر المحتوى:

امكانية الدخول على صفحة النظام الخاصة
بالموظفين.

ويمكن تحديد الهدف من الهجمات على أنظمة أمن المعلومات بالتالي:

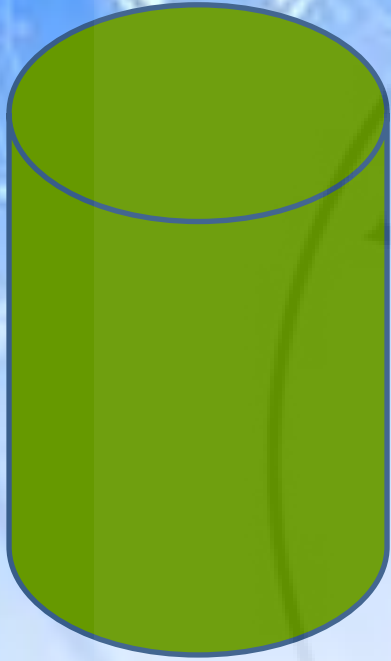
- عمل نسخة عن معلومات هذه الأنظمة.

- تغيير في محتوياتها.

- سرقة أو قرصنة المعلومات.

- التجسس عليها (مراقبة وسائط الاتصال، أو التحكم بكاميرات المراقبة)

- تدميرها.



ويمكن تحديد خطوات تحقيق الهجمات على أنظمة أمن المعلومات بالتالي:

- ١ - استكشاف المعلومات (الاستطلاع): كمعرفة نوع العتاد الصلب المستخدم وأرقام إصدارات البرمجيات المختلفة ومعلومات شخصية، ... إلخ.
- ٢ - اختراق الدفاعات.
- ٣ - تعديل الإعدادات الأمنية وذلك للسماح بإعادة النفاذ إلى النظام المعلوماتي مرة أخرى بسهولة أكبر.
- ٤ - تعميم التجربة على بقية الأنظمة الأخرى.
- ٥ - شل الشبكات والنظام المعلوماتي (حذف أو تعديل ملفات النظام، حقن برمجيات خبيثة، ... إلخ).

ويمكن تحديد خطوات تحقيق الدفاع عن أنظمة أمن المعلومات بالتالي:

- ١- التقسيم الطبقي Layering: من خلال وضع عدة طبقات أمنية لحماية النظام المعلوماتي (كلمة مرور، بطاقة، تشفير، موارد، ... إلخ).
- ٢- الحد Limiting: إن الحد من إمكانية النفاذ يقلل التهديدات المحيطة بها على سبيل المثال لا الحصر.
- ٣- التنوع Diversity: يرتبط هذا العامل مع فكرة التقسيم الطبقي ويمكن تحقيقه عن طريق استخدام الجدار الناري على سبيل المثال.
- ٤- الغموض Obscurity: عن طريق إخفاء بعض المعلومات المتعلقة بالنظام المعلوماتي.
- ٥- البساطة Simplicity: يجب أن تكون الأنظمة الأمنية بسيطة وسهلة الاستخدام والفهم من قبل الأشخاص الذين يتعاملون معها.

أخطار أمن المعلومات

Damascus University

بصفة عامة تواجه نظم المعلومات الإلكترونية الأخطار والتهديدات الأمنية الآتية:

التهديد الأول: الأخطار البيئية: ويتمثل بـ:

الكوارث الطبيعية مثل الحرائق، والفيضانات والزلازل، والبراكين والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي، إضافةً إلى المشاكل القائمة في تعطل أنظمة التكييف والتبريد، وتؤدي هذه التهديدات إلى تعطل عمل هذه التجهيزات وتوقفها لفترات طويلة نسبياً لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات ونظم تشغيلها، فالكوارث التي لا يمكن التنبؤ بها تستطيع تدمير نظام المعلومات بشكل كامل، وتتسبب في فشل المنظمة، ويمكن أن يؤثر حدوث هذه الكوارث في العديد من المنظمات في آن واحد، وكذلك حالات الفشل التقني تعتبر من أهم مهددات أمن المعلومات، وفي حال عدم الاستعداد الجيد لمواجهة هذه المهددات ربما تكون العواقب وخيمة.

التهديد الثاني: الأخطاء البشرية:

الأخطاء البشرية واردة من كل المستخدمين محترفين كانوا أو مبتدئين، ويمكن أن تتسبب الأخطاء البشرية بفقد البيانات أو عدم تكامليتها، وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات مما يتسبب بفشل وظائف هذه المعدات أو خلال عمليات البرمجة أو الاختبار أو تجميع البيانات أو أثناء إدخالها إلى النظام أو في عمليات تحديد الصلاحيات للمستخدمين وكذلك انهيار نظام التشغيل، وانقطاع وتقلب التيار الكهربائي، وأخطاء إرسال البيانات التي لم يتم الكشف عنها وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة نظم المعلومات.

التصرفات غير المقصودة مثل الحذف والأخطاء غير المقصودة، والتي تُعرض نظم المعلومات لمخاطر جسيمة وخسائر فادحة، فقد قدرت جمعية أمن نظم المعلومات المحاسبية أو ما يعرف بـ:

(The Information Systems Security Association)

أن ٦٥% من المشاكل ذات العلاقة بأمن هذه النظم سببها أخطاء العنصر البشري، وأن التصرفات غير العمدية للعنصر البشري تنتج عن الإهمال، والإخفاق في إتباع الإجراءات المرسومة، وضعف تدريب الأفراد والإشراف عليهم، فالمستخدمين للنظام غالباً ما يخسرون البيانات أو يضعونها في الأماكن غير الصحيحة ويمحون أو يبدلون الملفات والبيانات والبرامج بشكل غير مقصود، كما أن مشغلي الحاسوب والمستخدمين يمكن أن يقوموا بإدخال خاطئ أو إدخال مدخلات غير صحيحة، واستخدام نسخة خاطئة من البرنامج والتعامل مع الملفات غير الصحيحة للبيانات أو وضعها في الأماكن غير الصحيحة، أما محلي الأنظمة والمبرمجين فيمكن أن يقوموا بعمل أخطاء منطقية وتطوير أنظمة لا تفي باحتياجات المنظمة وغير قادرة على التعامل مع المهام المستهدفة لها، أو ممكن اختراقها بسهولة من قبل المهاجمين.

هناك أسباب عديدة قد تدفع الإنسان لشن هجوم ضد أنظمة معلومات الجهة التي يعمل فيها، ومن أهم هذه الأسباب مايلي:

- ١ - عدم الرضا.
- ٢ - اثبات الشخص مهارته الفنية وقدراته على تنفيذ هجوم إلكتروني.
- ٣ - تحقيق مكاسب مالية.
- ٤ - حجم التهديد.

التهديد الثالث: الجرائم المحوسبة:

التصرفات العمدية أو المقصودة والتي يشار إليها عادة كجرائم للحاسوب، وأغلب أنواع جرائم الحاسوب هو ما يعرف بالخداع أو الحيلة (Fraud) وفيه تكون النية موجهة نحو سرقة شيء ذو قيمة، ومن الأمثلة على جرائم الحاسوب: الكشف غير المصرح به عن البيانات، والعرض غير الصحيح للمعلومات، وتخصيص الموجودات لأغراض غير مصرح بها. ويمكن أن يتخذ هذا النوع من التهديد أيضاً شكل التخريب (Sabotage) وتكون النية فيه تحطيم أو إلحاق الأذى بالنظام أو بعض مكوناته.

التهديد الرابع: مخاطر إلكترونية:

- انتحال شخصية.
- التنصت.
- الفيروسات.
- الاعتماد على وحدة معالجة البيانات GPU بدلاً من وحدة المعالجة المركزية CPU.
- إلخ.

العوامل التي تساعد على اختراق أنظمة المعلومات

- مشاكل الأجهزة والمعدات المادية: مثل الأخطاء الناتجة عن الإعدادات غير الصحيحة الخاصة بالأجهزة والأعطال المتكررة.
- مشاكل برمجية: خطأ في البرمجيات، خطأ في تنزيل البرامج وتغييرات غير مسموح بها.
- الكوارث: مثل الحرائق، الفيضانات، مشاكل انقطاع التيار الكهربائي.
- استخدام الشبكات والحواسيب خارج سيطرة المؤسسة: مثل استخدام الشبكة من قبل شركات أخرى عالمية.

مصادر الاخلال بأمن المعلومات

- الاعتداء على حق الوصول.
- دخول شخص غير مصرح له إلى نظام المعلومات باستخدام كلمة سر مستخدم مشروع.
- خداع بروتوكولات النقل عبر الانترنت وذلك عن طريق اعتراض البيانات المنقولة عبر الشبكة باستخدام برامج خاصة كبرامج الاختراق والقرصنة ليتم تعديلها بما يتوافق مع غرض الاعتداء.
- عدم الاقرار بالقيام بالتصرف كأن ينكر الشخص إعطاء كلمة السر لشخص آخر غير مصرح له باستخدام النظام المعلوماتي.
- إرسال كميات كبيرة من الرسائل الإلكترونية إلى بريد الموقع المستهدف لإرباك النظام المعلوماتي وإضعاف برامج حماية المعلومات.

تهديدات أمن المعلومات

- إن من أساسيات المحافظة على أمن المعلومات هو فهم ومعرفة المهددات التي تواجهها، فبدون الفهم العميق للمخاطر، فإنه من الصعب الدفاع والحماية عنها.

لماذا تتزايد تهديدات أمن نظم المعلومات الإلكترونية؟

- ١ - زيادة عدد أنظمة المعلومات في المنشأة، وبالشكل الذي أدى إلى إتاحة المعلومات لعدد كبير من العاملين دون تحديد أولويات للحصول عليها.
- ٢ - صعوبة الرقابة على شبكات الحاسوب الموزعة (Distributed computer Networks)، مقارنة مع الحواسيب الكبيرة المركزية (Centralized mainframe).
- ٣ - تُمكّن الشبكات التي تغطي مساحة واسعة العملاء والمجهزين من الدخول إلى أنظمة وبيانات بعضهم البعض، الأمر الذي جعل من الثقة محل قلق واهتمام المؤسسات المستخدمة لهذه النظم.

تصنف التهديدات التي يتعرض لها أمن النظم المعلوماتي وفقاً للعديد من الأسس، إذ يمكن تصنيفها وفقاً لـ:

١ - حسب المصدر (Source): إلى تهديدات داخلية وتهديدات خارجية.

٢ - حسب المسبب فيها (Perpetrator): إلى تهديدات ناتجة عن العنصر البشري وتهديدات ناتجة عن العنصر غير البشري.

٣ - حسب العمدية أو القصدية (Intention): إلى تهديدات ناتجة عن تصرفات متعمدة وتهديدات ناتجة عن تصرفات غير متعمدة.

٤ - حسب علاقتها بمراحل النظام إلى تهديدات المدخلات (Input)، وتهديدات المعالجة (Processing)، وتهديدات المخرجات (Out put).

إضافةً إلى الأخطار
السابقة يوجد
مجموعة من
المهددات التي تؤثر
على أمن المعلومات،
وفيما يلي أهمها:



١ - انتحال الشخصية:

في هذه الحالة يتم استخدام هوية المستخدم (اسم المستخدم وكلمة المرور) للحصول على معلومات سرية أو أمنية أو مبالغ نقدية.

يتم ذلك بعدة طرق منها :-

- ١ - تخمين اسم المستخدم وكلمة المرور.
- ٢ - إرسال رسائل للمستهدفين يطلب منهم تحديث بياناتهم.
- ٣ - استخدام أجهزة أو برامج تقوم بتسجيل كل ما يتم النقر عليه.
- ٤ - الاتصال مباشرة على المستهدفين.

٢ - البرامج الخبيثة Malware: Malicious Software

هو مصطلح يشمل كل البرامج التي لها طابع العدائية والتي يمكن أن تسبب أضراراً للنظام أو للمستخدم، وتشتمل على أنواع مختلفة تعتمد على بعضها البعض للوصول لأهدافها التخريبية ومن أشهرها:

الفيروسات Viruses	الديدان Worms
برامج الفدية Ransom Ware	برامج التجسس Spyware
برامج الإعلانات المزعجة Adware	برامج الاحتيال او البلاغ الكاذب Hoax
برامج شبكة بوت نت Bot Net	أحصنة طروادة Trojan Horse
القنابل المنطقية Logic Bomb	الأبواب الخلفية (المستترة) Backdoor

البرمجيات الخبيثة التي تنتشر (فيروسات دودة).
البرمجيات الخبيثة التي تختفي (أحصنة طروادة، الجذور الخفية، القنابل المنطقية، الأبواب الخفية).
البرمجيات الخبيثة ذات التوجه الربحي (بوتنيت، التجسس، الاعلانات، مسجلات المفاتيح).

البرامج الخبيثة: هي أي برنامج يكون كل مهامه أو أحدها عمل خبيث من تجسس أو تخريب أو استنزاف للموارد (الوقت، المعالج، الذاكرة، وحدة التخزين، سعة النقل الشبكي، ...إلخ)، وكذلك تنفيذ المهام التالية:

- يغير المعطيات أو تدميرها.
- يسرق المعطيات.
- يسمح بنفاذ غير شرعي إلى المعطيات.
- يستثمر النظم ويلحق الأذى بها.
- يقوم بأفعال لا يريد المستخدم القيام بها.

طرق الإصابة بالبرامج الخبيثة

- ١ - وسائط التخزين.
- ٢ - البريد الالكتروني.
- ٣ - عن طريق المرفقات.
- ٤ - عن طريق قراءة الرسالة.
- ٥ - رابط في الرسالة.
- ٦ - تصفح مواقع مشبوهة.
- ٧ - المنافذ المفتوحة.
- ٨ - تحميل برامج من الانترنت.

دوافع تطوير البرامج الخبيثة:

١. إثبات الشخص لنفسه أو لغيره قدرته على تطوير هذه البرامج.
٢. الانتقام من الأفراد أو الشركات أو الدول.
٣. الابتزاز.
٤. التسويق التجاري.
٥. التجسس الصريح وسرقة المعلومات على مختلف المستويات (أفراد، شركات، دول).



هي برامج تعمل تلقائياً ويتم تصميمها لإلحاق الضرر بأجهزة الحاسب الآلي كتدمير البيانات وحذفها أو تشفيرها أو إتلاف مكونات النظام، ولها القدرة على الانتشار حيث تنتقل الفيروسات من ملف إلى آخر داخل الجهاز عن طريق وحدات التخزين المحمولة أو عن طريق شبكات الحاسب والبريد الإلكتروني.

أو هي عبارة عن برامج قام بتطويرها وكتابتها مبرمجين محترفين بهدف تنفيذ أوامر معينة في جهاز الضحية كالإلحاق الضرر بالحاسب وما يحتويه من بيانات أو سرقة معلومات هامة مثل رقم كود بطاقة الصراف على سبيل المثال لا الحصر.

والفيروس برنامج يلتصق ببرنامج آخر (مضيف) قادر على التكاثر أي يستطيع أن يخلق نسخاً من ذاته ليست بالضرورة متطابقة.
أو هي عبارة عن برامج حاسوبية والتي ترتبط مع برامج حاسوبية أخرى، أو ملفات بيانات من أجل تنفيذها بطريقة خاطئة.

من الأعمال التي يقوم بها الفيروس نذكر:

- ١ - التسبب بالتوقف المتكرر للحاسوب.
- ٢ - حذف الملفات من القرص الصلب.
- ٣ - صنع نسخة منه تفيد باستهلاك المساحات الفارغة في القرص الصلب.
- ٤ - إيقاف الإعدادات الأمنية للحاسوب.
- ٥ - إعادة تهيئة سواقة القرص الصلب.



والبنية العامة للفيروس موضحة بالشكل التالي:

M

Infect

Task

Carrier

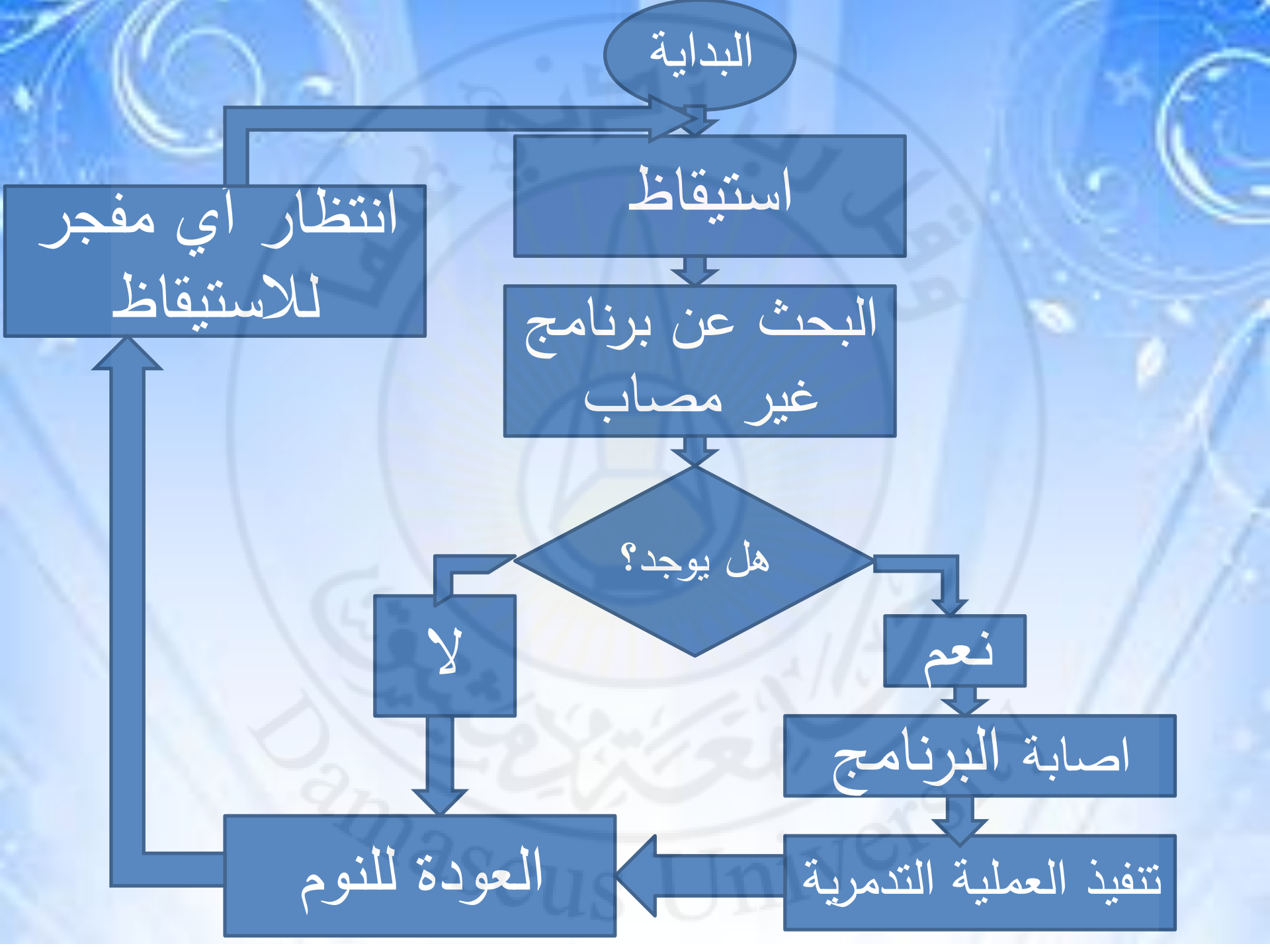
M: Mark Byte
علامة الإصابة.

برنامج نقل
الإصابة إلى
برامج أخرى

برنامج الوظيفة
التدميرية

برنامج حامل
للفيروس

يوضح الشكل التالي المخطط النهجي لعمل الفيروسات:



مصادر الفيروسات

الرسائل الإلكترونية المجهولة.

- صفحات الإنترنت المشبوهة.

- نسخ البرامج المقلدة.

- استخدام برامج غير موثقة.

- تبادل وسائل التخزين دون عمل فحص مسبق لها، مثل الأقراص والذواكر المتنقلة.

- إرسال الملفات داخل الشبكة المحلية.

خواص الفيروسات

- ١- التضاعف: تتم عملية تضاعف الفيروس عند التحاق الفيروس بأحد الملفات، وهنا تتم عملية زيادة عدد العمليات التي تتم إلى ملايين العمليات، مما يسبب البطء في العمل، أو توقف الحاسب عن العمل.
- ٢- التخفي: لابد للفيروس من التخفي حتى لا ينكشف، ويصبح غير فعال، ولكي يتخفي فإنه يقوم بعدة أساليب منها على سبيل المثال، صغر حجم الفيروس لكي يتسنى له الاختباء بنجاح في الذاكرة أو ملف آخر.
- ٣- إلحاق الأذى: قد يتراوح الأذى الذي يسببه الفيروس بالاكْتفاء بإصدار صوت موسيقي، أو مسح جميع المعلومات المخزنة لديك، ومن الأمثلة الأخرى في إلحاق الأذى: إلغاء بعض ملفات النظام، إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت مثلاً، أو إلغاء البرنامج المكتوب على BIOS.

أشكال الفيروسات

Damascus University

أولاً) فيروسات تقليدية Classic Virus: وهي برامج هدفها تخريب النظام وإحداث أعطال وأخطاء فيه بشكل رئيسي، وهناك نوع جديد من الفيروسات يستخدم أسلوب الإنحقان بالملفات، حيث يضيف جزء من كوده البرمجي إلى الملف، فيصيبه ويصبح جزء منه، وبشكل عام تضع الفيروسات قيوداً وتعديلات في الريجستري، فمثلاً تمنع المستخدم من استخدام إدارة المهام وإظهار الملفات المخفية، وملفات النظام بطئ بسبب استهلاكها لموارد النظام، وغيرها الكثير.

و تقسم الفيروسات من هذا النوع إلى:

١) فيروسات ملف File Viruses: وتتبع واحداً على الأقل من هذه الأساليب لإصابة النظام:

أ) فيروسات منحقته تصيب الملفات التنفيذية: وفي هذه الحالة عندما يكتشفه مضاد فيروسات يعطيك خيار التصحيح بأحد الأشكال التالية:

(Disinfect, Cure, Repair, ...etc)، حيث يختلف حسب نوع مضاد الفيروسات الذي تستخدمه، ومن أشهر هذه الفيروسات فيروس سالتى الشهير Sality، وفيروس Mabezat والتي تعتبر للأسف أكثر الفيروسات من هذا النوع.

(ب) فيروسات تكرر الملفات الموجودة على الجهاز Duplicate FilesK، حيث تمتلئ ذاكرة الجهاز بسبب تكرار الملفات (تخيل لديك ملفات و بيانات شركة، و تملئ ٧٥% من ذاكرة الجهاز، فإذا بدأ الفيروس بنسخ كل ملف مرة واحدة تكون النتيجة الجهاز لا يملك ذاكرة كافية)، ولهذا تسمى هذه الفيروسات بفيروسات الشركات مثل فيروس Temp.exe.

(ت) وهذه الفيروسات تعمل على نسخ نفسها في مسارات مشهورة بالجهاز، %systemdrive%, SystemRoot%, %userprofile%,...etc%

(ث) فيروسات تستعمل ميزات ملفات النظام: ولها أشكال عديدة:

(١) Boot sector viruses: وهي فيروسات تصيب الملفات المسؤولة عن إقلاع الجهاز والنظام، فتضيف نفسها إلى ملفات الإقلاع، وقد تغير مسار تلك الملفات، ولا تصيب إلا الأقراص المرنة. هذه الفيروسات انتشرت في التسعينيات من القرن الماضي، ولكن مع تقدم معالجات ٣٢ بت، وتناقص استخدام الأقراص المرنة تضاعل عددها مع أنه من الناحية التقنية يمكن إنشاء هكذا فيروسات على الـ Cd والفلاشات.

٢) **Macro viruses**: وهذه الفيروسات تصيب ملفات محررات النصوص مثل: MS Word- MS Exel- MS Power Point، وهذا النوع من الفيروسات غير منتشر ونادر، حيث بمجرد فتح مثل هذه الفيروسات تصاب الملفات الأخرى بهذا الجهاز، وكمثال عليها نذكر أحد الفيروسات ما أن تفتحه بالجهاز حتى تمحى كل ملفات الأوفس التي تعمل بالجهاز حتى ولو كانت مخزنة.

٣) **Script Viruses**: وهي فيروسات تستخدم الأكواد للغات رمزية (جافا سكريبت، فيجوال بيسك سكريبت، Php، ملفات باتش،...الخ)، وهي تصيب النظام وتؤدي إلى تحويل الأكواد إلى عمليات تخل بالنظام.

أعراض الإصابة بالفيروسات هي:

١ - نقص شديد في سعة الذاكرة المؤقتة RAM.

٢ - بطء تشغيل النظام بصورة ملحوظة.

٣ - عرض رسالة خطأ فجائية وغير عادية.

٤ - تغيير في حجم الملفات بدون سبب منطقي.

٥ - تغيير في عدد الملفات.

٦ - تغيير في مظهر العلامات (ICONS) الدالة على الملفات والأقراص المستخدمة.

٧ - ظهور أحرف غريبة عند الضغط على مفاتيح معينة في لوحة المفاتيح أو عدم ظهور حروف على الإطلاق.

٨ - توقف النظام الحاسوبي عن العمل.

٩ - التعامل مع القرص أكثر من المعتاد ويلاحظ ذلك من إضاءة لمبة البيان الخاصة بالقرص عدة مرات أكثر من المعدل الطبيعي.

• الديدان Worms:

■ هي نوع مخصص من البرامج الخبيثة والتي صممت للاستفادة من ضعف ما ضمن تطبيق أو نظام تشغيل بغية الدخول إلى الحاسوب وهي تشبه الفيروسات إلى حد كبير حتى أصبح البعض يعتبرها من أشكال الفيروسات ولكنها تختلف عن الفيروسات وبقية البرامج الخبيثة بأن لها خاصية اعتمادها على نفسها والتكاثر تلقائياً في النظام أو الشبكة مما يجعل العمليات بطيئة أو متوقفة وتعطل موارد الشبكات، ومن أشهر أمثلة الديدان "Blaster" والذي أصاب الملايين من أجهزة الويندوز في عام ٢٠٠٣م، وكذلك سلامر Slammer، والتي تميزت بسرعة انتشارها الهائلة ما مكنها من المرور على جميع عناوين الانترنت IP والبالغ عددها ٤ بليون عنوان في غضون ١٥ دقيقة، ومن العمليات التي يمكن أن تقوم بها الديدان هي حذف الملفات أو إضافة إمكانية تحكم المهاجم بالحاسوب عن بعد، وتستخدم الدودة الشبكات لإرسال نسخ عن نفسها إلى أجهزة أخرى مربوطة إلى الشبكة نفسها.

• أحصنة طروادة Trojan Horse:

- هي برامج خبيثة تحقق داخل برامج أخرى حاملة لها للدخول إلى النظام ويمكن أن تكون خاملة في الجهاز لفترات طويلة دون اكتشاف أمرها وتستخدم في العادة لتحمل برامج خبيثة أخرى، ومن أمثلة ذلك "Linux/LuaBot" والذي أصاب مليون جهاز من أجهزة انترنت الاشياء وخوادم مواقع الانترنت التي تشتغل بنظام الينكس عام ٢٠١٦.
- عند استخدام مصطلح حصان طروادة مع الحاسب فهو عبارة عن برنامج تنفيذي يهدف بشكل معلن إلى تحقيق وظيفة ما لكنه يقوم بوظيفة أخرى أو يقوم بالوظيفتين معاً، فمثلاً عندما يحمل المستثمر برنامج معلن على أنه تقويم Calander فإنه إضافةً إلى تنصيب برنامج التقويم يقوم بمسح النظام لمعرفة أرقام البطاقات المصرفية وكلمات المرور ... إلخ ومن ثم يرسلها إلى المهاجم.

أحصنة طروادة Trojan (حصان خشبي كبير الحجم) ولها أشكال مختلفة مثل:
(١) Backdoors: وهي الأخطر لأنها تأخذ صلاحيات مدير نظام وتعمل بسرية تامة، ومن دون علم المستخدم، وتستخدم شبكة محلية أو الإنترنت للتحكم بجهاز الضحية، وتتبع سلوك أدوات مدير النظام والمعروفة بـ:
AT = Remote Administrator Tool، والفرق الوحيد بين التروجانات وبرامج الإدارة هي: أن التروجانات تنزل وتعمل بدون علم المستخدم بينما أدوات الإدارة تكون واضحة وتعطيك رسالة أنها تراقب النظام.
هذا النوع يستخدم للتحكم بروتوكول TCP\IP.
يتكون هذا النوع من جزأين هما:
الأول بجهاز الضحية: ويعمل بشكل خفي بحيث يتلقى الأوامر من المخترق.
الثاني عند المخترق الذي بعث التروجان: وتكمن خطورتها في إرسال واستقبال الملفات من وإلى جهاز الضحية، والدخول للملفات الخاصة، وإمكانية حذفها وتعديلها، وتوجيه المستخدم إلى موقع إنترنت بدون إرادته، وتغيير الصفحة الرئيسية أيضاً، وسرقة المعلومات الخاصة، وكلمات سر تشغيل البرامج والأجهزة المرتبطة بالجهاز (طابعة أو كميرا....الخ)، وإعادة تشغيل الجهاز وإطفاءه.

٢) General Trojans: وهذا النوع يخرب الجهاز ويسرق البيانات من جهاز الضحية وأغلب مبرمجين البرامج الخبيثة يضيفون خصائص كثيرة لهذا النوع **PSW Trojans**، وهو سارق كلمات السر حيث يقوم بفحص المواقع التي تحفظ بها كلمات السر ويأخذها ثم يرسلها للشخص الذي كونه. وبالعادة يسرق معلومات عن النظام والرقم التسلسلي لنظام التشغيل (بالدول الغربية نظام التشغيل غالي فسرقة الرقم التسلسلي مهم جداً)، وبيانات الدخول للإنترنت (رقم البطاقة وكلمة المرور للإنترنت)، وكلمات السر للألعاب على الشبكات (بعض الألعاب على الشبكة تكون بمقابل مادي)، وكلمات السر للإيميل، والمواقع الأخرى الهامة.

٣) Trojan Clickers: وهذا النوع يقوم بتوجيه الضحية لموقع معين بدون إرادته والهدف منه هو إما زيادة العدد للزائرين لموقع معين أو إستنفاد حجم التبادل الشهري لموقع أو الهجوم على موقع أو مخدم معين بواسطة **DOS Attack** أو أخذ الضحية لموقع معين حيث يكون هذا الموقع مصاباً فيتم تنزيل فيروس أو برنامج آخر بجهاز الضحية، وقد تقوم هذه البرامج أيضاً بمنع المستخدم من الدخول إلى مواقع معينة كمواقع شركات الحماية والتحديث فلا يستطيع المستخدم تحديث مضاد فيروساته.

٤) Trojan Downloaders: وهي برامج تتميز بصغر حجمها ووظيفتها تنزيل برامج أخرى (تروجانات أو فيروسات) إلى جهاز الضحية، فمثلاً دمج أحدهم برنامج مكرّك مع تروجان كامل (١٠٠ كيلوبايت) سيلفت الانتباه فيلجاً إلى دمجها مع برنامج صغير لا يتعدى ٥ كيلوبايت وظيفته عند الاتصال بالإنترنت تحميل الملف الكبير من الإنترنت وفتحه بجهاز الضحية.

٥) Trojan Droppers: وهي برامج هدفها إخفاء البرامج الخبيثة عن أعين المستخدم أو عن مضاد الفيروسات كل ملف بالجهاز له توقيع رقمي يختلف عن غيره ومضاد الفيروسات يحوي بداخله توابع الفيروسات والبرامج الخبيثة (التحديث هو عملية إضافة توابع البرامج الحديثة المكتشفة إلى أرشيف البرنامج)، فيقوم هذا النوع من البرامج بتشفير الكود البرمجي للبرنامج الخبيث وتغيير توقيع الرقمي فيصبح ملفاً غير مكتشف بالنسبة لمضاد الفيروسات ويمر من قبضته. وتحوي هذه البرامج على خيارات لإيهام الضحية أن البرنامج الذي تم إخفاؤه ملف سليم عن طريق تشغيل تطبيق آخر أو إظهار رسالة خطأ توهم المستخدم أن الملف سليم.

مثال: دمج فيروس مع صورة فعند الضغط على البرنامج المشفر يظهر للضحية صورة أو دمج فيروس مع برنامج مسروق فيضغط الضحية على ملف التنصيب وينصب البرنامج بشكل طبيعي ولا يدري أنه ينصب وبشكل خفي في جهازه فيروساً.

٦ Trojan Proxies: وهي برامج تستخدم لتحويل جهاز الضحية لبروكسي يمكن الذي أرسل التروجان إلى استخدامه للدخول للإنترنت بشكل متخفي، وهذا النوع منتشر بكثرة بين الذين يستخدمون الرسائل المزعجة لكي يتمكنوا من الدخول لأعداد كبيرة من الأجهزة وبشكل متخفي لإرسال رسائل من أجهزة غيرهم.

٧ Trojan Spies: وهذا النوع يستخدم للتجسس على نشاطات الضحية (ليس فقط كلمات السر كما في PSW Trojans بل على نشاطات أخرى) مثل تصوير سطح المكتب أو صور مأخوذة من الكاميرا أو أية نشاطات يقوم بها المستخدم.

٨ Trojan Notifiers: وهي فقط لإعلام المخترق الذي أرسل التروجان بنجاح إصابة الجهاز بالبرنامج الخبيث، حيث ترسل للمخترق معلومات عن الجهاز و IP والمنافذ المفتوحة.

٩) Rootkits: وهي برامج تقوم بإخفاء نشاطات التروجانات عن البرامج ولكن بطريقة لا تثير الريبة أبداً، حيث تبقى مثلاً إدارة المهام فعالة ولكن لا تظهر فيها أية نشاطات للتروجانات ولا تظهر بلوحة العمليات وتقوم بإخفاء نفسها بمفاتيح بالريجستري وقد تقوم أيضاً بسرقة المعلومات الخاصة كسارق كلمات السر، وتفعل الجذور الخفية ذلك عن طريق إخفاء أو حذف أثر سجلات الدخول أو معلومات الإدخالات أو الإجراءات المتعلقة بها، كما يمكن لها أن تغير نظام التشغيل ليتجاهل أي نشاط خبيث وتتمثل إحدى الأساليب التي تتبعها الجذور الخفية في تعديل أو تبديل ملفات نظام التشغيل بإصدارات معدلة معمولة خصيصاً لتجاهل الأعمال الخبيثة، وتتميز هذه البرامج بأنها تضيف نفسها كملفات نظام وتأخذ حقوق المدير. البرامج التي تستطيع اكتشاف الجذور الخفية تقارن عادةً محتوى ملفات نظام التشغيل مع المحتوى الأصلي أي يجب تشغيل برنامج الاكتشاف من وسط نظيف مثل القرص المضغوط أو محرك USB مخصص.

من برامج مكافحة الأحصنة الطروادية نذكر على سبيل المثال لا الحصر:

Lockdown2000, Pest Patrol, The Cleaner, Tuscan,
Trojan Hunter, Trojan Remover , ... etc

برامج التجسس

Spyware:

هي برامج حاسوبية خبيثة وخطرة تتسلل إلى الحواسيب ولها القدرة على التخفي في الجهاز، ومتابعة كل العمليات على الجهاز، ومعرفة المعلومات الخاصة والسرية المخزنة بها، ويمكنها سرقة الهوية والمعلومات الشخصية، وتقوم بالنزول بشكل سري عبر الشبكة، وتقوم بتسجيل الكبسات أو الضغوطات التي استخدمت من أجل معرفة الكلمات السرية والأرقام المتسلسلة، وإرسالها إلى جهات خارجية، وتعتبر نوع من الاختراق الذي يقتصر على معرفة محتويات النظام المستهدف بشكل مستمر دون إلحاق الضرر به، وبناءً على طريق عملها يمكن تصنيفها إلى:



Damascus University

١- برامج رصد وتسجيل: كمسجل أو راصد المفاتيح وحركة الفأرة وكذلك راصدات ومسجلات البريد الإلكتروني والدردشة.

٢- برامج تتبع: وهي التي تراقب عادات الاستخدام وأنماطه وتخزنها كبيانات إحصائية بهدف إعداد التقارير بناءً عليها، حيث يتم تجميع هذه المعلومات عن الشخص الضحية ثم تحليلها واستخدامها في الهجوم عليه أو سرقة معلوماته.

٣- الصفحات الفقاعية أو الانبثاقية Popup: وهي برامج تخرج بين الفينة والأخرى كإعلانات أثناء تصفح الإنترنت وتستهلك موارد النظام والاتصال وقد تؤدي إلى مشاكل أمنية جراء الاختفاق في سد الثغرات الأمنية للحاسوب.

من برامج مكافحة برامج التجسس نذكر على سبيل المثال لا الحصر:

Ad-Aware Pro, Destroy & Search – Spybot, Pest Patrol

تقوم برمجيات التجسس بإحدى العمليات التالية: الاعلان أو جمع المعلومات الخاصة أو تغير إعدادات الحاسوب ومن التقنيات التي تستخدمها برمجيات التجسس نذكر:

- برمجيات التحميل الالى المستخدمة لتحميل وتنصيب البرامج دون إذن المستخدم.
- تقانات التعقب السلبية التي تجمع المعلومات عن نشاطات المستخدم دون تنصيب أي برنامج.
- برمجيات تعديل النظام.
- برمجيات التعقب المستخدمة لمراقبة سلوك المستخدم أو جمع معلومات عنه.

إضافةً إلى انتهاك خصوصية المستخدم يمكن لبرمجيات التجسس أن تؤثر سلباً على الحاسوب ك:

- أداء أخفض للحاسوب.
- عدم استقرار النظام.
- إضافة شريط أدوات أو قوائم جديدة على متصفح الانترنت.
- إضافة اختصارات جديدة.
- اختطاف الصفحة الرئيسة.
- زيادة عدد النوافذ الفجائية.

• برامج الإعلانات المزعجة :Adware

■ هي شبيهة ببرامج التجسس ولها نفس الخصائص تقريباً ولكن الهدف منها نشر الإعلانات وجمع بيانات من المستخدمين.



وهي عبارة عن برنامج لإيصال الاعلانات بطريقة غير متوقعة وغير مطلوبة من المستخدم ويمكن تتصيب هذه البرامج على الحاسوب عن طريق فيروس أو دودة، أو عن طريق حضان طروادة، وما أن يتم تتصيب البرنامج الدعائي حتى يبدأ بعرض شريط الاعلانات أو نوافذ الاعلانات الفجائية أو فتح نافذة ويب جديدة ضمن المتصفح، كما تقوم بعض البرمجيات بتعقب نشاطات المستخدمين على الانترنت وإرسال تقرير عن هذه النشاطات إلى طرف ثالث بدون معرفة المستخدم (اهتمام بالسيارات على سبيل المثال).

تعتبر فيروسات الحاسب الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات، والفيروس هو أحد البرامج الخبيثة، والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.

يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الحاسب وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها.

أما البرامج الخبيثة الأكثر خطورة، فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك.

أما بالنسبة لبرامج الدعاية وبرامج التجسس، فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة، كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.

• برامج شبكة بوت نت Botnet:

- هي برامج خبيثة تعمل في جهاز الضحية وتتصل بجهاز المهاجم دون علم الضحية حيث لا يشعر بوجودها وذلك بهدف استخدام جهاز الضحية في الهجوم على أجهزة أخرى ويسمى جهاز الضحية في هذه الحالة "Bot" بوت، ويكون المهاجم شبكة من أجهزة الضحايا تسمى البوت نت ويسمى مالك الشبكة بسيد الشبكة "Botmaster"، ويعتبر تحكم المهاجم بالحاسب البعيد من أهم أهداف البرمجيات الخبيثة، ومن الهجمات الممكن شنها باستخدام شبكات بوتنتيت نذكر: بريد غير مرغوب، حجب الخدمة، نشر البرمجيات الخبيثة، التلاعب بالتصويت الإلكتروني على الخط.
- كان يجري التحكم بشبكات البوتنتيت عن طريق البروتوكول IRC: Internet Relay Chat، ولكن حالياً يستخدم البروتوكول HTTP: HyperText Transport Protocol حيث أن تمرير أوامر التحكم عبر HTTP يصعب اكتشافها أو حجبها، وكذلك يجعل عملية التحكم والسيطرة أسهل وذلك عن طريق توجيه الضحية للدخول إلى موقع يتبع للمهاجم أو تحت تصرفه.

• برامج الفدية Ransom Ware:

■ هي نوع من أنواع البرامج الخبيثة تقوم بتشفير كامل الملفات والمعلومات في جهاز الضحية ويطلب البرنامج مقابل مادي من الضحية لفك التشفير وإرجاع المعلومات، وزاد ظهور هذا النوع من البرامج الخبيثة في السنوات الأخيرة ومن أشهر الأمثلة على ذلك برنامج الفدية المسمى "WannaCry" والذي ظهر في منتصف عام ٢٠١٧م، وأصاب خلال يوم واحد أكثر من ٢٣٠,٠٠٠ جهاز في ١٥٠ دولة..

• مسجلات المفاتيح Key logger:

■ يلتقط مسجل المفاتيح أي ضغطة مفاتيح يقوم بها المستخدم على لوحة المفاتيح ثم يسجلها ويمكن للمهاجم أن يستفيد من هذه المعلومات أو أن يتم إرسالها إلى موقع بعيد حيث يبحث المهاجم عن الأنواع المفيدة من المعلومات ضمن النصوص الملتقطة مثل كلمات المرور، أرقام بطاقات الائتمان وأي معلومات شخصية أخرى، ومسجل المفاتيح يمكن أن يكون جهاز صلب أو برنامج ويمكن تحميلها أو تنصيبها عن طريق فيروس أو حصان طروادة ولها القدرة العالية على التخفي.

• الأبواب الخلفية (المستترة) Backdoor:

■ هي ثغرات توضع عمداً في البرامج والأنظمة أثناء مرحلة تطويرها، وذلك لتسمح للمبرمجين تجاوز عمليات المصادقة لمتابعة مشاكل التعليمات البرمجية المعقدة أثناء عمليات التشغيل، إذاً، خلق باب شرعي من قبل مطوري البرامج هو ممارسة معروفة للنفاز إلى برنامج أو جهاز دورياً بدون تعقيدات طلب كلمة المرور أو أي إجراءات أمنية أخرى وتكون النية عادةً بحذف الباب الخلفي عند انتهاء تطوير البرنامج لكن غالباً ما يترك الباب الخلفي مفتوحاً الأمر الذي يسهل عملية الاختراق من قبل المهاجمين، وتحذف هذه الثغرات عند الإصدار الأساسي ولكن وبنفس الطريقة يستخدم المخربون أبواباً خلفية للتحكم في أجهزة الضحية، ومن امثلة ذلك OSX/Hellrts والذي أصاب نظام التشغيل ماكنتوش والأجهزة الخاصة بشركة ابل حيث كان عبارة عن باب خلفي في برنامج iPhoto يتيح الاتصال بخادم بعيد مما ساعد المخترقين بالدخول والتحكم بالأجهزة المصابة.

■ مرسل البيانات Data Sender:

ترسل هذه البرامج بيانات خاصة بمستخدم النظام المعلوماتي دون علمه عن طريق رسالة بريدية أو تزويرها لموقع المهاجم مباشرة.

• معطل خدمات النظام Denial of Service:

تعمل هذه البرامج بالتسيق مع نسخ أخرى مشابهة على أجهزة أخرى مهاجمة على مهاجمة حاسوب معين لتوقيفه عن العمل بشكل كامل أو جعله بطيئاً جداً.

• معطل البرامج Blocker:

تقوم هذه البرامج بتعطيل بعض البرامج وخاصة برامج مكافحة الفيروسات وجدران الحماية لكي يكون النظام المعلوماتي سهل الاختراق.

• الوصول عن بعد Remote Access:

تسمح هذه البرامج للمهاجم بأن يتحكم في الحاسوب عن بعد بشكل مخفي.

• القنابل المنطقية Logic Bomb:

■ هي برامج خبيثة تبقى خاملة في جهاز الضحية حتى يتحقق شرط منطقي كأن يتم ربط جهاز الضحية بالإنترنت عندها ترسل هذه البرامج تنبيهات للمخترق لتتم عملية الاختراق، أو أن الضحية قد زار موقع البنك لتتم مراقبة الاتصال وسرقة المعلومات، وعادة ما تدمج القنابل المنطقية ببرنامج خبيث آخر كفيروس أو باب خلفي أو غيرها.

• ArcBombs:

وهي ملفات مؤرشفة صممت لتخريب الملفات المضغوطة حيث تتضاعف أحجامها تلقائياً ألوف المرات فتتخرب ويمتلئ الجهاز بملفات فارغة تسمى قنابل الهواء وخطورتها تكمن في إصابة مخدمات الإنترنت ومخدمات البريد الإلكتروني. هناك ثلاث أنواع لها وهي:

النوع الأول: يملئ الملفات المضغوطة بمعلومات وبيانات مكررة.

النوع الثاني: يخرب الملفات المضغوطة النوع.

النوع الثالث: يضغط الملفات بشكل صغير جداً فمثلاً حجم ٥ جيجا يصبح ٢٠٠ كيلو بايت.



٣ - المخترقون (الهكرز):

الاختراق: محاولة الوصول إلى أجهزة وأنظمة الأفراد أو المؤسسات والشركات باستخدام برامج خاصة عن طريق ثغرات في نظام الحماية بهدف الحصول على معلومات أو تخريب تلك الأنظمة والحاق الضرر بها.

- هم المهاجمون الذين يقصدون الدخول إلى الأنظمة بهدف الاختلال في أمن المعلومات إما بتدمير المعلومات أو تسريبها أو تعديلها أو التجسس عليها، وتعود في الأصل كلمة الهكرز إلى المحترفين في مجال الحاسب الآلي ثم تحولت مع الزمن ليقصد بها المخترقين للأنظمة، ويمكن تقسيمهم إلى قسمين أساسيين:

- المخترقون الداخليون.

- المخترقون الخارجيون.

• المخترقون الداخليون:

- أو الموظفون المخربون، حيث تتم عادة أكبر الاختراقات في عالم أمن المعلومات من الموظفين الداخليين (المسمى الآخر لهم) في المؤسسات إما باختراقهم أنظمة المؤسسة بأنفسهم أو حتى بمساعدتهم لمخترقين خارجيين ويهدفون عادة إلى تسريب المعلومات أو تعديلها.

• المخترقون الخارجيون:

- ويمكن تقسيمهم أيضاً إلى:
- محترفون.

- غير محترفون أو أطفال البرمجيات.

محترفون: ولهم تقسيمات مختلفة أشهرها:

■ **ذوي القبعات السوداء:** وهم من يكون القصد من اختراقاتهم التخريب لذا يمكن تسميتهم بالمخربين ويكونون عادةً تابعين لمنظمات خارجة عن القانون.

■ **ذوي القبعات البيضاء:** وهم المختصين في أمن المعلومات والذين يخترقون الأنظمة بهدف اكتشاف الثغرات قبل أن يكتشفها المخربون ويتم سد هذه الثغرات وعادةً ما تستقطبهم المنظمات والشركات لاكتشاف قوة أنظمتها وينتهي عملهم عادة بإصدار التقارير عن الثغرات والمشاكل المكتشفة.

■ **ذوي القبعات الرمادية:** هم من يكون في الأصل من ذوي القبعات البيضاء ثم في أوقات معينة ولأي سبب كان يتحولون إلى ذوي القبعات السوداء.

غير محترفون أو أطفال البرمجيات:

– وهم غير ناضجين بما يكفي ولكنهم يحاولون الاختراق والتخريب باستخدام برامج جاهزة أو أدوات تم تطويرها من قبل الهاكرز المحترفين أو يستغلون الثغرات الأمنية المشهورة والتي تدل على الضعف في النظام المُخترَق.

– عادةً ما تكون الادوات المصنوعة من الهاكرز المحترفين سلاح ذو حدين حيث ربما تساعد هذه البرمجيات غير المحترفين على الاختراق ولكنها ربما تتيح لصانعيها امكانية اختراق أجهزة غير المحترفين واستغلالها في عمليات اختراق أكبر.

• أهم أشكال الهجمات الالكترونية على أنظمة المعلومات:

- تختلف أشكال الهجمات التي يشنها المخترقون على الأنظمة بهدف الاخلال في أمن المعلومات.
- إن عملية الاختراق الواحدة ربما تتكون من هجمة واحدة أو أكثر من هجمة وليس بالضرورة أن تكون جميع الهجمات بنفس الشكل.
- كما أن كل عملية اختراق متميزة بحد ذاتها حيث يعتمد ذلك على حاله النظام وقدرات المخترق.
- من أشهر أشكال الهجمات مايلي:
 ١. هجمات استغلال الثغرات.
 ٢. هجمات بالبرامج الخبيثة.
 ٣. هجمات حجب الخدمة DDoS.
 ٤. هجمات الهندسة الاجتماعية Social Engineering.

١. هجمات استغلال الثغرات:

■ الثغرات هي أخطاء غير مقصودة في التعليمات البرمجية للبرامج والأنظمة لا يخلو برنامج أو نظام عادة من الثغرات والتي يتم سدها حال اكتشافها مع كل تحديث للنظام أو للبرامج.

■ يستغل عادة المخترقون هذه الثغرات إذا تم اكتشافها من قبلهم للولوج إلى النظام وتختلف الثغرات من حيث قوتها فبعضها تكون محدودة بأن تتيح التحكم بجزء من البرنامج أو النظام وبعضها تكون قوية بحيث تسمح بالولوج لكامل النظام.

من أشكال هذا النوع من الهجمات نذكر الهجوم على حقوق النفاذ **Access Rights Attack**: حيث تعرف حقوق النفاذ على أنها امتيازات تمنح للمستثمرين للنفاذ إلى الموارد البرمجية والعنصرية مثل منح شخص ما حقوق قراءة ملف، بينما يمنح شخص آخر حقوق تعديله أو حذفه أيضاً، ومن أهم الهجمات التي تركز على حقوق النفاذ نذكر:

أ- تصعيد الامتيازات:

حيث يستطيع نظام التشغيل أو بعض التطبيقات حصر امتيازات المستثمر في الوصول إلى وظائف محددة وتصعيد الامتيازات هي عملية استغلال ضعف برمجي للوصول إلى موارد ممنوعة عنه، ويوجد نوعان لتصعيد الامتيازات هما:

- النوع الأول: حينما يحاول مستثمر ممنوح امتيازات قليلة تصعيد امتيازته.

- النوع الثاني: تنفيذ المستثمر ذو امتيازات محددة إلى وظائف باستخدام امتيازات مستثمر آخر.

ب- النفاذ المتعدي:

ويجري هنا استغلال الالتباس الذي يحصل عند عدم وضوح الصلاحيات الممنوحة لمجموعة من المستثمرين ينفذون وظائف متكاملة على مجموعة من الملفات أو بشكل آخر استغلال علاقة الثقة بين ثلاثة أطراف.

٢. هجمات بالبرامج الخبيثة:

- رغم أن البرامج الخبيثة هي تهديد بحد ذاته إلا أنها أيضاً ربما تستغل من قبل المخترقين للدخول واختراق الانظمة أو التجسس عليها ونقل البرمجيات التي تساعد على ذلك عن طريقها.

٣. هجمات حجب الخدمة DDoS:

- هي إحدى أنواع الهجمات والتي يقوم بها المخربين حيث يقومون بإرسال كمية هائلة من الأوامر إلى جهاز الخادم بهدف تعطيله وحجب خدماته عن المستخدمين وتستخدم عادة أجهزة ضحايا في شبكات البوت نت لعمل ذلك وتعتبر من اشكال الهجمات التي يصعب الحماية منها.

٤. هجمات الهندسة الاجتماعية Social Engineering:

- لا نحتاج دائماً إلى التقانة لمهاجمة النظام المعلوماتي، فالهندسة الاجتماعية هي طريقة لجمع المعلومات المطلوبة لشن الهجوم بالاعتماد على مواطن ضعف الأفراد.

هي الفن أو المهارة المبنية على التقنيات النفسية الاجتماعية التي عن طريقها يستطيع المهاجم الحصول على المساعدة أو على معلومات سرية أو مهمة من الضحية بدون أن يشعر الضحية بذلك.

الهندسة الاجتماعية هي عملية استخدام المهارات الاجتماعية لإقناع الأشخاص بالإفصاح عن المعلومات السرية وعلى المستوى المادي يمكن تعريفها بأنها انتحال شخصيات المهندسين وفنيي الصيانة ومن في حكمهم للدخول إلى أماكن حساسة ومهمة كون لديهم أعمالاً مركزية تتطلب وجودهم أو دخولهم ولكن في الحقيقة لهم أغراض أخرى غير ذلك.

أقرب التعريفات للهندسة الاجتماعية هو استخدام المهاجم حيلاً نفسية كي يخدع بها مستخدمي الموارد المتنوعة (حاسب، مخدم، هاتف، ... إلخ) ليتمكنوا من الوصول إلى المعلومات المخزنة فيها، وتعتبر من أنجح الوسائل التي يستخدمها المهاجم لسهولة مقارنتها مع الوسائل الأخرى، وفعاليتها العالية كونها تهاجم العنصر البشري الذي هو أضعف نقطة في منظومة حماية المعلومات.

من الممكن أن تشن هجمات أسلوب الهندسة الاجتماعية على عدة أصعدة وهي:

أ- الصعيد الحسي: حيث يكون التركيز على موضوع الهجوم والبيئة المحيطة به ويدخل ضمن هذا مايلي:

– مكان العمل.

– الهاتف.

– النفايات.

– الانترنت.

ب- الصعيد النفسي: وهذا المستوى يعنى بالمناخ النفسي المحيط بالطريقة التي ينفذ بها الهجوم، فالمهاجم يسعى إلى خلق الأجواء النفسية المناسبة لإيهام الضحية بأن المهاجم شخص موثوق به ولديه صلاحية الاطلاع على المعلومات الحساسة للشخص المستهدف أو المنشأة المستهدفة.

أساليب الهجوم باستخدام الهندسة الاجتماعية

يوجد عدة أساليب ولكن من أشهرها نذكر مايلي:

آ- أسلوب الإقناع: حيث بينت الدراسات التي أجريت في علم النفس الاجتماعي على وجود طريقتين لإقناع شخص لعمل شيء ما وهما:

١- طريقة الإقناع المباشرة: حيث يتذرع المهاجم بالحجج المنطقية والبراهين لتحفيز الضحية على التفكير المنطقي والوصول إلى نتيجة يرغب المهاجم في جر الضحية إليها.

٢- طريقة الإقناع غير المباشرة: حيث يعتمد المهاجم على الإيحاءات النفسية والقفز فوق المنطقة وتحاشي استنفار التفكير المنطقي لدى الضحية وحث الضحية على قبول مبررات المهاجم دون تحليلها والتفكير فيها جيداً، فيعتمد المهاجم في بداية لقائه بالضحية بإطلاق عبارات تستثير الشخص المستهدف نفسياً إما ببث مشاعر الخوف أو الحماس والعمل على تشتيت وتشويش ذهن ونظرة الضحية للأمور فتصعب قدراته على التفكير والتحليل المنطقي، ويصعب عليه مواجهة ضحيج المهاجم ومبرراته.

من أنجح الأساليب التي يعملها المهاجم ضد خصمه في هذه الطريقة مايلي:

- التزيي بمظهر صاحب السلطة: سرعة تلبية طلبات ذي السلطة من الناس، (وكمثال على ذلك طبيب وممرضات في المشفى).
- الإغراء بامتلاك شيء نادر: (شاشات عرض وتحميل موقع).
- إبراز أوجه التشابه مع الشخص المستهدف: من خصائص النفس البشرية الميل إلى من يشبهها في العرق، اللون، الطباع، إبراز اهتمامات، واحساس الضحية بوجود أوجه شبه مع المهاجم "دون معرفة نواياه الحقيقة" يجعله أقل حذراً عند التعامل معه.
- رد الجميل: إن من خصائص النفس السوية رغبتها في رد الجميل إلى من أحسن إليها، وهذه الخاصية تزداد رسوخاً في المجتمعات ذات الصبغة القبلية والأسرية، وكمثال على ذلك: ملف تم حذفه من قبل الضحية واسترجاعه من قبل المهاجم.

ب- أسلوب انتحال الشخصية (التمثيل): وتعني تقمص إنسان ما شخصية إنسان آخر.

ج- أسلوب المداهنة: عند تأمل الشخصيات التي يكثر انتحالها لشخصيات أخرى يتضح للعيان أنها في الأعم هي لأناس تدعهم سلطة قوية وأن المهاجم المنتحل لهذه الشخصيات يعلم يقيناً أن الكثير من الناس (موظفين على سبيل المثال) يسعون بشتى السبل لخلق صورة حسنة عن أنفسهم عند رؤسائهم

د- أسلوب مسايرة الركب: وهذا مسلك اجتماعي يملئ على الإنسان ألا يتخذ موقفاً مغايراً لمل عليه الآخرون تجاه مسألة ما.

هـ- أسلوب الهندسة الاجتماعية العكسية: وتقوم على:

- افتعال موقف.
- إبراز المهاجم نفسه على أنه الشخص ذو المعرفة أو الصلاحية اللازمة للتعامل مع الموقف.
- تقديم المساعدة.

يخلط هذا النوع من الهجوم بين النواحي الاجتماعية واهتمامات الناس وبين المهارات الفنية في خداع الضحايا وكسب ثقتهم للإدلاء بمعلومات سرية يتم استغلالها لسرقة المعلومات والأموال إلكترونياً وقد انتشر هذا النوع من الهجوم في الآونة الأخيرة انتشاراً واسعاً لأنه لا يعتمد على كسر أنظمة الحماية التقنية التي تطورت مع مرور الوقت وإنما يعتمد على كسب الضحايا وإيهامهم بأن من يطلب منهم معلوماتهم السرية (اسم المستخدم، كلمة المرور، رقم بطاقة الائتمان) هو جهة موثوقة (مصرف مثلاً) وبعد ذلك يتم استغلال هذه المعلومات وانتحال شخصيات الضحايا ومن ثم سرقتهم إلكترونياً عن طريق دخول يبدو شرعياً لأنظمة الحماية وكذلك الانتشار الواسع والتطور الهائل في وسائل التواصل الاجتماعي قد ساهم في الانتشار الكبير لهذا النوع من الهجوم، ومن الأمثلة على هذا النوع من الهجوم وهو الأكثر شهرة وانتشاراً نذكر:

هجمات الاصطياد الإلكتروني، والتي يتم فيها اقناع الضحية بأن المهاجم هو منشأة أو جهة شرعية مصرح لها، ويستغل مرسلو رسائل الاصطياد الإلكتروني الجانب الاجتماعي بالإضافة إلى الجانب الفني في عملية الاحتيال على الضحية وذلك من خلال اختيار فكرة رسالة الاصطياد بما يلامس اهتمامات الضحية ثم وضعها في قالب فني مخادع يولد القناعة لديها بأنها رسائل حقيقية من مصادر موثوقة.

ثمة طريقة ثانية لهجمات الهندسة الاجتماعية يتم فيها إقناع الضحية بأن المهاجم هو شخص أهم منه وأعلى منه مرتبة في المؤسسة أو في المجتمع من أجل كسب ثقته ومن ثم الحصول على معلوماته السرية واستخدامها بطريقة غير شرعية وعادةً ما يستخدم هذه الطريقة في هجمات الهندسة الاجتماعية الداخلية التي تتم في المنشأة. يمكن تقسيم الهجمة الواحدة من هذا النوع إلى عدة هجمات منفصلة عن بعضها البعض من أجل عدم إثارة الانتباه بحيث يتم الحصول من كل هجمة على معلومات سرية منفصلة ثم تجمع لاحقاً للحصول على معلومات سرية متكاملة يمكن استخدامها في هجوم متكامل لاحقاً.

من الأمثلة على ذلك هو قيام المهاجم بالاتصال بأحد أفراد المؤسسة ثم سؤاله عن اسم مدير المؤسسة بطريقة ذكية وبعد ذلك يستخدم هذه المعلومة لكسب ثقة أشخاص آخرين داخل المؤسسة يظهر لهم أنه يعرف مدير المؤسسة وأنه على اتصال دائم به ومن ثم الحصول على معلومات إضافية مثل بريده الإلكتروني أو رقم هاتفه أو اهتماماته التي يمكن أن يستغلها لصياغة رسالة الاصطياد الإلكتروني لمدير المؤسسة أو لأي شخص آخر داخلها.

ويمكن أن تتضمن هجمات الهندسة الاجتماعية على:

أ- المقاربات النفسية (التمثيل Impersonation، التصيد Phishing، بريد غير مرغوب Spam، الخدع Hoaxes).

ب- الإجراءات الفيزيائية (غوص في القمامة Dumpster Diving، والتمرير Tailgating).

- التمثيل: وفقاً للهندسة الاجتماعية فهي تعني خلق شخصية خيالية تلعب دور هذا الشخص للضحية، كتمثيل دور مسؤول الدعم الفني الذي يتصل بالضحية ويدعي وجود مشكلة في الشبكة أو النظام المعلوماتي ومن ثم يطلب اسم المستخدم وكلمة المرور لإعادة تهيئة الحساب.

- التصيد: ومن أكثر أشكال الهندسة الاجتماعية شهرةً حيث يجري التصيد عن طريق إرسال رسالة إلكترونية أو عرض إعلان على الويب يدعي كذباً أنه قادم من شركة شرعية في محاولة خداع المستخدم لكشف معلومات خاصة حيث يطلب من المستخدم الجواب برسالة إلكترونية أو يتم توجيهها إلى أحد مواقع الويب حيث يتم الطلب منه تحديث معلوماته الشخصية (كلمة المرور، رقم بطاقة الائتمان، .. إلخ).

• ويكون موقع الويب في هذه الحالة مزيف وهو معد لسرقة المعلومات التي يدخلها المستخدم، ويعود أحد أسباب نجاح عمليات التصيد إلى كون رسائل البريد الإلكتروني الموجهة أو مواقع الويب تظهر وكأنها شرعية ويوجد بعض الأشكال الأخرى للتصيد ونذكر منها:

آ- التزييف Pharming: حيث في هذه الحالة يتم إعادة توجيه المستخدم آلياً إلى الموقع المزيف ويتحقق ذلك عن طريق التسلل إلى مخدمات توجيه حركات المرور أو مخدمات الأسماء.

ب- التصيد الموجه Spear Phishing: حيث يهدف إلى إرسال رسائل عامة محددة لعدد من المستخدمين وتكون الرسالة مخصصة للمستقبلين عن طريق وضع الاسم وغيره من المعلومات الشخصية في سبيل جعل الرسالة تبدو شرعية أكثر.

ج- الحوالة Whaling: وهي تعتبر من أحد أشكال التصيد الموجه فبدلاً البحث عن الأسماك الصغيرة فإن الحوالة تبحث عن الأسماك الكبيرة أي الأثرياء الذين لديهم أموالاً طائلة في حساباتهم المصرفية وفي هذا النوع من التصيد يمكن للمهاجم استثمار وقتاً أكبر لضبط رسائله بدقة كبيرة الأمر الذي يزيد فرص النجاح.

د- التصيد بالهاتف Vishing: حيث يجري هنا التصيد باستخدام الهاتف Voice Phishing بدلاً عن البريد الإلكتروني فمثلاً يقوم المهاجم بالاتصال بالضحية الذي يسمع رسالة مسجلة تزعم أنها قادمة من مصرف الضحية حيث تعلمه بأن حسابه المصرفي عانى من مشاكل تزوير أو أي عملية غير عادية ويطلب من الضحية بعد ذلك الاتصال برقم محدد وبعد اتصال الزبون يسمع تعليمات آلية تطلب منه إدخال رقم بطاقة الائتمان أو رقم الحساب المصرفي أو أي معلومات أخرى على لوحة المفاتيح للهاتف.

- الرسائل غير المرغوبة Spam: إن ازدياد كمية الرسائل غير المرغوبة باضطراد تؤثر على الانتاجية إضافة إلى كونها مصدر أساسياً للمهاجمين لتوزيع الفيروسات ومسجلات المفاتيح والطروديات وغيرها من البرامج الخبيثة، ويفرض أن السبامر أرسل ٦ مليون رسالة في يوم واحد لمنتج يباع بمبلغ ٥٠ دولاراً ويكلف فقط ٥ دولارات ويفرض أن 0.001 من مستقبلي الرسالة اشتروا المنتج فإن السبامر يحقق ربحاً قدره ٢٧٠.٠٠٠ دولاراً.

بما أن مخدمات البريد الإلكتروني باتت تستخدم مصفيات السبم التي تبحث عن كلمات محددة (مفتاحية) وتتعرف على هذه الرسائل فقد توجه السبامر إلى طريقة أخرى لإرسال الرسائل تعرف باسم Image Spam حيث يرسلون النصوص على شكل صور لتجاوز مصفيات النصوص حيث تحوي هذه الرسائل على نص عادي بلا أي معنى محدد لخداع مصفيات النصوص وذلك لأنه يجري استبعاد الرسائل التي تحوي صور بدون أي نص عادةً

• برامج الاحتيالية أو البلاغ الكاذب "الخدع" Hoax:

■ الخدعة هي تحذير خاطئ غالباً ما يكون مضمناً ضمن رسالة إلكترونية تزعم كونها قادمة من مدير النظام المعلوماتي حيث تدعي الرسالة وجود فيروس ضار على الانترنت وأنه على المستقبل حذف ملفات معينة أو تغيير الاعدادات الأمنية والتي تتيح للمهاجم اختراق الحاسوب، أو هي إعلانات منبثقة تظهر للمستخدم تتظاهر بأنها برامج مكافحة للفيروسات وأن الجهاز يحتاج إلى تحديث أو مسح لاكتشاف الفيروسات ولكنها في الحقيقة يمكن أن تحتوى على برامج خبيثة أخرى قد تصيب النظام بمجرد الضغط ومتابعة تعليمات ذلك الرسالة، كما من الممكن أن تكون تنبيهات كاذبة كوجوب تحميل مشغل الفلاش مثلاً.

ومن الإجراءات الفيزيائية نذكر:

- الغوص في القمامة Dumpster Diving: حيث يتطلب الغوص في القمامة البحث ضمن حاويات القمامة لإيجاد معلومات يمكن أن تفيد في الهجوم من المعلومات التي يمكن الحصول عليها باستخدام هذه الطريقة نذكر: المفكرات الشخصية، بعض التجهيزات الحاسوبية زهيدة الثمن، المخططات التنظيمية، دليل الهاتف، كتيبات السياسة الأمنية، كتيبات أنظمة التشغيل، ... إلخ.

- التمرير Tailgating: تستثمر الشركات مبالغ كبيرة لتجهيز الأبواب بأجهزة دخول متطورة تسمح فقط للأشخاص المسموح لهم بالدخول عن طريق استخدام البصمات أو بطاقات الدخول وغيرها وتكمن المشكلة في هذا النوع من الأجهزة في أنها لا تستطيع التحكم بعدد الأشخاص الذين يدخلون عندما يسمح بالدخول بفتح الباب، أي عندما يسمح لموظف ما بالدخول فإنه يستطيع أن يدخل معه من يريد.

ومن المختصين من قسم أشكال وأساليب الهندسة الاجتماعية وفقاً لأساليب إلكترونية وأساليب غير إلكترونية وهذا واضح بالشرح التالي:

١. أساليب غير الكترونية: لا تحتاج إلى أجهزة الكترونية ليتم التواصل بين المخترق والضحية ومن أشكالها نذكر:

– البحث في المهملات: يمكن باستخدام هذه الطريقة الحصول على بعض المعلومات المهمة من أجهزة أو أوراق تم إلقاؤها في النفايات والتي ربما تساعد المهاجمين في عملية جمع البيانات عن الهدف.

– مراقبة الضحية من الخلف: هي تقنية تستخدم لالتقاط معلومات مهمة مثل رقم الهوية أو الرقم السري أو أي معلومات تساعد في عملية الاختراق وتتم بمراقبة الشخص من الخلف.

– التتبع والتمثيل: هي من أهم تقنيات الهندسة الاجتماعية والتي تساعد المخترق على الدخول الى الأماكن غير المصرح له الدخول إليها وذلك بتتبع شخص مصرح له ثم الدخول بكل ثقة قبل إغلاق الباب على أساس أنه مصرح له أيضا. والتمثيل هي طريقة شبيهة ولكن المخترق يتظاهر بأنه يحتاج لدخول المكان بهدف تقديم خدمات معينة كعامل نظافة أو صيانة والهدف من الدخول في كلا الطريقتين هي جمع المعلومات أو تنزيل برامج خبيثة في أحد أجهزة المنظمة.

٢. أساليب الكترونية: يكون التواصل الكتروني بين المهاجم والضحية.

– التمثيل عن طريق الهاتف: من أشهر أساليب هجمات الهندسة الاجتماعية يستخدم الهاتف للتواصل مع الضحية وإيهامه والتمثيل عليه لجمع بعض المعلومات المهمة من الضحية حتى تصل في بعض الأحيان بأن الضحية يعطي رقمه السري للمهاجم.

– التصيد الالكتروني Phishing Scam: هي واحدة من أهم تقنيات الهندسة الاجتماعية وتهدف لسرقة بيانات الضحية من اسم مستخدم والرقم السري وأرقام البطاقات الائتمانية وتستخدم رسائل البريد الالكتروني او برامج التواصل الاجتماعي للتواصل مع الضحية بحيث يبدو الرسالة المرسله عالية الثقة ومن جهة موثوقة كشركة أو جهة حكومية وتطلب الرسالة بيانات من الضحية ولأن شكل الرسالة المرسله تبدو عالية الثقة يقع الضحايا في هذه الخدعة ويتجاوبون بإرسال بياناتهم او تعبأتها عن طريق رابط مرفق في نفس الرسالة. وهناك نوع خاص من هذه الرسائل يبدو الشخص المرسل شخص قريب من الضحية كزميله في العمل أو أخوه فيتجاوب الضحية مع الرسالة دون تدقيق ويقع في الفخ.

– مواقع الانترنت الوهمية: هي نوع خاص من التصيد الالكتروني ولكن هنا يتم استخدام موقع على الانترنت يبدو شبيه بموقع عالي الثقة ويستخدم نفس تصميم الموقع وعندما يزور الضحية الموقع الوهمي ويحاول الدخول باستخدام بيانات دخوله أو الشراء من الموقع باستخدام بيانات البطاقة الائتمانية يظهر خطأ في عملية الدخول أو الشراء ويطلب الموقع إعادة كتابة البيانات في هذه اللحظة يوجه الموقع الى الموقع الاصلي ولأنه بنفس التصميم فغالبا لا يلاحظ الضحية ذلك ويكتب البيانات مره أخرى ويتم الدخول ولكن البيانات قد تم إرسالها الى المخترق.

٤ - الهجمات الإلكترونية:

الحروب الإلكترونية والإرهاب: تتعدد ساحات الحروب ويعتبر الفضاء الإلكتروني هو أحد أهم مجالات الحروب في عصرنا اليوم. مما يعني أنه مجال صراع بين دول أو منظمات خارجة عن القانون وإرهابية وحتى بين الشركات الكبرى، ومع أن المعلومات كانت ومازالت هي أحد أهم أسلحة الحروب فسرقة المعلومات وتدميرها يعد سلاحاً قاتلاً في هذه الحروب، ولكن الحروب الإلكترونية تتعدى سرقة المعلومات ويمكن أن تشمل التضليل والتأثير وغسل العقول وحتى تصل إلى تدمير البنى التحتية.

يستخدم هذا المصطلح للتعبير عن سرقة الهوية، وهو عمل إجرامي، حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية، وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول إلى الموقع، وهناك برامج لمكافحة الخصوصية والكشف عن هوية المرسل الحقيقي، وأفضل وسيلة لحماية الشخص من نشر معلوماته الشخصية لمن يطلبها هو أن يكون الشخص متيقظاً وحذراً ولديه الوعي الكافي، فلا يوجد هناك أي بنك معروف أو مؤسسة فعلية يطلبون من عملائهم إرسال معلوماتهم الشخصية عبر البريد الإلكتروني.

حماية أمن المعلومات

Damascus University

الإجراءات الإدارية

Damascus University

تحتاج المنشآت عامةً والمنشآت ذات الطبيعة التنافسية والعسكرية والأمنية خاصةً لتأمين عنصر السرية للمعلومات التي تتطلب توفير السرية، وعدم الإفشاء أو حمايتها من الانتهاك، ومن الإجراءات المتبعة عادةً توقيع الموظفين من داخل المنشأة والمتعاونين من خارجها على سن تعهد رسمي يتضمن في بنوده بنداً بوجوب الالتزام بعدم إفشاء الأسرار التي يطلع عليها بحكم واجباته الوظيفية، وإجراءات المحافظة على أمن المعلومات تُتبع في المنشآت التي تستخدم شبكات الحاسب لحماية المعلومات من التهديد بالإزالة أو النقل أو الحذف أو التعديل أو التوقف عن الخدمة.

وتاريخياً، نجد أن العديد من المؤسسات لم تقم بتوفير الحماية الكافية لبياناتها نتيجة لـ:

- عدم التقدير الكافي لأهمية مشاكل الرقابة ذات العلاقة بالحاسوب والنتائج السلبية المترتبة عليها، إذ تنظر المؤسسات إلى خسارة المعلومات الحساسة كتهديد بعيد الحدوث وضعيف الاحتمال، فالمشاركين في دراسة سابقة يعتقدون بأهمية قضية أمن الحاسوب قد انخفض من ٣٥% إلى ٢٥% على مدى سنة واحدة.
- عدم الفهم الكامل لتطبيقات الرقابة على التحول من أنظمة الحاسوب القائمة على أساس مركزي إلى أنظمة الحاسوب القائمة على أساس الشبكات والإنترنت.
- عدم إدراك العديد من المؤسسات أن أمن البيانات هو أمر حاسم للبقاء، فالمعلومات هي أحد الموارد الإستراتيجية، وتُعد حمايتها أحد المتطلبات الإستراتيجية.
- الضغط باتجاه زيادة الإنتاجية وتخفيض التكاليف حثَّ الإدارة على تجاهل الإجراءات الرقابية في هذا المجال.

وللحفاظ على أمن المعلومات ذات الخصوصية يجب أن تتضمن الإجراءات ذات الصلة مايلي:

- ١ - بيان درجة السرية (سري للغاية، سري جداً، سري) وطرق تأمين كل درجة.
- ٢ - حفظ الوثائق الهامة بوسائط حفظ الملفات الالكترونية المؤرشفة.
- ٣ - حُسن اختيار الأفراد العاملين في حقل تقنية المعلومات وحُسن تدريبهم.
- ٤ - ضمان أمن المعلومات المخزنة داخل أجهزة الحاسب الآلي بإجراءات ضرورية منها:

آ - استخدام أقفال وتسلم مفاتيحها للأفراد المخولين فقط.

ب - استخدام كلمات المرور القوية للدخول إلى جهاز خزن المعلومات.

ج - استخدام شفرة (Code) لفتح البرامج.

د - استخدام بطاقات ممغنطة للدخول إلى غرف الحاسب الآلي.

هـ - استخدام بطاقة خاصة للدخول إلى أجهزة المخدم.

و - حصر وتحديد الأفراد الذين لهم الحق بالتعامل مع أجهزة المخدم.

وتعتمد إجراءات الحماية في المؤسسات على استراتيجيات ويمكن تحديدها بالتالي:

١- وسائل الحماية المادية:

وهي أدوات محسوسة مادياً مثل (كاميرات، أجهزة الانذار، الجدران والأسوار والمفاتيح، بطاقات دخول الموظفين، بطاقات الائتمان، أجهزة اكتشاف الحركة والصوت).

– وتعني أن تكون أجهزة الخوادم والشبكات في مأمن من الهجوم المادي كدخول شخص غير مصرح له إلى غرفة الخوادم أو تعطل الخوادم بسبب عطل كهربائي.

– ويتم بوضع الخوادم بغرف خاصة واستخدام أبواب لا تفتح إلا بالبصمة مثلاً واستخدام مولدات كهرباء بديلة حال حدوث أي مشكلة في الكهرباء.

– كما تشمل أيضاً استخدام أجهزة المستخدمين أو سرقتها سواء داخل المنظمات أو خارجها وتكمن الحماية هنا بوضع كلمات سر على الأجهزة وتشفير المعلومات المهمة داخلها.

٢- وسائل الحماية الفنية أو حماية البنية التحتية لتكنولوجيا المعلومات :

البنية التحتية لتكنولوجيا المعلومات هي الإطار الكامل للوسائل المادية والبرمجية المطلوبة لتشغيل المنظمات وتشمل أجهزة الحاسب والشبكات والأنظمة البرمجية وأنظمة إدارة قواعد البيانات والتطبيقات.

وهي تقنيات لتحديد وإثبات هوية المستخدم وصلاحياته ومسؤولياته مثل (كلمة المرور، التشفير، الجدران النارية، البرامج المضادة للفيروسات، التوقيع الرقمي، القياسات الحيوية عين، يد صوت DNA).

٣- وسائل الحماية الإدارية:

وهي إعداد وصياغة سياسات أمن المعلومات، وتتضمن:

آ- تشريعات داخل المؤسسة لتنظيم أمن المعلومات، وتحديد المسؤوليات والأدوار.

ب- تحديد ما هو مسموح به، وما هو غير مسموح به للتعامل مع المعلومات ونظمها، وكأمثلة عليها نذكر البريد الإلكتروني، كلمات المرور، الخصوصية، اتفاقية صلاحيات المستخدم وقبول استخدام النظام.

٤) وثيقة سياسة أمن المعلومات:

تسعى المنظمات لحماية أمن معلوماتها، ولأن أمن المعلومات يشمل الأمن المادي والبرمجي والمستخدمين، ولأن قدرات المنظمات تختلف، مما أدى إلى أن تضع المنظمات سياسات أمن معلوماتها حسب إمكانياتها وأهمية المعلومات، وذلك بإعداد وثيقة تدعى سياسة أمن المعلومات، والتي تشمل التشريعات والقوانين اللازمة لحماية أمن المعلومات في المنظمة.

٥) الانذار المبكر والقدرة على التعامل مع حالات الهجوم والكوارث:

مهما كانت قوة الحماية في الأنظمة فلا يوجد نظام آمن بنسبة ١٠٠%، لذا فإن وضع استراتيجيات لمراقبة الأنظمة والتعامل مع الحالات في وقت مبكر أثناء الهجوم أو الكارثة يساعد على الحد من النتائج الكارثية على المنظمات.

٦) التعافي السريع بعد الهجمات والكوارث:

لا تنتهي استراتيجيات الحماية بمجرد انتهاء الهجمات أو الكوارث ولكن القدرة على التعافي السريع بعد وقوع المشاكل يعد أمراً مهماً جداً، ويشمل ذلك إرجاع المعلومات المفقودة من أنظمة النسخ الاحتياطي، وفحص وإصلاح المشاكل في الأنظمة والأجهزة، وتعد قلة الوقت المستغرقة للتعافي من الكوارث والهجمات دليل على قدرات المنظمات في مجال أمن المعلومات.

من أهم الطرق المستخدمة في حماية نظم المعلومات هي تطبيق إجراءات الرقابة الداخلية والتي يمكن معالجتها ومناقشتها من خلال ثلاثة مستويات هي:

المستوى الأول: إجراءات تتعلق بالرقابة الوقائية ونذكر منها:

آ- التوعية والتدريب المستمر لمستخدمي النظام المعلوماتي بالسياسات المتبعة والمتعلقة بأمن المعلومات.

ب- تقييد الدخول على النظام المعلوماتي والشبكة الحاسوبية بالأشخاص المصرح لهم بذلك.

ج- تحديد صلاحيات مستخدمي النظام المعلوماتي بما يتناسب مع حجم ونوع الأعمال الموكلة لهم.

د- استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة في الدخول إلى النظام المعلوماتي.

المستوى الثاني إجراءات تتعلق بالرقابة الاكتشافية وهي:

آ- إنشاء سجل دخول إلى النظام المعلوماتي.

ب- اختبار النظام والتدقيق عليه بشكل دوري.

المستوى الثالث إجراءات تتعلق بالرقابة التصحيحية وهي:

آ- وجود فريق استجابة للتهديدات التي يتعرض لها النظام المعلوماتي.

ب- تحديث البرمجيات المتخصصة بشكل دوري كتحديث برامج مضادات (مقاومات) الفيروسات.

طرق الوقاية والحماية

- في الغالب تختلف طرق الحماية سواءً في أمن المعلومات أو في الخصوصية بحسب نوع المهدد، ولكن هناك نصائح عامة تفيد في الحماية بشكل عام في أغلب المهددات ومنها:

١) التأكد من تحديث نظام التشغيل:

- يعتبر التأكد من أن نظام التشغيل محدث من أهم إجراءات الحماية، حيث يتم رقع الثغرات المكتشفة من قبل الشركة صانعة نظام التشغيل.
- يشمل ذلك كل أنظمة التشغيل مثل الويندوز أو اللينكس أو الماكنتوش، كما يشمل أنظمة تشغل الأجهزة الأخرى.
- كما يجب التأكد من أن نظام التشغيل جديد بحيث مازالت الشركة الصانعة للنظام تقوم بتحديثه لأن الشركات تتوقف عن رقع الثغرات لأنظمة التشغيل القديمة.

٢) استخدام برامج مضادة للبرامج الخبيثة:

- تساعد البرامج المضادة للبرامج الخبيثة باكتشاف بعض أنواع البرامج الخبيثة والمساعدة على الحماية منها أو مسحها.
- تستطيع البرامج المضادة الفيروسات Anti-Virus Software اكتشاف أنواع الديدان وأحصنة طروادة وبرامج التجسس وغيرها، والمساعدة على الحماية منها أو مسحها.

٣) استخدام جدار ناري Firewall:

- يعد الجدار الناري من أهم طرق الحماية من الاختراق والتجسس، حيث يتيح التحكم والحماية من دخول أجهزة أخرى على الجهاز المستخدم.
- يعمل الجدار الناري بحسب القوانين التي يضعها المستخدم وكلما كانت صارمة يكون أكثر أماناً ولكن تقل قابلية الاستخدام.
- ويمكن عن طريق الجدار الناري السماح وعدم السماح للبرامج بالاتصال بأجهزة بعيدة كما يمكن تحديد المواقع التي يمكن زيارتها أو المحجوبة وفتح وغلق المنافذ "Ports" المستخدمة في الاتصال لتلك البرامج.

٤) المحافظة على تحديث برامج جهازك (التحديث التلقائي):

إن بناء البرمجيات هي عملية معقدة ولا تخلو من أخطاء كما أنها بحاجة إلى تحسينات مستمرة تبعاً لظروف استخدامها وطلبات المستخدمين وتزايدات قدرات الأجهزة، ومن ناحية أخرى فإن الحاجة إلى التحسين المستمر يفرضها وجود الثغرات الأمنية التي تكتشف بشكل مستمر في هذه البرمجيات، مما يحتم إغلاق تلك الثغرات قبل أن تستغل وإغلاقها يتطلب تحديث البرمجيات وقد بينت التجارب والواقع العملي أن اكتشاف الثغرات كان يتم من قبل المتطفلين قبل شركات صنع البرمجيات حيث يقوم المتطفلون بتطوير برامج خبيثة تستغل هذه الثغرات، ومن أجل تحسين البرمجيات فهناك أمران يجب أن يؤخذا بعين الاعتبار وهما:

١ - إدخال وظائف جديدة أو تحسين الوظائف الموجودة في البرنامج.

٢ - سد الثغرات الأمنية المكتشفة في البرمجيات للحد من احتمال اختراقها من قبل المتطفلين.

نظراً لأن الفيروسات تتغير باستمرار، فمن الأهمية بمكان قيامك بالتحديث المستمر لنظام التشغيل الموجود في جهازك، وبرنامج جدار الحماية الناري وبرنامج مكافحة الفيروسات المركب في جهازك، وبحيث يتم إدخال آخر تحديثات صدرت عن هذه البرامج، وسيقوم برنامج مكافحة الفيروسات بسؤالك تلقائياً بتحديث البرنامج، وعليك التأكد من قيامك بالتحديث، علماً بأن الكثير من برامج مسح الفيروسات يمكن الحصول عليها مرة كل سنة، وينصح بترقية البرنامج بعد ذلك حفاظاً على تضمين جهازك آخر التحديثات.

إن مطالبة مستخدمي البرمجيات تحديثها بأنفسهم قد يكون صعباً من الناحية العملية، وبدلاً من ذلك فقد وفرت العديد من الشركات المصنعة للبرمجيات خاصية التحديث التلقائي أو الآلي من خلال قيام البرنامج المثبت في الحاسوب بالاتصال بالشركة الأم عند وجود التحديثات وإن وجد منها شيء بادر البرنامج بتنبيه المستخدم إلى ذلك، وعموماً تكون عملية التحديث التلقائي من المراحل التالية:

أ- مرحلة اتصال جهاز الحاسوب بالموقع الإلكتروني للشركة المصنعة.

ب- مرحلة البحث عن التحديثات التي لم يسبق تحميلها إلى جهاز الحاسب.

ت- مرحلة التحميل.

ث- مرحلة التنصيب.

ج- مرحلة فصل الاتصال.

لذلك تأتي أهمية التحديث التلقائي من أن البرامج لا يمكن أن تخلو من الأخطاء وتسعى الشركات المصنعة للبرامج إلى إصدار تحديثات لمعالجة تلك الأخطاء ومن أجل توفير الحماية للنظام المعلوماتي يجب تنزيل تلك التحديثات لبقاء البرامج في أفضل أوضاعها.

٥) الحذر عند إقفال النوافذ المنبثقة:

النوافذ المنبثقة: هي النوافذ التي تقفز على شاشة الحاسب لديك عند ذهابك إلى مواقع إلكترونية محددة، وبعض هذه المواقع تحاول خداعك لتنزيل برامج تجسس، أو برامج دعائية في جهازك من خلال الضغط على خيار موافق (OK) أو اقبل (Accept) الموجودة في النافذة المنبثقة، وعليك إتباع وسيلة آمنة لإقفال هذه النوافذ ألا وهي: الإقفال من مربع العنوان (X) الموجود في أعلى النافذة.

٦) لا تفتح رسائل البريد الإلكتروني المشكوك فيها:

تصل معظم الفيروسات إلى أجهزة الحاسب عبر البريد الإلكتروني، لذا لا تفتح أي مرفقات بريد إلكتروني لا تعرف مصدره أو غير متأكد من محتوياته حتى ولو كنت تستخدم برنامج مكافحة فيروسات، مع ملاحظة أنه يمكن أن تصلك رسائل بريد إلكتروني مصابة بالفيروسات حتى من أصدقائك وزملائك والمسجلين لديك في قائمة البريد الإلكتروني، ولا يكون الفيروس خطيراً إلا إذا فتحت المرفقات المصابة، وتأكد من أن محتويات الرسالة تبدو منطقية قبل فتح المرفقات، كما يجدر بك ألا تقوم بتمرير أو إحالة أي مرفقات قبل أن تتأكد من أنها آمنة، وقم بحذف أية رسالة تعتقد أنها مصابة، وكذلك قم بتفريغ الرسائل المحذوفة من المجلد الذي يحتوي عليها بشكل منتظم.

٧) النسخ أو التخزين الاحتياطي Backup:

- يعد النسخ الاحتياطي من أهم طرق الوقاية من فقد البيانات سواءً على مستوى المؤسسات أو حتى على مستوى الأفراد.
- فعند وجود نسخة احتياطية من البيانات والمعلومات في مكان آمن فإنه مهما حصل من فقد لأي معلومات ولأي سبب كان، كالكوارث التقنية أو الطبيعية أو الأخطاء البشرية أو مهما حصل من حوادث أخرى لهذه المعلومات كإصابة الأجهزة بفيروس أو تشفيرها ببرامج الفدية، فإنه من السهل الرجوع للنسخة المحفوظة في المكان الآمن واستعادة المعلومات إلى أقرب وقت ممكن.
- إن المؤسسات الكبرى، والتي تحتاج إلى كل البيانات المدخلة لحظة بلحظة كالبنوك مثلاً، فإنه لا مجال لفقد أي بيانات مدخلة، حيث تتم بها عمليات النسخ الاحتياطي بشكل آلي وبأجهزة وأنظمة خاصة.
- أما بالنسبة للأفراد، فإن عمل نسخة احتياطية من ملفاته الموجودة في الأجهزة الخاصة به ولو بشكل شهري كفيلة بالحد من فقد المعلومات لأي سبب كان.

يتألف التخزين الاحتياطي من:

- البيانات المراد تخزينها من ملفات ومجلدات وبرامج.

- وسيلة أو أداة التخزين (أقراص مرنة، صلبة، مدمجة، فلاشات، .. إلخ) وتختلف هذه الوسائل عن بعضها البعض بسعتها وعمرها الافتراضي وسعرها.

- برنامج التخزين الذي سيقوم بتخزين واسترجاع البيانات، وأفضل هذه البرامج هو Norton Ghost، والذي يأخذ نسخة (صورة مماثلة) كاملة لما في جهاز الحاسوب من برامج وملفات.

تدابير النسخ الاحتياطي

من أهم التدابير اللازمة لعمل النسخ الاحتياطي نذكر:

- ١- وضع جدول زمني للنسخ الاحتياطي بحيث يكون هناك نسخ يومية، أسبوعية، شهرية، وسنوية.
- ٢- أخذ نسخ احتياطية كاملة وأخرى للإضافات اليومية فقط بحيث يشمل كل منهما جميع معلومات المنشأة بما في ذلك جميع قواعد البيانات والملفات ومعلومات حسابات المستخدمين.
- ٣- يجب أن تكون المعلومات المنسوخة حديثة ويفترات زمنية متقاربة حتى يمكن استعادة آخر تحديث على المعلومات عند الحاجة.
- ٤- تخزين أشرطة أو وسائط النسخ الاحتياطي في أماكن تخزين مناسبة ومعدة لهذا الغرض.
- ٥- القيام بعملية استرجاع Restore للمعلومات من وسائط النسخ الاحتياطية إلى أجهزة فعلية مشابهة تماماً للأجهزة العاملة دورياً من أجل التأكد من صحة عملية الاسترجاع نفسها وأنه يمكن تنفيذها في أي وقت متى ما دعت الحاجة إلى ذلك وكذلك التأكد من سلامة النسخ الاحتياطية.

٨) التفكير ملياً قبل تنزيل ملفات من الإنترنت:

يمكن كذلك أن تُصاب بفيروسات وبرامج دعاية وبرامج تجسس من خلال تنزيل برامج وملفات أخرى من الإنترنت، فإذا كان البرنامج مجانياً ومزود من قبل مطور برمجيات مجهول، فهو من المرجح أن يحتوي على برمجيات إضافية وغير مرغوب فيها أكثر مما لو كنت قد قمت بتنزيل أو شراء برنامج من مطور برمجيات مشهور ومرموق، ولحسن الحظ، فإن نظام الترشيح المعمول به يحمي مستخدمي الإنترنت من الدخول مصادفةً إلى معظم المواقع الإلكترونية الخطيرة، ولكن من الحكمة والتعقل توخي الحذر عند تنزيل ملفات من الإنترنت أو إقفال النوافذ المنبثقة غير المرغوب فيها.

٩) إجراءات التحقق أو المصادقة Authentication:

- وهي إجراءات للتحقق من هوية مستخدم ما، فمثلاً عند كتابته اسم المستخدم للدخول على البريد الإلكتروني سوف يطلب النظام كلمة المرور ليتحقق من أن هذا المستخدم هو نفسه صاحب الحساب، ويمكن تصنيفها على ثلاثة أشكال:
- شيء يعلمه المستخدم: ومن أشهرها كلمة المرور والأرقام السرية.
- شيء يملكه المستخدم: مثل البطاقات أو أجهزة الجوال.
- شيء هو جزء من المستخدم أو يستطيع عمله: مثل بصمات الحيوية "biometric"، وأشهرها بصمات الأصبع والصوت والعين، أما ما يستطيع عمله المستخدم فأشهر مثال عليه هو التوقيع.

لغرض تنظيم و وصول الأفراد
الى المعلومات تتبع
عدة أساليب، أهمها :

Damascus University

١- كلمة السر (Password)



كلمة المرور: هي أحد مكونات منظومة حماية المعلومات فهي تساعد على التحقق من هوية المستخدم وفعاليتها تعتمد على درجة انضباط العنصر البشري في اختيار كلمة المرور والتعامل معها وفق الأساليب الصحيحة.

تشبه كلمة المرور مفتاح البيت من حيث الوظيفة، فكلاهما يمثلان أداة تخول الشخص الدخول لمكان خاص لا يدخله إلا أشخاص معينون وهي تساعد على التحقق من هوية المستخدم.

إن أول باب يطره المهاجم هو محاولة الحصول على كلمات المرور الضعيفة، ومن طرق حصول المهاجم على كلمات المرور ذكر:

١ - تصديع Cracking كلمات المرور الضعيفة.

٢ - استخدام الهندسة الاجتماعية.

٣ - البحث والتنصت التقليدي كالوقوف خلف أو بجانب الضحية عند كتابة كلمة المرور أو البحث عن كلمة المرور مكتوبة تحت لوحة المفاتيح، أما الطرق الحديثة فتعتمد على تركيب أو تحميل برنامج صغير يسجل جميع الأحرف والأرقام المدخلة عن طريق لوحة المفاتيح، كما يمكن معرفة كلمات المرور بطريقة أخرى فعند تخزين كلمة المرور في النظام كالدخول إلى الانترنت أو البريد الشخصي أو بعض الإعدادات الشخصية، فإنك عندما تعاود الدخول أو الاتصال فتظهر كلمة المرور المخزنة ولكن بهيئة نجوم أو دوائر صغيرة للتعتيم فقط ولكن هل هذا التعتيم آمن؟ للأسف الجواب لا. فهناك برامج متاحة لمعرفة ما تحت هذا التعتيم وهي برامج معرفة كلمات المرور المنسية.

المصادقة (الاستيقان) في الأنظمة المعلوماتية: هو إجرائية التأكد من كون الشخص الذي يحاول النفاذ إلى مورد ما هو المصرح له (شرعي، أصلي).

مثال: يركن موظف ما سيارته في الموقف المخصص للشركة أو المؤسسة التي يعمل بها ومن ثم يقفل باب السيارة باستخدام المفتاح أو جهاز التحكم عن بعد ويدخل من الباب الرئيسي للشركة حيث يتعرف عليه حارس المبنى ويركه يدخل وعندما يصل إلى القسم الذي يعمل فيه يقوم بإدخال رمز دخول أو (بطاقة تعريف) يعرفه على الجهاز لكي يفتح له باب الدخول إلى القسم.

لقد استخدم الموظف في هذا المثال ثلاثة أنواع من المصادقة وهي:

١ - قفل السيارة بمفتاح يملكه.

٢ - تعرف حارس المبنى عليه أو على ما يكون.

٣ - أدخل رمز الدخول الذي يعرفه.

إذاً، يمكننا تحقيق المصادقة بالاعتماد على ما يعرفه الشخص (كلمات مرور)، أو على ما يملكه (البطاقة، القطعة)، أو على ما يكون (القياس الحيوي).

الطريقة الشائعة لإعطاء حق الوصول إلى المعلومات تتمثل بكلمة مرور (أحرف، أرقام، رموز أو مزيج منهم) يعرفها المستخدم المعني فقط، ولا يسمح للمستخدم بالوصول إلى المعلومات المحمية دون إعطاء كلمة السر المطلوبة.



- تتميز هذه الطريقة بسهولةها، حيث أن لكل مستخدم كلمة سر واحدة.
- من سيئات هذه الطريقة الحاجة إلى حماية كلمة السر لكي لا يعرفها الآخرون، ويتحقق ذلك من خلال عدم كتابتها، أو البوح بها، واختيار كلمة السر التي يصعب توقعها.

لذا يتحتم علينا الأمور التالية:

١ - الاختيار الأمثل لكلمة المرور لكي لا تكون سهلة التخمين.

٢ - المحافظة عليها وعدم اطلاق الغير عليها.

٣ - تغييرها دورياً.

تعد كلمات المرور التقنية الأكثر انتشاراً في التعريف والوثوقية، وتعد تقنية التعريف الأضعف وذلك للأسباب التالية:

- عادةً يختار المستخدمون كلمات سهلة عليهم حفظها، وبالتالي يسهل تخمينها من قبل المهاجمين.

- كلمات المرور المولدة عشوائياً يصعب حفظها، لذلك لابد من تخزينها، وهذا يعرضها للسرقة.

- غالباً ما يتشارك المستخدمون كلمات المرور مما يسهل كشفها.

أقسام كلمة المرور

من الممكن تقسيم مخططات تحديد الهوية باستخدام كلمات المرور (السر) إلى فئتين وهما:

١ - كلمة السر الثابتة Fixed Password: وهي كلمات السر المستخدمة مرات ومرات مع كل محاولة وصول ويتوفر مخططات لبنائها وتحقيقها مثل:

أ - ملفات كلمة السر الموجودة بشكل افتراضي في أنظمة التشغيل.

ب - تهشير كلمات السر: وذلك يتطابق تابع التهشير عليها بغية ضمان سريتها وتخزينها ضمن جدول أو ملف كلمات السر.

ج - تلميح كلمات السر: حيث تقدم هذه الطريقة حلاً لمشكلة الهجوم باستخدام قاموس لكشف كلمة السر كما يمكن التقليل من ذلك بزيادة طول كلمة السر أو إضافة سلسلة عشوائية من الحروف إليها.

٢- كلمة السر لمرة واحدة One Time Password: حيث تعتمد فكرة هذا النوع على استخدامها لمرة واحدة فقط ويوجد ثلاث طرق لتحقيق ذلك وهي:

آ- استخدام كلمة من بين مجموعة من كلمات السر المتفق عليها بين المستخدم والنظام المعلوماتي.

ب- التوافق بين المستخدم والنظام المعلوماتي على تغيير كلمة السر تسلسلياً.

ج- التوافق بين المستخدم والنظام المعلوماتي على إنشاء كلمات سر يمكن تعديلها تسلسلياً باستخدام تابع التهشير.

الاختيار الأمثل لكلمة المرور

لتكوين كلمة مرور قوية علينا اتباع الخطوات التالية:

آ- لا تكون كلمة المرور من كلمة واحدة.

ب- لا تضمن كلمة المرور معلومات شخصية مثل تاريخ الميلاد، اسم البلد، اسم شخص تحبه، أو لون تحبه، ... إلخ.

ج- ينبغي ألا تقل كلمة المرور عن ١٠ خانات لأن السرعة الفائقة للحواسيب الحديثة تجعل من تصريح كلمة المرور اكتشافها أمراً يسيراً.

د- كون كلمتك من خليط من الحروف (كبيرة، صغيرة) وأرقام ورموز ... إلخ.

هـ- استخدم اختصار جملة فمثلاً: I live in Emirate Since 1990
1Lv@3\$1990. لاحظ كيف استبدلنا حرف I بالرقم 1 واستخدمنا الحرف L بصيغة الكبيرة واستبدلنا in بحرف @، S بـ \$ والرقم 1 بحرف 1 والرقم 0 بالحرف O.

٢- بطاقة الوصول (Access Card)

في الحالات التي لا تكون كلمة السر كافية

يمكن استخدام بطاقات خاصة للوصول.

البطاقة Cards: يوجد عدة أنواع من البطاقات التي يمكن استخدامها، فالبطاقات الذكية تحوي على رقاقة دارة متكاملة قادرة على تخزين معلومات يمكن استخدامها أثناء عملية المصادقة.

لمنع سرقتها عادة ما تستعمل هذه البطاقات مع كلمة سر قصيرة ، كما هو متبع في أجهزة الصراف الآلي في المصارف.



النوع الآخر من الثبوتيات التي يستطيع مستخدم ما بتقديمها تأتي على شكل قطع Tokens، أو بطاقات Cards يملكها، فالقطعة، هي جهاز صغير يمكن وضعه ضمن حمالة المفاتيح مزود بشاشة عرض وتتشارك القطعة مع مخدم مصادقة مركزي (خوارزمية فريدة)، حيث تولد القطعة رمزاً كل ٣٠ أو ٦٠ ثانية ويكون هذا الرمز صالحاً لمدة محددة تعرض على الشاشة وعندما يريد المستخدم الدخول فإنه يدخل اسم المستخدم والرمز الذي يظهر على شاشة القطعة، وما أن يستقبل مخدم المصادقة المعلومات حتى يقوم بالبحث عن الخوارزمية المقابلة للمستخدم ويولد رمزاً خاصاً به ويقارنه مع الرمز المستقبل من المستخدم حتى يسمح للمستخدم بالدخول في حال تطابق الرمزين ولا يحتاج المستخدم إلى حفظ كلمة المرور وإنما يكفيهِ امتلاك القطعة.

يوجد بعض أنواع من القطع التي تطلب كلمة مرور أيضاً وهذا ما يسمى بالمصادقة متعددة العوامل، وهناك نوع آخر من القطع يطلب من المستخدم خلق رقم شخصي PIN الذي يراكب مع الرمز المولد لتكوين رمز مرور، فمثلاً إذا كان $PIN = 1346$ ، والكود 22497، فإن المستخدم يدخل رمز الدخول التالي: 134622497.

تتميز القطع بعدة محاسن مقارنةً بكلمات المرور ومنها:

- ١ - كلمات المرور تكون ساكنة ولا تتغير طالما المستخدم لم يقم بذلك.
- ٢ - كلمة المرور التي تولدها القطعة لها مدة حياة قليلة جداً (حوالي الدقيقة) وهي تتغير باستمرار لذلك يطلق عليها اسم كلمة المرور لمرة واحدة أو ما يعرف بـ: OTP: One Time Password.



٣ - معلومات بيولوجية (Biometrics)



كلمة إغريقية مكونة من جزئين هما Bio وتعني الحياة، و Metrics وتعني القياس.

القياس الحيوي: هو العلم الذي يستخدم التحليل الاحصائي لصفات الانسان الحيوية، وذلك للتأكد من هويتهم الشخصية باستخدام صفاتهم الفريدة، ولها قسمين هما:

١- صفات فيزيائية (بصمة اصبع، يد، قزحية العين، الوجه، الحمض النووي DNA).

٢- صفات سلوكية (صوت، توقيع يدوي، ضربات لوحة المفاتيح).

٣- المعلومات الحيوية المعرفية: تعتمد المعلومات الحيوية المعرفية على امكانات التمييز واجراءات التفكير والفهم لدى المستخدم، حيث تعتبر هذه الطريقة سهلة بالنسبة للمستخدمين لأنها تعتمد على تذكر أحداث من الحياة الطبيعية كما تصعب عملية شن الهجوم، وكأمثلة على المعلومات الحيوية المعرفية نذكر الطلب من المستخدم التعرف على الوجوه أو سؤال المستخدم أسئلة متعلقة بحادثة معينة حصلت ضمن حدث ما خلال تقضية إجازة أو أثناء حفل الزفاف (كم كان عمرك عندما تزوجت؟ أو عندما تخرجت؟

تستخدم هذه التقنية لتعريف المستخدم فقط، أي عندما يكون الموضوع هو إنسان، وتعتمد هذه التقنية على اختبار صفة سلوكية أو فيزيولوجية تكون معرفة للموضوع بشكل وحيد وتتخذ كطابع مميز له.

تعمل نظم التعريف من هذا النوع على الشكل التالي:

تحول المواصفات الفيزيائية إلى نماذج رقمية لتخزن في قواعد المعطيات وعندما يقدم المستخدم نفسه من أجل الوثوقية تقاس الصفات الفيزيائية من قبل قارئ وترمز رقمياً ثم تقارن مع النموذج المخزن.

وهذه الطرق تتطلب جهاز خاص للقراءة قبل إرسالها للحاسوب والتأكد.

تتميز القياسات الحيوية عن كلمات المرور بالآتي

١ - إنها لا تحتاج إلى تذكر كلمات بل تحتاج إلى صفات بشرية للتعرف على المستخدم.

٢ - يصعب إعطاء غيرك هذه الصفات للدخول إلى النظام.

٣ - هذه الصفات دائماً مع الشخص ويصعب نسيانها أو انتفاؤها عنه.

يوفر القياس الحيوي عدد من المزايا ولعلا أهمها:

١ - الأمن والخصوصية وذلك من خلال:

- منع الأشخاص الآخرين من الدخول غير المصرح لهم على البيانات الشخصية.
- إيقاف سرقة الهوية مثل استخدام البطاقات الائتمانية أو الشيكات المسروقة.

٢ - البديل لحمل الوثائق الثبوتية (هوية شخصية، رخصة قيادة، ... إلخ).

٣ - البديل لحمل المفاتيح للدخول إلى البيت، المكتب، السيارة.

٤ - تأمين سرية العمليات المالية (مكائن الصراف الآلي ATM، التجارة الإلكترونية).

تسجيل الدخول الوحيد :Single Sign On

تتجلى المشكلة الأساسية في استخدام كلمات المرور في حاجة المستخدم إلى عدة كلمات مرور لعدة منصات عمل وأنظمة تشغيل، الأمر الذي يؤدي بالمستخدم في النهاية إلى استخدام كلمة مرور واحدة لجميع الحسابات وهذا ما يجعلها سهلة الكسر، ويكمن حل هذه المشكلة في توفير اسم مستخدم وكلمة مرور واحدة للمستخدم يستخدمها للدخول إلى جميع الحسابات، وهذه الفكرة هي وراء إدارة الهوية Identity Management التي هي استخدام ثبوتيات مصادقة واحدة مشارك بها على جميع الشبكات وعندما تكون الشبكات مملوكة لمؤسسات مختلفة فيطلق عليها اسم إدارة الهوية الموحد أو ما يعرف بـ:

FIM: Federated Identity Management ويعتبر الدخول الوحيد هو أحد تطبيقات FIM حيث تستخدم ثبوتيات مصادقة واحدة للدخول إلى عدة حسابات أو تطبيقات.

يوجد عدة تحقيقات لما يعرف باسم نظام Web Based FIM وهي:

١ - هوية Windows Live ID: تطورت هذه الهوية من

Net Passport إلى Microsoft Passport Network حتى أخذت الاسم الحالي عام ٢٠٠٦ وتعتمد هذه الطريقة على خلق اسم مستخدم وكلمة مرور على مخدم مركزي كما تعتمد أيضاً على توليد كوكيز عامة مشفرة محدودة زمنياً ولصيقة هوية مشفرة أيضاً وتخزينهما عند حاسوب المستخدم بغية المصادقة من أي موقع ويب يعتمد هوية ويندوز حيث يقوم موقع الويب بعد المصادقة على توليد كوكيز أخرى محلية ومشفرة ومحدودة زمنياً وهذه الطريقة مطبقة فقط في شركة مايكروسوفت العالمية أو بعض الشركات التي تدور في رحاها.

٢- هوية Open ID: هي عبارة عن FIM غير مركزية ومفتوحة المصدر ولا تحتاج إلى تثبيت أي برنامج على حاسوب المستخدم، أي هي عبارة عن نظام يعتمد على URL-Based، والهوية هي URL مدعومة باسم مستخدم وكلمة مرور حيث تزود Open ID وسيلة التحقق من كون المستخدم يملك URL محددة.

٣- هوية Oauth: Open Authorization: حيث تسمح هذه الهوية مفتوحة المصدر للمستخدمين بمشاركة موارد موجودة ضمن موقع مع موقع ثان دون توجيه ثبوتياتهم إلى الموقع الثاني كما يسمح أيضاً لعدة تطبيقات بمشاركة المعطيات عبر المواقع.

١٠) طمس البيانات (Wiping): يظن المبتدئون في تعلم الحاسوب أنه بمجرد حذف ملف ما، فإنه يكون قد فقد نهائياً، ولا يعلمون أن الملف قد تم نقله إلى سلة المحذوفات ويمكن استرجاعه، ويظن كثيراً من المستخدمين أن حذف الملف من سلة المحذوفات هو الإتلاف النهائي لهذا الملف، وهذا غير صحيح، فحذف ملف ما من وحدة التخزين يتم بحذف المؤشر الذي يدل عليه وليس الملف نفسه، أي أن محتويات الملف تظل في وحدة التخزين ولكن على هيئة مساحة فارغة يمكن الكتابة عليها، ولما كان كذلك، فإنه يمكن بواسطة برامج استرجاع متخصصة استرجاع ذلك الملف، وعملية طمس البيانات في وحدات التخزين تتم بالكتابة المتكررة على البيانات الموجودة ببيانات عشوائية وبعدها مرات، وهناك معايير معروفة لطمس البيانات، فمثلاً، معيار وزارة الدفاع الأمريكية يتطلب طمس البيانات بالكتابة عليها ٧ مرات ومعيار Peter Gutmann الكتابة ٣٥ مرة. يوجد ثلاثة أنواع لطمس البيانات وهي:

١- طمس الملف عند حذفه.

٢- طمس المساحة الفارغة في وحدة التخزين.

٣- طمس ما يعرف بملف المبادلة (Swap File)، وهو ملف خاص بنظام التشغيل الذي يستخدم لدعم الذاكرة الافتراضية.

(١١) الإخفاء (المواراة) Steganography: تعني هذه الكلمة باليونانية الكتابة المغطاة Covered Writing، ويفيد هذا الأسلوب في إخفاء الرسالة وتغطيتها بشيء آخر (ضمن نص آخر أو ضمن صورة)، ويمثل الاخفاء أسلوباً بديلاً للتشفير، والذي يعمل على إخفاء الرسالة باستخدام بعض الأساليب والفرق بين الاخفاء والتشفير يتمثل بأن الاخفاء حقيقة وجود الرسالة أصلاً بينما تبقى أساليب التشفير النص ظاهراً ومبهم والإخفاء يحتاج إلى مجهود كبير لإخفاء قليل من ثنائيات المعلومات فيما يمثل قصوراً لهذا الأسلوب، وفي بعض التطبيقات يتم تشفير الرسالة أولاً ثم يتم إخفائها لمزيد من السرية.

أساليب الإخفاء:

١- تعليم الحروف: وهنا يتم الكتابة فوق الحروف المختارة المطبوعة وذلك باستخدام قلم رصاص مثلاً، بحيث لا تكون الحروف المضافة مرئية ما لم تتوجه الورقة بزاوية محددة بالنسبة للضوء.

٢- الحبر السري (غير المرئي): هناك العديد من المواد التي تستخدم بحيث لا تترك أي أثر عند الكتابة بها، ويتم إظهار الكتابة عند تعرض الورقة للحرارة أو مواد كيميائية معينة.

٣- التنقيب بالدبوس: وهنا يتم إحداث ثقوب دقيقة فوق حروف مختارة من الرسالة المطبوعة بحيث لا تكون هذه الثقوب مرئية ما لم تتعرض الورقة مباشرة للضوء.

٤- إخفاء الرسالة في عناصر الصورة (Pixels) الأقل أهمية في المناظر والصورة.

تشفير المعلومات

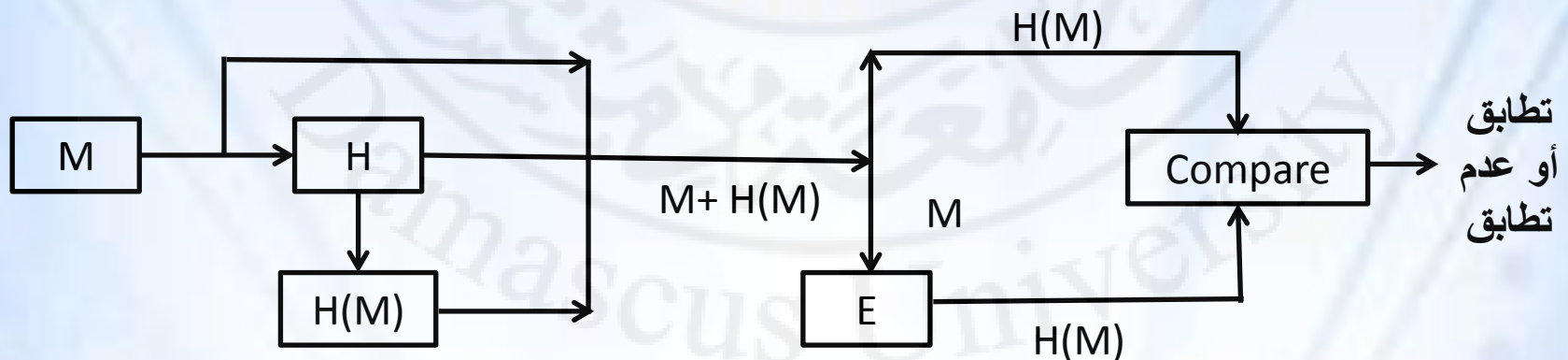


Cryptography مصطلح يدل على التعمية، وهي كلمة يونانية وتعني **Secret Writing** كتابة الأسرار أو الكتابة السرية ولكن هذه الكلمة ترمز لنا إلى علم وفن تحويل الرسائل لتصبح آمنة ضد كافة أشكال الهجوم وكانت هذه التقنية تقتصر في الماضي على أساليب التشفير **Encryption** وفك التشفير **Decryption** للرسائل المتبادلة باستخدام مفاتيح سرية، أما اليوم فهي تدل على ثلاث تقنيات مختلفة ورئيسة يمكن استخدامها كوحدات بناء أساسية لتحقيق عناصر أمن المعلومات كالتحقق من الهوية والتحكم بالوصول والسرية وسلامة المعلومات وتكاملها وهي:

- ١ - التشفير بنوعيه المتماثل **Symmetric Encryption** وغير المتماثل **Asymmetric Encryption**.
- ٢ - التصديق (التوقيع) الرقمي **Digital Signature**.
- ٣ - البصمة الرقمية أو القيمة المركزة **Hash Value**: وهي سلسلة قصيرة وثابتة الطول من البتات تشكل بصمة فريدة لكل رسالة وإن أهم ما يميز البصمات الرقمية هو أن أي تعديل ولو كان بسيطاً جداً في الرسالة ينتج عنه تغير كبير في البصمة الرقمية.

ف عندما تكون الرسائل طويلة (قد يصل طولها في بعض الأحيان إلى مئات الصفحات) مما يجعل تطبيق التصديق أو التوقيع الرقمي عليها صعباً جداً، ومن هنا جاءت البصمة الرقمية لتحل مشكلة التعامل مع الرسائل الطويلة.

ويجري التهشير وفقاً لهذه التقنية بإنشاء تلخيص من طول ثابت لمحتوى الرسالة **Fixed Length Digest**، وهو أصغر بكثير من الرسالة، ويجري بعدها إرسال الرسالة وملخصها إلى الطرف الثاني الذي يعيد بدوره إنشاء ملخص للرسالة المستقبلية لمطابقته مع ملخص الرسالة المرسل في الأصل، فإذا حدث التطابق، فهذا يعني أن الرسالة صحيحة، ولم يطرأ على محتواها أي تعديل، والشكل التالي يوضح ذلك:



* من الناحية التاريخية يمكن القول بأن تقنيات أمن الاتصال قديمة قدم التاريخ، ولكن علم الاتصالات المعماة قد تبلور على يد العرب، فمن مصطلحات الرياضيات العربية انتقلت كلمة صفر "Cipher" إلى الغرب، والتي استخدمت لتشير إلى التشفير أو التعمية، وقد أشارت دراسة ديفيد_كان إلى أن أول دراسة كاملة عن علم الاتصال المعماة مكتوبة كجزء من موسوعة "صبح الأعشى" من قبل الكاتب العربي "شهاب الدين أبو العباس بن علي بن أحمد عبد الله القلقشندی" الذي عاش في مصر، وقد أتم هذه الموسوعة في عام ١٢٤١م، إلا أنه اعتمد في كتابه ذلك على مغلطات العلامة العربي "تاج الدين بن محمد الموصلي" والملقب "ابن الدريهم"، وأهمها "مفتاح الكنوز في إيضاح المرموز" الذي عاش ١٣٦١م بين المماليك، وقد أثبتت الدراسات الحديثة إلى أن علم الاتصالات السرية قد ولد قبل "ابن الدريهم" بخمسة قرون، وذلك على يد العلامة العربي "يعقوب بن إسحاق الكندي"، والذي توفي ٨٧٣م، وأشهر أعماله "رسالة استخراج المعنى".

ظهرت التعمية قبل حوالي ألفي عام، واقتصرت على الكتابة السرية وانشصر استخدامها على التطبيقات العسكرية والحكومية.
Cryptography: مصطلح يدل على التعمية.
Encryption: مصطلح يدل على التشفير.



عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري، فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة، وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير "يعقوب بن اسحاق الكندي"، واستخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب، فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو.

* يرجع تاريخ الكتابة بالشفرة إلى ما يزيد عن ٤٠٠٠ سنة، وذلك عندما كان المصريون يستخدمون ترميز الهيروغليفيا للنقش، أو الكتابة على القبور، وبعدها تم استخدام العديد من التقنيات، وتطويرها في مجال الترميز، والتشفير، وعبر تلك القرون قامت الشفرة بحماية الكثير من الاتصالات الخاصة بالثقافات مع نقل هذه الاتصالات خلال الحروب، والمعاهدات مع الجيران وغيرها. في السنوات الحديثة تم تصعيد اتصالات البيانات الإلكترونية إلى هذا الحجم، وهذه الأهمية في حياتنا لدرجة أننا بدون الشفرة الإلكترونية أو الرقمية لن نكون قادرين على الاستمرار في حياتنا وحماية معلوماتنا.

نحتاج عادةً إضافة أجهزة حماية المعلومات مثل جدار النار إلى تشفير المعلومات الهامة بغية منع المهاجم من قراءة المعلومات حتى ولو تمكن من الحصول عليها إذا لم يكن يعرف مفتاح التشفير المستخدم، ونحتاج أيضاً التشفير عندما ننقل المعلومات عبر الشبكات لمنع المتطفلين من معرفة محتوياتها فيما لو كانوا يتجسسون على الاتصال.

تؤمن التعمية خمسة أنواع من الحماية وهي:

- ١- الخصوصية Confidentiality: تحمي التعمية خصوصية المعلومات بحيث فقط المصرح لهم يستطيعون رؤيتها.
- ٢- السلامة Integrity: يمكن أن تؤمن التعمية سلامة المعلومات من التعديل عن طريق طرف ثالث.
- ٣- التوافر (المتاحة) Availability: يمكن أن تؤمن التعمية متاحة المعطيات بحيث يستطيع الأشخاص المصرح لهم والذين يملكون المفتاح من الاطلاع عليها عندما يريدون.

٤- المصادقة Authentication: يمكن المصادقة على هوية المستخدمين عن طريق التعمية.

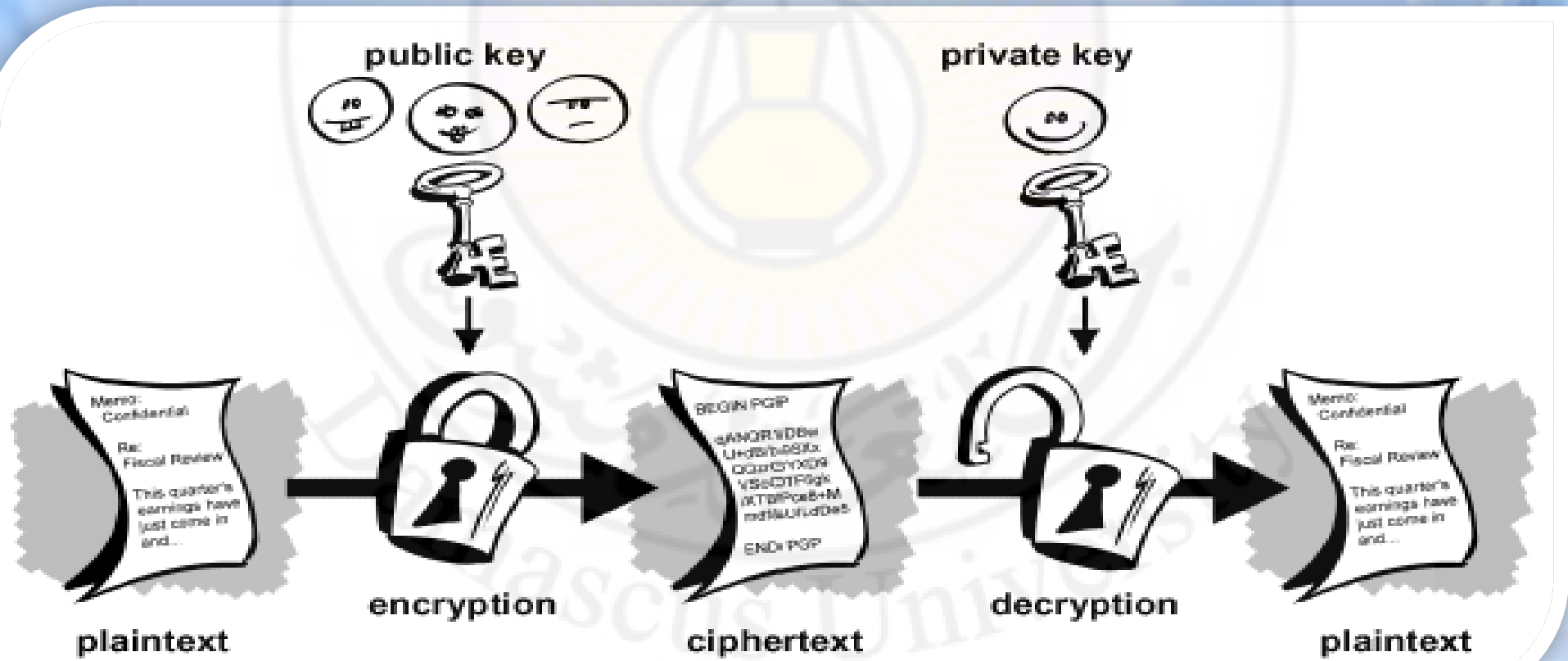
٥- عدم الإنكار Non-repudiation: يمكن أن تفرض التعمية عدم الإنكار، أي التحقق من كون مستخدم ما نفذ فعل ما وعدم إنكاره.

وأفضل طريقة استخدمت في القدم هي طريقة القيصر جوليوس، وهو أحد قياصرة الروم، أما في عصرنا الحالي، فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لارتبط العالم ببعضه البعض عبر شبكات مفتوحة، وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المؤسسات الخاصة والعامة، عسكرية كانت أم مدنية، فلا بد من طرق تحفظ سرية المعلومات، وقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات، وما زال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للحاسب، والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.

تطورت التعمية خلال العقود الماضية لتشمل استخدام الرياضيات في تعريف مجموعة من التقنيات التي تساعد على تحقيق مجموعة أوسع من الأهداف الأمنية مثل السرية والتكاملية والوثوقية وعدم النكران وانتشر استخدامها في التطبيقات التجارية، حيث تساعد التعمية على تخزين المعلومات ونقلها عبر شبكة غي آمنة مثل شبكة الانترنت بطريقة تكون فيها غير قابلة للقراءة إلا من قبل المخول له.

بعض أنواع برامج التشفير :
Best Crypt, Fine Crypt

لغرض حماية المعلومات أثناء نقلها عبر الشبكات أو تخزينها على وسائط التخزين المتنوعة يجري تشفيرها بطريقة يتفق عليها المرسل والمستقبل، وذلك يتحويل النص العادي الصريح الى نص مشفر غير مفهوم لكل من ينظر إليه، عدا المستقبل المعني، والشكل التالي يوضح ذلك:



التشفير:

هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور (مفتاح) لفك شفرة تلك البيانات، ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية (خوارزميات) غير قابلة للعكس، مما يجعل تشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.

المفتاح الخاص: وهو مفتاح سري يستخدمه صاحبه لفك تشفير الرسائل المرسله له، وكذلك يستخدمه للتوقيع الالكتروني، ومن مسؤولية صاحبه المحافظة على سرية.

المفتاح العام: وهو مفتاح ليس سري، ويستخدم لتشفير الرسائل المرسله لصاحب هذا المفتاح، وكذلك للتحقق من توقيع.

الخوارزمية: هي مجموعة من الخطوات المسلسلة منطقياً ورياضياً اللازمة لحل مشكلة ما، والاختلاف الرئيسي في خوارزميات التشفير هو بكمية المعطيات الممكن معالجتها في لحظة ما.

تم مؤخراً ادخال نوع يعرف بالتابع الاسفنجي **Sponge Function**، حيث يأخذ التابع الاسفنجي سلسلة من أي طول، ويولد سلسلة أخرى حسب الطول المطلوب.

تصنف خوارزميات التشفير بناءً على:

أولاً: العملية المستخدمة في التشفير: ولها نوعين هما:

أ- التعويض (الاحلال) **Substitution**: استبدال حرف مكان حرف أو مقطع مكان المقطع.

ب- الازاحة (التبديل) **Transportation**: حيث يتم ازاحة الحروف الموجودة في النص تبعاً لمفتاح معين أي، تبديل مكان الحرف دون تغييره (خوارزمية الخط المتعرج).

بعض الأمثلة على أنظمة التشفير التقليدي:

١- طريقة تبديل الموقع: وفيها يتم إعادة ترتيب رموز النص الصريح للحصول على النص المعنى، وكمثال على ذلك نذكر معمي السياج rail-fence، حيث يعتمد هذا المعمي على كتابة الرسالة بطريقة معينة (على شكل سياج الأسلاك الشائكة)، وإرسالها بطريقة أخرى (على شكل صفوف).

مثال:

* إذا أردنا تعمية النص الصريح التالي: أرسلوا الامدادات بسرعة. يمكن كتابة هذه الجملة وفق هذه الطريقة كمايلي:

أ و ا م ل ا ل ر
س د ا ب ر ع
ة

* الإرسال يتم كمايلي: أوادسرلا لما ابرق سادتع، وهذا هو النص المعمي.

* عند الاستقبال يتم كتابة هذا النص المعمى على شكل صفوف، ومن ثم يتم قراءته على شكل زكزاك (أسلاك شائكة)، والمفتاح هنا يكون ارتفاع السياج أي، عدد الخطوط الأفقية في السياج، حيث أن طول السياج قياسي، ومتفق عليه بين الطرفين.

* الطريقة الكلاسيكية لتنفيذ إعادة الترتيب للرموز كانت تتم بمساعدة شكل هندسي معين، حيث تنفذ عملية التعمية على مرحلتين وكمايلي:

* يتم في المرحلة الأولى كتابة النص الصريح بالشكل الهندسي حسب مسار كتابة معين.

* في المرحلة الثانية تتم القراءة من الشكل الهندسي حسب مسار قراء مختلف، ومن الأشكال الهندسية المعروفة في معميات تبديل الموقع العمودي، نذكر المصفوفة ثنائية الأبعاد (3×4) ، حيث يكتب النص الصريح على السطور الأفقية للمصفوفة، ومن ثم نحصل على النص المعمى من خلال قراءة الأعمدة حسب تسلسل معين.

* يطلب تسمية الرسالة التالية: RENAISSANCE بواسطة معمي تبديل الموقع العمودي.

* واضح أن طول كلمة النص الصريح هي ١١ حرف، وعلى الرغم من وجود ١٢ موقع في المصفوفة. في حال كان طول النص الصريح أكثر من ١٢ حرف، فإنه يتم تقسيم هذا النص إلى رزم كل منها بطول ١٢ حرف، ومن ثم تكتب هذه الرزم في المصفوفة حسب ترتيب السطر من اليسار إلى اليمين، ومن الأعلى إلى الأسفل، وتتم القراءة (قراءة الأعمدة) حسب ترتيب مختلف، فمثلاً إذا أخذنا ترتيب الأعمدة التالية ٤، ١، ٣، ٢، فإن النص المعمي يكون: AARINNSEESC، وعند إظهار النص المعمي تكتب الأحرف حسب الأعمدة، وحسب الترتيب السابق للأعمدة ٤، ١، ٣، ٢، ومن ثم تقرأ بشكل أسطر من اليسار إلى اليمين، ومن الأعلى إلى الأسفل مع تجاوز فراغ واحد إذا وجد.

الشكل التالي يوضح ذلك:

	1	2	3	4
1	R	E	N	A
2	I	S	S	A
3	N	C	E	

٢ - شيفرة قيصر:

وهي طريقة قديمة ابتكرها القيصر جوليوس لعمل الرسائل المشفرة بين قطاعات الجيش، وقد أثبتت فاعليتها في عصره، ولكن في عصرنا الحديث ومع تطور الحاسب، فلا يمكن استخدام هذه الطريقة وذلك لسرعة كشف محتوى الرسائل المشفرة بها، والمثال التالي يوضح طريقة عمل شيفرة قيصر: إذا شفرنا كلمة "SECRET" واستخدمنا قيمة المفتاح ٣، فإننا نقوم بتغيير مواضع الحروف ابتداءً من الحرف الثالث، وهو الحرف "D"، وعليه فإن ترتيب الحروف سوف يكون على الشكل التالي:

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

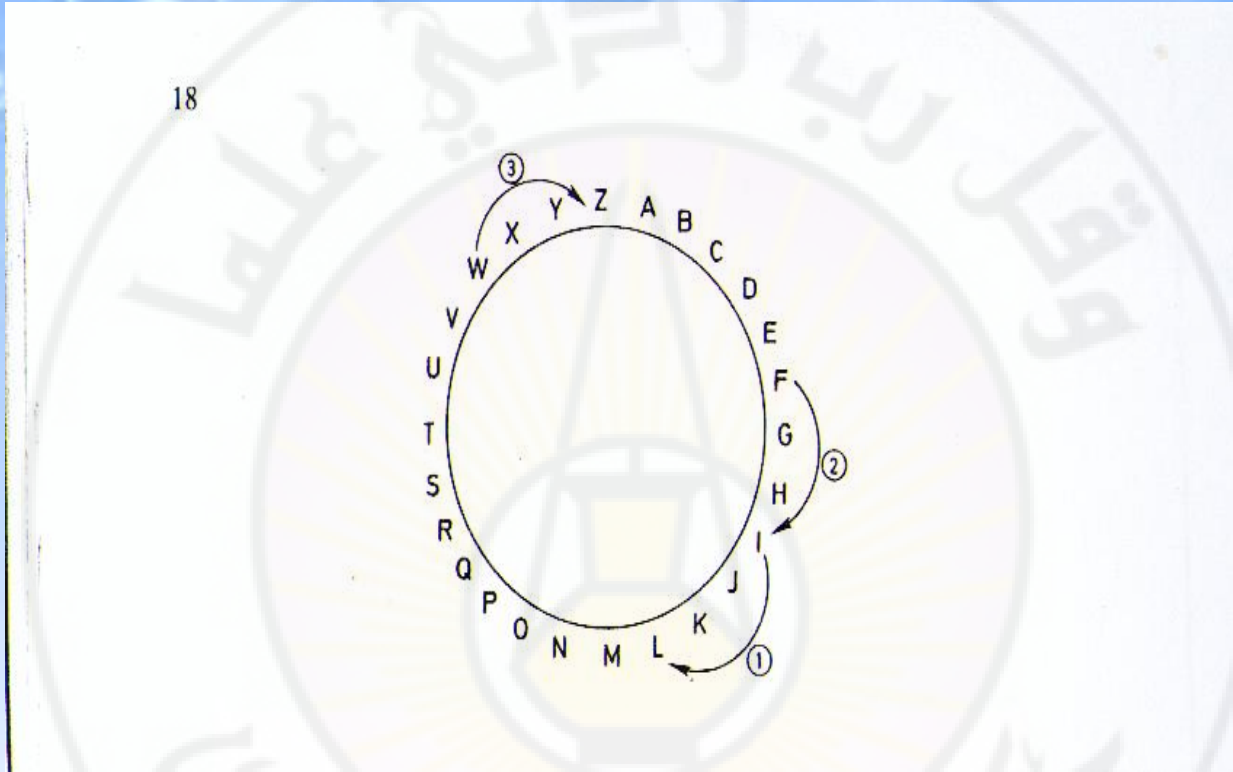
الحروف بعد استخدام القيمة الجديدة لها من المفتاح "٣" تكون على الشكل الحالي:

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

الآن قيمة الـ $A \rightarrow D$ ، $B \rightarrow E$ ، $C \rightarrow F$ ، وهكذا.

بهذا الشكل فإن كلمة "SECRET" سوف تكون "VHFUHW". لتعطي أي شخص آخر إمكانية قراءة رسالتك المشفرة؛ يجب أن ترسل له قيمة المفتاح "٣".

* يوضح الشكل التالي شفرة Caesar :



مثال:

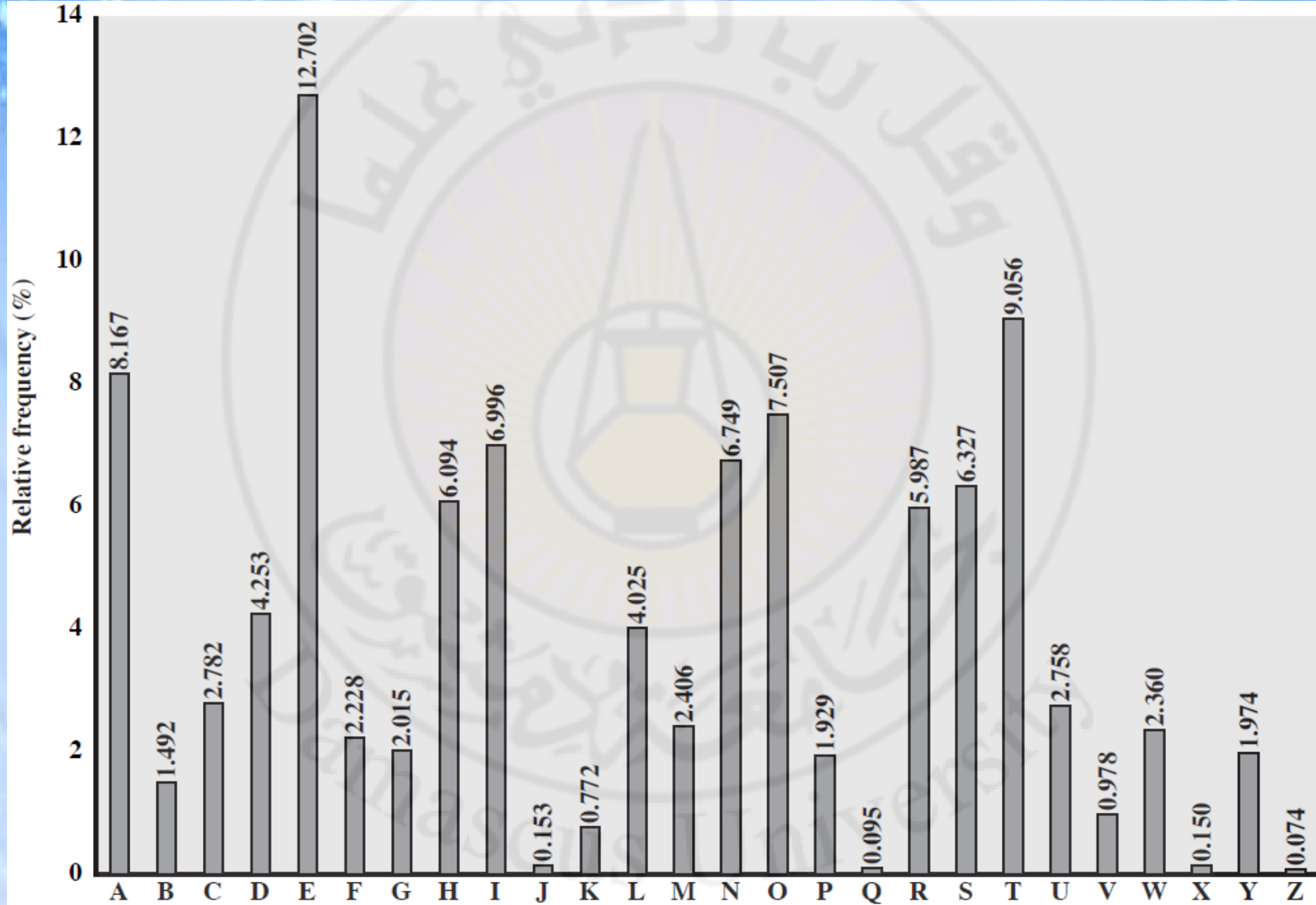
IFWEWISHTOREPLACELETTERSOF

النص الصريح:

LIZHZLVKWRUHSODFHOWWHUVRI

النص المعنى:

يوضح الشكل التالي معدل تكرار الحروف في اللغة الإنكليزية:



٣- معمي كثير الأبجديات MONOALPHABETIC: من أجل زيادة الأمن والسرية، فإن هذه الطريقة تعتمد على خلط (مزج) الأحرف، فمثلاً يمكن الحصول على نتيجة مزج أحرف اللغة الإنكليزية ٢٦! = ٤ x ٢٦١٠، وهذا الرقم يدل على مدى قوة نظام التشفير هذا. المثال التالي يوضح ذلك:

الصريح: ABCDEFGHIJKLMNOPQRSTUVWXYZ

المشفر: DKVQFIBJWPESCXHTMYAUOLRGZN

النص الصريح: IFWEWISHTOREPLACELETTERS

النص المعمي: WIRFRWAJUHYFTSDVFSFUUFYA

٤ - معميات التعويض كثير الحدود:

* يتم فيها استخدام أكثر من تحويل واحد من النص الصريح إلى النص المعمي (استخدام أكثر من أبجدية)، حيث يعمل على تلافي مشكلة معمي التعويض البسيط من خلال استخدام أكثر من أبجدية نص معمي، ويعتقد أن مبدأ التعويض كثير الأبجديات يعود إلى ليون بانيسا ألبرتي، حيث نشر سنة ١٥٦٨ مقالاً يصف فيه قرص تعمية للاستخدام في التعويض كثير الأبجديات، حيث في الدارة الخارجية رتب ٢٠ حرف من حروف النص الصريح من اللغة اللاتينية، ولم يستخدم H, W, U، وذلك كون هذه الحروف لم تكن من الحروف اللاتينية في ذلك الوقت. بالإضافة إلى الأعداد ١، ٢، ٣، ٤ على الدائرة المتحركة الداخلية، فقد كتبت وبشكل عشوائي حروف الأبجدية اللاتينية بالإضافة إلى الرمز &، والمصمم في فكرة ألبرت هو طرح إمكانية تغيير التعويض (تدوير القرص أثناء عملية التعمية).

* من الممكن القول أن معظم المعميات كثير الأبجديات ذات طبيعة دورية وتعتمد على دور ما وهو دور التعمية (دور التابع المعبر عن الإزاحات). ومن أشهر المعميات التي ظهرت وتنطوي ضمن هذا النوع نذكر:

آ- معمي فيجينر VEGENER: أول ظهور لهذا النوع كان سنة ١٥٨٦، وهنا لا يتم مزج الأحرف، وإنما يتم استبدالها وفق إزاحة دائرية.

ويعتمد على اختيار أبجديات نص معمي، وهي عبارة عن إزاحة حلقية من الأبجدية الأصلية. يحدد المفتاح K بتتابع من الرموز التالية: $K_1, K_2, K_3, \dots, K_n$ ، وتحدد كمية الإزاحة اللازمة للرمز i في الأبجدية بواسطة K_i ، وعلاقة التعمية لهذا المعمي هي:

$$F_i(a) = (a + K_i) \bmod n$$

حيث n هي حجم الأبجدية، K_i كمية الإزاحة، a موقع الحرف في أبجدية النص الصريح.

والجدول التالي يوضح ذلك:

جامعة دمشق
Damascus University

ABCDEFGHIJKLMNOPQRSTUVWXYZ

A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
D	DEFGHIJKLMNOPQRSTUVWXYZABC
E	EFGHIJKLMNOPQRSTUVWXYZABCD
F	FGHIJKLMNOPQRSTUVWXYZABCDE
G	GHIJKLMNOPQRSTUVWXYZABCDEF
H	HJKLMNOPQRSTUVWXYZABCDEFG
I	IJKLMNOPQRSTUVWXYZABCDEFGH
J	JKLMNOPQRSTUVWXYZABCDEFGHI
K	KLMNOPQRSTUVWXYZABCDEFGHIJ
L	LMNOPQRSTUVWXYZABCDEFGHIJK
M	MNOPQRSTUVWXYZABCDEFGHIJKL
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
P	PQRSTUVWXYZABCDEFGHIJKLMNO
Q	QRSTUVWXYZABCDEFGHIJKLMNOP
R	RSTUVWXYZABCDEFGHIJKLMNOPQ
S	STUVWXYZABCDEFGHIJKLMNOPQR
T	TUVWXYZABCDEFGHIJKLMNOPQRS
U	UVWXYZABCDEFGHIJKLMNOPQRST
V	VWXYZABCDEFGHIJKLMNOPQRSTU
W	WXYZABCDEFGHIJKLMNOPQRSTUV
X	XYZABCDEFGHIJKLMNOPQRSTUVW
Y	YZABCDEFGHIJKLMNOPQRSTUVWX
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

* يوضح التالي خوارزمية تشفير، وفك التشفير **vigener** (كثير الحدود):

m: عدد ثابت موجب صحيح.

K ($k_1, k_2, \dots, k_m$): المفتاح.

عملية التشفير:

$$E_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$

عملية فك التشفير:

$$D_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$$

مثال ١:

* لتكن الكلمة المفتاحية CIPHER، وفيها تكون ($m=6$)، وهذا يكافئ القيم العددية التالية: (2, 8, 15, 7, 4, 17).

* إذا كان النص الصريح: thiscryptosystemisnotsecure

19	7	8	18	2	17	24	15	19	14	18	24	18	19	4	12	8	18	13	14	19	18	4	2	20	17	4
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7	4	17	2	8	15
21	15	23	25	6	8	0	23	8	21	22	15	20	1	19	19	12	9	15	22	8	25	8	19	2	25	19

* يوضح السطر الأول في الجدول السابق الأرقام المقابلة لكل حرف من النص الصريح، ويوضح السطر الثاني توزيع الكلمة المفتاحية، والسطر الأخير هو ناتج جمع السطرين الأول، والثاني module 26.

* بإجراء مقابلة الأعداد التي حصلنا عليها (السطر الثالث) مع ما يقابلها من آخر، فنحصل على النص المشفر كمايلي:

VPXZGIA XIVWPUBTTMJPWIZITWZT

مثال ٢ :

* النص الصريح: RENAISSANCE

* مفتاح التعمية: BAND

* ناتج عملية التعمية:

RENAISSANCE
BANDBANDBAN
SEADJSFDOCR

* حيث تمت إزاحة الحرف الأول من كل مجموعة مؤلفة من أربعة حروف بمقدار $1 \bmod 26$ ، والحرف الثاني $0 \bmod 26$ ، والحرف الثالث يكون $13 \bmod 26$ ، والحرف الرابع $3 \bmod 26$ ، وهذا يعني أنه يمكن استبدال المفتاح K بالمقياس التالي للأرقام $K = 1, 0, 13, 3$.

ب- معمي بوفورت BUFORT: لقد ظهر هذا النوع سنة ١٧١٠، ويعتبر مشابهاً لمعمي فيجينر من ناحية التعويض، والدورية، ولكن يختلف عنه بعلاقة التعويض، والتي تكون حسب العلاقة التالية:

$$F_i(C) = (K_i - a) \bmod n$$

مثال:

* إذا كان $K_i = D$ عندها تكون علاقة التعمية هي: $F_i(a) = (D - a) \bmod 26$
 $26 = (3 - 0) \bmod 26 = 3$ أي أن الحرف A من النص الصريح يقابل الحرف C من نص التعمية، وهكذا.

* يوضح التالي حروف النص الصريح وما يقابلها من حروف التعمية:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DCBAZYXWVUTSRQPONMLKJIHGFE

٥- تعويض الحروف: لقد تم استخدام هذه الطريقة سنة ١٨٦٣، وفيها لا يوجد مزج، أو خلط لمرة واحدة بالنسبة للأحرف المستخدمة في جدول التعويض، وإنما عدد من المرات، وعندما نستخدم آخر حرف سنبدأ مرة ثانية من الأول، وذلك لأن كل حرف من النص الصريح لا يمكن تمثيله بنفس الحرف بالنص المشفر. المثال التالي يوضح ذلك:

النص الصريح: THEREISNOOTHERMATTER

النص المشفر: MBSRBMSPBMBJSZTNYFE

واضح من هذا المثال أن عملية التكرار تحققت بعد ٥ حروف.

بعد ذلك انطلق مفهوم الكلمة المفتاحية، والتي عادةً ما تكون مؤلفة من (١٠-١٢) حرف مما سهل تذكر مفتاح التشفير على العنصر البشري.

مثال:

النص الصريح: ABCDEFGHIJKLMNOPQRSTUVWXYZ

النص المعنى: EXHAUSTINGBCDFJKLMOPQRVWYZ

Damascus University

٦- معميات التعويض الهوموفوني:

* يعتقد المؤرخون أن هذا المعمي تم استخدامه أول مرة في الغرب حوالي عام ١٤٠٠م، وهو أصعب كسراً من المعميات البسيطة، وخصوصاً عندما يكون عدد الهوموفونات المخصص لكل حرف متناسباً مع المعدل التكراري لذلك الحرف. إن التطبيق المستخدم هو واحد إلى مجموعة، وهذا يعني أن كل رمز من رموز النص الصريح يتم تعميته بعنصر من عناصر مجموعة محددة من رموز النص المعمي، والتي تدعى الهوموفونات.

مثال:

* لنفرض أن الحروف الإنكليزية تمت تعميته على شكل أعداد صحيحة تتراوح بين الصفر و ٩٩، حيث أن عدد الأعداد الصحيحة المخصص لكل حرف يتناسب مع المعدل التكراري لهذا الحرف مع ملاحظة أنه لا يمكن أن يتواجد عدد ما يدخل في أكثر من مجموعة هوموفونات واحدة.

* لنفرض أن النص الصريح المراد تعميته هو: PLAIN PILOT، عندها من الممكن أن تكون العلاقة بين حروف أبجدية النص الصريح، ومجموعة الهوموفونات المناظرة كمايلي:

A	05 13 26 77 80 85 90 97
I	00 10 33 95 99 70
L	09 22 55
N	12 29 91 42 93
O	20 11 21 36 44 53 61 89
P	37 83
T	01 17 27 31 49 50 67 71

فسيكون النص المعمى: 17 11 09 95 83 91 00 26 22 37

* يلاحظ من النص المعمى أنه لا يوجد أي تكرار لرقم من الصفر، وحتى ٩٩ على الرغم من تكرار بعض الحروف في النص الصريح مثل P, L, I.

وفيمايلي مراحل معمي الهوموفونات:

١- نرتب النص الصريح وفقاً للترتيب التسلسلي لوروده في الأبجدية.

٢- نضع لكل حرف مجموعة من الهوموفونات بحيث عددها يتناسب طرذاً مع المعدل التكراري لهذا الحرف.

٣- للحصول على النص المعمي نقرأ النص الصريح بعكس ما هو مكتوب ونختار الهوموفون بشكل اختياري وبحيث لا يجوز اختياره مرةً أخرى، أي لا يوجد تكرار على الرغم من وجود تكرار لبعض الحروف في النص الصريح.

* قام Hammer بتوضيح طريقة تعمية هوموفوني من درجة أعلى من الواحد، حيث بواسطة هذه الطريقة يمكن تحليل النص المعنى ليصبح أكثر من رسالة نص صريح واحدة ذات معنى، وذلك من أجل مفاتيح مختلفة، وهذا ما يضل محلل المعميات، وخصوصاً إذا كانت الرسائل البديلة متساوية الاحتمال مع الرسالة الأصلية، ولإنشاء معي تعويض هوموفوني من الدرجة الثانية نتبع مايلي:

١ - نكتب مجموعة الأعداد الواقعة ما بين ١ و n^2 بشكل عشوائي في مصفوفة $(n \times n)$ ، ونسميها مصفوفة K ، حيث أن n هي حجم أبجدية النص الصريح.

٢ - نكتب رموز أبجدية النص الصريح فوق السطر الأول، وعلى يسار العمود الأول، وبذلك، فإنه من أجل كل رمز a هناك مجموعة واحدة من الهوموفونات في الأسطر $F_1(a)$ ، ومجموعة أخرى من مجموعة الأعمدة نسميها $F_2(a)$ ، أي أن مجموعة الأسطر تناظر المفتاح الأول F_1 ، ومجموعة الأعمدة تناظر المفتاح الثاني F_2 .

٣- نختار رسالة مزيفة ذات معنى، ولتكن $X = X_1 X_2 X_3$.

٤- نعي النص الصريح باستخدام X ، والمصفوفة K .

مثال:

$n=5$ ، وبالتالي لدينا مصفوفة (5×5) ، ولنفرض أن رموز النص الصريح هي $\{E, I, L, M, S\}$ ، بفرض أن النص الصريح SMILE، عندئذ النص المشفر LIMES، والمصفوفة التالية توضح ذلك:

10	22	18	02	11
12	01	25	05	20
19	06	23	13	07
03	16	08	24	15
17	09	21	14	04

M = S M I L E

X = L I M E S

21 16 05 19 11

٧- شفرة الإزاحة:

هي حالة خاصة من شفرة التعويض، وهذا النوع من التشفير يعتمد على علاقة حسابية $\text{module } 26$ ، وذلك بعد استبدال الأحرف بما يقابلها من أعداد، وخوارزمية هذه الشفرة موضحة كمايلي:

For $0 \leq K \leq 25$

$$e_K(x) = x + K \bmod 26$$

$$d_K(y) = y - K \bmod 26$$

حيث k هو مفتاح التشفير، و k فك التشفير.

X هي الرسالة المراد تشفيرها.

الجدول التالي يوضح ذلك:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

مثال:

إذا كان المفتاح $K=11$ ، والمطلوب تعمية النص الصريح التالي:

wewillmeetatimdnight

خطوات التشفير:

١- نعبّر عن كل حرف من النص الصريح بما يقابله من رقم، فنجد:

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

٢- نضيف قيمة المفتاح ($K=11$) إلى كل قيمة من قيم النص الصريح،
ونحسب الناتج Module 26، فنحصل على:

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

٣- نقابل كل رقم بما يقابله من حرف، فنحصل على النص المشفر المقابل
للنص الصريح:

HPHTWWXPPELEXTOYTRSE

* من أجل إجراء عملية فك التشفير نقوم بوضع الرقم المقابل لكل حرف من
أحرف النص المشفر، ثم نضيف قيمة المفتاح $k=11$ ، ونحسب ناتج
الإضافة module 26، فنحصل على النص الصريح، وذلك بعد استبدال
الأرقام بما يقابلها من أحرف.

* في هذا التشفير، فإن الكلمة المفتاحية تحدد أي حرف مستبدل يكون مستخدم لتشفير كل حرف من رسالة النص الصريح، فمثلاً:

النص الصريح:

THISPROCESSCANALSOBEEEXPRESSED

الكلمة المفتاحية: CIPHERCIPHERCIPHERCIPHERCIPHE

النص المشفر: VPXZTIQKTZWTCVPSWFDMTEIGAHLA

* يختار محلل التشفير الكلمة، والتي يعتبرها تشبه رسالة نص الصريح،
وعندها يحسبها MODULE 26.

ج- شفرة المبادلة TRANSPOSITION:

* هي حالة خاصة من شفرة Hill، والشرح التالي يوضح خوارزمية هذه الشفرة:

m : عدد صحيح موجب وثابت.

$K(1, 2, 3, \dots, m)$: مفتاح التشفير.

* من أجل المفتاح μ نعرف التشفير، وفك التشفير وفق هذه الخوارزمية كمايلي:

$$e_{\mu}(x_1, x_2, \dots, x_m) = (x_{\mu(1)}, x_{\mu(2)}, \dots, x_{\mu(m)})$$

$$d_{\mu}(y_1, y_2, \dots, y_m) = (y_{\mu^{-1}(1)}, y_{\mu^{-1}(2)}, \dots, y_{\mu^{-1}(m)})$$

حيث μ^{-1} هو معكوس μ .

مثال:

$\mu =$

1	2	3	4	5	6
3	5	1	6	4	2

$\mu^{-1} =$

1	2	3	4	5	6
3	6	1	5	2	4

النص الصريح:

Shesel Isseas hellsb ythese ashare

النص المشفر:

EESLSHSALSESLSHBLEHSYEETHRAEOS

* شفرة المبادلة: يهدف هذا النوع من التشفير إلى إخفاء محتوى الرسالة، وذلك بأخذ الحروف الشخصية أو البتات، وإعادة ترتيبها وفق أسلوب نظامي، ومن أجل فك التشفير، فإن العملية العكسية تتم، وإن كلمة المبادلة هي الكلمة الشائعة والمستخدم لهذه النوع من العمليات، ومن المفضل استخدام PERMUTATION، والمفتاح هو الأحرف المكررة والمستخدم، والأمثلة التالية توضح ذلك:

مثال ١:

النص الصريح: THE SIMPLEST POSSIBLE TRANSPOSITIONS XX

المفتاح:

4 1 5 3 2
S T I E H
E M S L P
S T S O P
E I T L B
S R P N A
T O I I S
X O X S N

النص المشفر: STIEHEMSLPSTSOPEITLBSRPNATOIISXOXSN

مثال ٢:

النص الصريح: ACONVENIENTWAYOEXPRESSTHEPERMUTATION

المفتاح:

C O M P U T E R
1 4 3 5 8 7 2 6
A N O V I N C E
E W T A O T N Y
E R P E T S X S
H E P R T U E M
A O I N Z Z T Z

النص المشفر: ANOVINCEEWAOTNYNERPETSXSHEPRTUEMAOINZZTZ

* في هذا الأمثلة، يتم كتابة النص الصريح على شكل سطر، ثم يصار إلى توزيع النص الصريح حسب موقع تكرار حروف مفتاح التشفير (أي يتم أخذ الحرف المقابل من النص الصريح حسب رقم موقع العدد المقابل في الكلمة المفتاحية)، وبعد ذلك يصار إلى ترتيب النص لنحصل على النص المعنى.

آ- تشفير NIHILIST: يعتمد هذا النوع من التشفير على اتحاد مبادلة الأسطر والأعمدة (نرتب حروف النص الصريح وفق الكلمة المفتاحية للسطر، ومن ثم نرتب التشفير وفق ترتيب الأعمدة). يتم كتابة النص الصريح ثانيةً في أسطر تحت الكلمة المفتاحية، ولكن أيضاً تكون الكلمة المفتاحية مكتوبة بشكل عمودي، فمثلاً:

النص الصريح: NOWISTHETIMEFORALLGOODMEN

الكلمة المفتاحية: L E M O N

2 1 3 5 4

* عندها، ويطبق هذا النوع من التشفير نحصل على:

	LEMON
	2 1 3 5 4
L 2	ONWSI
E 1	HTEIT
M 3	EMFRO
O 5	LALOG
N 4	DOMNE

وبالتالي تشفير NIHILIST يكون:

HTEITONWSIEMFRODOMNELALOG

* إن الهجوم على هذا النوع من التشفير يعتمد على إعادة ترتيب العمود والسطر، ويتكرر عدد من المحاولات، وتفادي الأخطاء يمكن الوصول إلى إزالة الغموض في بناء الكلمات، أضف إلى الاعتماد على تكرار الحروف.

* إن التشفير البسيط يعتمد على استخدام الحروف، تعداد تكرار الحرفان اللذان يمثلان صوتاً منفرداً وثلاثة حروف التي يرسم بها صوت واحد، وعلى قدرته على إعادة ترتيب مجموعات الحروف بسهولة.

ح- معميات تعويض البولي غرام: وهي تمثل الحالة العامة، وفيها يتم تعمية مجموعة من رموز النص الصريح بمجموعة من حروف النص المعمي دفعة واحدة، وهذا ما يصعب عمل محلل المعميات، وكأمثلة على هذه المعميات نذكر:

١- معمي بلي فير play – fair: لقد تم استخدام هذا النوع من التشفير من قبل الإنكليز في الحرب العالمية الأولى، ويعرف المفتاح في هذا المعمي من خلال مصفوفة 5 x 5، والتي تحوي على ٢٥ مربع، وحيث أن الحرف J غير مستخدم، وتم استبدله بالحرف I كما هو موضح في الشكل التالي:

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

* إن حروف الأبجدية في هذه المصفوفة موزعة من اليسار إلى اليمين، ومن الأعلى إلى الأسفل، وبكلمة مفتاحية، وإذا افترضنا أن الكلمة هي HARPSHORD، فإن التعمية تتم لكل زوج من أزواج حروف النص الصريح حسب القواعد التالية:

١- إذا وقعت m_1, m_2 في سطر واحد عندها يكون الرمز c_1, c_2 هما الرمز الموجودين على يمين m_1, m_2 على التوالي مع اعتبار العامود الأول هو على يمين العامود الأخير. فمثلاً H, R يتم تعميتهما بـ A, P .

٢- إذا كانت m_1, m_2 في نفس العامود فيكون الرمز c_1, c_2 هما الرمز الموجودين تحت m_1, m_2 على التوالي وأيضاً اعتبار السطر الأول تحت السطر الأخير. فمثلاً تعمية R, X هي O, R .

٣- إذا كانت m_1, m_2 في سطر وعامود مختلفين عندها يكون الرمز c_1, c_2 هما الرمز m_1, m_2 الواقعين على الزاويتين من المستطيل الذي تكون فيه m_1, m_2 واقعيتين على رأسيه المتقابلين حيث أن c_1 تقع في سطر m_1 و c_2 تقع في سطر m_2 . فمثلاً تسمية H, O هو R, I ، و A, Z هو S, W .

٤- إذا كانت $m_2 = m_1$ عندها يضاف حرف عديم المعنى مثل x بين m_1, m_2 في النص الصريح لإلغاء هذا التساوي.

٥- إذا كان عدد الرموز مفرداً عندها يضاف حرف عديم المعنى مثل x عند نهاية النص الصريح.

مثال:

النص الصريح: RENAISSANCEX

النص المعنى: HGWCBHHRWFGV

٢ - شفرة Hill:

* قام هيل سنة ١٩٢٣ بنشر مقال تشرح طريقة التعمية هذه حيث يقوم معمي هل بإجراء تحويل خطي على d رمز من رموز النص الصريح للحصول على d رمز من رموز النص المعمي وللسهولة سنأخذ مثال على $d=2$ أي $M=m_1 m_2$ ، وعندها يتم تعمية M كمايلي:

$$C_1 = (k_{1,1} m_1 + k_{1,2} m_2) \bmod n$$
$$C_2 = (k_{2,1} m_1 + k_{2,2} m_2) \bmod n \quad \text{حيث } n$$

حجم الأبجدية.

* يوضح الشرح التالي خوارزمية هذه الشفرة:

التشفير

$$y = x \cdot k$$

فك التشفير

$$x = y \cdot K^{-1}$$

النص المعمي

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m)$$

النص الصريح

$K_{1,1}$ $k_{1,2}$ $k_{1,m}$

$K_{2,1}$ $k_{2,2}$ $k_{2,m}$

.

.

$K_{m,1}$ $k_{m,2}$ $k_{m,m}$

مفتاح التشفير

* وكحالة خاصة، فإذا اعتبرنا M, C على شكل شعاع عامودي أي:

$$M = \begin{Bmatrix} m_1 \\ m_2 \end{Bmatrix}$$

$$C = \begin{Bmatrix} c_1 \\ c_2 \end{Bmatrix}$$

$$K = \begin{Bmatrix} k_{1,1} & k_{1,2} \\ k_{2,1} & k_{2,2} \end{Bmatrix}$$

$$C = \begin{Bmatrix} k_{1,1} & k_{1,2} \\ k_{2,1} & k_{2,2} \end{Bmatrix} \begin{Bmatrix} m_1 \\ m_2 \end{Bmatrix} \pmod n$$

مثال:

* مفتاح التشفير K: موضح بالمصفوفة التالية:

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

* معكوس المفتاح (المصفوفة) هو:

$$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

* إذا كان النص الصريح july، والتي تقابل الأعداد التالية: 9, 20, 11, 24.

$$(9 \ 20) \times \begin{Bmatrix} 11 & 8 \\ 3 & 7 \end{Bmatrix} = (99 + 60, 72 + 140) = (3, 4)$$

$$\begin{Bmatrix} 11 & 8 \\ 11 & 24 \end{Bmatrix} \times \begin{Bmatrix} 3 & 7 \\ 11 & 22 \end{Bmatrix} = (121 + 72, 88 + 168) = (11, 22)$$

* بالتالي النص المشفر الذي يقابل الأرقام (٣، ٤، ١١، ٢٢) هو DELW.

* من أجل فك التشفير نقوم بمايلي:

$$\begin{pmatrix} 7 & 18 \\ 3 & 4 \end{pmatrix} \times \begin{Bmatrix} 23 & 11 \end{Bmatrix}$$

$$= (9, 20)$$

$$\begin{pmatrix} 7 & 18 \\ 11 & 22 \end{pmatrix} \times \begin{Bmatrix} 23 & 11 \end{Bmatrix}$$

$$= (11, 24)$$

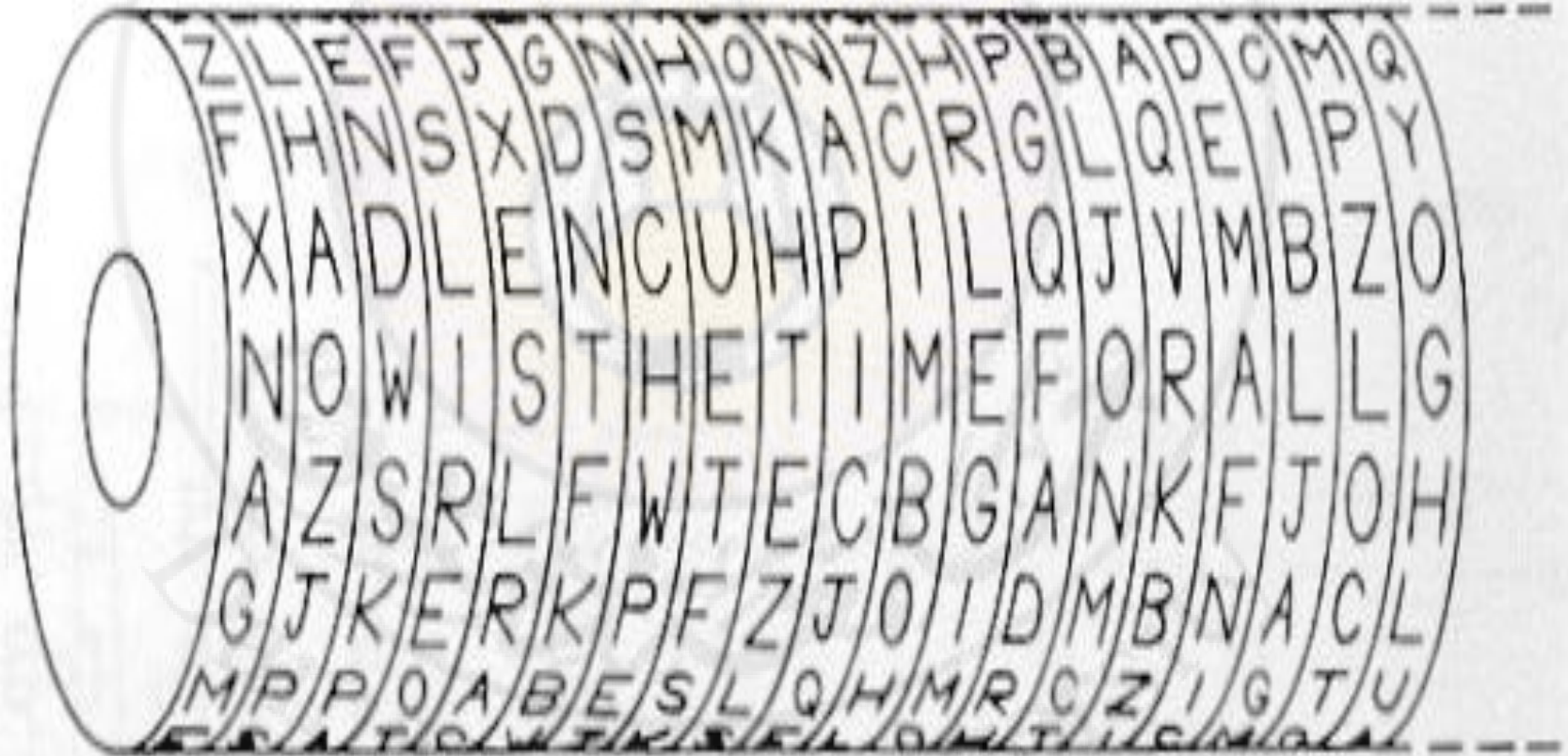
ملاحظة: هذه الشفرة يمكن تطبيقها عندما يكون معكوس المفتاح معروف (يمكن حسابه).

خ- آلات التشفير:

١- جهاز تشفير JEFFERSON: هذا الجهاز ممتع، ويعود الفضل إلى الرئيس الأمريكي THOMAS JEFFERSON الذي قام بتطوير آلة في عام ١٧٩٠ من أجل تعويض متعدد الحروف.

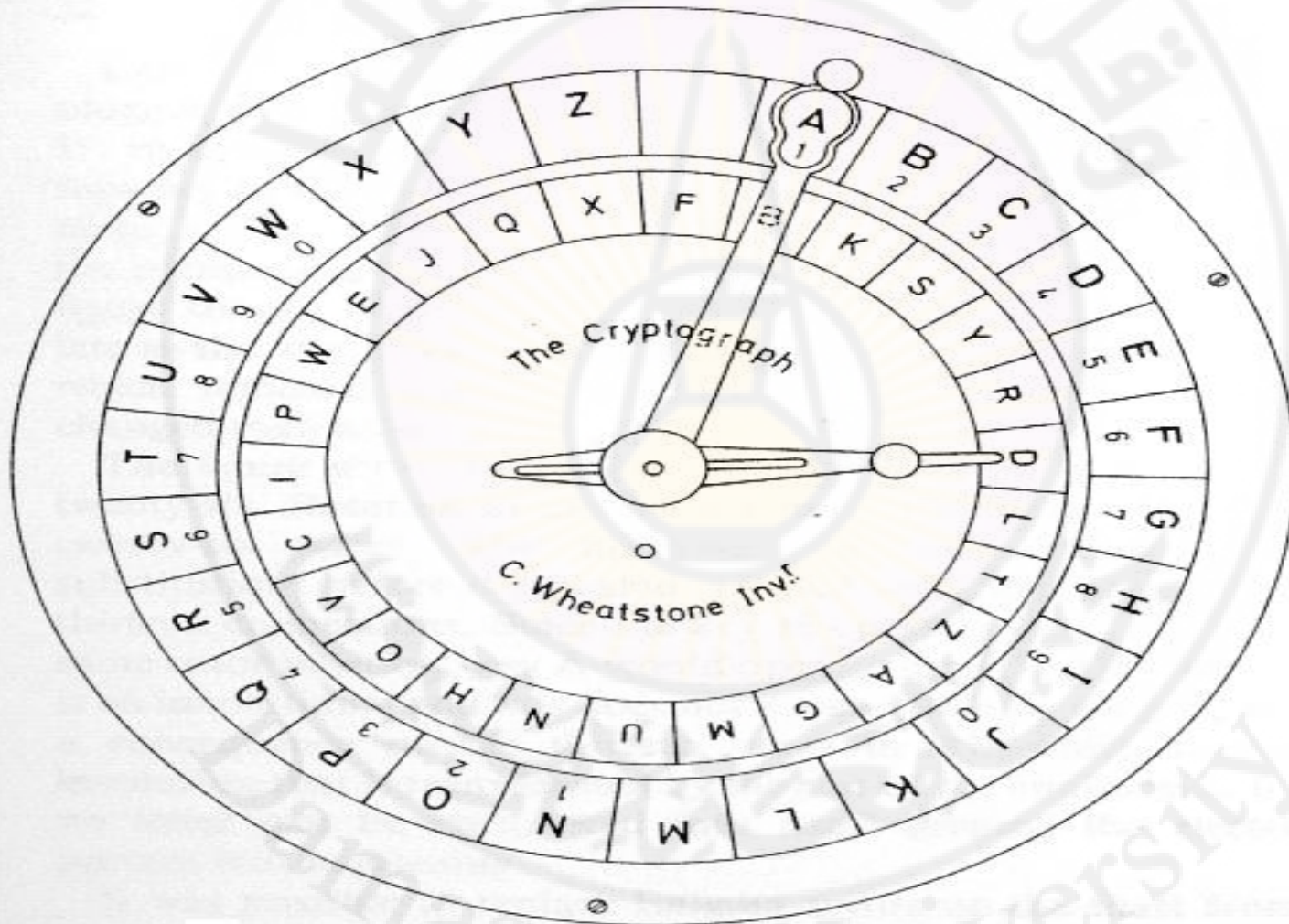
* هذه الآلة تتألف من ٣٦ قرصاً، وكل منهم يحمل حروف خليطة (مزيجة) على نفس السطح الخارجي للقرص، والتي تكون مثبتة على محور عام. يوضح الشكل التالي ذلك. يتم ترقيم الأقراص، وترتيبها على المحور، وتحديدتها بحيث تتوافق مع المتصل. طلب القرص يطابق المفتاح، وعدد الطرق المختلفة في الـ ٣٦ محور، والتي يمكن ترتيبها بطرق مختلفة حتى ١١٠، وخلال عملية التشفير يتم تنصيب الرسالة على الجهاز، وذلك بتدوير الأقراص حتى وقوف حروف الرسالة على نفس السطر مقابل القضيب، ولقراءة النص المشفر يتم تحريك القضيب إلى ٢٥ كموقع حول الأسطوانة، والسطر عندئذ يشير إلى النص المشفر. تم استخدام هذا النوع من التشفير من قبل القوات البحرية الأمريكية، وبشكل جدي عام ١٩٢٠ ولعقود طويلة.

* يوضح الشكل التالي جهاز شفرة دولاب Jefferson:



٢- قرص WHEATSTONE: تم تصميم هذا القرص من قبل WADSWORTH سنة ١٨١٧، وبعدها تم تطويره من قبل WHEATSTONE سنة ١٨٦٠، وهذا النوع من الأجهزة يكون مستخدم بشكل فعال في تشفير تعويض متعدد الحروف، ولكن الطريقة، والتي فيها الحروف المختلفة والمستخدمات تعتمد على تتابع (تتالي) حروف النص الصريح. قرصان متحدا المركز يحملون الحروف حول محيطهم الخارجي. القرص الخارجي يمتلك ٢٦ حرف مرتبة بشكل منتظم مع فراغ واحد، بينما القرص الداخلي يمتلك ٢٦ حرف، ولكن بترتيب عشوائي.

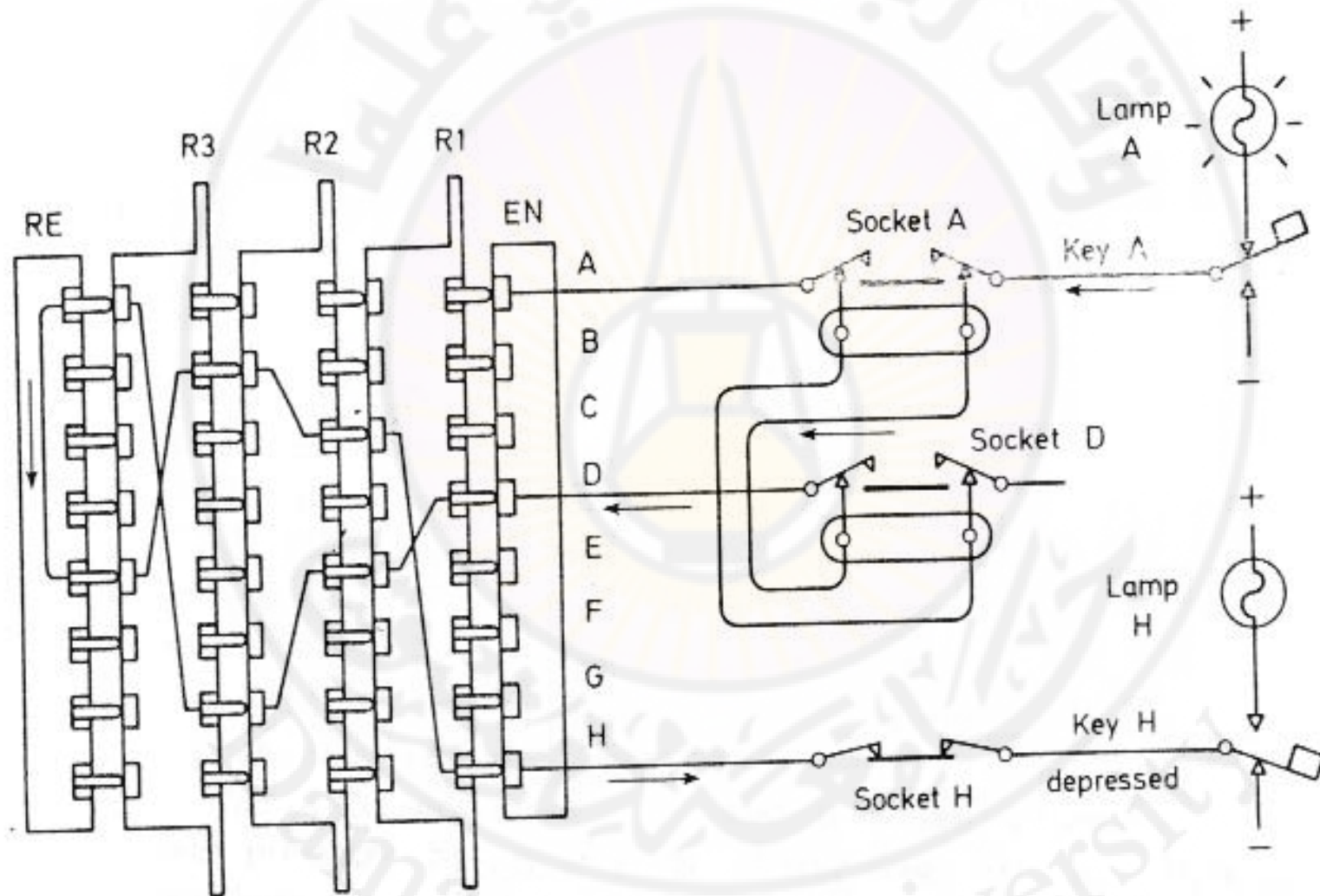
* يوضح الشكل التالي جهاز شفرة قرص: Wheatstone:



* يوجد مؤشرين بحيث يمسح المؤشر الخارجي ٢٧ حرف، بينما يمسح المؤشر الداخلي ٢٦ حرف، وعندما يدور المؤشر الخارجي دورة كاملة (٢٧ حرف)، فإن المؤشر الداخلي يمسح ٢٦ حرف + حرف آخر، وهكذا بحيث يوجد دائماً فاصل بين المؤشرين بمقدار حرف واحد. من أجل عملية التشفير، المؤشر الخارجي يتحرك بنجاح إلى الحروف التي تشكل النص الصريح (الحركة دائماً مع عقارب الساعة)، بينما حرف النص المشفر يشار إليها بالمؤشر الداخلي.

٣- آلة ENIGMA: تعتبر أحد الآلات المشهورة في عملية التشفير، والخاصة بـ POLYALPHABETIC SUBSTITUTION، والتطوير كان من قبل DUTCH سنة ١٩٢٠، وقد تم استخدامها من قبل القوات الألمانية في الحرب العالمية الثانية.

* يوضح الشكل التالي آلة شفرة Enigma:



٤- الآلات طباعة التشفير: أول آلة عرفت لهذا الغرض كانت DE VIARIS سنة ١٨٨٠، وفيها يتم كتابة النص الصريح، وعلى خرج هذه الآلة نحصل على النص المشفر. بعد ذلك تم تطوير مثل هذه الآلات، وأصبح بالإمكان كتابة النص الصريح، والآلة تشفر وترسل الرسالة المشفرة عبر وسط الاتصال إلى الطرف الآخر، وكمثال على ذلك نذكر M-209، والتي استخدمت بشكل واسع خلال الحرب العالمية الثانية. نموذج آخر هو T52.

٥- الآلات التشفير الحديثة: مجال واسع من الآلات التشفير يكون حالياً متوفر من قبل العديد من المصانع، وتتميز هذه الآلات بأن تصميمها سري حتى على الناس الذين يشترونها، وأيضاً قوة السرية تعتمد على خوارزمية التشفير المستخدمة (مفتاح التشفير).

٦- معميات الدوار، وآلات هاجلين Rotar & Hgelin: تمثل هذه الآلات جيلاً من أجيال التعمية لم يكن فيه لاستخدام الحاسبات استخداماً واسعاً، وقد استخدمت هذه الآلات لتوليد دور طويل جداً للاستخدام في معميات تعويض كثير الأبجديات وغالباً ما ينفذ هذا بواسطة آلي طباعة كهربائيتين والشكل التالي يوضح ذلك:



* يتم كتابة النص الصريح على الآلة الأولى ليظهر بعدها النص المعمي على الآلة الثانية.

* تعتبر آلات دوار من أقدم آلات هاجلين، حيث يعود أقدم أنواعها إلى وزير الخارجية الأمريكي "توماس جيفرسون" سنة ١٧٩٠، ويعتبر المعمي الأرجواني purple المستخدم في الحرب العالمية الثانية من قبل اليابان، ومعمي اينغما enigma المستخدم في الحرب العالمية الثانية من قبل الألمان معميات آلات الدوار.

* تتألف آلة الدوار من مجموعة من الأقراص عددها t ، وعلى كل من وجهي القرص يوجد هناك ٢٦ تماس كهربائي (تماس واحد لكل حرف من حروف الأبجدية موزعة بشكل متجانس على دائرة قطرها أقل قليلاً من قطر القرص)، وكل تماس موجود على الوجه الأمامي موصول مع تماس ما من تماسات الوجه الخلفي، وهذا يناظر تطبيقاً من نص صريح إلى نص معمي من أبجدية النص الصريح إلى أبجدية النص المعمي. من الواضح أن القرص R ذو الرقم i يستطيع أن يدور ليستقر على أحد التماسات (المواقع) الـ ٢٦، وكل موقع يعني تطبيقاً مستقلاً، وعندما يكون الدوار R_i على الموقع j نعرف التطبيق التالي:

$$F_i(a) = [F_i(a-J_i) \bmod 26 + J_i] \bmod 26$$

حيث F_i تحدد توصيلات الأسلاك، J_i هو موقع التماس رقم J في الدوار رقم i .

* تتم التعمية بإدخال حرف النص الصريح إلى مجموعة الدورات من أحد الأطراف، ويسري عبر الدورات على التوالي لينبثق كحرف معمي من الطرف الآخر.

* إن التوصيلات السلكية، بالإضافة إلى المواقع الأولية للدورات تحدد المفتاح الأولي.

* فمثلاً إذا احتوت الآلة على t دوار، فهذا يعني أنه لن تعود الآلة إلى وضعها الأولي إلا بعد تسمية 26^t حرف، فإذا كانت $t=4$ ، فإن الدور سيكون مساوياً إلى $26^4 = 456976$ ، وحركة الدوار تتم مع حركة عقارب الساعة، أي أن الدوار الأول يتقدم إلى الموقع التالي بعد تسمية كل حرف من حروف النص الصريح، وبعد أن يقوم الدوار الأول بدورة كاملة يتقدم الدوار الثاني إلى الموقع التالي، وهكذا حتى تتحرك جميع الدورات على المواقع.

* أما معميات هاجلين، فهي تتألف من عدة عجلات (أقراص)، وعلى الأكثر عشرة عجلات، والتي تولد بمجملها تتابع مفتاحي طويل جداً، وتحتوي كل عجلة على عدد من المواقع الدبوسية، وهذه المواقع موزعة بشكل متساوي على محيط العجلة، حيث تنفذ عملية التسمية بتسمية كل حرف على حدى، وتدور العجلات كلها بأن واحد بمقدار موقع واحد، وباتجاه واحد من أول كل حرف، فعلى سبيل المثال، إذا كان عدد مواقع عجلة ما يساوي ١٧ موقع دبوس، فإنه بعد تسمية ١٧ حرف تعود العجلة إلى موقعها الأصلي.

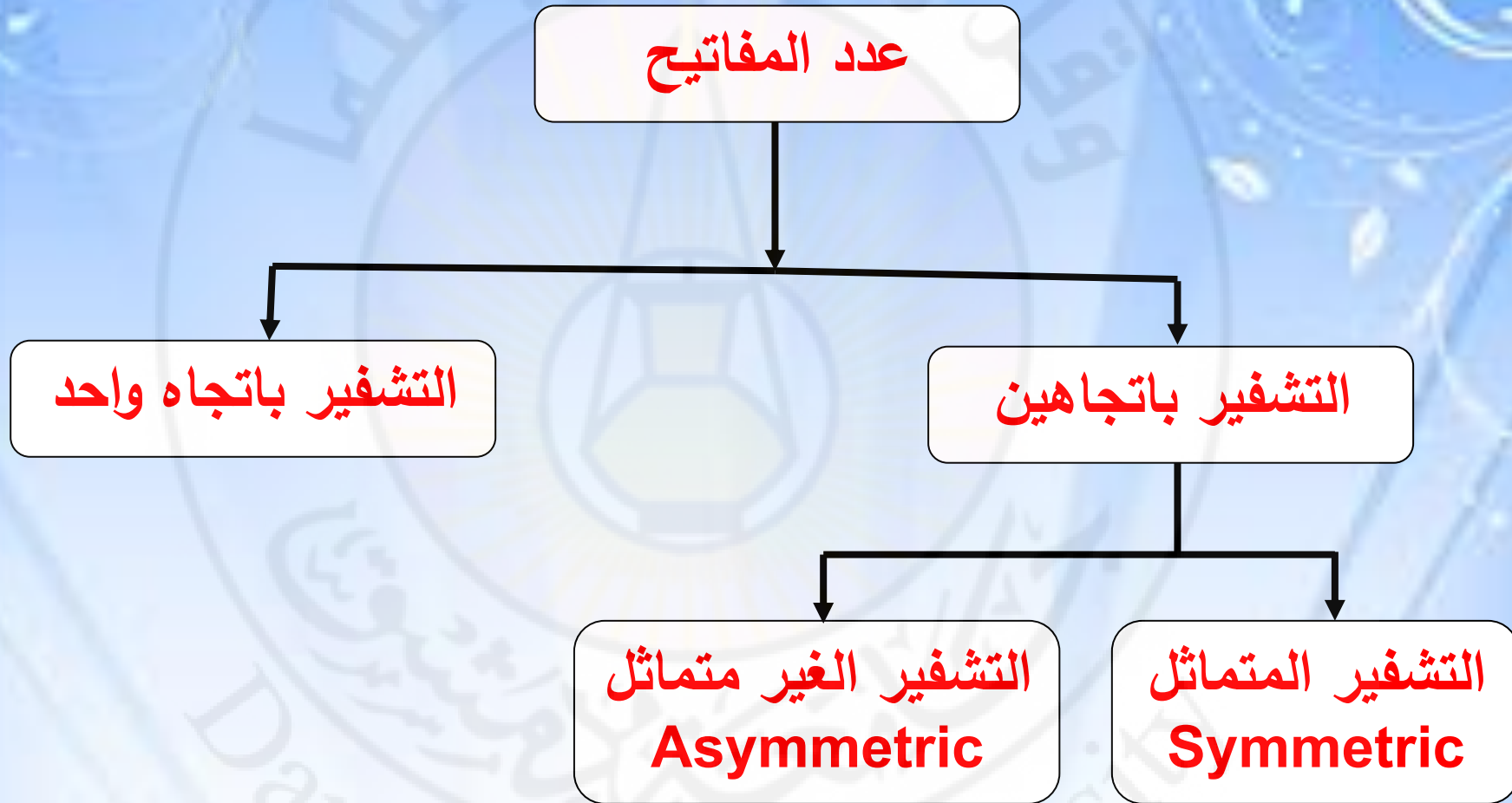
٧- معمي فيرنام Vernam:

* يعتمد هذا المعمي على مفتاح وحيد الاستخدام، وإذا كان المفتاح المستخدم في معمي التعويض هو تتابع عشوائي من الرموز، وبطول لانهائي عندها لا يكون هناك معلومات كافية لكسر المعمي، ويدعى مثل هذا المعمي بالمعمي ذو المفتاح وحيد الاستخدام (لا يتكرر استخدامه).

* لقد صمم غيلبرت فيرنام سنة ١٩١٧، والذي كان يعمل في شركة AT&T، والتي كان اسمها آنذاك شركة BELL جهاز تعمية يطبق على الاتصالات البرقية، ويعتمد على رمز بودوت، والخاص بالطابعات التي طورتها شركة AT&T، حيث أن كل رمز يتم تمثيله بتركيبة من خمس علامات (واحدات، وأصفار)، وفيه يتم توليد تتابع عشوائي غير مكرر على شكل رموز ممثلة ثنائياً، ويتم الجمع قياس ٢، ويعبر عن ذلك رياضياً كمايلي:

$$C_i = (M_i + K_i) \bmod 2$$

ثانياً: المفتاح المستخدم: أمن الرسالة يعتمد على سرية المفتاح وليس تفاصيل خوارزمية التشفير.



التشفير باتجاه واحد

هو التشفير الذي لا يمكن الرجوع فيه من النص المشفر إلى النص الأصلي مثل التشفير باستخدام خوارزميات التهشير (MD5 , SHA).

لماذا تستخدم هذه الطريقة مادامنا غير قادرين على استعادة النص الأصلي؟

تستخدم هذه الآلية عادةً في إثبات صحة المعلومات من التعديل وهويات المستخدمين والتوقيع الرقمي، وفي هذا النوع من التشفير عادةً يتم استخدام دالة الاختزال أو الـ (Hash Function)، وهي عبارة عن عملية تحويل الرسالة أو البيانات إلى قيمة عددية (Numeric Hash Value)، ودالة الـ Hash تعتبر إما أحادية الاتجاه أو مزدوجة، فإذا كانت أحادية الاتجاه، فلا تسمح للرسالة بأن تعود إلى قيمتها الأصلية، أما في حالة الدالة مزدوجة، فيسمح للرسالة بأن تعود إلى قيمتها الأصلية، وعلى الغالب، فإن أكثر دالات الهاش أحادية الاتجاه، أي يستحيل فهم النص المشفر أو العودة منه للنص الأصلي.

التشفير باتجاهيين

التشفير هو تغيير محتوى الرسالة الأصلية من خلال مزجها بمعلومات أخرى، أو استبدال الأحرف الأصلية، أو تغيير لمواقع الأحرف بحيث لن يفهمها إلا المرسل والمستقبل.

عناصر عملية التشفير:

- ١ - خوارزمية التشفير: وهي الخطوات المستخدمة لتحويل الرسالة الصريحة إلى رسالة مشفرة.
- ٢ - مفتاح التشفير: سلسلة الرموز المستخدمة في خوارزمية التشفير وقوة المفتاح تمثل قوة التشفير.
- ٣ - النص الصريح: وهي محتوى الرسالة الأصلية قبل التشفير وبعد فك التشفير.
- ٤ - نص الشيفرة: الرسالة بعد عملية التشفير.

تستخدم هذه الطريقة من التشفير عندما نكون بحاجة لاستعادة المعلومات التي قمنا بتشفيرها، أي إعادتها للنص الأصلي.

وصف الدالة الرياضية لعملية التشفير هي: $C = E(P, K)$,

وتعني تشفير الرسالة الصريحة وتحويلها إلى نص مشفر باستخدام المفتاح K .

وصف الدالة الرياضية لعملية فك التشفير هي: $D = (E(P, K), K)$,

وتعني إعادة الرسالة المشفرة إلى أصلها بعد تحويلها بواسطة المفتاح K الثاني.

حيث:

P : الرسالة الصريحة.

C : الرسالة المشفرة.

E : عملية التشفير.

D : عملية فك التشفير.

K : مفتاح التشفير وفك التشفير.

يوجد لهذا النوع من التشفير قسمين وهما:

أ- مفتاح خاص (تناظري) Symmetric Encryption: نفس المفتاح للتشفير وفك التشفير.



مزايا خوارزميات التشفير المتناظر:

١ - مفاتيح التشفير المتناظرة السرية تكون قصيرة نسبياً.

٢ - توفر هذه الخوارزميات معدلات عالية من سرعة تشفير البيانات.

مساوئ أو عيوب خوارزميات التشفير المتناظر:

١ - يجب أن يبقى المفتاح سرياً بين جهتي الاتصال.

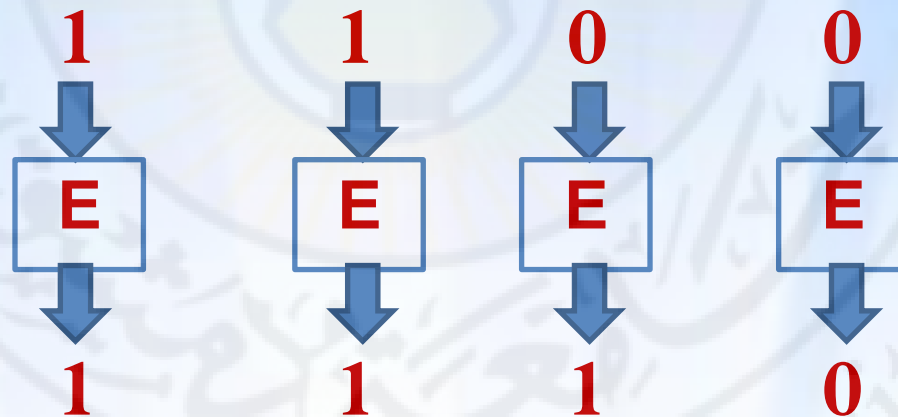
٢ - مشكلة نقل المفتاح السري بشكل آمن بين جهتي الاتصال دون وقوعه بيد طرف ثالث.

٣ - دورة حياة المفتاح يجب أن تكون قصيرة.

يمكن تقسيم خوارزميات التعمية التناظرية حسب طريقة معالجة الخوارزمية للنص المراد تشفيره إلى نوعين: هما التشفير الدفقي والتشفير الكتلي.

١- التشفير الدفقي Stream Cipher: وهي عملية تشفير كل حرف أو بت من النص الصريح بمفردها، والمثال التالي يوضح ذلك:

10011011010001011101

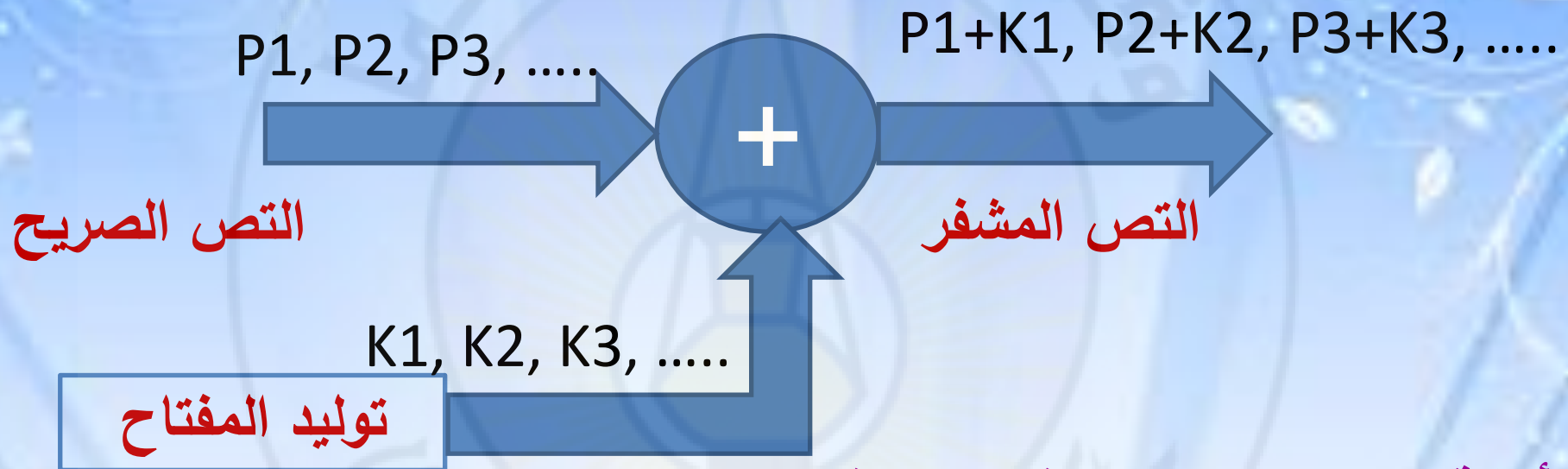


في الشكل السابق يتكون النص الصريح والمراد تشفيره من مجموعة من البتات وعملية التشفير تجري كمايلي:

- يدخل إلى خوارزمية التعمية البت الأول مع مفتاح التشفير وينتج عن هذه العملية أول بت من النص المشفر، وبعد ذلك يدخل إلى خوارزمية التعمية البت الثانية مع مفتاح التشفير وينتج عن هذه العملية ثاني بت من النص المشفر، وتستمر هذه العملية بنفس الطريقة إلى أن ينتهي طول الرسالة أو النص المراد تشفيره.

غالباً ما تكون خوارزمية التشفير الدفقي بسيطة مثلاً أن تكون مكونة من عملية (XOR).

يستخدم التشفير الدفقي مفتاح التشفير لإنتاج مفتاح دفي بطول النص المراد تشفيره والشكل التالي يوضح ذلك:



كأمثلة على خوارزميات هذا النوع نذكر:

(OTP: One-Time-Pad, RC4)

يوجد مجموعة متنوعة من خوارزميات التشفير التناظري مثل عائلة

RC: Rivest Cipher، وأحدث هذه الإصدارات هي RC6 وهو يمتلك ٣ أطوال للمفاتيح (١٢٨، ١٩٢، ٢٥٦) بت، وينفذ ٢٠ جولة على كل كتلة.

الحشوة لمرة واحدة OTP: One-Time Pad:

يكون في هذا المشفر طول المفتاح السري العشوائي مساوياً لطول النص غير المشفر مما يجعل من المستحيل عملياً كسر هذا المشفر، ومعرفة النص المرسل في الأصل، وتزداد سرية هذا المشفر عند تغيير المفتاح عند تغيير النص المرسل، حيث لا يجري استخدامه إلا مرة واحدة فقط، ويؤدي ذلك إلى ضمان السرية بشكل كبير ولكن يستحيل عملياً تحقيق ذلك بشكل سهل وتبادل المفتاح من وقت إلى آخر بين الطرفين المتصلين.

يركب النص الصريح مع مفتاح عشوائي، وهذه الطريقة غير قابلة للكسر رياضياً، كما أنها لا تتطلب استخدام الحاسوب، والحشو هو عبارة عن سلسلة طويلة من الأحرف العشوائية يتم تركيب هذه الأحرف مع النص الصريح لتوليد النص المشفر، وحتى نستطيع فك التشفير، فيجب أن نملك نسخة عن السلسلة العشوائية لعكس العملية، ويجب هنا استخدام الحشو مرة واحدة فقط ومن ثم حذفها.

النتيجة	الحساب	رقم موقع الحروف	الحشو Pad	رقم موقع الحروف	النص الصريح
U	$19+3-1=21$	3	C	19	S
F	$5+2-1=6$	2	B	5	E
A	$3+25-1=1$ (warp 26)	25	Y	3	C
W	$18+6-1=23$	6	F	18	R
I	$5+5-1=9$	5	E	5	E
T	$20+1-1=20$	1	A	20	T

٢- التشفير الكتلي Block Cipher: وهي عملية تشفير تعتمد على تجزئة النص الصريح إلى كتل متساوية في الطول قبل أن يتم تشفير كل كتلة بمفردها لينتج عنها كتلة مشفرة بنفس طول الكتلة غير المشفرة.

لقد انصبت الجهود بشكل أساسي على تطوير التشفير الكتلي، ويعود السبب في ذلك إلى المجال الأكبر للتطبيقات التي يمكن أن تستخدم هذا النوع من التشفير، فمعظم تطبيقات التعمية المتناظرة الخاصة بالشبكات تستخدم التشفير الكتلي، وهي طريقة تشفير تعمل على مدونة كتلة بيانات واحدة ثابتة الحجم في الوقت الواحد- تقوم بتشفير البيانات في مجموعات محددة الحجم (عادة ٦٤ بت)- وذلك خلافاً لتشفير تيار بيانات متدفقة stream cipher، والتي تشفر البيانات بوصفها تيار من البتات بشكل حرف واحد في وقت واحد. كتلة البيانات المرمزة (المشفرة) تحتوي على نفس العدد من الـ «بت» مثل الأصل.

أنماط التشفير الكتلي

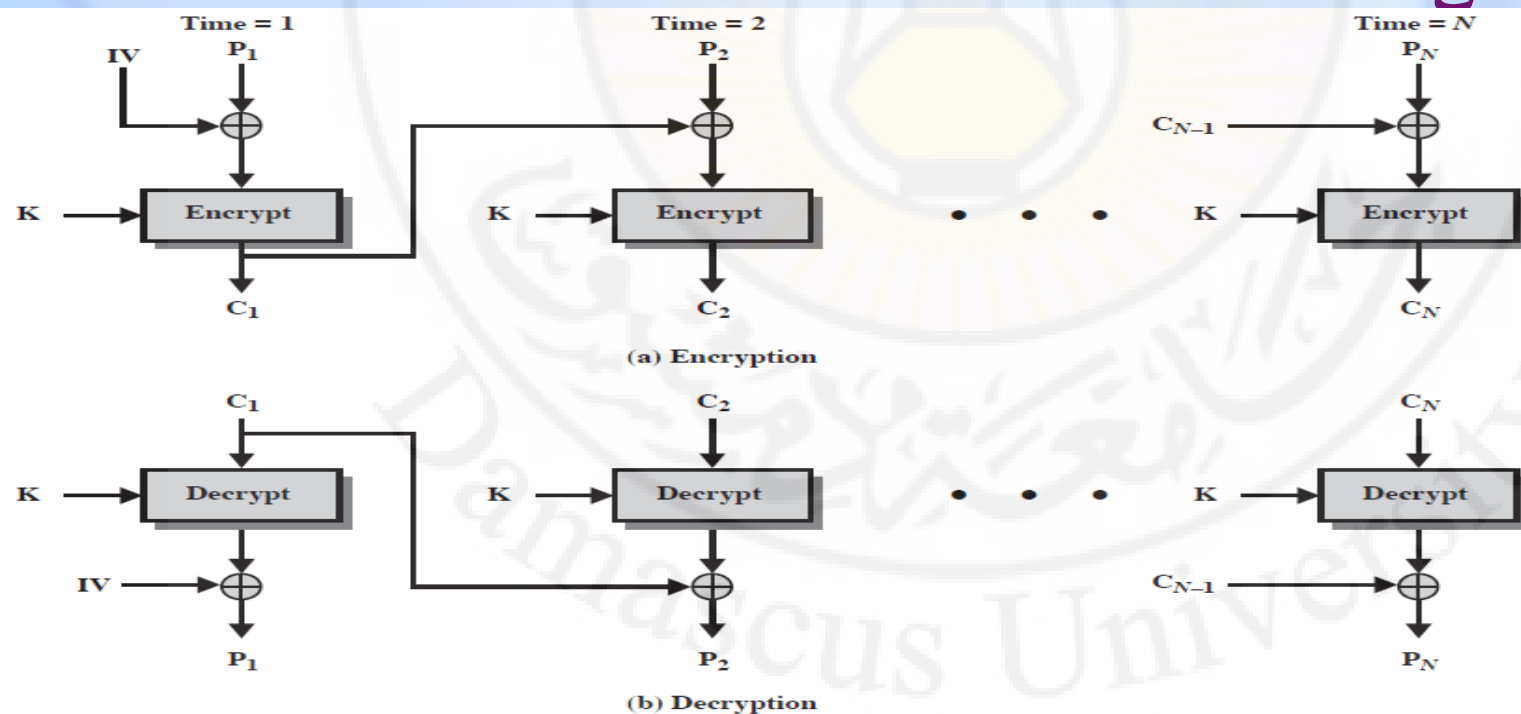
يوجد خمسة أنماط لهذا النوع من التشفير وهي:

- 1- ECB: Electronic Code Book mode.
- 2- CBC: Cipher Block Chaining mode – most popular.
- 3- OFB: Output Feed Back mode.
- 4- CFB: Cipher Feed Back mode.
- 5- CTR: Counter mode.

أشهر هذه النماذج هي CBC: Cipher Block Chaining، وفي هذا النمط سوف يتم تطبيق العملية XOR على النص الأصلي الحالي والنص المشفر السابق، أي:

(كتلة النص الأصلي الحالي) XOR (كتلة النص المشفر السابقة) وبعدها سوف ننفذ عملية التشفير.

بالنسبة إلى كتلة النص الأول، فلن يكون هناك نص مشفر سابق، لذلك سوف نطبق العملية مع متغير اسمه IV : Initialization Vector. يوضح الشكل التالي ذلك:



فيمايلي خطوات تنفيذ عملية التشفير بهذا النوع:

- يتم تقسيم النص الصريح إلى كتل $P1, P2, P3, \dots \text{etc}$.

- ينفذ على كل كتلة النص الصريح عملية XOR مع كتلة نص مشفرة مسبقاً، وذلك قبل تنفيذ عملية التشفير، والعلاقات التالية توضح عملية التشفير:

$$C_i = E_k (C_{i-1} \oplus P_i)$$

$$C_0 = IV$$

- يستخدم العامل الأولي IV لبدء العملية.

- فك التشفير وفقاً للعلاقة التالية:

$$P_i = C_{i-1} \oplus D_k(C_i)$$

كأمثلة مشهورة على التشفير الكتل نذكر على سبيل المثال لا الحصر النماذج التالية:

DES : Data Encryption Standard

RC2 : Rivest Cipher 2

RC5 : Rivest Cipher 5

3DES: Triple Data Encryption Standard

AES: Advanced Encryption Standard

IDEA: International Data Encryption Algorithm

Blowfish

وهي أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير.

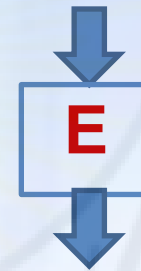
مثال:

تتمثل آلية عمل هذا النوع من التشفير بالخطوات التالية:
يعتمد طول الكتلة على خوارزمية التشفير.

تقسيم النص الصريح
إلى أطوال متساوية.

1001101101000101111010010

100110 110100 010111 101001 0



ادخال الكتلة الأولى إلى
خوارزمية التشفير مع
المفتاح السري لينتج
عنها كتلة مشفرة مكونة
من بتات طولها نفس
كتلة الدخل.

110010 011101 010010 001001

110010011101010010 0010010

تكرار الخطوة السابقة على باقي الكتل.



التشفير القياسي (المعياري)

* معظم اتصال المعطيات تكون ضمن المؤسسة أو المنظمة الواحدة، وغالباً ما يتم نقلها عن طريق شبكة خاصة، أو عن طريق خطوط مؤجرة (الاتصالات الفضائية)، وفي مثل هذه الحالات أو الظروف، فإن المعيارية تكون غير مطلوبة، ولكن في حال انتماء المستخدم إلى أكثر من منظمة، وكان المطلوب إرسال /استقبال المعطيات بين هذه المنظمات، عندها سيتم استخدام تجهيزات تشفير مختلفة، وهذا يتطلب المعيارية لتحقيق التوافقية، والانسجامية بين تجهيزات التشفير هذه (مكونات مادية، برمجيات، بروتوكولات، ... الخ)، وبالتالي يجب أن تكون خوارزميات التشفير معيارية أيضاً لتحقيق الاستخدام الواسع.

* إن التحرك الأول باتجاه التشفير العام القياسي كان قد أتى من الحكومة الفيدرالية الأمريكية، وتم تنفيذ ذلك سنة ١٩٤٧.

* هذه المعميات تم اقتراحها لأول مرة من قبل شارون، حيث استخدم تابع تعمية مركب من أنواع مختلفة من التوابع، فعلى سبيل المثال تابع مؤلف من توابع تبديل موقع، وتوابع تعويض بأنواعها المختلفة، وهذا ما هو مطبق في معمي Lucifer المصمم من شركة IBM، حيث يستخدم هذا المعمي تحويلاً يطبق بشكل متتابع تحويل تعويض، ثم تحويل تبديل موقع.

* في عالم الكمبيوتر، يعرف المعيار الذي يحكم الأساليب، والطرق اللازمة لتشفير البيانات باسم DES: Data Encryption Standard، وهناك معايير جديدة أخرى مازالت تحت الاختبار، والتي سوف تحل محل DES في المستقبل، مثل: AES: Advanced Encryption Standard، وتشمل المعايير الأخرى التي سوف يتم التحكم بها خوارزمية التوقيع الرقمي على سبيل المثال.

* يمكن أن تتم عملية التشفير حرفاً حرفاً، أو على بلوك (كتلة كاملة من الحروف) بالكامل، وحجم البلوك يعتمد على جهاز التشفير المستخدم، فمثلاً يعمل تشفير المعطيات القياسي DES بشكل أساسي على بلوك ٦٤ بت، وميزة تشفير البلوك عن تشفير البت تكمن بسرعة إنجاز عملية التشفير فقط وصعوبة الحصول على المعلومات الصريحة.

معييار التشفير المتقدم

AES: Advanced Encryption Standard

اعتمدت خوارزمية التشفير AES والمعروفة أيضاً باسم Rijndael من قبل الحكومة الأمريكية بعد منافسة من عدة جولات لتحل محل خوارزمية DES.

تقسم خوارزمية AES النص الصريح إلى كتل طول كل منها ١٢٨ بت، وتقوم بثلاث خطوات على كل كتلة، وضمن الخطوة ٢ يتم تنفيذ عدة جولات يتعلق عددها بطول المفتاح: ٩ جولات لمفتاح بطول ١٢٨ بت، و ١١ جولة لمفتاح بطول ١٩٢ بت، و ١٣ جولة لمفتاح بطول ٢٥٦ بت والمعروف بخوارزمية AES-256، حيث يتم في كل جولة استبدال البايتات، وإعادة ترتيبها، ومن ثم تحقيق بعض عمليات الضرب الخاصة حسب الترتيب الجديد.

لم ينجح أي هجوم على AES حتى الآن.

خوارزمية تشفير المعطيات العالمية

IDEA: International Data Encryption Algorithm

يعتمد هذا النوع على التشفير الكتلي الذي يعالج ٦٤ بت باستخدام مفتاح بطول ١٢٨ بت مع ٨ جولات وتعتبر هذه الخوارزمية آمنة أيضاً.

هناك أيضاً خوارزمية بلوفيش Blowfish الكتلية التي تستخدم كتل بطول ٦٤ بت ومفاتيح بأطوال مختلفة من ٣٢ بت إلى ٤٤٨ بت، ولا يوجد حتى الآن عيوب في هذه الخوارزمية، ويوجد لها تحديث يعرف باسم Towfish لكنها غير معروفة مثل سابقتها.

خوارزمية التشفير المعيارية

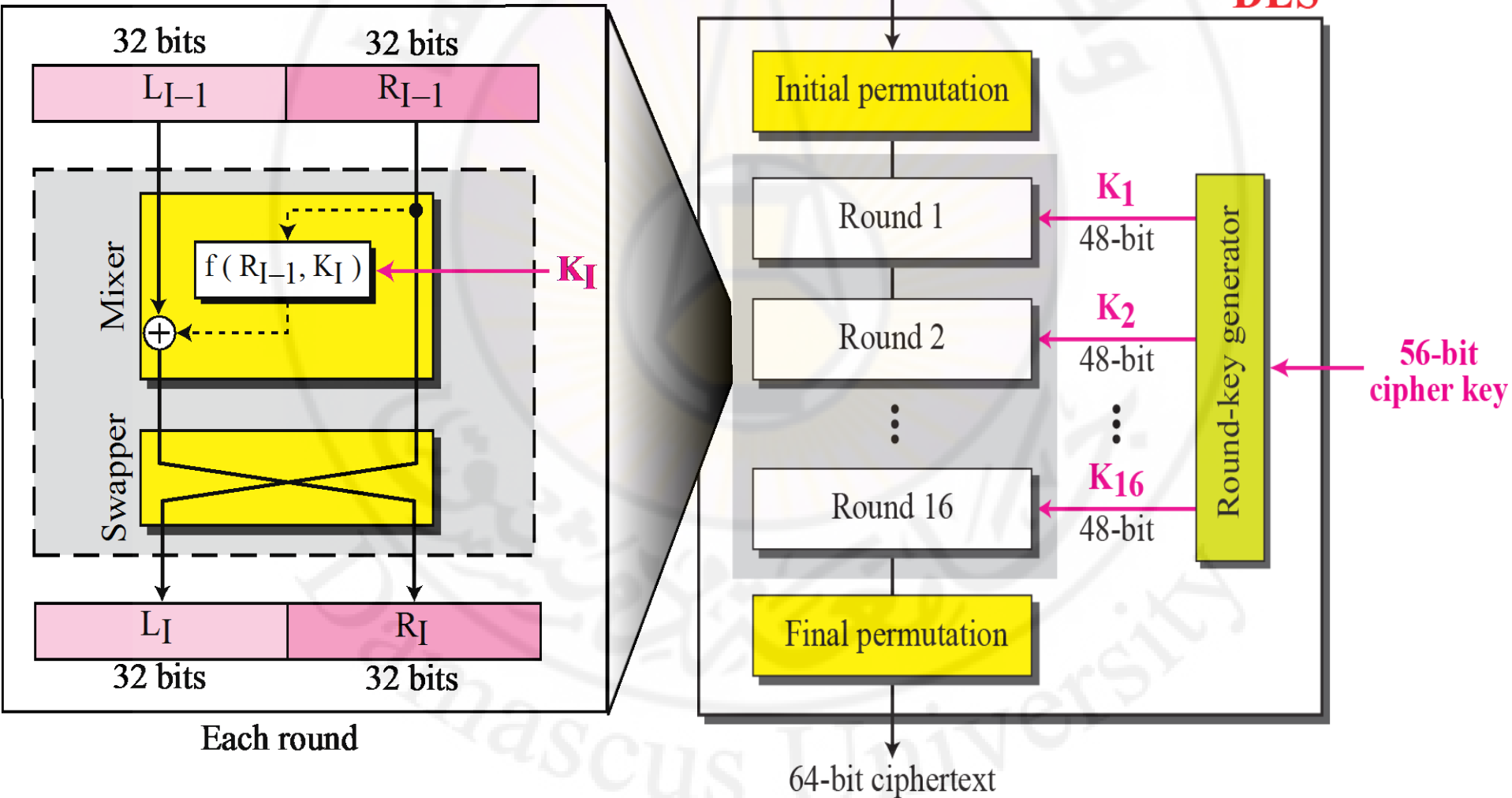
DES: Data Encryption Standard

* لقد تم اقتراح خوارزمية DES سنة ١٩٧٧ من قبل المكتب القومي للأمن، وهو تطوير لمعمي Lucifer، وهو يعمل على تعمية بلوكات (رزم) بطول ٦٤ بت، وذلك باستخدام مفتاح بطول ٥٦ بت، حيث تبدأ عملية التعمية بتبديل مواقع البلوك ذو الطول ٦٤ بت، وذلك طبقاً لتبديلة أولية IP، وبعد أن يتم إخضاعها إلى ١٦ مرحلة تعويض وتبديل من التتابع F يتم تبديل مواقع المحصلة تبعاً لمعكوس التبديلة الأولية (IP^{-1})، وذلك للحصول على النص المعمي النهائي، وكل من هذه العمليات لها مفتاح مختلف.

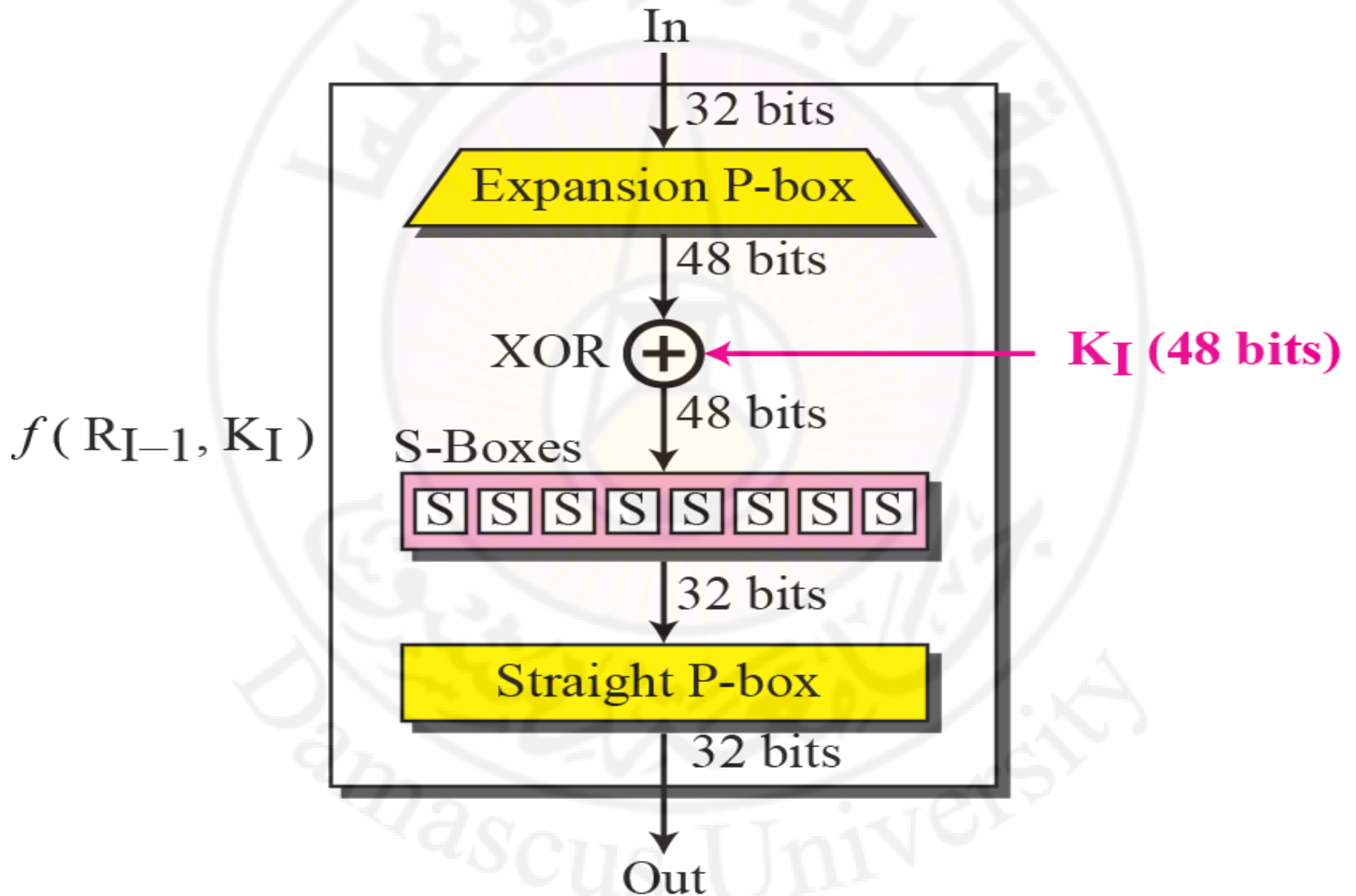
* DES موجود كمكون مادي، وبرمجي، لذلك يستخدم في الكثير من التطبيقات، وقد تم كسره في نهاية ١٩٩٩، وتم تعديله، وأصبح طول المفتاح ٩٦ بت، ثم ١٢٨ بت، وذلك لزيادة قوة أمن التشفير فيه.

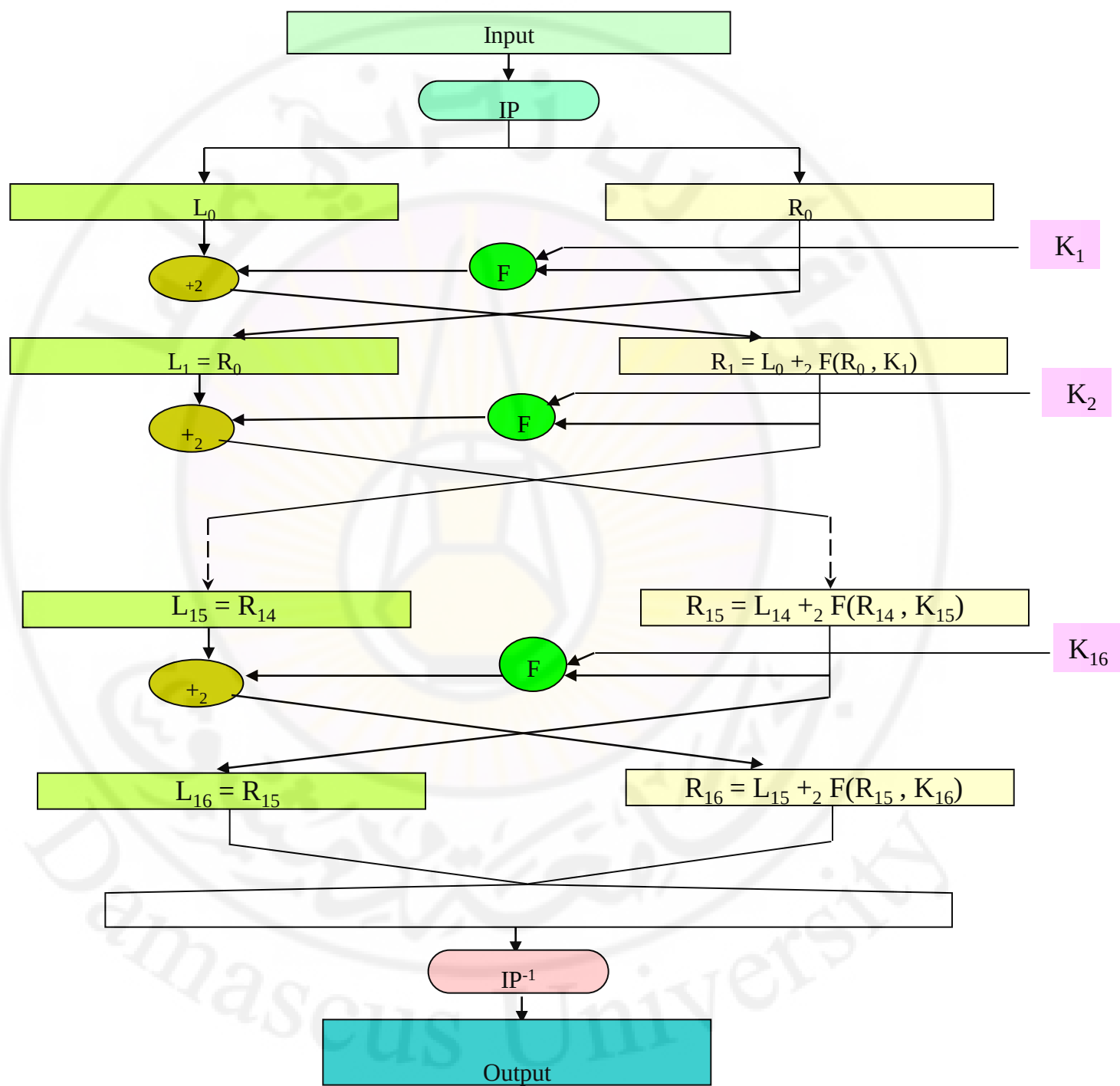
* يوضح الشكل التالي عملية التشفير وفك التشفير باستخدام خوارزمية DES:

البنية العامة لخوارزمية DES



تابع DES





* يمكن تمثيل النتائج بشكل رياضي كمايلي:

$$L_j = R_{j-1}$$

$$R_j = L_{j-1} +_2 P_j$$

حيث $+_2$ تمثل عمل دارة XOR.

$$P_j = F(R_{j-1}, K_j)$$

$$R_j = L_{j-1} +_2 F(R_{j-1}, K_j)$$

* خطوات تطبيق هذه الخوارزمية هي:

١- نص صريح مكون على الأقل من ٦٤ بت. تتم مبادلة أولية IP على المسجل الأول. $X_0 = IP(X) = L_0 R_0$.

٢- إعادة عملية المبادلة ١٦ مرة، وتكون قيمة كلا من R, L كمايلي:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} +_2 F(R_{i-1}, K_i)$$

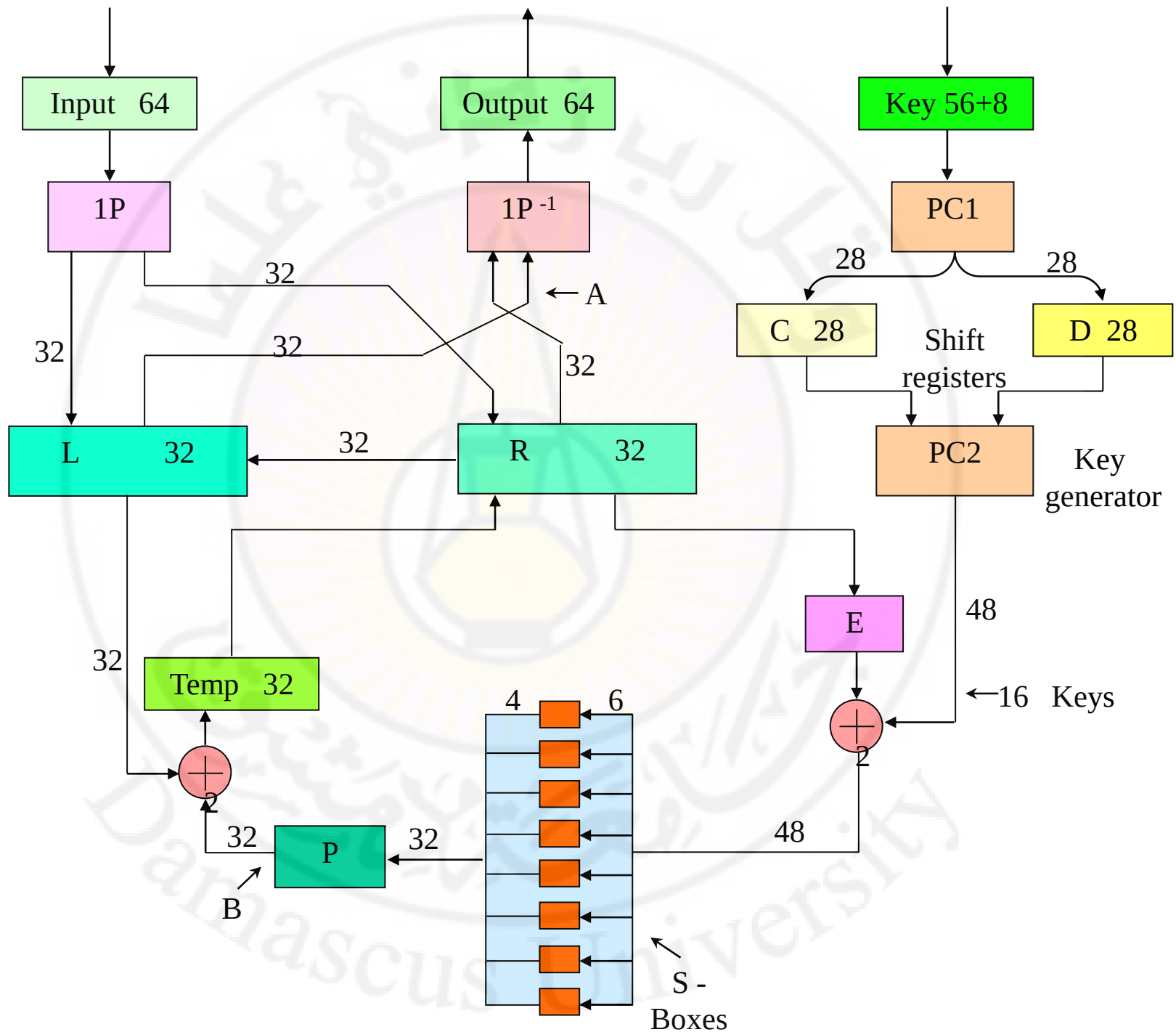
حيث $+_2$ هي دارة exor.

F : تابع أسي.

K : مفتاح.

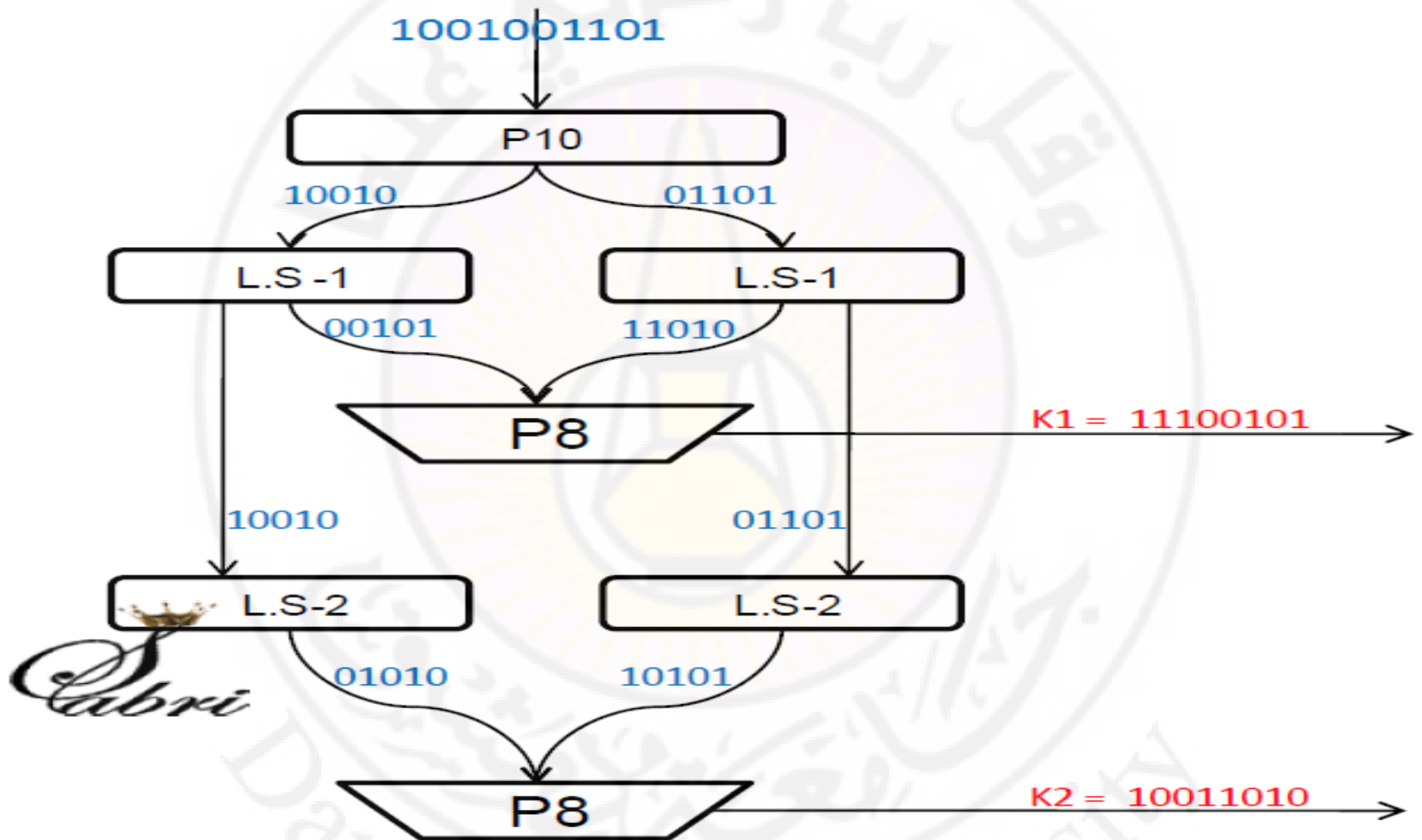
٣- تطبيق مبادلة عكسية IP^{-1} على المسجل الأخير R_{16}, L_{16} .

* يوضح الشكل التالي مخطط تشفير المعطيات، والذي يضم التشفير، وفك التشفير:



To Find (Generate) The keys

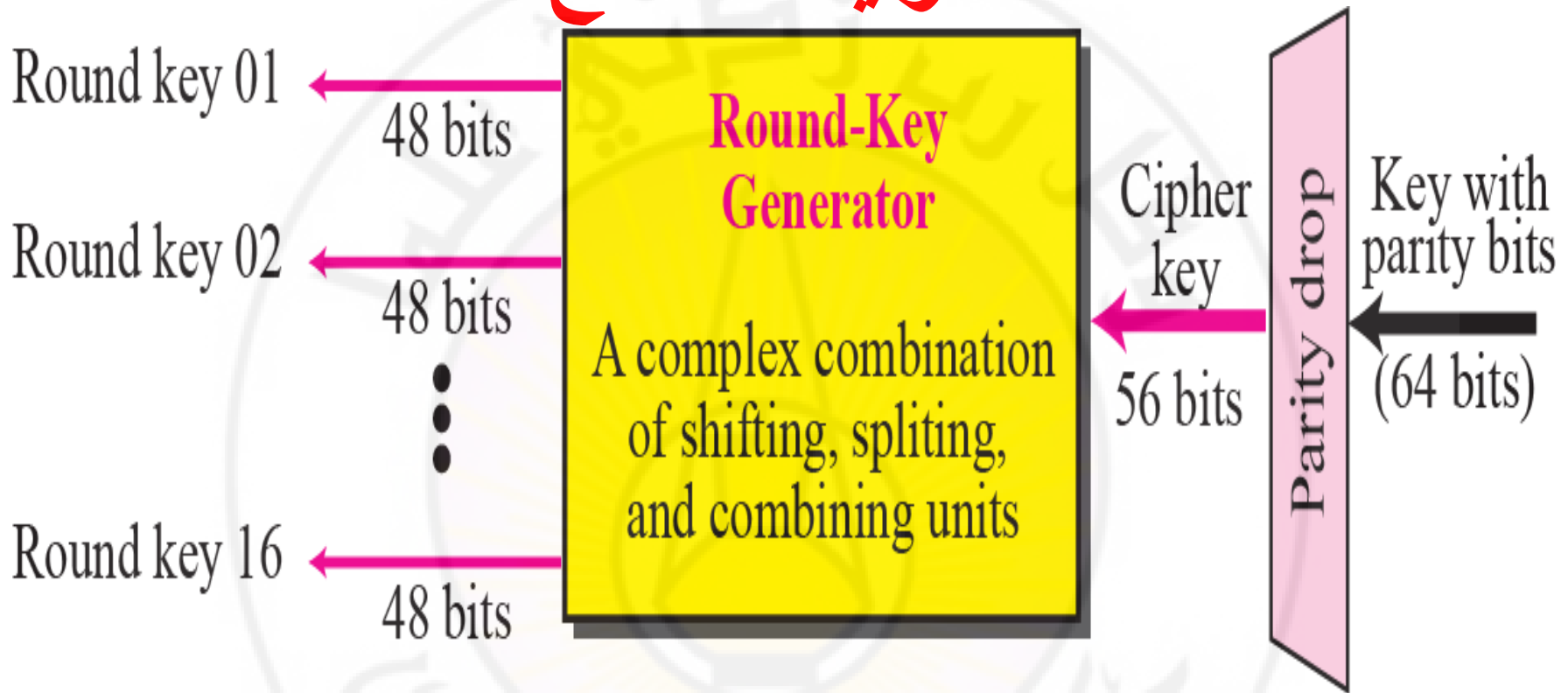
Key Generation



K1 = 11100101

K2 = 10011010

توليد المفتاح



مثال:

Plaintext:

123456ABCD132536

Key:

AABB09182736CCDD

CipherText:

C0B7A8D05F3A829C

Plaintext:

0000000000000000

Key:

22234512987ABB23

Ciphertext:

4789FD476E82A5F1

Plaintext:

00000000000000001

Key:

22234512987ABB23

Ciphertext:

0A4ED5C15A63FEA3

مثال ١ :

Plaintext:

123456ABCD132536

Key:

AABB09182736CCDD

CipherText:

C0B7A8D05F3A829C

مثال ٢ :

Plaintext:

0000000000000000

Key:

22234512987ABB23

Ciphertext:

4789FD476E82A5F1

Plaintext:

00000000000000001

Key:

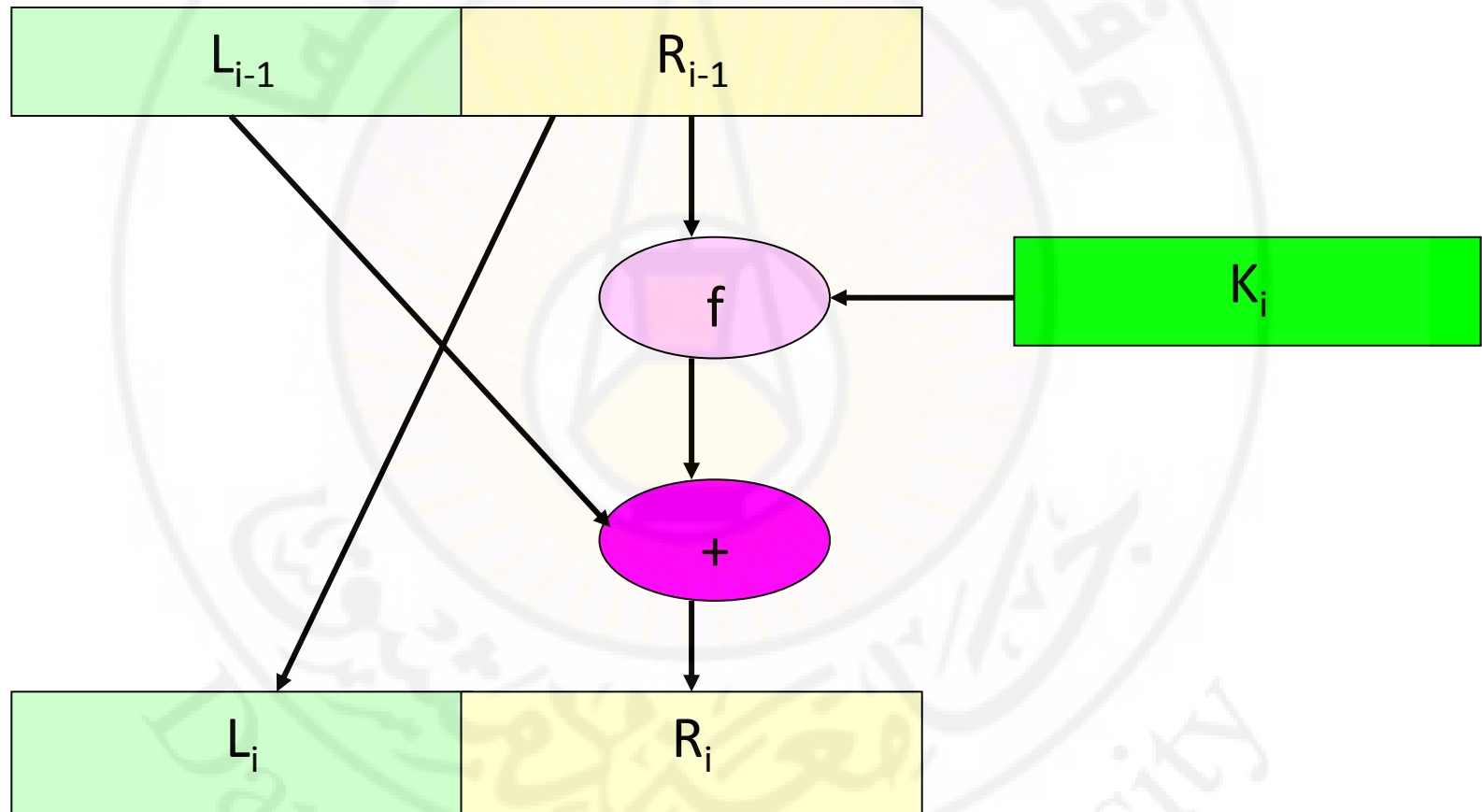
22234512987ABB23

Ciphertext:

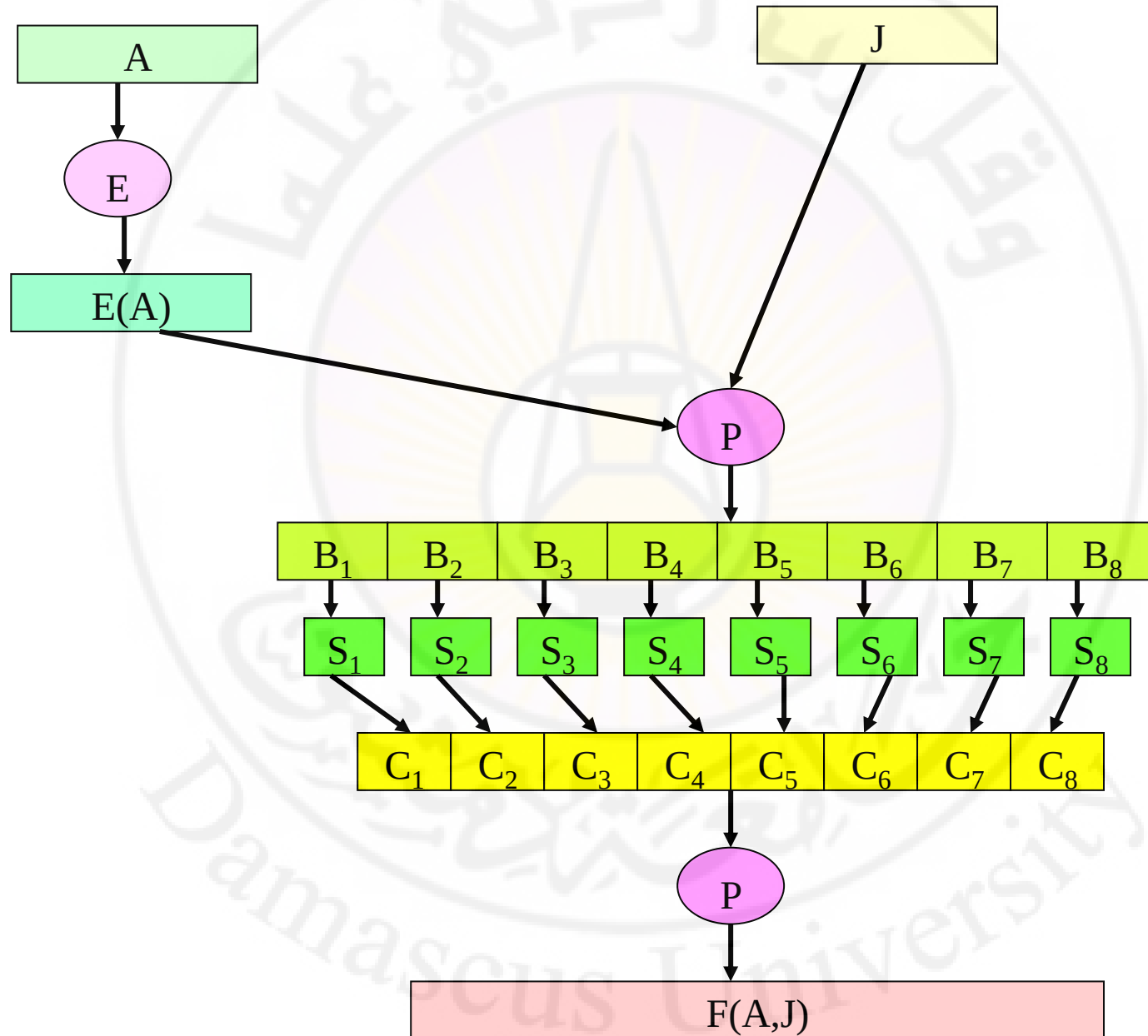
0A4ED5C15A63FEA3

لاحظ تغير بت واحد بالنص الصريح كيف حصلنا على نصي مشفرين مختلفين كلياً عن بعضهما البعض.

* سنوضح فيمايلي شرح هذه الخوارزمية، حيث يوضح الشكل التالي جولة واحدة لمعمي DES:

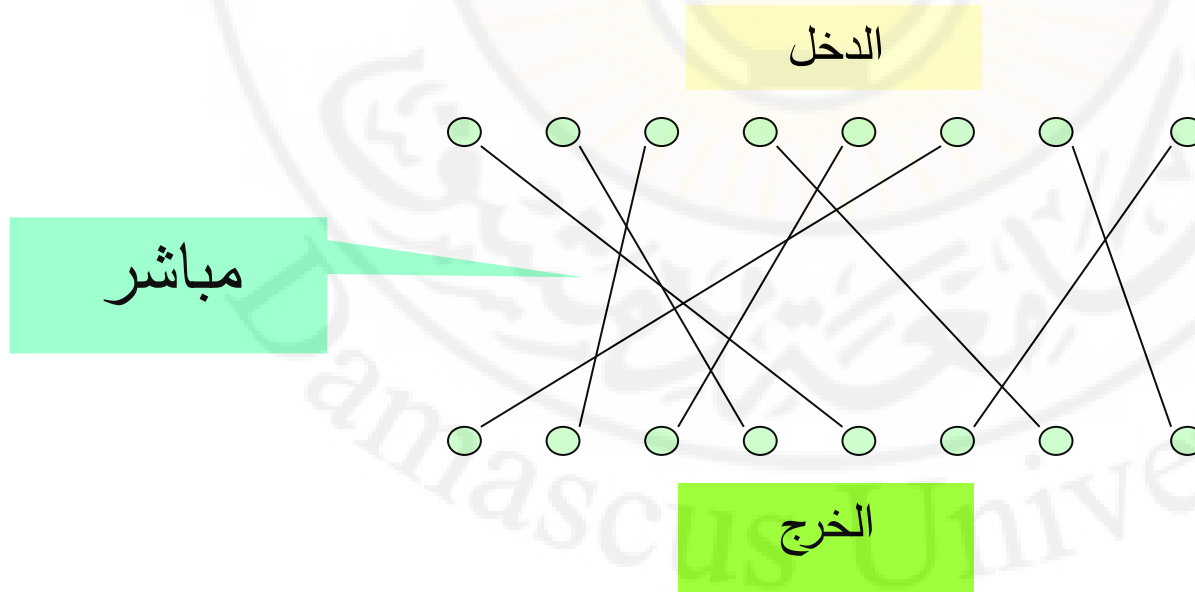


* يوضح الشكل التالي التابع f المستخدم في DES:



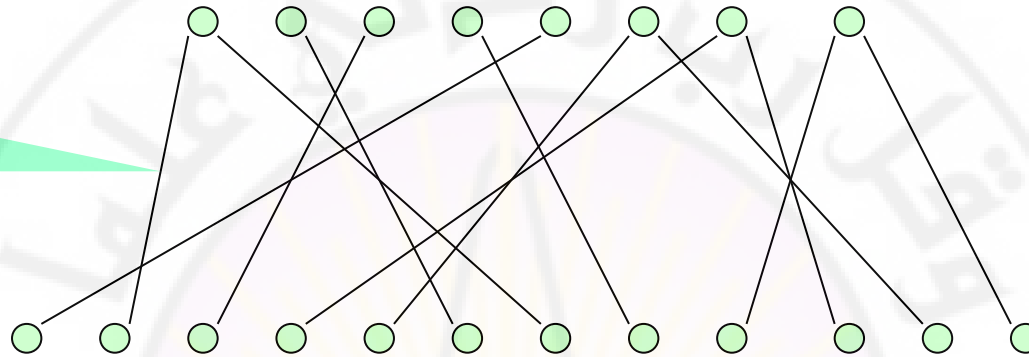
والعمل يتم كمايلي:

* الدخل (النص الصريح) يكون ٦٤ بت، الخرج (النص المشفر) يكون ٦٤ بت، وطول مفتاح التشفير/ فك التشفير ٦٤ بت، وخوارزمية التشفير تحول النص الصريح إلى نص مشفر وبالعكس. بالنسبة لمفتاح التشفير فقط ال ٥٦ بت تدخل بشكل مباشر في خوارزمية التشفير، والخانات الباقية (٨ بت) من أجل تكافؤ مفرد. كتل بناء الخوارزمية تكون معتمدة على التعويض، والتبديل، و XOR، وإن التبدل يأخذ ثلاثة أصناف هي: مباشر، موسع، اختيار متبدل. والشكل التالي يوضح هذه النماذج:



الدخل

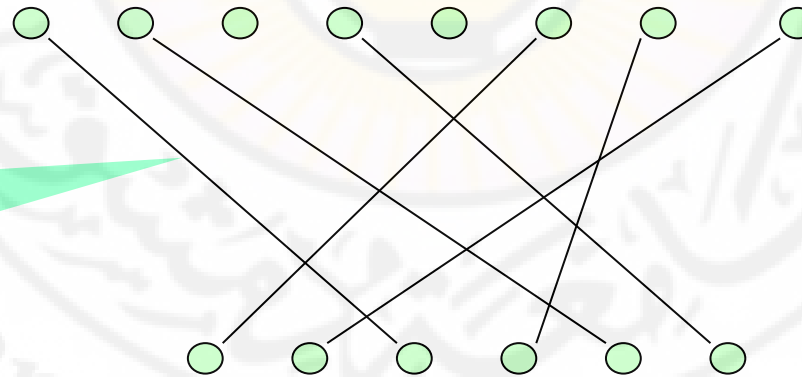
موسع



الخرج

الدخل

متبدل



الخرج

* في التصنيف المباشر تكون البتات مسجلة، بينما في الموسع بعض البتات تكون مضاعفة، وكامل حقول النتيجة تسجل، أما الصنف الثالث، فإن بعض البتات يتم تجاهلها، والباقي يتم تسجيلها.

* بالنسبة لمعميات التعويض تكون معروفة بالصناديق S-BOX، وتكون محددة بثمانية جداول مختلفة، وكل صندوق يملك ٦ بتات للدخل، و ٤ بتات للخروج، وإن أول خطوة هي قبول المعطيات في المسجلات الثمانية، وعندما يكون الدخل كامل (٦٤ بت)، فإن محتوى مسجلات الإزاحة تكون مقدمة بالتتالي، والطريقة الصحيحة تكون موضحة بالجدول التالي:

* يوضح الجدول التالي القيمة الأولية IP:

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

* بعد عملية التبديل الأولى، فإن حقل المعطيات ٦٤ بت تكون مقسمة إلى ٣٢ بت، والتي يتم إرسالها إلى المسجلات R, L قسم من الحلقة الأساسية لمنطق الخوارزمية.

* يوضح الجدول التالي معكوس القيمة الأولية IP^{-1} :

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

* عندئذ عمل الحلقة الأساسية للخوارزمية يبدأ. من المسجل R 32 بت يتم إقرارها إلى التبدیل الموسع، والذي يكون تحويل نظامي، وخرج التبدیل يتألف من ٤٨ بت، ومن أجل كل ٤ بت (الأول، الرابع، الخامس، الثامن) تكون مضاعفة، والشرح الكامل للتبدیل يكون موضحاً بالجدول التالي:

جدول اختيار بت E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

* في هذا التبديل يستجيب البت الأول إلى الدخل ٣٢، وخرج البت الثاني يستجيب إلى دخل البت الأول، وهكذا الخرج الآخر من المسجل R يكون موجه ٣٢ بت ليتحول إلى المسجل L. الخرج ٤٨ بت من التبديل الموسع تعتبر المرور الثاني إلى عمل دائرة XOR، والتي تضم مع اختيار البت من مفتاح التشفير.

* الخرج ٤٨ بت من عمل XOR يكون مقسم إلى ثمان ستات من أجل الدخل لوضع ٨ صناديق، وهكذا فإن الصندوق يستقبل ٦ بت كدخل، ولكن يعطي بالخرج ٤ بت، وتوضح الجداول التالية الثمانية صناديق S-Boxes، والمبادلة P:

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4															
7	13	1 4	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	0	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S ₅															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S ₆															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

* في هذا التبديل يستجيب البت الأول إلى البت ١٦ كدخل، والبت الثاني يستجيب إلى البت ٧ كدخل، والجدول التالي يوضح ذلك:

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

* من أجل إكمال الحلقة الأساسية للخوارزمية يكون الخرج من التبديل متحد مع محتويات المسجل L في عمل XOR، والنتيجة تتحرك في المسجل R، ومن أجل اختبار هذا العمل بدون تضارب بالمسجل، فإن مسجل مؤقت يكون ظاهر في الشكل بين المسجل R و XOR.

* دورة الحلقة الأساسية هذه يتم إعادتها (تكرارها) ١٦ مرة قبل أن يتم تجميع محتوى المسجلات R, L في بلوك ٦٤ بت في تتابع R, L، وكل دورة من الحلقة الأساسية تعرف بالجولة.

* بقي أن نوضح كيف أن مفتاح التشفير يشارك في العملية. لقد رأينا بأن الخرج ٤٨ بت من التبديل الموسع يتحد مع البتات المختارة من مفتاح التشفير قبل الدخول إلى الصندوق، والبتات المختارة تكون مختلفة في كل الجولات الـ ١٦.

* في الجانب الأيمن من الشكل السابق الطريقة لتوليد هذه البتات تكون ظاهرة (مرئية) بعد إدخال المفتاح إلى مسجل المفتاح، ويتم قراءة المفتاح في الخيار الأول المبدل PC1، حيث كل ثامن بت يهمل.

C

* تبادلات PC-1, PC-2 (Permuted Choice) المستخدمة في
تقدير جدول المفتاح موضحة بالجدول التالية:

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

D

* هنا البت الأول من الدخل إلى المسجل C يستجيب إلى البت الخامس من مفتاح التشفير، والبت الأول من الدخل إلى المسجل D يستجيب إلى البت ٦٣ من مفتاح التشفير. البتات ٥٦ تقسم إلى ٢٨ بت، ويتم تحميلها في المسجلات D,C.

* تدور الرسالة بمسجلات الإزاحة، ومن أجل التشفير يتم تدويرها يساراً بموقع أو موقعين لكل ١٦ جولة من الخوارزمية.

* يوضح الجدول التالي الإزاحات اليسارية قبل التشفير:

عدد الإزاحات اليسارية قبل PC2	كتلة المفتاح	الدور
١	K1	١
١	K2	٢
٢	K3	٣
٢	K4	٤
٢	K5	٥
٢	K6	٦
٢	K7	٧
٢	K8	٨
١	K9	٩
٢	K10	١٠
٢	K11	١١
٢	K12	١٢
٢	K13	١٣
٢	K14	١٤
٢	K15	١٥
١	K16	١٦

* لإنتاج اختيار ٤٨ بت المطلوبة للضم مع الخرج الموسع في الحلقة الأساسية للخوارزمية، محتوى الاتحاد لـ C, D، يتم إرسالها إلى الخيار المبدل الأبعد PC2، وهذا يملك بنية غير نظامية البت الأول للخرج يستجيب إلى البت ١٤ كدخل. الخرج الثاني يستجيب إلى الدخل ١٧ وهكذا الخرج من PC2.

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

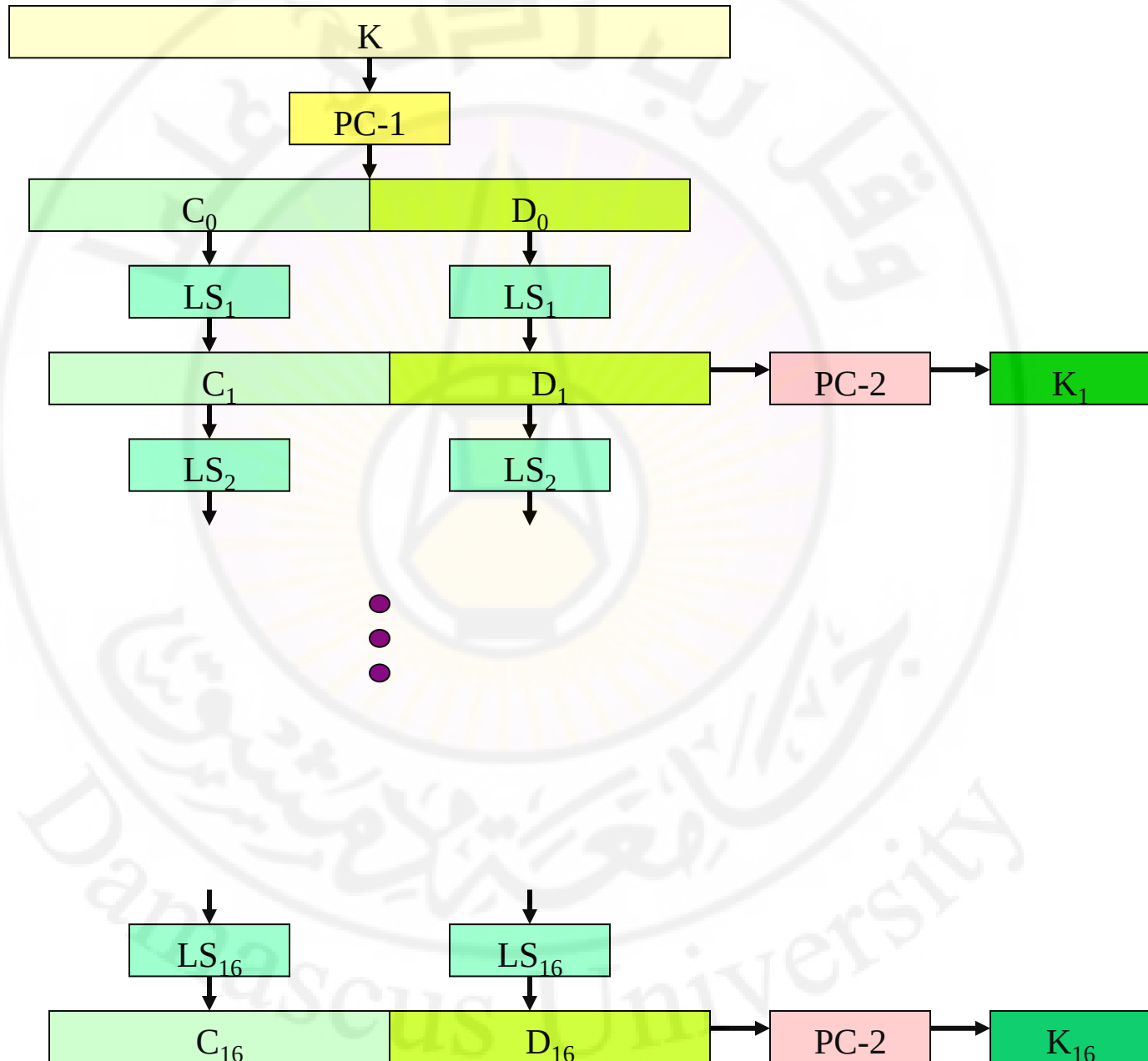
* يتألف من ٤٨ بت من أجل كل جولة من الخوارزمية خرج PC2 يشكل مفتاح جزئي في الحلقة الأساسية. عملية فك التشفير تتم بنفس الطريقة، والاختلاف الوحيد فقط يكون بتوليد المفاتيح الفرعية.

* من أجل عملية التشفير، فإن مسجلات الإزاحة C, D تكون ملتفة إلى اليمين. والمنظر العكسي من ذلك يستخدم في التشفير، وتنظم الإزاحات اليمينية من أجل فك التشفير تكون معطاة بالجدول التالي:

* يوضح الجدول التالي الإزاحات اليمينية قبل فك التشفير:

عدد الإزاحات اليمينية قبل PC2	كتلة المفتاح	الدور
٠	K1	١
١	K2	٢
٢	K3	٣
٢	K4	٤
٢	K5	٥
٢	K6	٦
٢	K7	٧
٢	K8	٨
١	K9	٩
٢	K10	١٠
٢	K11	١١
٢	K12	١٢
٢	K13	١٣
٢	K14	١٤
٢	K15	١٥
١	K16	١٦

* يوضح الجدول التالي بيان تقدير مفتاح DES:



* توضح الجداول التالية جولات ٤٨ بت من المفتاح:

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

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

ROUND 3

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

ROUND 4

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

ROUND 5

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

ROUND 6

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

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

ROUND 8											
36	41	60	50	10	43	59	18	57	35	9	3
58	25	52	51	34	19	49	27	26	17	44	2
12	54	61	13	31	30	6	20	62	47	45	23
55	15	28	22	37	46	39	4	7	21	14	53

ROUND 9

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

ROUND 10

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

ROUND 11

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

ROUND 12

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

ROUND 13

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

ROUND 14

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

ROUND 15

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

ROUND 16

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



أمثلة على DES

* الشكل التالي يوضح عملية التشفير، وفك التشفير لنصوص مختلفة:

مفتاح التشفير KEY	النص الصريح	النص المشفر	مسافة هامنج
0	1	CDE872D4A471346F	CD3D0AA4C4024B4A
1	2	8BCDEFABCD	801F8A2968BC4473
2	3	38A9CDEFABCD	5D98C47DDDBA6F30
3	4	ABDDEFABCD	ABCFEFABCD
4	5	265	6ABCD6FABCD
5	6	67C269F2542791F9	F8C98F79ADC06EA4
6	7	337ABCEBABCDEFABCD	87D3240ABB F44074
7	8	348ABCDFFDBCDEFABCD	DB998B67046CDCE7
8	9	9ABCDEF9CDEFABCD	2F6E5470E4E351AC
9	10	10ABCDEFABEDEFABCD	B53E42DE30F97AD0
10	11	11ABCDEFABCCEDEFABCD	4F4067726B35B014
11	12	12ABCDEFABCD6FABCD	AB155289660C60B2
12	13	13ABCDEFABCDE7ABCD	5BDA93F7D427B8D2
13	14	14ABCDEFABCDEF2BCD	9853C511ED56887E
14	15	15ABCDEFABCDEF9AFCD	70AA2407959F04B1
15	16	16ABCDEFABCDEFABDD	892BEC47C9712BE3
16	17	2617ABCDEFABCDEFABC5	

* الشكل التالي يوضح عملية التشفير ، وفك التشفير لنصوص مختلفة:

	Plaintext	A B C D E F A B C D E F A B C D
Key	Ciphertext	Hamming distance
	C D E 8 7 2 D 4 A 4 7 1 3 4 6 F	1 0 1 2 3 4 5 6 7 8 9 A B C D E F
1 B 7 3 F E 8 B C 0 B 8 8 6 0 6	35	2 8 0 2 3 4 5 6 7 8 9 A B C D E F
0 F 9 2 F 6 0 D 2 F D 4 D 8 B 7	32	3 0 2 2 3 4 5 6 7 8 9 A B C D E F
3 1 A F D 8 C 5 4 F B F 4 B C D	37	4 0 1 6 2 4 5 6 7 8 9 A B C D E F
C 7 9 F 5 9 6 3 D 4 6 5 A 7 E E	29	5 0 1 2 6 4 5 6 7 8 9 A B C D E F
3 6 5 2 9 C C 1 0 7 1 7 A 3 8 9	39	6 0 1 2 3 0 4 6 7 8 9 A B C D E F
7 F 3 5 F 7 E 6 C E C 5 7 E E 3	30	7 0 1 2 3 4 6 6 7 8 9 A B C D E F
C 9 F 3 F D 9 2 6 0 C 6 8 1 8 A	27	8 0 1 2 3 4 5 4 6 8 9 A B C D E F
E 6 9 2 8 3 2 2 E E 8 B 9 A 6 9	36	9 0 1 2 3 4 5 6 4 8 9 A B C D E F
0 9 9 7 A 5 A F 6 E 4 E 1 4 6 0	37	10 0 1 2 3 4 5 6 7 A 8 A B C D E F
C 7 B 4 1 C 4 F 3 8 D 9 A F 7 A	31	11 0 1 2 3 4 5 6 7 8 A A B C D E F
4 B 4 A A 2 0 A B 2 1 4 4 D D D	30	12 0 1 2 3 4 5 6 7 8 9 E A C D E F
1 2 9 9 7 E E 8 0 0 1 B D 2 7 C	32	13 0 1 2 3 4 5 6 7 8 9 A 8 C D E F
4 2 D 1 7 B 7 D F 5 3 4 3 B 7 9	28	14 0 1 2 3 4 5 6 7 8 9 A B 4 C E F
8 7 F 6 4 9 3 C 4 C 8 9 8 3 2 7	33	15 0 1 2 3 4 5 6 7 8 9 A B C E E F
F C 3 0 F 6 F 7 6 B D 4 2 5 9 2	31	16 0 1 2 3 4 5 6 7 8 9 A B C D 6 E
17 0 1 2 3 4 5 6 7 8 9 A B C D E C	1 C B D E C 4 B 7 9 B C A 7 A 1	39
Mean Hamming distance 32.88		

* الشكل التالي يوضح عملية التشفير، وفك التشفير لنصوص، ومفاتيح تشفير مختلفة:

Encipherment with key 08192A3B4C5D6E7F

Plaintext 1 0000000000000000

Plaintext 2 0000000000000001

Round	Register L	Register R	Register L	Register R	Haming Distance
1	00000000	00000000	00000080	00000000	1
2	00000000	AF0D68FD	00000000	AF0D687D	1
3	AF0D68FD	CE0A36EA	AF0D687D	CE3A32E2	5
	CE0A36EA	0BDCC5FE	CE3A32E2	81BDED5F	15
5	0BDCC5FE	5D181CC3	81BDED5F	F8CA39B2	26
6	5D181CC3	1744B978	F8CA39B2	A994B918	26
7	1744B978	9B1CB0D8	A994B918	3E9D05D8	22
8	9B1CB0D8	7AE8C7E0	3E9D05D8	23F48DFF	26
9	7AE8C7E0	A2AC7B3F	23F48DFF	9D58DCFB	34
10	A2AC7B3F	580E51EF	9D58DCFB	3F076303	34
11	580E51EF	2865DBD4	3F076303	97AE4AE3	35
12	2865DBD4	BF68F77C	97AE4AE3	68ABB612	37
13	BF68F77C	8F57F629	68ABB612	09D9C398	32
14	8F57F629	0827B240	09D9C398	44B0435C	31
15	0827B240	F2DEBFAC	44B0435C	319FD4B8	29
16	F2DEBFAC	16CD0EB8	319FD4B8	42684FF9	24

Ciphertext 1 25DDAC3E96176467

Ciphertext 2 1BDD183F1626FB43 22

* يوضح الشكل التالي مثال تفصيلي عن عمل شفرة DES:

$$\begin{array}{lcl} L_0 & = & 11001100000000001100110011111111 \\ L_1 = R_0 & = & 11110000101010101111000010101010 \end{array}$$

The 16 rounds of encryption are then performed, as indicated.

$$\begin{array}{lcl} E(R_0) & = & 0111101000010101010101011110100001010101010101 \\ K_1 & = & 00011011000000101110111111111000111000001110010 \\ E(R_0) \oplus K_1 & = & 011000010001011110111010100001100110010100100111 \\ \text{S-box outputs} & & 01011100100000101011010110010111 \\ f(R_0, K_1) & = & 00100011010010101010100110111011 \\ L_2 = R_1 & = & 11101111010010100110010101000100 \end{array}$$

$$\begin{array}{lcl} E(R_1) & = & 011101011110101001010100001100001010101000001001 \\ K_2 & = & 011110011010111011011001110110111100100111100101 \\ E(R_1) \oplus K_2 & = & 000011000100010010001101111010110110001111101100 \\ \text{S-box outputs} & & 11111000110100000011101010101110 \\ f(R_1, K_2) & = & 00111100101010111000011110100011 \\ L_3 = R_2 & = & 11001100000000010111011100001001 \end{array}$$

$$\begin{array}{lcl} E(R_2) & = & 11100101100000000000010101110101110100001010011 \\ K_3 & = & 010101011111110010001010010000101100111110011001 \\ E(R_2) \oplus K_3 & = & 101100000111110010001000111110000010011111001010 \\ \text{S-box outputs} & & 00100111000100001110000101101111 \\ f(R_2, K_3) & = & 01001101000101100110111010110000 \\ L_4 = R_3 & = & 10100010010111000000101111110100 \end{array}$$

$E(R_{10})$	=	01011010111111010101011111010101111110110100101
K_{11}	=	00100001010111111010011110111101101001110000110
$E(R_{10}) \oplus K_{11}$	=	01111011101000010111100000101000010111000100011
S-box outputs	=	01110011000001011101000100000001
$f(R_{10}, K_{11})$	=	11100001000001001111101000000010
$L_{12} = R_{11}$	=	11000101011110000011110001111000

$E(R_{11})$	=	011000001010101111110000000111111000001111110001
K_{12}	=	011101010111000111110101100101000110011111101001
$E(R_{11}) \oplus K_{12}$	=	0001010111011010000000101100010111110010000011000
S-box outputs	=	0111011100010110010011000110101
$f(R_{11}, K_{12})$	=	11000010011010001100111111101010
$L_{13} = R_{12}$	=	01110101101111010001100001011000

$E(R_{12})$	=	0011101010111110111111010100011110000001011110000
K_{13}	=	1001011111000101110100011111110101011101001000001
$E(R_{12}) \oplus K_{13}$	=	101011010111100000101011011101011011100010110001
S-box outputs	=	10011010110100011000101101001111
$f(R_{12}, K_{13})$	=	11011101101110110010100100100010
$L_{14} = R_{13}$	=	00011000110000110001010101011010

$E(R_{13})$	=	0000111100010111000000110100010101010101011110100
K_{14}	=	0101111110100001110110111111100101110011100111010
$E(R_{13}) \oplus K_{14}$	=	010100001010101101000101110000100110111001110
S-box outputs	=	01100100011110011001101011110001
$f(R_{13}, K_{14})$	=	10110111001100011000111001010101
$L_{15} = R_{14}$	=	110000101000110010010111000001101

$E(R_{14})$	=	111000000101010001011001010010101100000001011011
K_{15}	=	101111111001000110001101001111010011111100001010
$E(R_{14}) \oplus K_{15}$	=	010111111100010111010100011101111111111101010001
S-box outputs	=	10110010111010001000110100111100
$f(R_{14}, K_{15})$	=	01011011100000010010011101101110
$L_{16} = R_{15}$	=	010000110100001000111001000110100

$E(R_{15})$	=	001000000110101000000100000110100100000110101000
K_{16}	=	110010110011111011000101100001110000101111110101
$E(R_{15}) \oplus K_{16}$	=	111010110101011110001111000101000101011001011101
S-box outputs	=	10100111100000110010010000101001
$f(R_{15}, K_{16})$	=	11001000110000000100111110011000
R_{16}	=	00001010010011001101100110010101

$E(R_{10})$	=	01011010111111010101011111010101111110110100101
K_{11}	=	001000010101111111010011110111101101001110000110
$E(R_{10}) \oplus K_{11}$	=	011110111010000101111000011010000101111000100011
S-box outputs	=	01110011000001011101000100000001
$f(R_{10}, K_{11})$	=	11100001000001001111101000000010
$L_{12} = R_{11}$	=	11000101011110000011110001111000

$E(R_{11})$	=	011000001010101111110000000111111000001111110001
K_{12}	=	011101010111000111110101100101000110011111101001
$E(R_{11}) \oplus K_{12}$	=	0001010111011010000000101100010111110010000011000
S-box outputs	=	01111011100010110010011000110101
$f(R_{11}, K_{12})$	=	11000010011010001100111111101010
$L_{13} = R_{12}$	=	01110101101111010001100001011000

$E(R_{12})$	=	00111010101111011111010100011110000001011110000
K_{13}	=	100101111100010111010001111110101011101001000001
$E(R_{12}) \oplus K_{13}$	=	101011010111100000101011011101011011100010110001
S-box outputs	=	10011010110100011000101101001111
$f(R_{12}, K_{13})$	=	11011101101110110010100100100010
$L_{14} = R_{13}$	=	00011000110000110001010101011010

$E(R_{13})$	=	0000111100010111000000110100010101010101011110100
K_{14}	=	0101111110100001110110111111100101110011100111010
$E(R_{13}) \oplus K_{14}$	=	010100000101010110110001011110000100110111001110
S-box outputs	=	01100100011110011001101011110001
$f(R_{13}, K_{14})$	=	10110111001100011000111001010101
$L_{15} = R_{14}$	=	11000010100011001001011000001101

$E(R_{14})$	=	111000000101010001011001010010101100000001011011
K_{15}	=	1011111111001000110001101001111010011111100001010
$E(R_{14}) \oplus K_{15}$	=	010111111100010111010100011101111111111101010001
S-box outputs	=	10110010111010001000110100111100
$f(R_{14}, K_{15})$	=	01011011100000010010011101101110
$L_{16} = R_{15}$	=	01000011010000100011001000110100

$E(R_{15})$	=	001000000110101000000100000110100100000110101000
K_{16}	=	110010110011110110001011000011100001011111110101
$E(R_{15}) \oplus K_{16}$	=	111010110101011110001111000101000101011001011101
S-box outputs	=	10100111100000110010010000101001
$f(R_{15}, K_{16})$	=	11001000110000000100111110011000
R_{16}	=	00001010010011001101100110010101

* يسعى مصمموا التشفير بشكل عام إلى عدم إيجاد علاقة، أو رابطة بين النص الصريح، والنص المشفر، وذلك لوضع العقبات أمام العناصر البشرية التي تبحث عن مفاتيح التشفير.

* إن تطوير خوارزميات تشفير قياسية في المستقبل سيعتمد على مجال واسع من العوامل، والتأثيرات، وعلى التطبيقات المستخدمة، وهذا نابع من اعتقاد قوي بضرورة حماية المعلومات على شبكات الاتصال (وسط الاتصال)، والتخزين الآمن للمعطيات على الحواسيب، وإن قوة التشفير تعتمد على طول (حجم) المفتاح، وذلك كون محللون الشفرة يعتمدون على كتل (رزم) النص الصريح، والنص المشفر.



منظومات الاتصال المعماة ذات المفتاح العمومي

* لقد طرحت فكرة هذه المنظومات في عام ١٩٧٦ من قبل العالمان Devi & Hilman، وفيها تم اقتراح طريقة جديدة للتعمية، والتي يكون فيها لكل مستثمر مفتاحين مفتاح عمومي، ومفتاح خصوصي، حيث يستطيع المستثمران أن يتراسلا من خلال معرفة المفتاح العمومي لكل منهما. في هذه المنظومة يملك كل مستثمر تحويل تعمية عمومي EA، والتي يمكن أن تدون في دليل عمومي، كما يكون لديه تحويل إظهار خاص DA، والذي يكون معروفاً من قبله فقط. يتم الحصول على المفتاح العمومي من المفتاح الخصوصي بواسطة التحويل باتجاه واحد، ويجب أن يكون من الصعب جداً تحديد DA من EA. ومثال على هذا النوع من المعميات نذكر شفرة RSA والتي كانت سنة ١٩٧٨.

تم تطوير هذا النظام في السبعينات في بريطانيا، وكان استخدامه حكراً على قطاعات معينة من الحكومة، ويعتمد في مبدأه على وجود مفتاحين وهما: المفتاح العام Public key، والمفتاح الخاص Privet key، حيث أن المفتاح العام هو لتشفير الرسائل، والمفتاح الخاص لفك تشفير الرسائل، وأن المفتاح العام يرسل للعموم، أما المفتاح الخاص فيحتفظ به صاحبه، ولا يرسله لأحد، فمن يحتاج أن يرسل لك رسالة مشفرة، فإنه يستخدم المفتاح العام لتشفيرها، ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص، وفيمايلي بعض الأمثلة على أنظمة تشفير المفتاح العام:

PGP: Pretty Good Privacy

RSA: Rivest Shamir Adleman

DSA: Digital Signature Algorithm

DSS: Digital Signature Standard

Deffie–Hellman

Elgamal

المفتاح عام (غير تناظري) Asymmetric Encryption: في هذا النوع من التشفير، يستخدم مفتاحين الأول عام يستخدم للتشفير ويكون معروفاً للمرسل والمستقبل، والمفتاح الثاني يستخدم لفك التشفير، ويكون معروفاً فقط للمستقبل.

إن الهدف من التشفير غير المتناظر هو:

- ١- التخلص من مشكلة تبادل كلمات السر غير الآمنة، والتي تتعرض للسرقة من خلال طرف آخر وكذلك يقوم بكشف المعلومات كما في التشفير المتناظر.
- ٢- يمكن استخدام هذا النوع من التشفير لتداول كلمة السر الخاصة بالتشفير المتناظر.



التعمية اللاتناظرية وتدعى أيضاً تعمية المفاتيح العامة، حيث تستخدم زوج مفاتيح، الأول يكون مفتاح عام ويستخدم لتشفير المعطيات، والثاني مفتاح خاص مرتبط بالمفتاح العام، ويستخدم لفك التشفير، وآلية العمل تكمن بمايلي:

- ينشر الطرف المستقبل مفتاحه العام، ويحتفظ بمفتاحه الخاص بشكل سري.

- يمكن لأي شخص أن يستخدم المفتاح العام لتشفير المعطيات التي يريد أن يرسلها إلى صاحب المفتاح.

- يقوم المستقبل بفك شيفرة المعطيات المستقبلية بالاعتماد على المفتاح الخاص به.

مجموعة من الملاحظات على هذا النوع من التعمية نذكرها:

- لا يمكن لأي شخص آخر أن يفك تشفير هذه المعطيات.

- لا يمكن لأي شخص آخر أن يستنتج المفتاح الخاص انطلاقاً من المفتاح العام.

- تعتمد قوة هذا النوع من خوارزميات التعمية على طول الكتلة وطول مفتاح التشفير.

مزايا خوارزميات التشفير غير المتناظر:

١ - المفتاح الخاص يبقى سرياً.

٢ - بحسب طبيعة الاستخدام، فإن استخدام زوج مفاتيح عامة وخاصة يمكن أن يدوم فترة طويلة من الوقت يصل إلى عدة سنوات.

مساوئ أو عيوب خوارزميات التشفير غير المتناظر:

١ - أحجام المفاتيح عادةً تكون أكبر من المطلوبة في التشفير المتناظر.

٢ - تعد هذه الخوارزميات أبطأ من خوارزميات التشفير المتناظر لأنها تتطلب قوة معالجة حسابية.

RSA: Rivest Shamir Adleman خوارزمية

- نقوم بإنتاج مفتاحين أحدهما المفتاح العام الذي تشفر به الرسالة والآخر المفتاح الخاص.
- توليد المفتاح:

p, q هما عددين أوليين (يفضل أن تكون أرقام كبيرة).

$$N = p * q$$

$$Z = (p-1) * (q-1)$$

- نختار عدد أولي e أكبر من الواحد وأقل من Z .
- المفتاح هو $(N - e)$.
- الرسالة بعد التشفير هي:

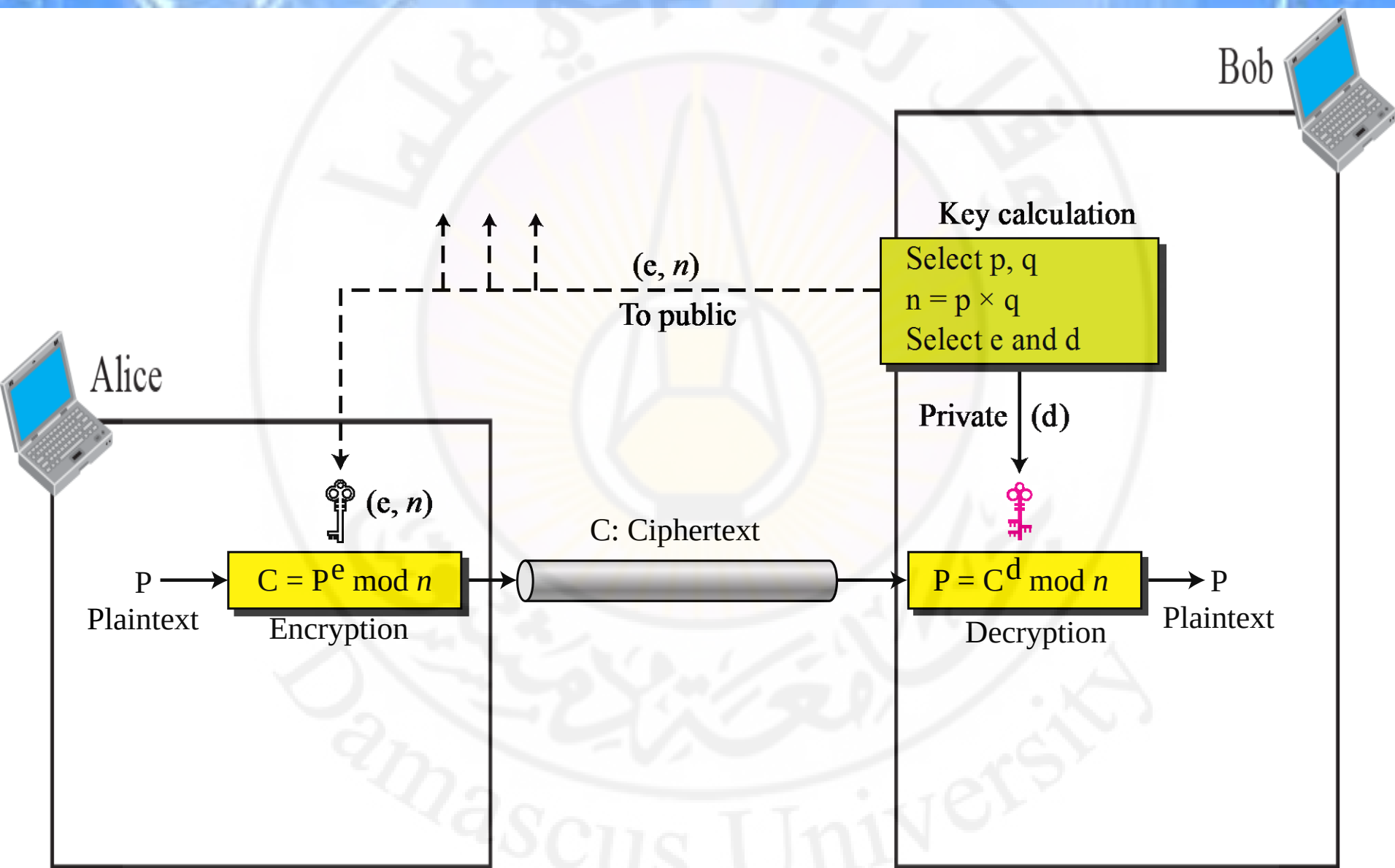
$$C = M^e \bmod N$$

-الرسالة المراد فك تشفيرها هي:

$$M = C^D \bmod N$$

$$D = e^{-1} \bmod Z$$

يوضح الشكل التالي عمليتي التشفير وفك التشفير وتوليد المفتاح لخوارزمية RSA: Rivest Shamir Adleman





RSA: Rivist Shamir Adelman شفرة

* العلاقات التالية توضح خوارزمية هذا النوع من التشفير:

* يقوم الشخص الأول بتوليد رقميين أوليين كبيرين p, q ، ثم يقوم بحساب ناتج جداءهما، وكذلك قيمة $\theta(n)$ ، وهذا موضح بالعلاقات التالية:

$n = p \cdot q$ where p, q are prime numbers.

$$\theta(n) = (p - 1)(q - 1)$$

$K(n, p, q, a, b)$ where $a \bmod b = 1$

* يختار الشخص الأول قيمة عشوائية b ، وبحيث تحقق:

$\gcd(b, \theta(n)) = 1$ ($0 < b < \theta(n)$)، حيث يمثل الرمز $\gcd$ القاسم المشترك الأعظم بين عددين، ثم يقوم بعدها بحساب قيمة a باستخدام خوارزمية Euclidean على الشكل التالي: $a = b^{-1} \bmod \theta(n)$

* بعد حساب قيم n, a, b يقوم بتشفير النص الصريح وفق العلاقة التالية:

$$e_k(x) = x^b \bmod n$$

* إذا أراد معرفة النص الصريح من النص المشفر، فإنه يستخدم العلاقة التالية:

$$d_k(y) = y^a \bmod n$$

حيث قيم n, b هي قيم عامة بينما a, p, q قيمها سرية.

* يوضح الشكل التالي ملخص شفرة RSA:

المعروف للمرسل	العام	المعروف للمستقبل
رسالة x $y = e^x \text{ module } m$	تشفير y	فك التشفير $x = y^d \text{ module } m$
المعروف للمرسل m e	العام m e	المعروف للمستقبل p, q أعداد أولية. $m = p \cdot q$ المفاتيح: d, e هي أولية لـ $p-1, q-1$. $d \cdot e = 1 \pmod{n}$ $n = \text{lcm}(p-1, q-1)$

مثال:

$$n=p.q = 11413, p = 101, q = 113$$

$$\theta(n) = (p - 1)(q - 1) = 100 \times 112 = 11200 \\ = 2^6 \times 5^2 \times 7$$

* إذا اختار الشخص الذي يريد عمل التشفير قيمة $b = 3533$ ، عندئذ، وبالاستعانة بخوارزمية Euclidean نجد أن معكوس b هو:

$$b^{-1} = 6597 \bmod 11200, \text{ وقيمة } a = 6597$$

* إذا رغب أحدهم بإرسال نص صريح 9726 إلى شخص آخر، عندئذ النص المشفر يكون:

$$\text{النص المشفر} = 9726^{3533} \bmod 11413 = 5761$$

$$\text{النص الصريح} = 5761^{6597} \bmod 11413 = 9726$$

RSA: Rivest Shamir Adleman مثال على

$$(p, q) = (3, 7)$$

$$N = p * q = 3 * 7 = 21$$

$$Z = (p-1) * (q-1) = 2 * 6 = 12$$

- نختار عدد أولي e أكبر من الواحد وأقل من Z ، وليكن على سبيل المثال: $(e = 7)$ ، وهو يقع ما بين الواحد و 12 .
- المفتاح هو (N, e) ، أي: $(21, 7)$.
- مثلاً نقوم بتشفير $M = 4$.
- الرسالة بعد التشفير هي:

$$C = M^e \bmod N = 16384 \bmod 21 = 4$$

-الرسالة المراد فك تشفيرها هي:

$$M = C^D \bmod N$$

$$D = e^{-1} \bmod Z = 7^{-1} \bmod 12 = 6$$

$$M = 4^6 \bmod 21 = 16384 \bmod 21 = 4$$

Example

For the sake of demonstration, let Bob choose 7 and 11 as p and q and calculate $n = 7 \times 11 = 77$. The value of $\phi(n) = (7 - 1)(11 - 1)$, or 60. If he *chooses* e to be 13, then d is 37. Note that $e \times d \bmod 60 = 1$. Now imagine that Alice wants to send the plaintext 5 to Bob. She uses the public exponent 13 to encrypt 5. This system is not safe because p and q are small.

Plaintext: 5

$$C = 5^{13} = 26 \bmod 77$$

Ciphertext: 26

Ciphertext: 26

$$P = 26^{37} = 5 \bmod 77$$

Plaintext: 5

Example

Here is a more realistic example calculated with a computer. We choose a 512-bit p and q , calculate n and $\phi(n)$, We then choose e and calculate d . Finally, we show the results of encryption and decryption. The integer p is a 159-digit number.

$p =$	961303453135835045741915812806154279093098455949962158225831508796 479404550564706384912571601803475031209866660649242019180878066742 1096063354219926661209
-------	--

The integer q is a 160-digit number.

$q =$	120601919572314469182767942044508960015559250546370339360617983217 314821484837646592153894532091752252732268301071206956046025138871 45524969000359660045617
-------	---

Example

The modulus $n = p \times q$. It has 309 digits.

$n =$	115935041739676149688925098646158875237714573754541447754855261376 147885408326350817276878815968325168468849300625485764111250162414 552339182927162507656772727460097082714127730434960500556347274566 628060099924037102991424472292215772798531727033839381334692684137 327622000966676671831831088373420823444370953
-------	---

$\phi(n) = (p - 1)(q - 1)$ has 309 digits.

$\phi(n) =$	115935041739676149688925098646158875237714573754541447754855261376 147885408326350817276878815968325168468849300625485764111250162414 552339182927162507656751054233608492916752034482627988117554787657 013923444405716989581728196098226361075467211864612171359107358640 614008885170265377277264467341066243857664128
-------------	---

Example

Bob chooses $e = 35535$ (the ideal is 65537). He then finds d .

$e =$	35535
$d =$	580083028600377639360936612896779175946690620896509621804228661113 805938528223587317062869100300217108590443384021707298690876006115 306202524959884448047568240966247081485817130463240644077704833134 010850947385295645071936774061197326557424237217617674620776371642 0760033708533328853214470885955136670294831

Alice wants to send the message “THIS IS A TEST”, which can be changed to a numeric value using the 00–26 encoding scheme (26 is the space character).

$P =$	1907081826081826002619041819
-------	------------------------------

Example *Continued*

The ciphertext calculated by Alice is $C = P^e$, which is

C =	475309123646226827206365550610545180942371796070491716523239243054 452960613199328566617843418359114151197411252005682979794571736036 101278218847892741566090480023507190715277185914975188465888632101 148354103361657898467968386763733765777465625079280521148141844048 14184430812773059004692874248559166462108656
------------	--

Bob can recover the plaintext from the ciphertext using $P = C^d$, which is

P =	1907081826081826002619041819
------------	------------------------------

The recovered plaintext is “THIS IS A TEST” after decoding.