جامعة حماة
الكلية التطبيقية
قسم تقنيات الحاسوب

- المقرر: أمن المعلومات
- المحاضرة : الأولى

Dr. Mohammed AL-Mohammed

Chapter 1

مقدمة

أسس ومبادئ أمن المعلومات

1. مقدمة:

ساهمت شبكة الانترنت بتغيير حياتنا اليومية بعدة طرق، وذلك على اعتبار أن هذه الشبكة أضحت وسيلة الاتصال العالمية، فقد سمحت هذه الشبكة للأفراد والمؤسسات حول العالم بالمشاركة بالمعلومات وبالتواصل التجاري وتبادل رسائل البريد الالكتروني. مما جعل الاعتماد على شبكة الانترنت أمراً ملحاً ولا يمكن تفاديه.

أدى ذلك إلى ظهور الكثير من المشاكل الأمنية، حيث برزت الحاجة لتوفير:

السرية **Confidentiality**

- تكامل المعطيات **Integrity**.
- تحديد هوية المتصل **Authentication**.

يعد التشفير **Cryptography** أحد أهم الوسائل المستخدمة لتوفير بيئة آمنة لتبادل المعلومات وحمايتها.

حتى عقود سالفة كان يجري تخزين المعلومات ضمن ملفات ومصنفات ورقية. يجري ضمان سرية هذه الملفات من خلال تخزينها ضمن أماكن محمية ولا يمكن الوصول إليها أو تعديلها من دون تصريح خاص أو من قبل عدد محدود ومحدد من الأشخاص.

كان يجري توفير إتاحية الوصول إلى هذه المعلومات من خلال تعيين شخص واحد على الأقل قادر على الوصول إلى هذه المعلومات في أي وقت.

مع ظهور الحواسيب، بدأ التفكير بتخزين المعلومات إلكترونياً بدلاً من تخزينها ورقياً. ولكن بقيت متطلبات أمنها الثلاث السابقة هي نفسها:

السرية والتكامل والإتاحية

أما المختلف في هذه الوضعية الجديدة فهو طريقة تحقيق هذه المتطلبات.

ساعد استخدام الحواسيب خلال فترة العقدين السابقين على خلق ثورة في طريقة التعامل مع المعلومات واستخدامها. المعلومات في زمننا الحالي موزعة ومخزنة في عدة أماكن ويمكن للأشخاص المصرح لهم بالوصول إليها سواء كان محلياً أو عن بعد من خلال الشبكة الحاسوبية.

أدى ذلك كله أن تأخذ متطلبات أن المعلومات الثلاثة التي تحدثنا عنها فيما سبق أبعاداً أخرى، إذ لا يكفي أن يجري المحافظة على سرية المعلومات أثناء تخزينها وإنما يجب تحقيق ذلك أثناء نقلها وإرسالها من حاسوب إلى آخر.

1. أهداف أمن المعلومات Security Goals

نقوم في هذه الفقرة بتعريف أهداف أمن المعلومات التي تحدثنا عنها في الفقرة السابقة.

- **السرية Confidentiality**: يعد ذلك من أهم أهداف أمن المعلومات. نحن كأشخاص أو مؤسسات بحاجة إلى حماية معلوماتنا السرية لعدة أسباب لها علاقة بعملنا وبنواحي عملية مختلفة. لا يطبق هذا الهدف على المعلومات عند تخزينها فقط ولكن يطبق أيضًا أثناءنقلها وتبادلها.

- **التكاملIntegrity** : نحتاج إلى تبادل المعلومات من وقت إلى آخر. يعني تكامل المعطيات أن:

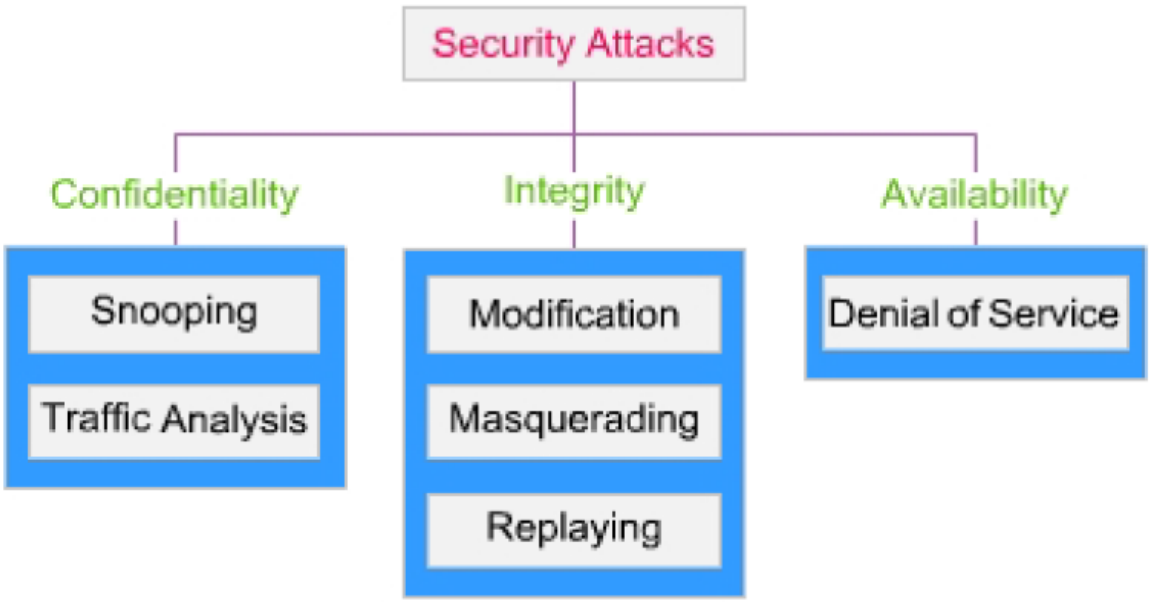
تعديلها يجب أن يتم حصرا من قبل الأشخاص المصرح لهم بذلك. يجب ملاحظة أن تعديل المعلومات لا يمكن أن يحدث بنتيجة فعل غير قانوني فقط، وإنما يمكن أن يؤدي انقطاع التيار الكهربائي في بعض الحالات إلى تعديل بعض المعلومات.

➢ **الإتاحيةAvailability :** يجب أن تتوفر إمكانيات إتاحة المعطيات للجهات المصرح لها بذلك حصرًا، حيث تعتبر المعلومات غير المتاحة لأحد غير مفيدة لأحد. كما تحتاج

المعلومات إلى أن يجري تعديلها من وقت إلى آخر ولكن يجب أن يجري ذلك من قبل من يملك تصريح بذلك. يمكن أن يؤدي عدم توفر الإتاحية إلى نتائج سيئة مماثلة لتلك الناتجة عن عدم مراعاة سرية المعلومات.

3. الهجماتAttacks:

يمكن تهديد أهداف أمن المعلومات بواسطة عدد من الهجمات. هنالك عدة تصنيفات لهذه الهجمات سنقوم فيما يلي بفرزها ضمن ثلاث مجموعات حسب هدف أمن المعلومات الذي تهدده، كما هو مبين في الشكل التالي:



وسنشرح فيما يلي معنى هذه الهجمات المختلفة.

الهجمات التي تهدد السرية Attacks Threatening Confidentiality

يتوفر بشكل عام نوعين من الهجمات التي تشكل تهديدًا للسرية، هما:

- ✓ **التصيدSnooping:** ويرمز ذلك للوصول غير المصرح به للمعطيات أو التقاط معطيات سرية أثناء نقلها على شبكة الانترنت، ثم استخدام هذه المعطيات لأغراض مسيئة. لمنع التصيد يمكن جعل المعطيات غير مفيدة للأطراف الأخرى باستخدام أحد وسائل التشفير التي سنتحدث عنها لاحقًا.
- ✓ **تحليل المعطيات المتبادلةTraffic analysis:** رغم استخدام وسائل التشفير لجعل المعطيات غير مفيدة للأطراف الأخرى، إلا أنه يمكن الحصول على معلومات أخرى مفيدة من خلال تحليل ومراقبة المعلومات المتبادلة من خلال الشبكة. يمكن مثلاً: معرفة العنوان الإلكتروني للمرسل أو المستقبل، أو يمكن تجميع الطلبات والردود عليها لمحاولة معرفة طبيعة حركة المعطيات المنفذة.

الهجمات التي تهدد التكاملAttacks Threatening Integrity

يمكن تهديد تكامل المعطيات بعدة أنواع من الهجمات، التي نذكر منها:

- **التغيير أو (التعديل)Modification:** بعد تصيد المعطيات المتبادلة أو الوصول إليها، يمكن للمهاجم تغييرها لجعلها مفيدة له. كما يمكن أن يقوم المهاجم بحذف أو تأخير وصول رسالة لفائدة مرتبطة به أو لتعطيل النظام.
- **انتحال الصفةMasquerading:** ويحدث ذلك عندما يقوم المهاجم بانتحال صفة شخص آخر. كما يمكن أن يتظاهر المهاجم بكونه الطرف المستقبل للرسائل
- **الإعادة Replaying :** يقوم المهاجم بإعادة الاتصال مع المستقبل باستخدام نفس الرسائل التي أرسلها المرسل بعد قيامه بنسخها أثناء عملية اتصال حقيقية بين الطرفين.
- **الإنكارRepudiation :** يختلف هذا الهجوم عن غيره لأنه يحتاج إلى طرف أو طرفي الاتصال لإنجازه المرسل أو المستقبل. يمكن لمرسل الرسالة أن ينكر لاحقًا أنه أرسل الرسالة، أو يمكن للمستقبل أن ينكر لاحقًا استقباله للرسالة.

الهجمات التي تهدد الإتاحية Attacks Threatening Availability

سنتحدث هنا عن نوع واحد من الهجمات التي تهدد الإتاحية، ألا وهو:

تعطل(إنكار) الخدمة Denial of service (DoS): وهو نوع شائع من الهجمات التي تؤدي إلى إبطاء النظام الحاسوبي المستهدف أو قد تؤدي إلى توقفه تمامًا. يمكن أن يتبع المهاجم عدة استراتيجيات لتنفيذ ذلك.

يمكن مثلاً أن يقوم بإرسال كمية كبيرة من الطلبات مما يؤدي إلى تعطل النظام الحاسوبي المستهدف. أو يمكن أن يعترض المهاجم أجوبة المخدم بتعديلها أو حذفها مما يظهر المخدم كما لو أنه لا يتجاوب مع طلبات الزبائن.

يمكن أيضاً تصنيف الهجمات بطريقة أخرى ضمن فئتين حسب طريقة عملها، كما هو مبين في الجدول التالي:

الهجمات	الفئة (فعال أو غير فعال)	التهديد الذي يمثله
التصيد Snooping المعطيات المتبادلة Traffic analysis	غير فعال	السرية Confidentiality
التغيير Modification انتحال الصفة Masquerading الإعادة Replaying الإنكار Repudiation	فعال	التكامل Integrity
تعطل الخدمة Denial of service	فعال	الإتاحية Availability

الهجمات غير الفعالة Passive Attacks:

يكون هدف المهاجم في هذا النوع من الهجمات تجميع المعلومات، فهو لا يقوم بتعديل المعلومات أو بالتسبب بأي أذى للنظام الحاسوبي. يمكن لعملية تجميع المعلومات أن تسبب أذى للمرسل أو المستقبل لكنها لا تؤثر على النظام الحاسوبي الذي يتابع عمله بشكل طبيعي. تعتبر الهجومات المهددة للسرية هجمات غير فعالة، وهي هجمات من الصعب جدًا التقاطها حتى يكتشف المرسل أو المستقبل تسرب معلومات سرية تخصه. يمكن منع هذا النوع من الهجومات من خلال تشفير المعطيات.

الهجمات الفعالة Active Attacks:

يتسبب هذا النوع من الهجومات بتغيير المعطيات أو بأذى للنظام الحاسوبي. تعتبر الهجومات المهددة للتكامل والإتاحية من هذا النوع، ومن السهل التقاطها أكثر من منعها لأن المهاجم يقوم بتنفيذها بعدة أساليب وطرق.

Security Attacks Classification

الهجمات السلبية Passive Attacks : الهدف منها هو الحصول على المعلومات المنقولة لتمييز محتوى الرسالة وتحليل سيالة المعلومات الجارية.

1- **محتوى الرسالة:** قد يحتوي على معلومات سرية وحساسة لذلك يجب منع الهجمات على المعلومات.

2- **تحليل سيالة المعلومات :** يمكن استخدام التعمية في عملية التمويه لمنع المهاجم من الاطلاع على مضمون الرسائل وبالتالي كامل سيالة المعلومات.

يعتبر من أنواع الهجوم صعب الاكتشاف وبالتالي يجب التركيز لمنعه وليس لاكتشافه.

Security Attacks Classification

الهجمات الفعالة **Active Attacks** : تعتمد على إجراء تعديلات على سيالة المعلومات أو إنشاء سيالة كاذبة ويقسم إلى:

1- **هجوم التخفي Masquerade**: تقديم شخص نفسه على أنه شخص آخر بعد تحديد هوية الأول.

2- **هجوم إعادة البث Replay Attacks**: التقاط معطيات ما ثم إعادة إرسالها من أجل التشكيك.

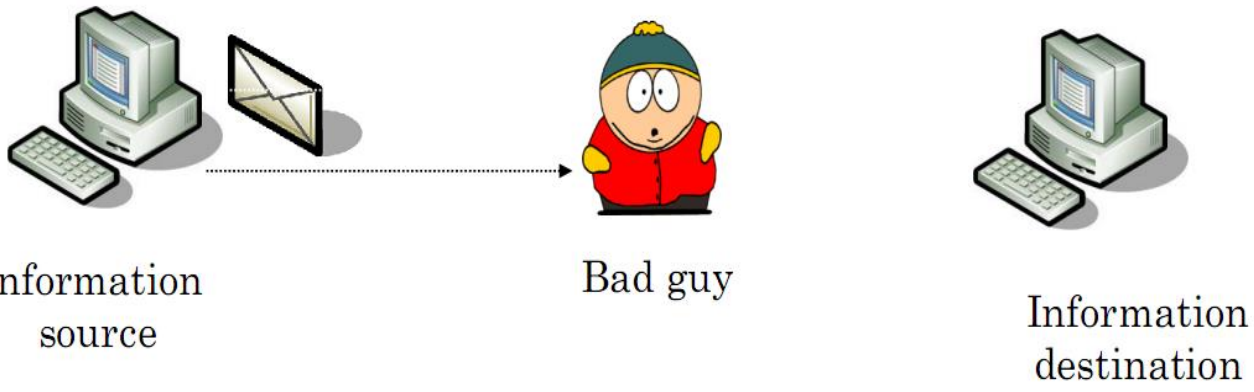
3- **هجوم التعديل Modification of Messages**: تغيير جزء من رسالة ما أو تغيير ترتيبها ومعناها.

4- **هجوم حجب الخدمة Denial of Service**: منع مرور كل الرسائل الموجهة لجهة ما أو تعطيل الشبكة الكلية عن طريق تحميل زائد للرسائل وإرسالها.

Security Threats

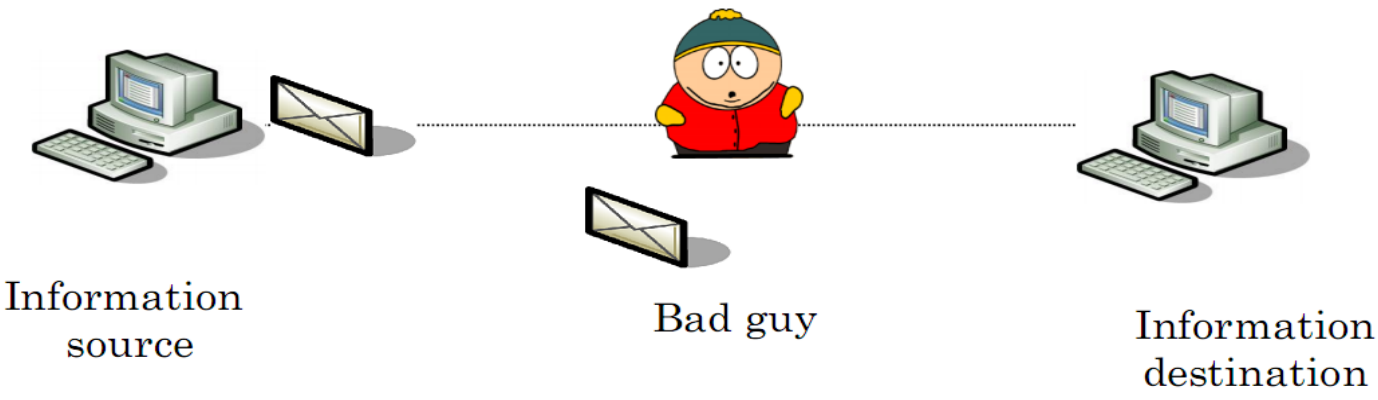
1. Interruption(المقاطعة)
2. Interception(الاعتراض)
3. Modification(التعديل)
4. Fabrication(التلفيق)

1. Interruption(المقاطعة)



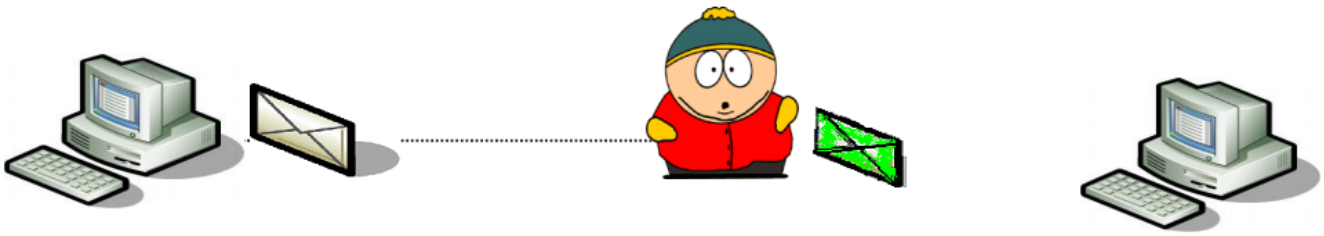
- The system becomes unavailable or unusable.
- Attack on the Availability.
- النظام يُصبحُ غير متوفرَ أو غير صالح للإستعمالَ.
- الهجوم على التوفرِ.

2. Interception(الاعتراض)



- Unauthorized party gains access to the information.
- يتمكّنُ الطرف الغير مخوّل من الدخول إلى المعلوماتِ
- Attack on the Confidentiality.الهجوم على السريّةِ
- Example: unauthorized copying of files.
- النَسْخ الغير مخوّل للملفاتِ

3. Modification(التعديل)



Information source | Bad guy | Information destination

- Unauthorized party alters with asset..يُعدّلُ الطرف الغير مخوّلُ الاصول
- Attack on the Integrity..الهجوم على السلامةِ
- Examples: changing values of database, altering programs, modify content of a message.

تغيير القِيَم لقاعدةِ البيانات، تبديل البرامجَ، تعدّيلْ محتوى الرسالة.

4. Fabrication(التلفيق)

Information source | Bad guy | Information destination

- Unauthorized party inserts counterfeit object into the system.

يدخلُ الطرف الغير مخوّل جسم مزوّر إلى النظامِ.

- Attack on the Authenticity..الهجوم على الأصالةِ(الوثوقية)
- Examples: addition of records to a file, etc.

إضافة السجلاتِ إلى الملف، الخ.

4. الخدمات والأدوات Services and Mechanisms

يقدم اتحاد الاتصالات العالمي - قسم معايرة الاتصالات(ITU-T)
International Telecommunication Union -Telecommunication Standardization Sector

بعض من الخدمات الأمنية ويوفر عدد من الأدوات لبنائها. لا يوجد فرق كبير بين الخدمات والأدوات لأنه في بعض الحالات يمكن لأداة ولتجميع عدد منها أن يشكل خدمة.

كما يمكن استخدام نفس الأداة مع عدة خدمات. نقوم فيما يلي بإعطاء فكرة عامة عن:

1. الخدمات الأمنية.
1. الأدوات الأمنية المهمة.

الخدمات الأمنيةSecurity Services

عرف المعيار ITU–T (X.800) خمس خدمات مرتبطة بالأهداف الأمنية والهجمات التي تحدثنا عنها في الفقرات السابقة. نعرض فيما يلي بشكل مختصر فكرة عن هذه الخدمات التي من السهل الربط بينها وبين هدف أو أكثر من أهداف أمن المعلومات. من السهل أيضًا أن نلاحظ أن هذه الخدمات من أجل منع الهجومات التي تحدثنا عنها فيما سبق.

- **سرية المعطيات Data Confidentiality:** وهي خدمة مصممة من أجل حماية المعطيات ضد الهجومات التي تستهدف الكشف عنها. تتضمن هذه الخدمة ضمان سرية الرسائلبكاملها أو جزء منها والحماية ضد هجمات تحليل المعطيات والتصيد.
- **تكامل المعطياتData Integrity:** وهي خدمة مصممة لحماية المعطيات ضد التغيير أو الإضافة أو الحذف أو إعادة التنفيذ. يمكن لها حماية كامل الرسالة أو جزء منها.
- **التعرف / تحديد الهوية Authentication:** وتفيد في التعرف وتحديد هوية الطرف الآخر المتصل (Peer entity authentication). يفيد ذلك في تحديد هوية المرسل أو المستقبل في حال الاتصالات الموجهة بالربط Connection-oriented communication. كما أنها تفيد في تحديد مصدر المعطيات(Data origin authentication) في حالة الاتصالات غير الموجهة بالربطConnectionless communication.

- **منع الإنكار** Nonrepudiation تفيد هذه الخدمة بالحماية ضد إنكار المرسل أو المستقبل بتنفيذ عملية الاتصال. يستطيع المستقبل مع خدمة منع الإنكار المزودة بوسيلة الدلالة على المصدر **Proof of origin** أن يحدد مصدر المعلومات وهوية المرسل. أما مع خدمة منع الإنكار المزودة بوسيلة الدلالة على الاستلام **Proof of delivery** فيمكن للمرسل أن يحدد مكان استلام المعطيات وهوية المستقبل.

- **التحكم بالوصول Access Control:** توفر هذه الخدمة الحماية ضد الوصول غير المصرح به إلى المعطيات. وتتضمن كلمة الوصول إلى المعطيات كل ما له علاقة بعمليات القراءة والكتابة والتعديل والتنفيذ للبرامج وغيرها من العمليات من هذا النمط.

الأدوات الأمنية Security Mechanisms

عرف المعيار **ITU-T (X. 800)** أيضًا عددًا من الأدوات الأمنية اللازمة لتوفير الخدمات الأمنية التي تحدثنا عنها في الفقرة السابقة. نعرض فيما يلي بشكل مختصر فكرة عن هذه الأدوات:

- **التشفير Encipherment:** تفيد هذه الأداة في إخفاء المعطيات للحفاظ على سريتها. يمكنأيضًا استخدامها كتتمة وتكملة للأدوات الأخرى اللازمة لبناء خدمة أمنية. يتوفر لدينا حالياً تقنيتان للتشفير، هما:

التعمية **Cryptography** والتورية **Steganography**

- **تكامل المعطيات Data Integrity:** تفيد هذه الأداة في إضافة بعض المعلومات الإضافية(مجاميع قصيرة للتحققShort checkvalues)وفقًا لإجراء معين إلى المعطيات نفسهاقبل إرسالها. يقوم المستقبل باستقبال المعطيات مع مجاميع التحقق، ثم يحاول حساب هذه المجاميع بنفسه على المعطيات الحقيقية للتحقق من صحة المجاميع. إذا تطابقت المجاميع فهذا يعني أنه جرى المحافظة على تكامل المعطيات.

- **التوقيع الإلكتروني Digital Signature :** تفيد هذه الأداة في توفير إمكانية توقيع المرسل للمعطيات المرسلة من قبله الكترونياً بحيث يمكن للمستقبل أن يتحقق من هذا التوقيع عنداستلام المعطيات للتأكد من هوية المرسل يتم ذلك باستخدام المفتاح الخاصKey **Private** بالمرسل لتوقيع المعطيات قبل إرسالها، ثم يستخدم المستقبل المفتاح العام **Public Key.** للمرسل والمعروف من قبل الجميع للتحقق من صحة التوقيع على نفس المعطيات المستقبلة من قبله

- **تبادل التعارف Authentication Exchange:** تعني هذه الأداة أن طرفي الاتصال يتبادلان بعض الرسائل ليتحقق كً لا منهما من هوية الآخر. يمكن مثلاً أن: يثبت أحد الطرفين أنه يعلم سراً لا يفترض بأحد آخر أن يعرفه.

- **حشو المعطياتTraffic Padding:** ويفيد ذلك في إدراج كمية من المعطيات غير المفيدة ضمن المعطيات الحقيقية بحيث تصبح هذه المعطيات بمجملها مضللة لهجمات تحليل حركة المعطيات.

- **التحكم بالتوجيه Routing Control** ويعني ذلك اختيار طرق توجيه مختلفة بين المرسل والمستقبل والتبديل بينها من وقت إلى آخر لتضليل المتصنت على أحد هذه الطرق المتاحة.

- **المرور بطرف ثالثNotarization :** ويعني ذلك اختيار طرف ثالث موثوق به للتحكم بالاتصال بين طرفين آخرين. يمكن اللجوء إلى هذه الأداة لمنع الإنكار. يمكن مثلاً أن: يلجأ المستقبل باختيار طرف ثالث موثوق به لتخزين طلبات المرسل بهدف منعهمن الإنكار لاحقًا بأنه أرسل هذه الطلبات.

- **التحكم بالوصول Access Control :** يمكن اللجوء إلى هذه الأداة لتحديد سماحيات وصول المستخدم إلى المعطيات والمصادر المملوكة من قبل النظام، مثل: السماحيات الممنوحة وفقاً لكلمات السر **Passwords** أو الرموز السرية **PINs**

العلاقة بين الخدمات والأدوات Relation between Services and Mechanisms

يوضح الجدول التالي العلاقة بين الخدمات الأمنية والأدوات الأمنية :

الخدمة الأمنية	الأداة / الأدوات الأمنية
سرية المعطيات **Data Confidentiality**	التشفير **Encipherment** والتحكم بالتوجيه **Routing Control**.
تكامل المعطيات **Data Integrity**	التشفير **Encipherment** والتوقيع الإلكتروني **Digital Signature** وتكامل المعطيات **Data Integrity**.
التعرف / تحديد الهوية **Authentication**	التشفير **Encipherment** والتوقيع الإلكتروني **Digital Signature** وتبادل التعارف **Authentication Exchange**.
الإنكار **Nonrepudiation**	التوقيع الإلكتروني **Digital Signature** وتكامل المعطيات **Data Integrity** والمرور بطرف ثالث **Notarization**.
التحكم بالوصول **Access Control**	أداة التحكم بالوصول **Access Control**

5. التقنيات Techniques

تعتبر التقنيات التي نتحدث عنها هنا هي تقنيات نظرية من أجل تحقيق أمن المعلومات، حيث يتطلب تحقيق الأهداف الأمنية استخدام بعض التقنيات. من هذه التقنيات لدينا اليوم:

1- التعمية Cryptography

1- التورية Steganography

التعمية Cryptography

يمكن تحقيق العديد من الأدوات الأمنية التي تحدثنا عنها سابقًا باستخدام تقنيات التعمية التي تعني باليونانية: Cryptography

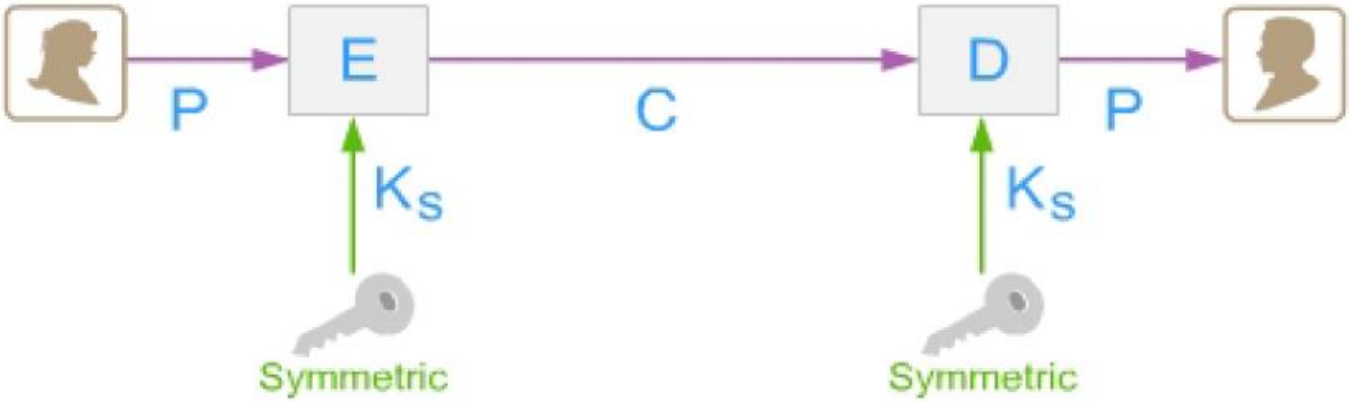
كتابة الأسرار أو الكتابة السرية **Secret writing**

لكن هذه الكلمة ترمز بالنسبة لنا إلى علم وفن تحويل الرسائل لتصبح آمنة ضد كافة أشكال الهجوم. كانت 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، وهي:

1. التشفير بمفاتيح متناظرة **Symmetric-key encipherment**
1. التشفير بمفاتيح غير متناظرة **Asymmetric-key enciphermen**
3. التهشير **Hashing**

التشفير بمفاتيح متناظرة **Symmetric-key encipherment**

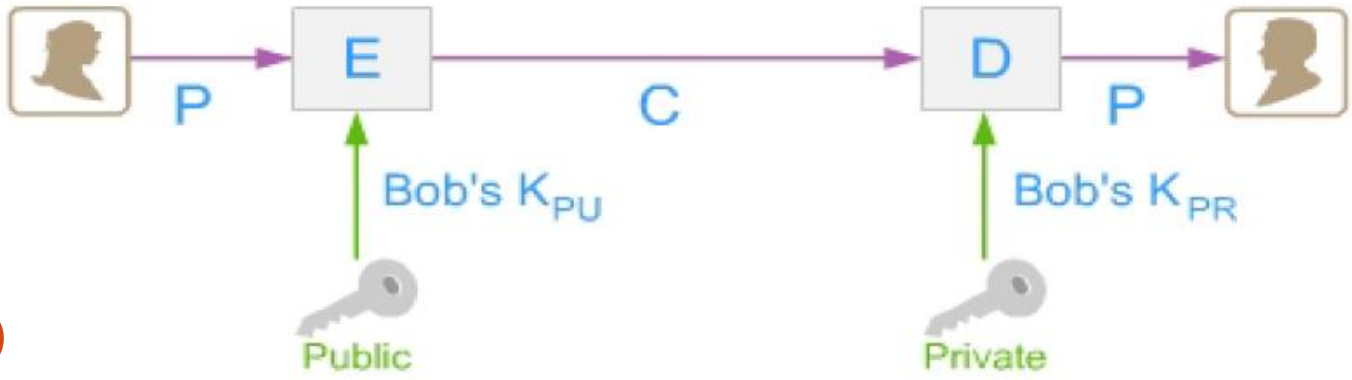
يجري التشفير وفقًا لهذه التقنية باستخدام مفتاح سري **Secret-key** مشترك من قبل الطرفين المتصلين كما هو مبين في الشكل التالي:



التشفير بمفاتيح غير متناظرة Asymmetric-key encipherment

يجري التشفير وفقًا لهذه التقنية باستخدام مفتاحين أحدهما معلن وهو المفتاح العام **Public Key** والآخر سري وهو **Private key**

ولإرسال رسالة مشفرة من طرف إلى آخر يجب تشفيرمعطياتها باستخدام المفتاح العام المعلن للطرف المستقبل الذي يقوم بدوره فك تشفير الرسالة بعد وصلها بواسطة مفتاح الخاص السري، ولن يتمكن أي شخص آخر من تنفيذ ذلك لأنها شفرت في الأصل بمفتاحه العام المرتبط به، كما هو مبين في الشكل التالي:

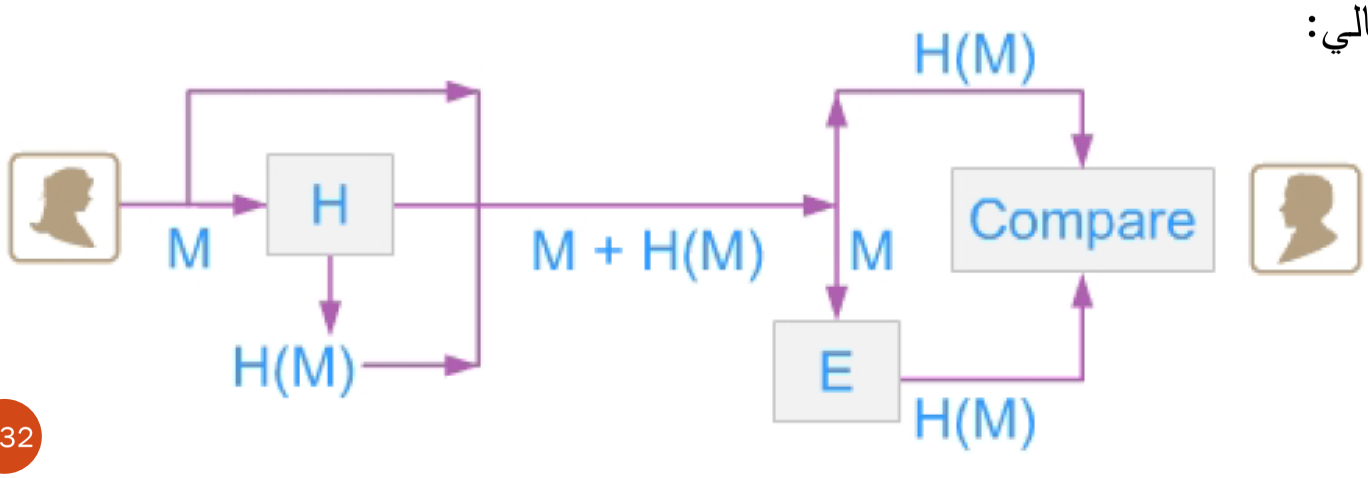


1-31

التهشير Hashing

يجري وفقًا لهذه التقنية إنشاء تلخيص من طول ثابت لمحتوى الرسالة **Fixed-length message digest** وهو أصغر بكثير من الرسالة. يجري بعدها إرسال الرسالة وملخصها إلى الطرف

الثاني الذي يعيد بدوره إنشاء ملخص للرسالة المستقبلة لمطابقته مع ملخص الرسالة المرسلة في الأصل. إذا حدث التطابق فهذا يعني أن تكامل المعطيات محقق، كما هو مبين في الشكل التالي:



1-32

التورية Steganography

تعني هذه الكلمة باليونانية:الكتابة المغطاة **Covered writing**

ويفيد هذا الأسلوب في إخفاء الرسالة وتغطيتها بشيء آخر (ضمن نص آخر أو ضمن صورة).

ولا يشكل هذا المجال من التشفير جزءًا من المواضيع التي سنتعرض لها من خلال دراستنا لتقنيات وأساليب التعمية.

جامعة حماة
الكلية التطبيقية
قسم تقنيات الحاسوب

- **المقرر: أمن المعلومات**
- **المحاضرة : الثانية**

Dr. Mohammed AL-Mohammed

Chapter 2

التعمية وأمن المعلومات

مبادئ وتطبيقات

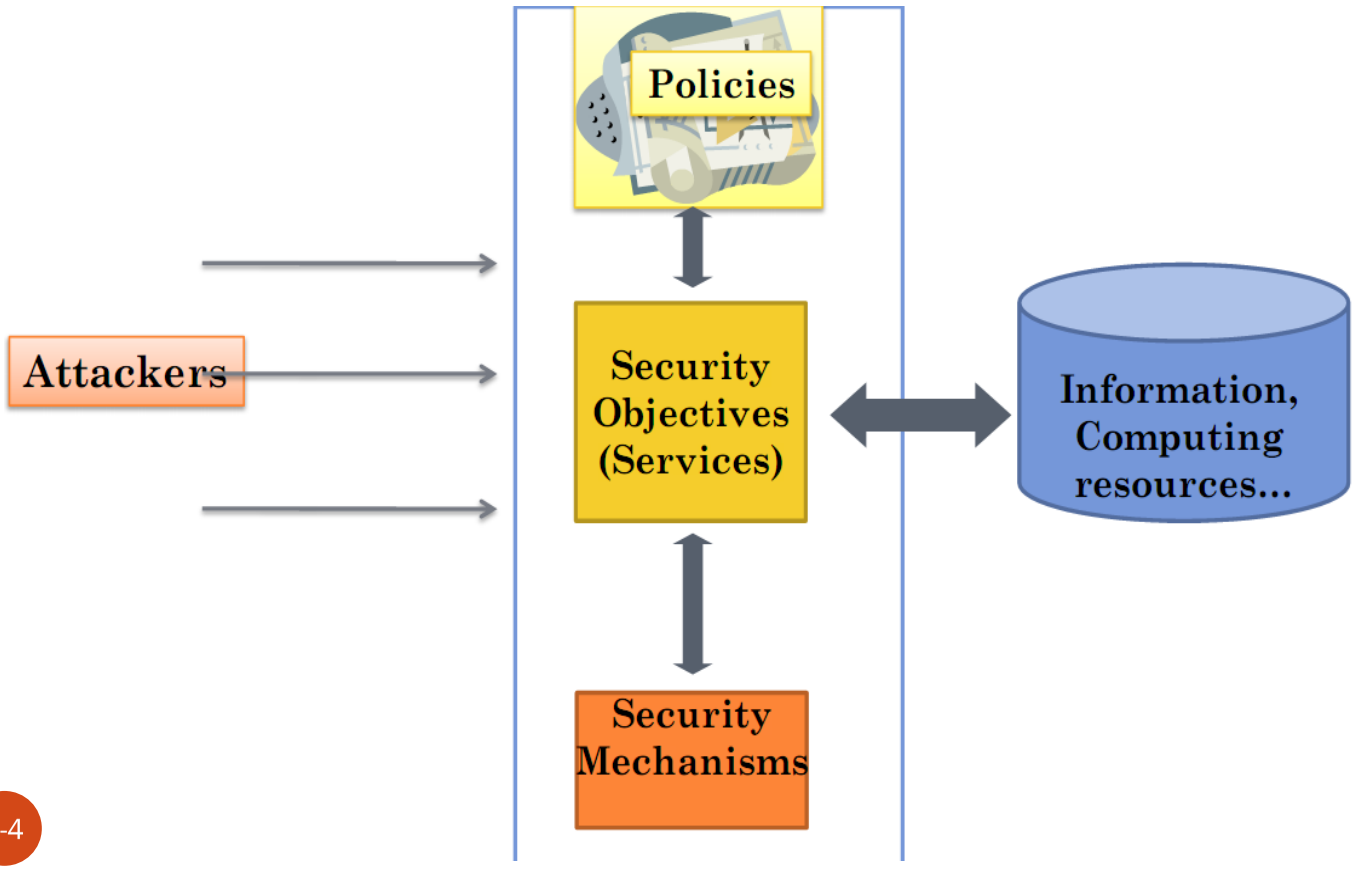
Introduction to Information Security

أضحت متطلبات أمن المعلومات غاية في الأهمية ولاسيما ما نشهده حاليا من تهديدات أمنية على مستوى العالم وخصوصا في مجالات الحياة العلمية أو العسكرية وذلك لما ينشأ من مخاطر حقيقية للدخول غير المشروع إلى البيانات المخزنة والسرية وكذلك ما تتعرض له المعلومات من سرقة عند نقلها بين الشركات أو المؤسسات.

والهدف من ذلك هو الحصول على المعلومات أو تخريبها أو تدميرها أو الاستفادة منها في مآرب أخرى.

كل هذه الأسباب أدت بالعلماء إلى تطوير أفكار جديدة في مجال الأمن وظهر ما يدعى بعلم حماية المعطيات أو **"Data Security"** تسعى كلها لحماية المعلومات.

Information Security
Attacks, Mechanisms and Services



أمن المعلومات

ثلاثة جوانب لأمن المعلومات

علم التعمية:
يشكل أهم وأخطر عنصر في أمن المعلومات .

تعريف الخطر Risk

الخطر Risk هو أنه يوجد على الأرجح تهديد يمكن إستغلاله، وبالتالي إذا استغل ذلك التهديد يمكن أن نطلق عليه Vulnerability (ثغرة)، حيث أنه يوجد ثغرة أمنية في تلك المنظمة.

ومن هذا التعريف يمكن أن نقسم الـ Risk إلى قسمين رئيسيين هما :

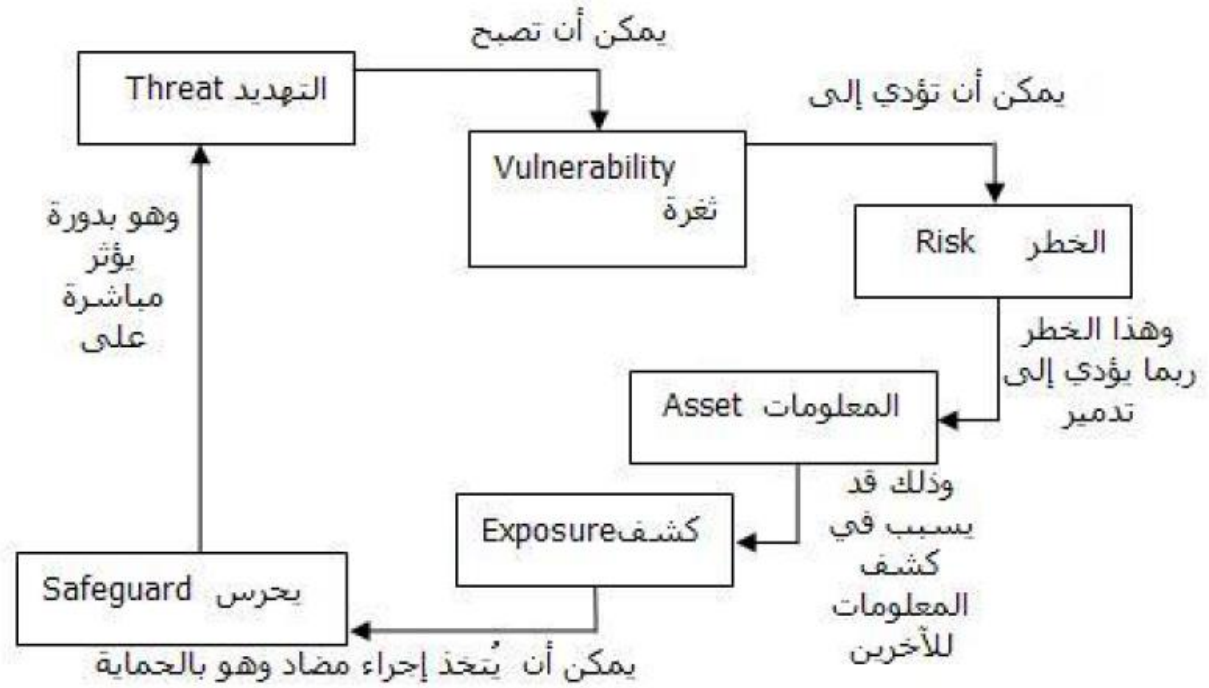
- التهديد Threat: وهو عملية المحاوله الى الوصول إلى المعلومات السرية الخاصة بالمنظمة.
- الثغرات Vulnerabilities وهي أنه يوجد ضعف في المنظمة يستطيع المهاجم Attacker الدخول من خلالها

Threat

A threat can be:

1. Malicious(الخبيث) (attackers, insider fraud,…..)
2. Accidental العرضي (natural disasters, human error (misuse), …)

وهناك مكونات أخرى للـ Risk وهي كما يوضح الشكل التالي :



أولاً: التهديد Threat :

هناك ثلاث مكونات أساسيه للتهديد Threat وهي :

- الهدف Target: وهي المعلومات المراد سرقتها.
- الطريقة أو العميل Agent: وهي الأشياء المكونة والمنشأة للتهديد.
- الحدث Event : وهي نوعية التأثير لوضعية التهديد .

1. الهدفTarget : وهي المعلومات الخاصة بالمنظمة ويمكن للمهاجم Attacker بعمل الآتي على كل من :

- الخصوصية Confidentiality : وذلك بكشف المعلومات السرية للآخرين.
- سلامة المعلومات Integrity: يمكنه تغيير المعلومات الخاصة بالمنظمة.
- التواجد Availability : بواسطة رفض الخدمة عن طريق DoS
- قابلية محاسبة المهاجم Accountability: لكي لا يحاسب المهاجم فإنه يقوم بإخفاء الهجوم (على سبيل المثال تغيير سجل الأحداثEvents logs (تغيير الـ IP).

2. الطريقة Agents (أو العميل) : لابد من توفر ثلاث سمات :

- الوصول إلى الهدف Access to the target قد يكون وصول مباشرDirect أي أن لديه حساب دخول على النظام وقد يكون غير مباشر Indirect(وذلك بالدخول عن طريق وسيط).
- معلومات عن الضحية Knowledge about the target
- الدوافع أو أسباب الهجومMotivation

3. الأحداث Events : وهي تكون بطرق عديدة من أهمها إساءة الدخول المخول Authorized وغير المخول Unauthorized إلى المعلومات أوالنظام. وإما عن طريق وضع أكواد خبيثة Malicious في الأنظمة.

ثانياً :الثغرات Vulnerabilities: تتكون من نوعين وهما:

- تحصين تقني Technical Vulnerability :إذا كان التحصين ضعيفا واستغل الضعف من قبل المهاجم يعرف هذا الهجوم بما يسمى بالهجوم التقني.

  التحصين التقني: استخدام الأجهزه للحمايه مثل أجهزة التشفير.

- تحصين غير تقني Administrative Vulnerability:وهو ما يسمى بالهجوم الغير تقني أو هجوم الهندسة الاجتماعية social engineering Attack

مثال : عندما يقوم شخص بالإتصال على Administrator ويدعي أنه مدير القسم ويقول لقد نسيت كلمه السر الخاصه بي هلا أرسلتها لي مثلا.

التحصين الغير تقني : مثل برامج الجدران النارية و مضادات الفيروسات

ويمكن تقسيمها من حيث الصعوبة والسهولة إلى قسمين:

- تحصينات ضعيفة High-level Vulnerability: وهو سهل الاستغلال، ومثال عليه كتابه كود برمجي لاستغلال تلك الثغرة.
- تحصينات قوية Low-level Vulnerability:وهذا النوع صعب الاستغلال ويتطلب الكثير من المصادر ، مصادر ماليه أو وقت طويل على المهاجم Attacker

الإجراءات المضادة عند حدوث الخطر **Countermeasures**

لا شك أن المعلومات تختلف من منشأة إلى منشأة وعلى حسب أهمية المعلومات فأن المنشأة تتخذ الإجراء المناسب وقد يكون التدخل قبل حدوث الخطر ويسمى Proactive Model وقد يكون تدخل بعد حدوث الخطر (انفعالي أو عاطفي) ويسمى Reactive Model

وهنا بعض أمثلة الإجراءات المضادة للتهديدThreats أو الهجوم Attacks :

- وضع جدران نارية Firewalls
- برامج مكافحة الفيروسات Anti-virus software
- التحكم بالدخول Access Control
- مضاعفة أنظمة التحقق من المستخدم Two-factor authentication systems
- التدريب الجيد للموظفين Well-trained employees

وهنالك الكثير من الإجراءات

كيفية إدارة الخطر و احتمال حدوثه:

الخطوات المتبعة في إدارة الخطر Risk هي:

أولا: تحليل الخطرRisk Analysis

ثانيا: اتخاذ قرار بشأن هذا الخطرDecision Management

ثالثا: تطبق ذلك القرارImplementation

ويوضحها الشكل التالي:

إدارة الخطر من حيث التدخل ينقسم إلى قسمين هما:

1. تدخل بعد حدوث الخطر Reactive Model وهذا النوع مشهور جدا وهو ما يسمى بالتدخل الانفعالي أو العاطفيEmotional على سبيل المثال يقوم مسؤول الأمن في الشركة بتحميل برنامج مكافح الفيروسات بعدما ينتشر الفيروس ، ويدمر بعض الأجهزة ويمكن حسابه كما يلي :

تكلفة الحماية = مجموع تكلفة هذا الخطر + تكلفة الإجراء المضاد.

2. يستعد للتدخل أي قبل حدوث الخطر Proactive Model: وهذا النوع أفضل بكثير من ناحية التكلفة، حيث يقلل منقبل حدوث الخطر تكلفة الخطر. كما يلي:

تكلفة الحماية = الحد الأدنى من الخطر + تكلفة الإجراء المضاد

مبادئ التعمية

التعمية (التشفير السري) وهي عملية تحويل البيانات من صورتها الواضحة الى صورة غير مفهومة بطرق رياضية متقدمة وباستخدام مفاتيح سرية غير متاحة لغير المصرح لهم.

تاريخياً: ودور العرب

التعمية

- متماثلة
- غير متماثلة

مراجعة دورية لتحسين هذه الشفرات وسد أي ثغرات.

التشفير أو (التعمية) استخدم قديما في الحضارات القديمة لإخفاء المعلومات والمراسلات مثل الحضارة الفرعونية والدولة الرومانية. ولكن التشفير كعلم مؤسسمنظم يدين بولادته ونشأته للعلماء الرياضيين واللغويين العرب إبان العصر الذهبي للحضارة العربية ومن أشهرهم الفراهيدي والكندي، وقد ألف هؤلاء العلماء مفاهيم رياضية متقدمة من أهمها التوافيق والتباديل . وكذلك توظيف الكندي ومن تبعه مفاهيم الإحصاء والاحتمالات في كسر الشفرة ، وقد سبقت هذه الكتابات كتابات باسكال وفيرما بحوالي ثمانية قرون !!!

وقد شاع في أيامنا استخدام مصطلح "التشفير" ليدل على إخفاء المعلومات. ولكن كلمة "التشفير" وافدة من اللغات الاوربية (Cipher) وهذه بدورها جاءت أصلا من اللغة العربية ولكن بمعنى آخر لكلمة "الصفر". فكما هو معلوم أن العرب قد تبنوا مفهوم الصفر والخانات العشرية واستخدموه في الحساب، وهو ما لم يكن الأوربيون يعرفونه في القرون الوسطى وكان مفهوم الصفر جديدا وغريبا لدرجة أنهم أخذوه بنفسالاسم فأسموه"Cipher"ولأن مفهوم الصفر الجديد كان في منتهى التعقيد والغموض فقد صاروا يستخدمون كلمة Cipher للدلالة على الأشياء المبهمة وغير الواضحة"

علم التعمية Cryptography

Definitions

حماية المعلومات Information security : هو العلم الذي يبحث في مجال الحفاظ على سرية المعلومات وأمنها والذي يقوم على مبادئ واضحة

التعمية Cryptography: طريقة تستعمل لتحويل نص واضح إلى صيغة غير مقروءة أو مفهومة تدعى نصا مشفرا أو Cipher Text حيث يجب إعادة فك تشفير النص للتمكن من قراءته لاحقا ويتم ذلك باستخدام خوارزمية معاكسة لخوارزمية التشفير الأصلية.

عرف علم التشفير أو التعمية منذ القدم فقد استخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، حيث استخدم في المجال الحربي والعسكري, وبلغ هذا الاستخدام ذروته في فترات الحروب، خوفاً من وقوع الرسائل الحساسة في أيدي العدو

علم التعمية Cryptography

Definitions

Plain text:هو النص الصريح الواضح والمفهوم Data من الرسالة أو البيانات والتي تعطى للخوارزمية كدخل.

Plaintext: An original message.

Cipher text:هو خرج الخوارزمية المطبق على دخلها ويسمى النص المعمى ويعتمد على كل من النص الصريح والمفتاح السري.

Ciphertext: The coded message.

Substitution: هي الطريقة التي يتم بها استبدال حرف برمز ما إما من نفس الأبجدية أو من غيرها من الأبجديات المختلفة.

Transposition: هي الطريقة التي تقوم بتقسيم النص إلى مجموعة بلوكات مثلا كل /5/ حروف وكل بلوك يقوم بذاته بتغيير موقعه بشكل مرتب وفق مفتاح ما أو طريقة ما.

علم التعمية Cryptography

Encryption Algorithm:هي الخوارزمية التي تؤدي مختلف عمليات الإستعاضة والاستبدال والتي تطبق على النص الصريح.

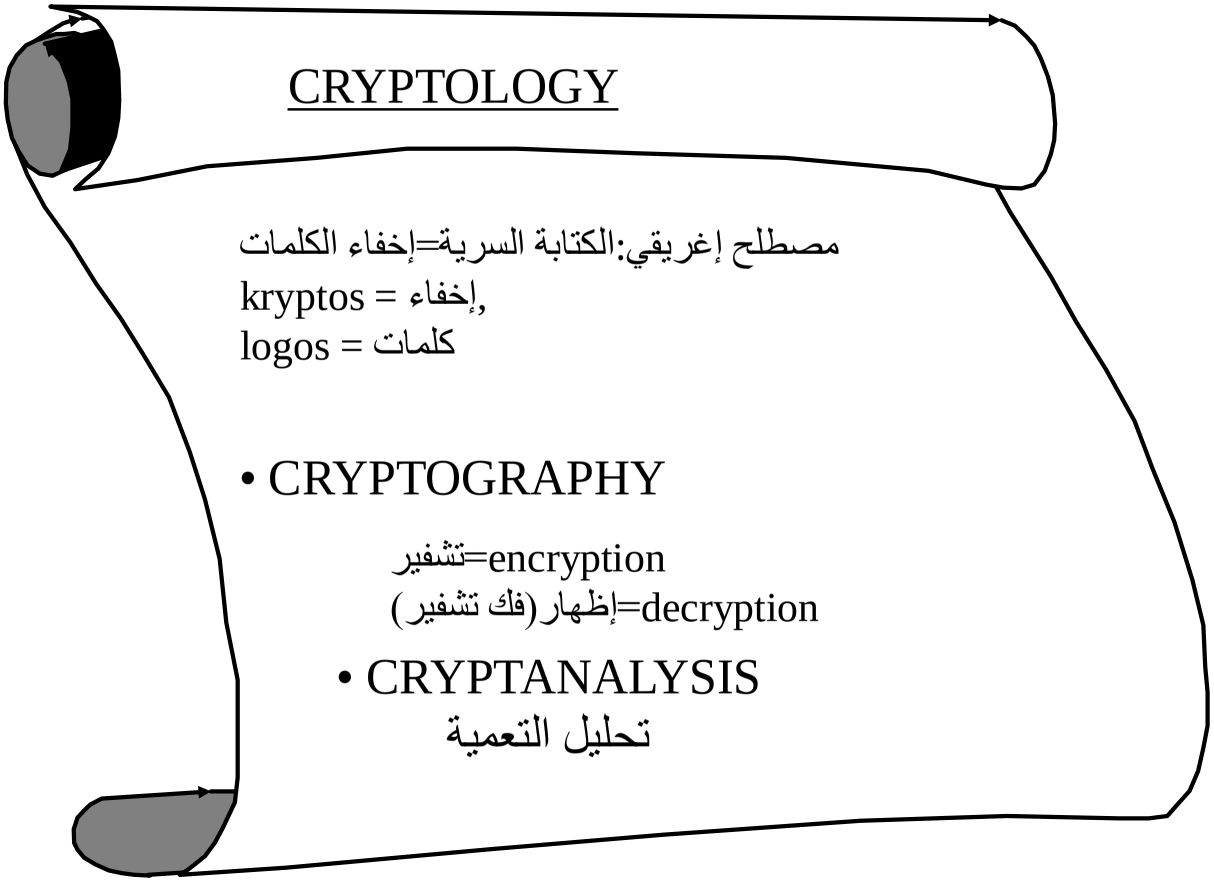
صفات خوارزميات التشفير المعتمدة

1- أن يكون ثمن كسر النص المعمى يفوق قيمة المعلومات المشفرة.

2- أن يكون الزمن اللازم لكسر النص المعمى يفوق الفترة المفيدة لحياة المعلومات.

Secret Key:المفتاح السري المشترك بين المرسل والمستقبل وهو دخل لخوارزمية التشفير ومستقل عن النص الصريح ويتعلق بكل من الإستعاضة والاستبدال.

علم التعمية CRYPTOGRAPHY



CRYPTOLOGY

مصطلح إغريقي:الكتابة السرية=إخفاء الكلمات

kryptos = إخفاء,

logos = كلمات

- CRYPTOGRAPHY

  تشفير=encryption

  إظهار(فك تشفير)=decryption

- CRYPTANALYSIS

  تحليل التعمية

علم التعمية Cryptography

- علم التعمية أو الكتابة المشفرة المسماة بالـ Cryptographyهو فن أو علم إخفاء المعلومات بحيث تكون بأمان عند إرسالها أو تخزينها، ويعتبر مجال ذو أهمية كبيرة للحكومات، والشركات الخاصة، و مع ثورة الإنترنت وازدياد مستخدميه ازدادت أهميته.
- فالأفراد يحتاجون للخصوصية عندما يتعلق الأمر بالمعلومات الشخصية والحساسة،
- الشركات كذلك تريد حماية سجلاتها المالية، وأسرارها التجارية، ومعلومات عملائها وموظفيها وغيرها من المعلومات المهمة والخاصة.
- تستعمل الحكومة الكتابة المشفرة للمساعدة على ضمان الأمان والاستقرار لمواطنيها.

علم التعمية Cryptography

أقسام الـ cryptography

ينقسم علم التشفير إلى **ثلاثة** أقسام هي :

1. الكتابة المشفرة الطبيعية (Physical Cryptography)

تتضمن الكتابة المشفَرة الطبيعية أنواع مختلفة من الطرق، والطرق الأكثر شيوعاً تستخدم الإحلال أو تبديل الحروف أو الكلمات، ومن الطرق الطبيعية أيضاً طريقة التشفير المسماة بفن الاختزال أو المواراة (Steganography) ، وهي لإختفاء المعلومات ضمن معلوماتٍ أخرى، كصورة مثلاً. عموماً تشير الكتابة المشفرة الطبيعية إلى أي طريقة لا تعدّل القيمة باستعمال عملية رياضية.

علم التعمية Cryptography

هناك ثلاثة أنواعِ رئيسية من الكتابة المشفرة أَو التشفير:

- cipherهي طريقة تستعمل لتشفير الحروف وذلك لإخفاء قيمتها.
- أما التَشفير Cipheringهي عمليةُ استعمال cipher لتشفير رسالة.
- النموذج الهجين hybrid model يستخدم طريقة واحد أَو أكثر للتشفير.

علم التعمية Cryptography

2. الكتابة المشفرة الرياضية (Mathematical Cryptography)

تتعامل الكتابة المشفرة الرياضية مع القضايا المتعلقة باستعمال العمليات الرياضية على الحروف أَو الرسالةِ. الأكثر شيوعاً هي دالة تسمى الهاش (Hashing) وهي عبارة عن عملية حسابية تتم على الرسالة وتحولها إلى قيمة عددية (numeric hash value)

و هي فقط عدد وحيد. و لا يمكن أن تستعمل لاشتقاق معنى الرسالة. هذا العددِ يمكن أن يرسل بالرسالة إلى المستلم. الطَرف الآخر يمكن أن يستعمل نفس دالة الهاش لتقرير أن الرسالةِ موثوق بها. إذا كانت قيمةِ الهاش مختلفة، فهذا يدل على أن الرسالة عُدّلت بطريقةٍ ما. هذه العملية معروفة كذلك بحساب المجموع (checksum)

علم التعمية Cryptography

3.الكتابة المشفَرة الكمية (Quantum Cryptography)

الكتابة المشفَرة الكَمية هي طريقة جديدة نسبياً من التشفيرِ. قبل 2002، تطبيقها كان محدوداً على عمل المختبر وربما بعض التطبيقات الحكومية السرية. هذه الطريقة تعتمد على خصائص أصغر جزيئات عُرفت. من الممكن الآن صنع شفرات مستحيلة الكسر باستخدام الطرق الكمية.

علم التعمية Cryptography

علم دراسة الكتابة المعمّاة (السرية).

عملية الإظهار
Decryption

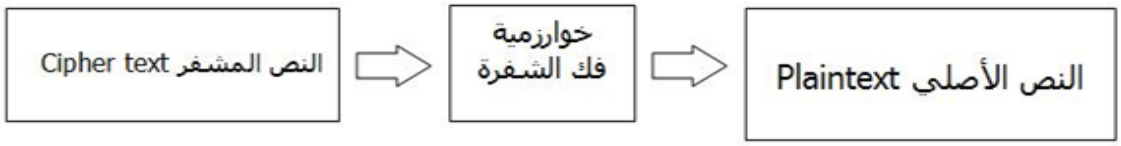
عملية التعمية
Encyption

مفاتيح التعمية والإظهار
(Cryptographic Keys).

علم التعمية Cryptography

التشفير Encryption : عملية تحويل النص الواضح إلى نص مشفر باستعمال خوارزميات التعمية وذلك لجعل المعلومات سرية.

فك التشفير Decryption/Deciphering : عملية الحصول أو استرجاع البيانات المشفرة إلى نص واضح ومفهوم.



علم التعمية Cryptography

Cryptography: Many schemes used for encryption.
Encryption: Process of converting from plaintext to ciphertext
Decryption: Process of restoring plaintext from ciphertext.
Cryptanalysis: Techniques used for deciphering a message without any knowledge of the enciphering details

علم التعمية Cryptography

فعلم التعمية قائم على العناصر التالية:

مرسل- مستقبل ـ رسالة - النص الواضح - النص المعمى - مفتاح التعمية.

التعريف الرياضي لنظام التعمية.

يتكون نظام التعمية من الخماسي (P,C,K,E,D) حيث:

P مجموعة منتهية من الرموز تسمى النص الواضح.

C مجموعه منتهية من الرموز تسمى النص المعمى.

K مجموعة منتهية من المفاتيح يسمى فضاء المفاتيح.

علم التعمية Cryptography

من أجل كل $k \in K$ يوجد تحويل تعميه $e_k \in E$

يقابله تحويل كسر تعميه $d_k \in D$

بحيث يكون:

$$e_k : p \to c$$

$$d_k : c \to p$$

$$d_k(e_k(x)) = x \quad ; \quad \forall x \in p$$

$$Encryption : C = E_k(P)$$

$$Decryption : P = D_k(C)$$

$$D_k(E_k(x)) = E_k(D_k(x)) = x$$

علم التعمية Cryptography

يصدر المبلغ رسالة على شكل نص صريح هو $X=\{x_1,x_2,....x_m\}$ إن العناصر M من الرسالة X هي عبارة عن أحرف منتمية إلى مجموعة محارف منتهية وهي المحارف التقليدية 26 حرفا حيث نستخدم عوضا عنها {0.1}.

لانجاز التعمية يولد مفتاح بالشكل $K=\{k_1,k_2,k_3.....k_j\}$.

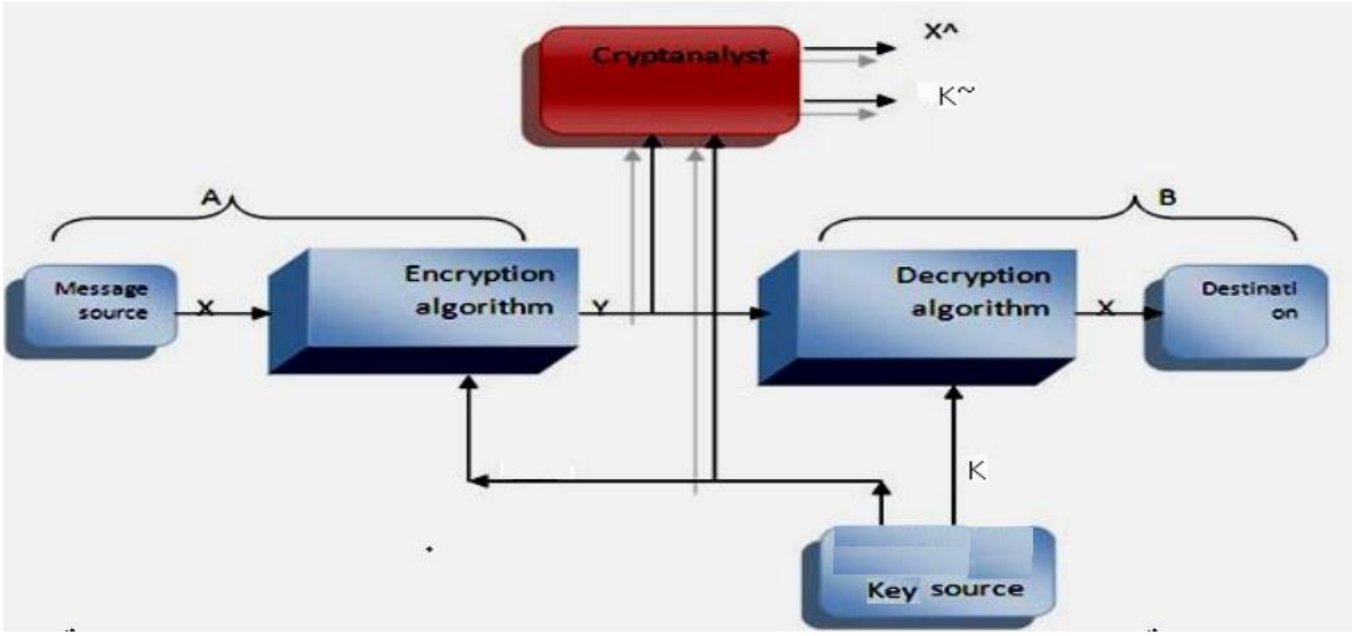
إذا ولد المفتاح عند مصدر الرسالة يجب نقله إلى وجهة الهدف عبر قناة آمنة للطرف الآخر.

ملاحظة: أفضل طريقة هي توليده عند طرف ثالث ويصل إلى كل من المصدر والهدف.

تقوم الخوارزمية باستخدام النص الصريح والمفتاح ويتولد نص معمّى هو $Y=\{y_1,y_2,.....y_n\}$ حيث يمكن كتابة الأمر بشكل صيغة رياضية: $\mathbf{Y=E_k(X)}$

تقرأ إنتاج Y باستخدام الخوارزمية E المعتمدة على النص X والمفتاح الخاص K

علم التعمية Cryptography



علم التعمية Cryptography

أثناء سير النص للوصول إلى الوجهة سيحاول المعتدي الحصول على Y
ولكن لا يمكنه الوصول إلى Xو K
وعند معرفة المعتدي للخوارزمية E ولخوارزمية الفك D عندها سيسعى المعتدي للوصول إلى النص الأصلي X عن طريق توليد النص الأصلي المقدر X~وذلك باستخدام المفتاح K عن طريق توليد المفتاح المقدر K~.

جامعة حماة
الكلية التطبيقية
قسم تقنيات الحاسوب

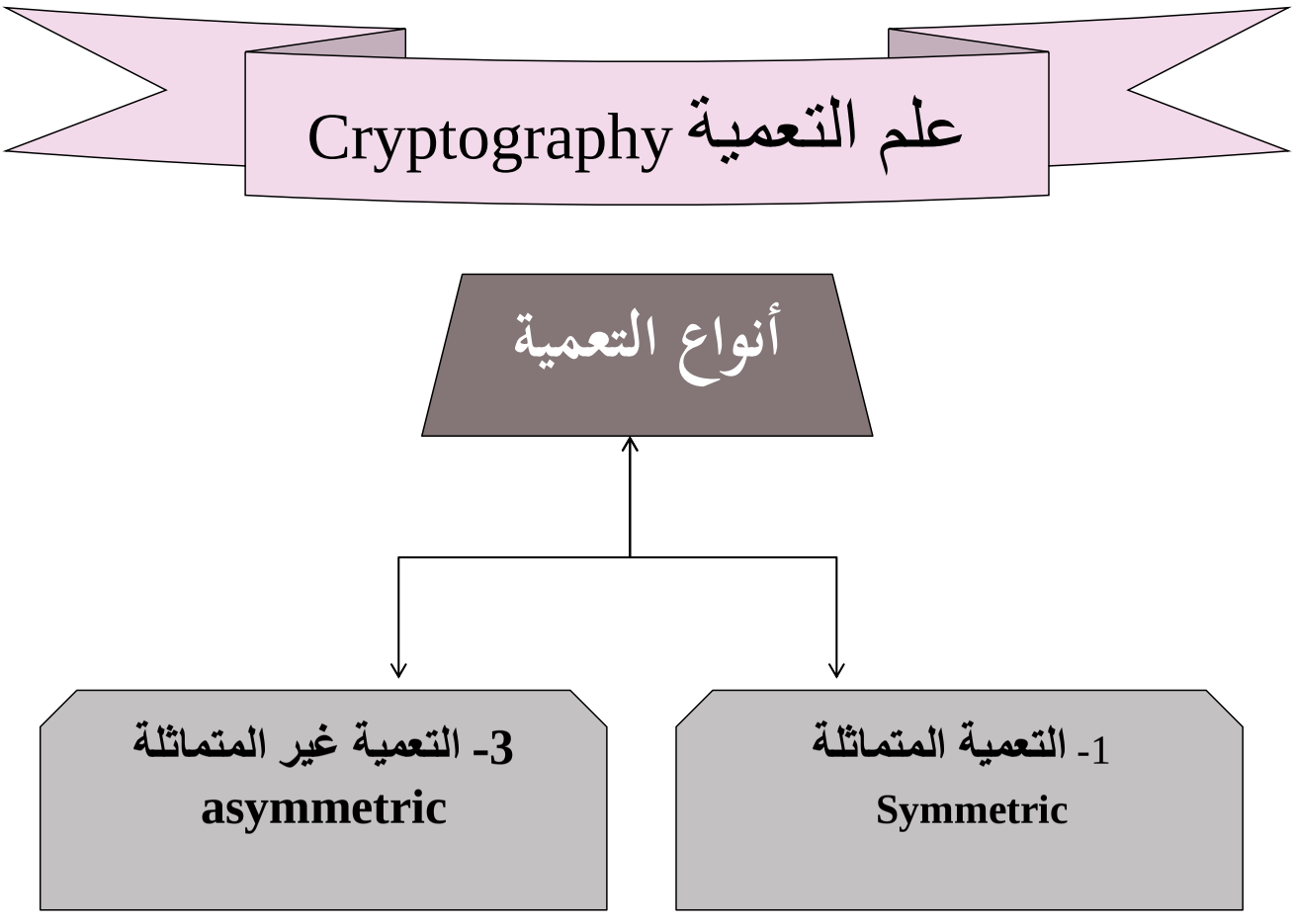
- **المقرر: أمن المعلومات**
- **المحاضرة : الثالثة**

Dr. Mohammed AL-Mohammed

Chapter 3

التعمية وأمن المعلومات

مبادئ وتطبيقات



علم التعمية Cryptography

أنواع التعمية

1- التعمية المتماثلة
Symmetric Cryptography

علم التعمية Cryptography

1- **نظام التعمية المتناظر Symmetric Cipher Model:** وهو نوع من التعمية يكون فيه كل من المرسل والمستقبل لديهم نفس المفتاح "Single_Key".

يسمى أيضاً التشفير التقليدي (Conventional Cryptography):

وهو يستخدم مفتاح واحد لعملية التشفير وفك التشفير للبيانات. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدم .حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. أما الثغرة الكبيرة في هذا النوع من التشفير فكانت تكمن في تبادُل المفتاح السري دون أمان

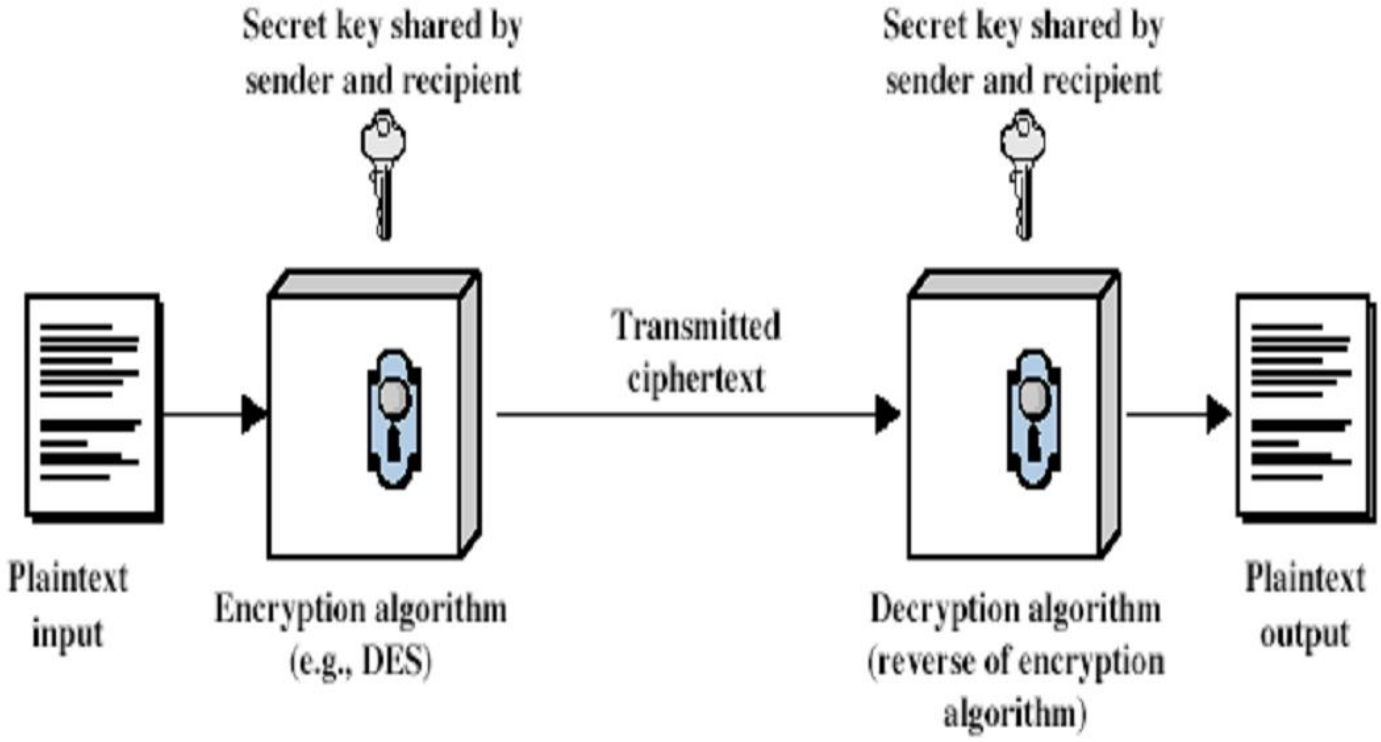
علم التعمية Cryptography

المتطلبات الأساسية لاستخدام التشفير الآمن Requirement of Encryption:

- وجود خوارزمية قوية للتشفير : بحيث إذا تم كشف الخوارزمية وكشف النص لا يمكن الوصول إلى النص الصريح ولا يمكن الوصول إلى المفتاح .
- كل من المرسل والمستقبل يجب أن يكون لديهم نسخ من المفتاح السري بشكل آمن ويحفظ لديهم بسرية تامة.

$$Encryption: C = E_k(P)$$
$$Decryption: P = D_k(C)$$
$$D_k(E_k(x)) = E_k(D_k(x)) = x$$

علم التعمية Cryptography



أنواع التعمية

1- التعمية المتماثلة
Symmetric

- (التقنيات الكلاسيكية)

معميات الإعاضة Substitution ciphers

معميات إبدال الموقع Transposition ciphers

(التقنيات الحديثة)

- معيار تعمية المعطيات Data Encryption Standard (DES)
- الخوارزمية العالمية لتعمية المعطيات (IDEA): International Data Encryption Algorithm
- معيار تعمية المعطيات الثلاثي Triple -DES (3DES)
- **المعيار AES**

علم التعمية Cryptography

- من أشهر خوارزميات منظومات التعمية التقليدية أوالمتماثلة

Caesar Cipher, DES, 3DES, IDEA,Towfish,RC4, Rijndael وجميعها تستخدم المعيار الأمريكي في التشفير. تدعى هذه الخوارزميات بخوارزميات التشفير متناظرة المفاتيح لكوننا نستخدم مفتاح تشفير واحد لعمليتي التشفيرencryption-key وفك التشفيرdecryption-key.

أنواع التعمية

3- التعمية غير المتماثلة
aSymmetric

علم التعمية Cryptography

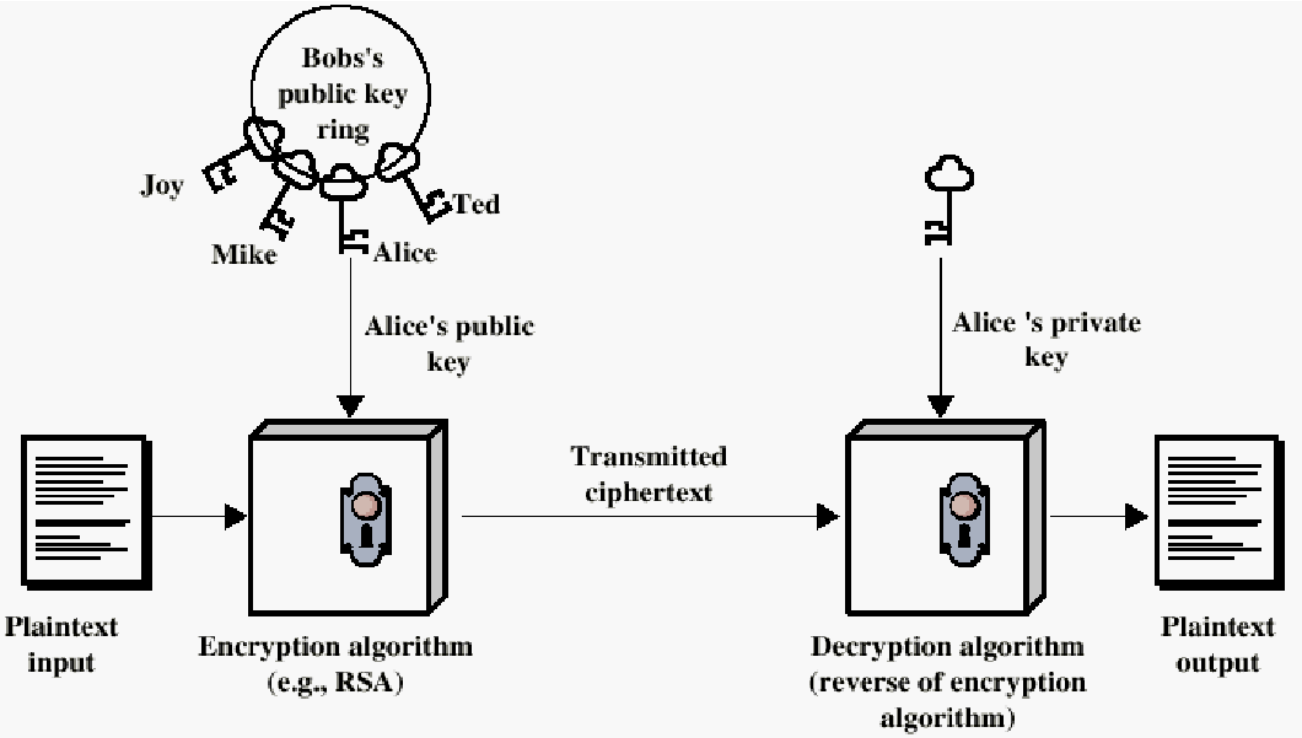
2- **نظام التعمية غير المتناظر Asymmetric Cipher Model** :كل من المرسل والمستقبل لديهما مفتاحين مختلفين واحد خاص بالمرسل وآخر مختلف للمستقبل ولا يعرف كل واحد منها مفتاح الآخر

أو التشفير اللا متماثل Asymmetric Cryptography

ويعرف بتشفير المفتاح العام (العمومي) Public Key Cryptography :

والتي يختلف فيها مفتاح التشفير عن مفتاح فك التشفير أي أن هنالك مفتاحين: مفتاح خاص (private key) ومفتاح عام (public key). المفتاح العام يوزع على جميع الناس أما المفتاح الخاص فهو شخصي يحتفظ به صاحبه ولا يرسله لأحد, تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة, حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل. وأي رسالة أو ملف يتم تشفيره بالمفتاح العام لا يمكن فك تشفيره إلا بالمفتاح الخاص والعكس صحيح. فالتشفير اللا متماثل جاء حلاً لمشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل.

علم التعمية Cryptography



علم التعمية Cryptography

- يعد تطور تعمية المفتاح العمومي الأعظم ولربما كان الثورة الحقيقية الوحيدة في تاريخ علم التعمية بأكمله وتقدم تعمية المفتاح العمومي تحولاً ثورياً عن كل ما سبقها. وذلك لسببين، أولهما أن خوارزميات تعمية المفتاح العمومي مبنية على توابع رياضية إضافة إلى الإعاضة والإبدال.

علم التعمية Cryptography

- تدعى منظومات تعمية المفتاح العمومي بالمنظومات غير المتماثلة asymmetricويكون فيها مفتاح التعمية encryption key مغايراً لمفتاح الإظهار decryption keyوبالتالي يمكن الإعلان عن أحدهما (المفتاح العمومي public-key) دون الخوف على الآخر(المفتاح الخصوصيprivate-key) .
- ويتم الحصول على المفتاح العمومي من المفتاح الخصوصي بواسطة تحويل One-way Transformationبينما يجب أن يكون من باتجاه واحد فقط الصعوبة بمكان تحديد المفتاح الخصوصي من المفتاح العمومي

علم التعمية Cryptography

أنواع التعمية

3- التعمية غير المتماثلة aSymmetric ⟺ منظومات تعمية المفتاح العمومي Public-Key Cryptographic Systems

أشهر الخوارزميات

- خوارزمية RSA (Rivest, Shamir and Adleman)
- خوارزمية الجمل ELGamal Algorithm
- خوارزمية المنحني الإهليلجي Elliptic Curve Algorithm EC

مبدأ كيرشوف Kerckhoff's Principle

قد يبدو أن من الآمن أكثر أن نقوم بتخبئة خوارزميتي التشفير وفك التشفير والمفتاح السري كلها دون الإعلان عنها وهو الأمر الذي لا ننصح به.

يجب علينا وفقًا لمبدأ كيرشوف أن نفترض أن الآخرين يعلمون بخوارزمية التشفير أو فك التشفير. وبالتالي تنحصر مهمتنا في مقاومة هجومات فك التشفير في الحفاظ على المفاتيح السرية. سنتبين أهمية هذا المبدأ عندما سنتحدث فيما بعد عن أساليب التشفير الحديثة التي تتمتع بمجال لتوليد المفاتيح واسعًا مما يجعل من الصعب الوصول إليها.

1. التشفير بالاستبدال Substitution Ciphers

يهدف هذا الأسلوب من التشفير إلى استبدال رمز بآخر. إذا كان الرمز هو عبارة عن حرف من الحروف الأبجدية ضمن نص غير مشفر فإننا نقوم باستبداله بحرف آخر. يمكن مثلا استبدال الحرف A بالحرف D والحرف T بالحرف Z وهكذا.. إذا كانت الرموز عبارة عن خانات عددية (من **0** حتى **9**)، فيمكن مثلا استبدال 3 ب **7** و **3** ب **6** وهكذا

يمكن تقسيم طرق الاستبدال ضمن فئتين، هما:

1. المشفرات وحيدة الحرف **Monoalphabetic ciphers**
3. المشفرات متعددة الحروف **Polyalphabetic ciphers**

المشفرات وحيدة الحرف

يجري هنا استبدال حرف (أو رمز) ضمن النص غير المشفر دائمًا بحرف (أو رمز) آخر هو نفسه دائمًا بغض النظر عن موضعه ضمن النص. أي ان العلاقة بين الحروف ضمن النص غير المشفر والنص المشفر هي علاقة واحد لواحد.

مثال:

Plaintext: hello نص غير مشفر

Ciphertext: KHOOR نص مشفر

وتشمل:

1. المشفرات بالجمع.
3. المشفرات بالضرب.
3. المشفرات بالتبديل وحيدة الحرف.

المشفرات بالجمع Additive Ciphers

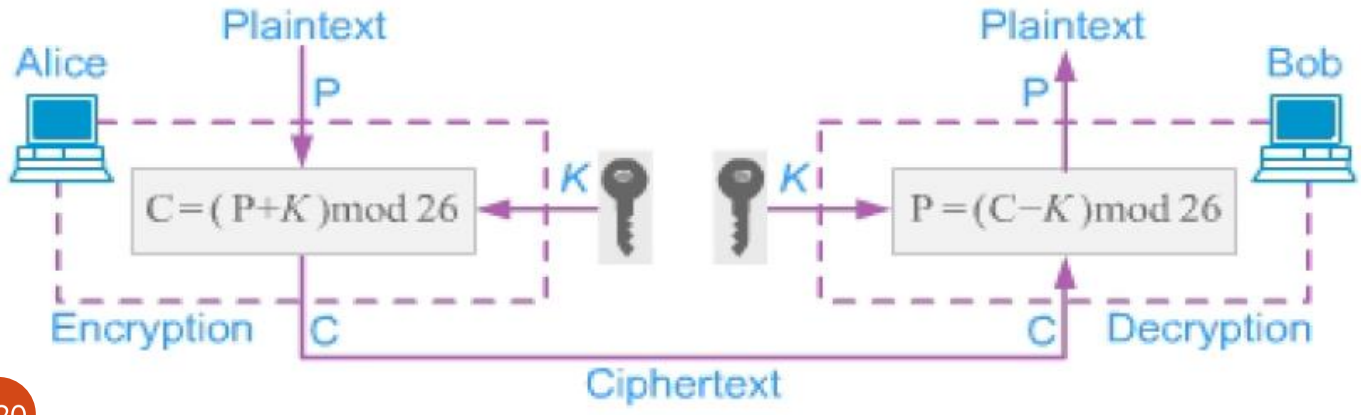
يعد هذا النوع من المشفرات أبسط مشفرات الاستبدال وحيدة الحرف. وتسمى أحيانًا مشفرات الإزاحة **Shift ciphers** أو مشفرات قيصر **Caeser ciphers** ولكن تبقى التسمية مشفرات الجمع أكثر تعبيرًا عن الطبيعة الرياضية لهذا النوع من المشفرات. بفرض أن النص غير المشفر يتضمن حرف أبجدية صغيرة (من a إلى z) وأن النص المشفر يتضمن حروفًا كبيرة (من A إلى Z) فبالتالي من أجل تطبيق عمليات حسابية ورياضية على النصين غير المشفر والمشفر يجب أن نخصص قيمًا عددية لكل حرف صغير أو كبير كما هو مبين في الشكل التالي:

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

خصص لكل حرف كبير وصغير ضمن الشكل السابق عددًا صحيحًا ضمن المجموعة Z_{36} (وهي مجموعة الأعداد الصحيحة من 0 حتى 35 : $Z_n = \{0,1, 3,3,\ldots, n-1\}$).

المفتاح السري بين Alice و Bob هو أيضًا عدد صحيح من المجموعة Z_{36}

تقوم خوارزمية التشفير بإضافة المفتاح إلى حروف النص غير المشفر. أما خوارزمية فك التشفير فتقوم بطرح هذا المفتاح من حروف النص المشفر. تجري كافة العمليات الحسابية ضمن المجموعة Z_{36} يوضح الشكل التالي كيفية تنفيذ ذلك:



خوارزمية قيصر Caesar Cipher

أبسط أنواع طرق التبديل تنتج عن طريق تبديل أحرف الرسالة الأصلية بأحرف أخرى تبعد عنها مسافة ثابتة في الترتيب الأبجدي. أول من استخدم هذه الطريقة يوليوس قيصر.

قام القيصر بعمل إزاحة للأحرف ثلاث خانات، حيث استبدل الحرف A بالحرف D، والحرف B بالحرف E، والحرف C بالحرف F، وهكذا... كما موضح في الجدول:

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
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

تبديل الحروف بطريقة قيصر.

يمكن أن نبرهن بسهولة أن عمليتي التشفير وفك التشفير هما عمليتان متعاكستان وأن النص غير المشفر $P1$ والمولد من قبل **Bob** هو نفسه النص P المرسل من قبل **Alice** :

$$P1 = (C - k)\bmod 36 = (P + k - k)\bmod 36 = P$$

مثال:

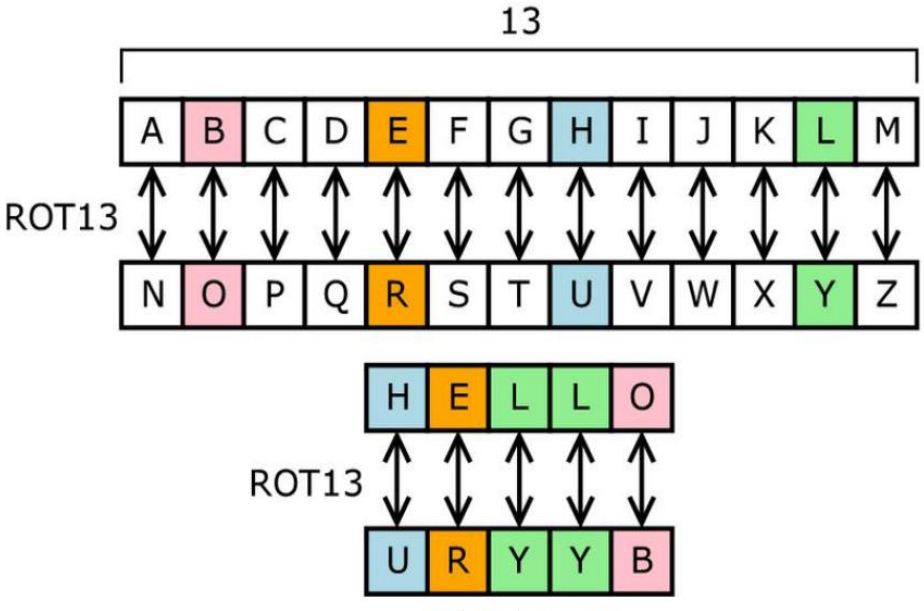
K = 3 , P = RUNAWAY

E(RUNAWAY) ⟶ UXQDZDB

D(UXQDZDB) ⟶ RUNAWAY

خوارزمية الإزاحة 13 ROT13

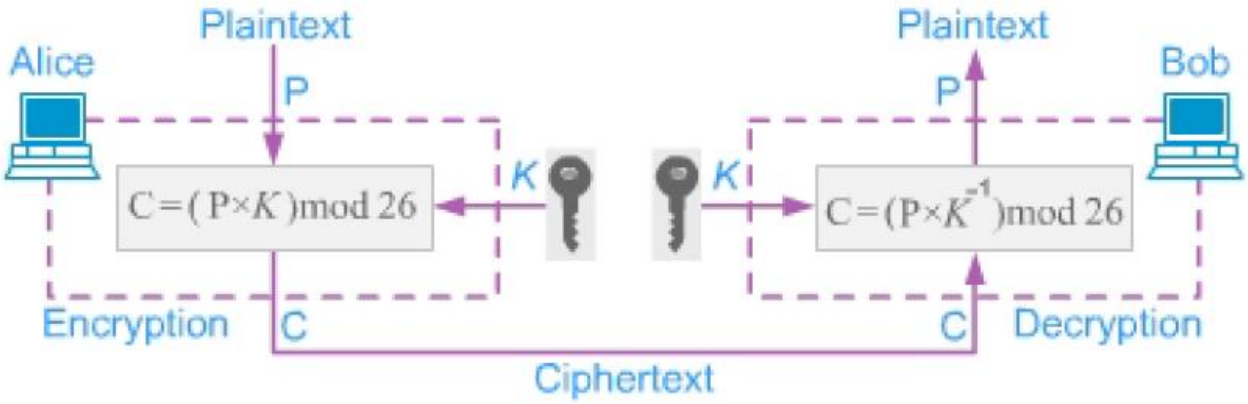
في هذه الطريقة يتم إزاحة Rotate كل حرف من الرسالة الأصلية ثلاث عشرة مرة فنحصل على النص المشفر وإذا أردنا إرجاع النص المشفر إلى أصله نقوم بعمل إزاحة لكل حرف ثلاث عشرة مرة أخرى، الشكل يوضح عملية الإزاحة المتبعة.



عمل خوارزمية الإزاحة 13.

المشفرات بالضرب Multiplicative Ciphers

تعتمد خوارزميات التشفير هنا على ضرب قيمة حروف النص غير المشفر بقيمة المفتاح للحصول على النص المشفر. أما خوارزميات فك التشفير فتعتمد على قسمة قيم حروف النص المشفر على قيمة المفتاح للحصول على النص غير المشفر، كما هو مبين في الشكل التالي:



يجب أن تجري العمليات الحسابية ضمن المجموعة Z_{36} كما يجب أن يكون المفتاح عنصراً من عناصر المجموعة Z_{36} التي تضم فقط **13** عنصرًا، وهي:

1, 3, 5, 7, 9, 11, 15, 17 , 19 , 31 ,33 ,35

ملاحظة:

المجموعة Z_{36}^{*} هي مجموعة جزئية من Z_{36} وتضم فقط الأعداد التي لها أزواج جداء عكسية، أي أزواج التي يكون نتيجة جدائها مساوي للقيمة **1**، كما هو مبين في الجدول التالي:

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

مثال:

K = 7, P = hello
E(hello) → XCZZU
D(XCZZU) → hello

المشفرات بالتبديل وحيدة الحرف Monoalphabetic Substitution Ciphers

على اعتبار أن المشفرات بالجمع وبالضرب لديها مجال صغير لاختيار المفتاح المرتبط بها، فإنه من الممكن أن يكون من السهل كسرها. يمكن أن نوفر حلاً أفضل بأن يتفق كلا الطرفين على جدول للمطابقة بين الحروف المتبادلة. يعرض الشكل التالي مثالا عن هذا الجدول:

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

مثال:

"runaway" ⇨ **"HJGNPNS"**

المشفرات متعددة الحروف Polyalphabetic Ciphers

مع هذا النوع من المشفرات، يمكن أن يتوفر عدة خيارات لاستبدال كل حرف من الحروف. فالعلاقة بين أي حرف من حروف النص غير المشفر مع أي حرف ضمن النص المشفر هي علاقة حرف واحد مع أكثر **one-to-many** يمكن مثلاً استبدال الحرف **"a"** بالحرف D إذا ورد في بداية النص أو بالحرف **N** إذا ورد في منتصفه.

- يضمن هذا النوع من المشفرات إخفاء تواتر ورود الحروف ضمن النص. وبالتالي تصبح محاولات كسر التشفير المعتمدة على تواتر ورود الحروف ضمن النص غير فعالة.
- لبناء مشفر متعدد الحروف، يجب الربط بين الحرف ضمن النص المشفر والحرف المقابل له ضمن النص غير المشفر ومكان تواجده ضمن هذا النص. هذا يعني أن المفتاح في هذهالحا لة، هو عبارة عن مجموعة من المفاتيح الجزئية. يرتبط كل واحد منها بموقع الحرف ضمن النص غير المشفر. بمعنى آخر:

3-28

فإن المفتاح $k = (k1, k\,3, k3, \ldots.)$ يفيد أنه يمكن استخدام $k\ i$ لتشفير الحرف رقم i ضمن النص غير المشفر لبناء الحرف رقم i ضمن النص المشفر.

أمثلة:

التشفير بمفتاح ذاتي التوليد Autokey Cipher: يتكون المفتاح مع هذا النوع من المشفرات من مجموعة من المفاتيح الجزئية متتابعة حيث يجري استخدام كل مفتاح جزئي لتشفير الحرف الموافق لترتيب المفتاح ضمن النص غير المشفر. يجري الاتفاق حول قيمة المفتاح الجزئي الأول. ويكون المفتاح الجزئي الثاني هو قيمة الحرف الأول ضمن النص غير المشفر. أما المفتاح الجزئي الثالث، فهو قيمة الحرف الثاني ضمن النص غير المشفر وهكذا دواليك.

$P = P_1P_3P_3\ldots.$

$C = C_1C_3C_3\ldots.$

$k = (k_1, P_1, P_3, \ldots)$

$Encryption: C_i = (P_i + k_i) \bmod 36$

$Decryption: P_i = (C_i - k_i) \bmod 36$

3-29

أمثلة:

- **المشفر فيجينر Vigenere Cipher:** جرى تصميم هذا المشفر من قبل الرياضي الفرنسي فيجينر في القرن السادس عشر. يعتمد هذا المشفر على تكرار استخدام مفتاح مع دفق حروف النص غير المشفر بشكل متتالي. يجب أن يكون طول المفتاح **m** محقق للشرط $1 \leq m \leq 36$.
  - نساوي كل حرف من المفتاح والنص بقيمته العددية من 0 إلى 25 حسب ترتيب حروف أبجدية اللغة الإنجليزية، مثلاً نجعل: a = 0، b=1، c= 2 وهكذا...
  - نجمع المفتاح مع النص الأصلي للحصول على النص المشفر، كما هو موضح في المعادلة التالية:

النص المشفر = النص الأصلي + الحرف الموازي له من المفتاح.

  - لفك التشفير نستخدم المعادلة التالية:

النص الأصلي = النص المشفر – الحرف الموازي له من المفتاح.

$$P = P_1 P_2 P_3 \cdots$$
$$C = C_1 C_2 C_3 \cdots$$
$$K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \cdots]$$
$$Encryption: C_i = (P_i + k_i) \bmod 26$$
$$Decryption: P_i = (C_i - k_i) \bmod 26$$

مثال:

Key: "python"
Plaintext: "rabbitwithbigpointyteeth"
Ciphertext:

R	a	b	b	i	t	w	i	t	h	b	i	g	p	o	i	n	t	y	t	e	e	t	H
p	y	t	h	o	n	p	y	t	h	o	n	p	y	t	h	o	n	p	y	t	h	o	N
G	Y	U	I	V	G	L	G	M	Y	M	V	V	N	H	P	B	G	N	R	P	L	H	U

مثال:

لنفرض أن المفتاح المستخدم للتشفير هو كلمة danger، والرسالة المراد تشفيرها هي:

Tomorrow is the time

نقوم بإتباع نفس الخطوات السابقة للتشفير ولفك التشفير:

1. نكرر المفتاح حسب عدد حروف النص الأصلي، كالتالي:

key : dangerdangerdange

plaintext : tomorrowisthetime

2. نجمع الحروف المتناظرة معاً للحصول على النص المشفر، بعد تحويل جميع الحروف إلى أرقـــام، مثلا: t+d تساوي 3+19=22 وهي قيمة الحرف w، إذا w=t+d، كـــذلك o+a تســـاوي 0+14=14 وهو حرف o، وهكذا... كما هو موضح في الجدول التالي:

d	a	n	g	e	r	d	a	n	g	e	r	d	a	n	g	e
t	o	m	o	r	r	o	w	i	s	t	h	e	t	i	m	e
w	o	z	u	v	i	r	w	v	y	x	y	h	t	v	s	i

وبعد تشفير الرسالة نحصل على النص المشفر:

Wozuvirwvyxyhtvsi

3. لفك التشفير نطرح كل حرفين متناظرين من بعضهما بعد تحويلهما إلـــى أرقـــام، مـــثلا:

d - w = 3 -22 = 19

والرقم 19 يساوي الحرف t، وهكذا حتى نحصل على النص الأصلي.

خوارزمية الكراسة الواحدة One time pad

ظهرت سنة 1917ف من قبل العالم فيرنام Vernam، في هذه الطريقة مفتاح التشفير يكون طويل جداً، أحيانا أطول من النص الأصلي. من الممكن استخدام كتاب أو قصة أو مجلة لتكون المفتاح، وذلك حسب الاتفاق بين المرسل والمستقبل.

يتم التشفير بأخذ جزء من المفتاح، جملة أو كلمة، بحيث يكون طوله مساوياً لطول النص الأصلي، وتحويل هذا الجزء إلى أرقام، بعد ذلك نزيح كل حرف من النص الأصلي بمقدار الرقم الذي يوازيه من الجزء المأخوذ من المفتاح. ولفك التشفير نستخدم نفس الطريقة ولكن بالمعكوس، أي أنه إذا كانت الإزاحة في التشفير إلى الأمام نرجع الأحرف إلي الخلف عند فك التشفير والعكس صحيح.

المشفر لمرة واحدة One-time Pad:يكون في هذا المشفر طول المفتاح السري العشوائي مساويًا لطول النص غير المشفر. مما يجعل من المستحيل عمليًا كسر هذا المشفر ومعرفة النص المرسل في الأصل وفقًا لما جاء في دراسة قام بها العالم شانون بهذا الخصوص. تزداد سرية هذا المشفر عند تغيير المفتاح عند تغيير النص المرسل حيث لا يجري استخدامه إلا مرة واحدة فقط. يؤدي ذلك إلى ضمان السرية بشكل كبير ولكن يستحيل عمليًا تحقيق ذلك بشكل سهل وتبادل المفتاح من وقت إلى آخر بين الطرفين المتصلين.

مثال:

Ciphertext: NZAKBMK

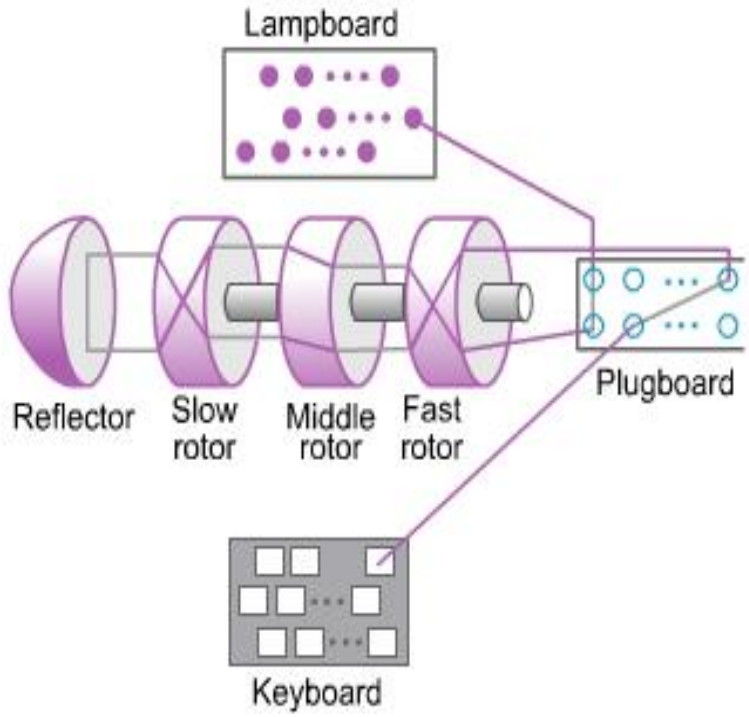
Possible Vigenére keys: wtnkxmm and nlvwker

Ciphertext: NZAKBMK NZAKBMK

Possible keys: nlvwker wtnkxmm

Plaintext: goforit runaway

- **آلة انيغما Enigma Machine:** جرى تطوير هذه الآلة من قبل الألمان أثناء الحرب العالمية الثانية. وهي آلة معقدة تعمل وفقاً لمبدأ التشفير بالتبديل. يبين الشكل التالي منظر الآلة التي سنشرح فيما يلي طريقة عملها:

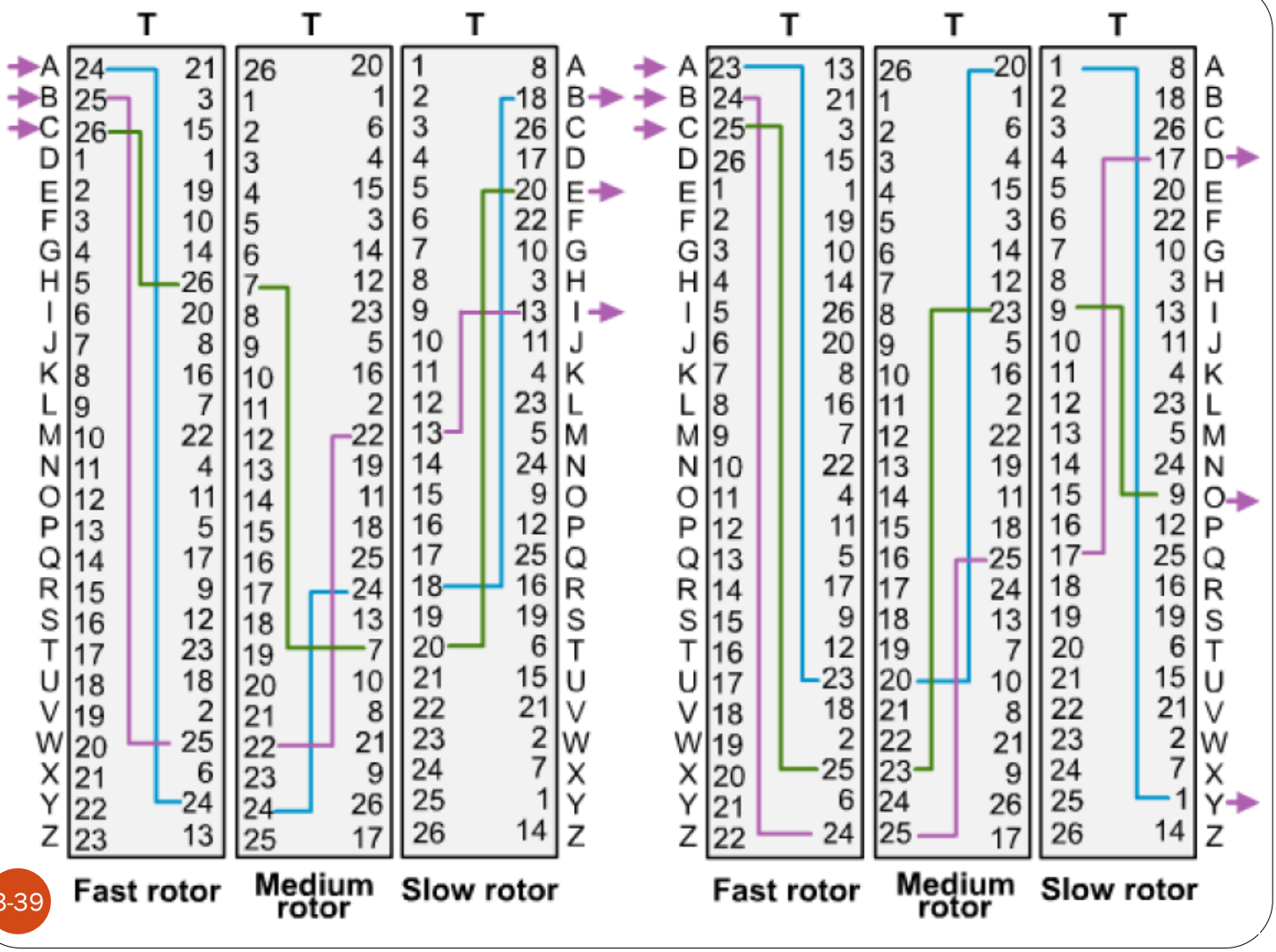


تتضمن الآلة ثلاثة دواليب من بين خمسة يمكن تركيبها. تعمل هذه الدواليب على الشكل التالي:

1. يقوم كل دولاب بعملية تشفير بالتبديل وحيدة الحرف.
3. يجري تمرير نتيجة تشفير كل دولاب إلى الدولاب التالي ليجري تشفيرها مرة أخرى وهكذا وصولاً إلى الدولاب الثالث.
3. تدور الدواليب من أجل كل حرف من حروف النص غير المشفر وفقًا لما يلي:

- الدولاب السريع **Fast rotor**: من أجل كل حرف.
- الدولاب المتوسط **Middle rotor**: من أجل كل **36** حرف.
- الدولاب البطيء **Slow rotor**:من أجل كل **676** = **26x 26** حرف.

- إذا جرى إدخال الحرف **C** على لوحة المفاتيح كحرف أول فإنه سيجري ما يلي:
  1. سيطابق هذا الحرف الرقم **26** على الدولاب السريع.
  2. الرقم **26** مرتبط بالرقم **7** على الدولاب الوسيط.
  3. الرقم **7** مرتبط بالرقم **20** على الدولاب البطيء.
  4. يوافق الرقم **20** الحرف **E** كنتيجة لعملية التشفير.
- إذا جرى إدخال الحرف **C** على لوحة المفاتيح كحرف ثاني فإنه سيجري ما يلي بعد دوران الدولاب السريع لحرف واحد:
  1. سيطابق هذا الحرف الرقم **25** على الدولاب السريع.
  2. الرقم **25** مرتبط بالرقم **23** على الدولاب الوسيط.
  3. الرقم **23** مرتبط بالرقم **9** على الدولاب البطيء.
  4. يوافق الرقم **9** الحرف **O** كنتيجة لعملية التشفير.
- يجري تكرار التشفير للحروف بعد **17,576** = **26 x 26 x 26** حرف.



جامعة حماة
الكلية التطبيقية
قسم تقنيات الحاسوب

- المقرر: أمن المعلومات
- المحاضرة : الرابعة

Dr. Mohammed AL-Mohammed

Chapter 4

التعمية وأمن المعلومات

التشفير الكتلي

4. التشفير لدفق المعطيات والتشفير الكتلي Stream and Block Ciphers:

جرى تقسيم المشفرات ذات المفاتيح المتناظرة ضمن فئتين رئيسيتين، هما:

مشفرات دفق المعطيات Stream Ciphers:

يجري مع هذه المشفرات التعامل مع المعطيات على الرمز الواحد (أو الحرف الواحد) في نفس الوقت. ويكون لدينا بالتالي: دفق لمعطيات النص غير المشفر، دفق لمعطيات النص المشفر، دفق لمعطيات مفتاح التشفير:

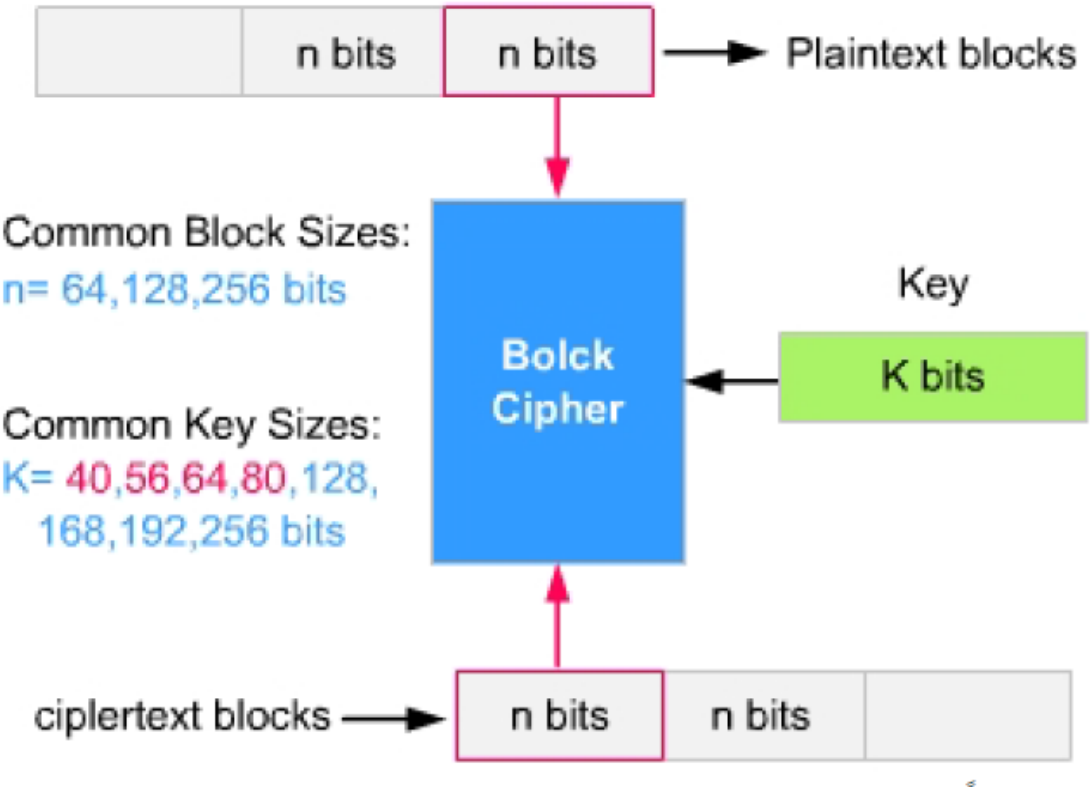
$$P = P_1 P_2 P_3 \cdots$$
$$C = C_1 C_2 C_3 \cdots$$
$$K = (k_1, k_2, k_3, \cdots)$$
$$C_1 = E_{k1}(P_1)$$
$$C_2 = E_{k2}(P_2)$$
$$C_3 = E_{k3}(P_3) \cdots$$

المشفرات الكتلية Block Ciphers:

يجري مع هذه المشفرات تقسيم النص غير المشفر إلى كتل من الحجم $m > 1$ ليتم بعد ذلك ليتم بعد ذلكتشفيرها معًا وإنشاء كتلة من نفس الحجم ضمن النص المشفر. يجري مع هذه المشفرات استخدام مفتاح واحد من كامل الكتلة حتى ولو كان هذا المفتاح مؤلفًا من عدة قيم جزئية.

1. المشفرات الكتلية الحديثة Modern Block Ciphers:

تعتمد هذه المشفرات على التعامل مع كتل بحجم n بت وتستخدم خوارزميات التشفير وفك التشفير الخاصة بها مفتاح سري مشترك بطول k بت، كما هو مبين في الشكل التالي حيث يجري التعامل مع ملفات ثنائية Binary files:



إذا تضمن الرسالة نصًا ذو حجم أقل من n بت، يجري عندها إضافة بتات حشو إلى النص ليصل إلى الحجم المطلوب.

وتشمل:

1. الاستبدال أو المناقلة **Substitution or Transposition**
2. المشفرات الكتلية وزمر التدوير **Block Ciphers as Permutation Groups**
3. مكونات المشفر الكتلي الحديث **Components of a Modern Block Cipher**

الاستبدال أو المناقلة Substitution or Transposition

يمكن استخدام أحد أسلوبي الاستبدال أو المناقلة مع المشفرات الكتلية الحديثة بنفس طريقة عمل المشفرات التقليدية، لكن نقوم مع المشفرات الحديثة بالتعامل مع بتات وليس مع رموز أو حروف.

إذا كان المشفر معتمد على أسلوب الاستبدال فإنه بتبديل بت قيمتها 1أو 0 ضمن النص غيرالمشفر ببت قيمتها 0 أو 1 يعني ذلك أن النصين غير المشفر والمشفر سيكون لديهما عدد مختلف من بتات 0 و 1. أما إذا كان المشفر معتمد على أسلوب المناقلة، فإننا سنقوم بتغييرمواضع البتات فقط وسنحصل على نفس عدد بتات **1** و **0** ضمن النصين غير المشفر والمشفر.

في كلا الحالتين السابقتين، فإن القيم المحتملة لكتلة من n بت هي 2^n قيمة، لأن كل بت يمكن أن تأخذ أحد قيمتين: إما 0 أو 1 .

جرى تصميم المشفرات الكتلية الحديثة على أنها مشفرات استبدال لأن خواص المناقلة التي تؤدي إلى المحافظة على عدد خانات **0** وال **1**، تجعل المشفر قابل للكسر بسهولة.

المشفرات الكتلية وزمر التدوير Block Ciphers as Permutation Groups

يمكن أثناء دراستنا للمشفرات الكتلية الحديثة أن نسأل فيما إذا كان يمكن النظر إلى المشفر الكتلي الحديث على أنه زمرة رياضية **Group** ؟

يجب أن نفترض:

أولاً ً أن مفتاح التشفير طويل بشكل كافٍ لتحديد الخيار المناسب من بين الخيارات الممكنة التي تربط بين الدخل والخرج.

نسمي المشفر الذي يتمتع بهذه الصفة بالمشفر ذو المفتاح الكامل **Full-size key cipher** غالباً ما يكون المفتاح عملياً ًأصغر وبالتالي تصبح بعض الخيارات للمطابقة بين الدخل والخرج ممكنة فقط وليس كلها.

كما يجب ملاحظة أيضًا أنه على الرغم من أن المشفرات الكتلية تعتمد على وجود مفتاح سري مشترك بين طرفي تبادل المعلومات، إلا أنه يوجد داخل المشفر مكونات لا تعتمد على وجود مفتاح.

وتشمل:

1. المشفرات الكتلية بالمناقلة ذات المفتاح الكامل.
2. المشفرات الكتلية بالاستبدال ذات المفتاح الكامل.
3. زمرة التدوير المرتبطة بمشفرات المفتاح الكامل.
4. المشفرات ذات المفتاح الجزئي.
5. زمرة التدوير المرتبطة بمشفرات المفتاح الجزئي.
6. المشفرات عديمة المفتاح.

المشفرات الكتلية بالمناقلة ذات المفتاح الكامل Full-Size Key Transposition Block Ciphers

تقوم هذه المشفرات بتغيير موضع الخانات دون تغيير قيمتها. أي محاكاة عملها كما لو أنه اختيار لعنصر من n خانة من أحد جداول التدوير Permutation Tables التي يبلغ عددها **n!** جدول وذلك وفقًا للمفتاح الذي يحدد الجدول المناسب. نحتاج إذاً أن يتوفر لدينا **n!** مفتاح ممكن ويجب أن يضم كل مفتاح $\lceil \log_2 n! \rceil$ خانة

المشفرات الكتلية بالاستبدال ذات المفتاح الكامل Full-Size Key Substitution Block Ciphers

لا تقوم هذه المشفرات بتغيير موضع الخانات وإنما باستبدال قيمتها. قد يبدو للوهلة الأولى أنه لا يمكن محاكاة عملها كما لو أنه اختيار لعملية تدوير Permutation ممكنة. لكن ذلك ممكن إذا كان بالإمكان فك كود **Decoding** الدخل وتكويد الخرج **Encoding** .

- نعني بعملية فك الكود **Decoding:** تحويل الأعداد الصحيحة المؤلفة من n خانة إلى سلسلة طولها 2^n خانة مؤلفة من خانة واحدة ذات قيمة مساوية لـ **1** و 2^n -1 خانة مساوية لـ 0 . يعبر موضع الخانة **1** عن قيمة العدد الصحيح الذي يمكن أن يأخذ أحد القيم من **0** إلى 2^n -1.

- أماعمليةالتكويد **Encoding** فتعني العملية العكسية لما سبق. وعلى اعتبار أن الدخل والخرج الجديدين يتضمنان دائماً قيمة خانة **1** وحيدة، فإنه يمكن النظر إلى هذا النوع من المشفرات على $2^n!$ عنصر ممكن.

زمرة التدوير المرتبطة بمشفرات المفتاح الكامل Permutation Group for full-size key ciphers

على اعتبار أن المشفرات الكتلية الحديثة بالاستبدال أو المناقلة ذات المفتاح الكامل هي عمليات تدوير، فإنه إذا جرى التشفير (أو فك التشفير) أكثر من مرحلة فإن النتيجة تكون مكافئة إلى زمرة تدوير وفقاً لعملية التركيب **Composition Operation** .

أي يمكن الاستعاضة عن عمليتي تدوير متتاليتين أو أكثر بعملية تدوير واحدة. هذا يؤكد أنه من غير الضروري وجود أكثر من مرحلة تشفير بمفتاح كامل لأنها ستكون مكافئة لمرحلة واحدة بالنتيجة.

المشفرات ذات المفتاح الجزئي Partial-Size Key Ciphers

لا يمكن للمشفرات الفعلية أن تستخدم مفاتيح كاملة لأنها ستكون طويلة جدًا، خاصً ة إذا كانت هذه المشفرات هي مشفرات كتلية بالاستبدال. من بين المشفرات الكتلية بالاستبدال لدينا مثلاً المشفر **(DES)** الذي يعتمد على تشفير كتل من حجم 64 بت فقط

أي أننا نحتاج من أجل هذه الكتل إلى مفتاح كامل بطول $\log_2 (2^{64}!) \approx 2^{70}$ خانة.
لكن عملياً، يبلغ طول مفتاح هذا المشفر 56 بت فقط. يعني ذلك أنه لدينا فقط 2^{56} خيار من بين $\mathbf{2^{2^{70}}}$ خيار ممكن المطابقة معها.

زمرة التدوير المرتبطة بمشفرات المفتاح الجزئي Permutation Group for partial-size key ciphers

السؤال الذي يطرح نفسه الآن، هل تشكل مراحل المناقلة أو الاستبدال المتعددة باستخدام مفتاح جزئي زمرة تدوير وفقاً لعملية التركيب Composition Operation؟

الإجابة على هذا السؤال مهمة لأنها تعلمنا فيما إذا كانت المراحل المتعددة والمتتالية من المشفر يمكن أن تؤدي إلى تحقيق مستوى تشفير أعلى (كما سنلاحظ أثناء الحديث عن المشفر DES لاحقًا).

يمكن أن يشكل المشفر المزود بمفتاح جزئي زمرة **Group** إذا كان يشكل زمرة جزئية **Subgroup** من المشفر المزود بمفتاح كامل موافق له. على سبيل المثال:
جرى البرهان على أن عدة مراحل من المشفر DES المزود بمفتاح طوله 56 بت لا يشكل زمرة لأنه لا تشكل الخيارات الممكنة له (وهي 2^{56} خيار للمطابقة معها) زمرة جزئية من زمرة الخيارات الكلية (والتي يبلغ عدد عناصرها $2^{64}!$ خيار)

المشفرات عديمة المفتاح Keyless Ciphers:

على الرغم من أن المشفرات عديمة المفتاح ليست مفيدة بحد ذاتها إلا أنها مستخدمة ضمن مكونات المشفرات ذات المفاتيح:

- نسمي المشفرات عديمة المفتاح التي تعتمد على أسلوب المناقلة بـ "صناديق التدوير" **p–boxes** " والتي سنتحدث عنها فيما بعد. يمكن تخيلها كما لو أنها مكونات الصلبة للمناقلة المسبق تعريفها أو جدول التدوير للإمكانيات الممكن الإختيار من بينها لتحقيق المناقلة إذاجرى تحقيقها برمجيًا.

نسمي المشفرات عديمة المفتاح التي تعتمد على أسلوب الاستبدال ب "صناديق الاستبدال **"S–boxes"** والتي سنتحدث عنها فيما بعد. يمكن تخيلها كما لو أنها مكونات الصلبة للمطابقة المسبق تعريفها أو جدول أو تابع رياضي لحساب الإختيار المطلوب لتحقيق الاستبدال إذا جرى تحقيقها برمجيًا.

1. المشفرات الكتلية الحديثة Modern Block Ciphers

مكونات المشفر الكتلي الحديث Components of a Modern Block Cipher

المشفر الكتلي الحديث هو عادةً مشفر كتلي بالاستبدال مزود بمفتاح.

يسمح هذا المفتاح بمطابقة جزئية بين الإمكانات المتاحة للدخل مع الإمكانات المتاحة للخرج.

إضافة إلى أن هذا النوع من المشفرات ليس مصممًا على شكل وحدة واحدة، وإنما جرى بناؤه على شكل تجميع لوحدات للمناقلة (والتي نسميها صناديق التدوير **P-boxes**) ووحدات الاستبدال (والتي نسميها صناديق الاستبدال **S-boxes**) ، إضافة إلى وحدات أخرى.

وتشمل:

1. صناديق التدوير.
2. صناديق الاستبدال.
3. مشفرات الجداء.
4. صفوف مشفرات الجداء.

❖ صناديق التدوير P-Boxes

يهدف صندوق التدوير إلى تبديل موضع الخانات. يوجد ثلاثة أنواع منها: المباشرة **Straight** والموسعة **Expansion** ، **والمضغوطة Compression** :

صناديق التدوير المباشرة: وهي صناديق لها **n** مدخل و **n** مخرج لإمكانية تدوير ممكنة.

يوجد مع هذه الصناديق $n!$ إمكانية تدوير ممكنة.

صناديق التدويرالمضغوطة:وهي صناديق لها لها **n** مدخل و **m** مخرج لإمكانية تدوير ممكنة $(m < n)$. يجري هنا إيقاف بعض المداخل بحيث لا تصل إلى مخارج الصندوق. تستخدم هذه الصناديق لتنفيذ عملية تدوير واستبعاد عدد من الخانات من المرحلة التالية من التشفير.

صناديق التدوير الموسعة: وهي صناديق لها وهي صناديق لها لها **n** مدخل و **m** مخرج لإمكانية تدويرممكنة $(m>n)$. يجري هنا تكرار وصل بعض المداخل مع أكثر من مخرج. تستخدم هذه الصناديق لتنفيذ عملية تدوير وزيادة عدد الخانات كدخل للمرحلة التالية من التشفير.

قابلية العكس Invertibility: تعتبر صناديق التدوير المباشرة صناديق قابلة للعكس، أي تمكن استخدامها لتنفيذ أعمال التشفير وفك التشفير بعد عكس محتوى جداول التدوير. أما بالنسبة لصناديق التدوير المضغوطة والموسعة فلا يمكن عكسها. فيمكن مثً لا في صندوق التدوير المضغوط تجاهل أحد المداخل أثناء عملية التشفير ولكن لا يوجد أية طريقة للتعويض عنه أثناء عملية فك التشفير. كذلك الأمر مع صناديق التدوير الموسعة.

❖ صناديق الاستبدال S-Boxes

يمكن التفكير بها كما لو أنها مشفرات تبديل مصغرة. يمكن لهذه الصناديق أن يكون لها عدد مختلف من المداخل والمخارج. يمكن أيضًا أن تكون مزودة بمفتاح أو عديمة المفتاح، لكن تستخدم المشفرات الكتلية الحديثة صناديق الاستبدال عديمة المفتاح ذات المطابقة بين المداخل والمخارج المعرفة مسبقًا:

1. صناديق الاستبدال الخطية.
2. قابلية العكس.
3. التوابع الثنائية.

صناديق الاستبدال الخطية Linear S-boxes

بفرض أنه كان لدينا ضمن صندوق استبدال المداخل التالية : $x_o , x_1,\ldots, x_n$ والمخارج التالية: $y_o , y_1,\ldots, y_m$ وكان يمكن تمثيل العلاقة بين المداخل والمخارج على شكل مجموعة من المعادلات كما يلي:

$$y_1 = f_1(x_1, x_2, \ldots, x_n)$$
$$y_2 = f_2(x_1, x_2, \ldots, x_n)$$
$$\ldots$$
$$y_m = f_m(x_1, x_2, \ldots, x_n)$$

فيمكن عندها التعبير عن صندوق الاستبدال الخطي على الشكل التالي:

$$y_1 = a_{1,1}x_1 \oplus a_{1,2}x_2 \oplus \cdots \oplus a_{1,n}x_n$$

$$y_2 = a_{2,1}x_1 \oplus a_{2,2}x_2 \oplus \cdots \oplus a_{2,n}x_n$$

...

$$y_m = a_{m,1}x_1 \oplus a_{m,2}x_2 \oplus \cdots \oplus a_{m,n}x_n$$

أما بالنسبة لصناديق الاستبدال غير الخطية فلا يمكن ايجاد مثل هذه العلاقة.

قابلية العكس Invertibility:

يمكن لصناديق الاستبدال قابلة للعكس إذا كان عدد المداخل مساويًا لعدد المخارج.

التوابع الثنائية Binary Functions:

على اعتبار النص غير المشفر والمفتاح مؤلفين من قيم ثنائية فيمكن استخدام توابع ثنائية للتشفيروفك التشفير.

مثال1:

استخدام التابع **AND**

- **Plaintext:** 1001101110101100
- **Key:** 1101100011001010
- **Ciphertext:** 1001100010001000

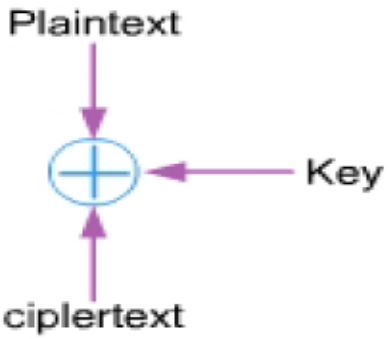
تكمن المشكلة في التعامل مع بعض التوابع الثنائية في كونها غير قابلة للعكس. التابعAND غير قابل للعكس فلا يمكن باستخدامه استنتاج النص غير المشفر في حال معرفة المفتاح والنص المشفر، كما هو مبين في المثال التالي:

- **Plaintext:** يمكن أن تكون 0 أو 1 ← ?
- **Key:** 0
- **Ciphertext:** 0

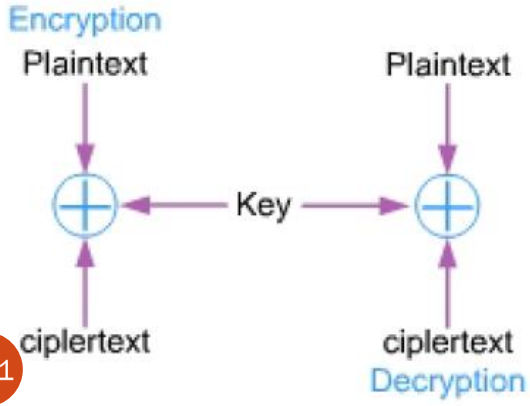
مثال 2

استخدام التابع **XOR (Exclusive OR)** الذي يمكن تعريفه واستخدامه للتشفير كما هو مبين في الشكل التالي:

P	K	C = P ⊕ K
1	1	0
1	0	1
0	1	1
0	0	0



يتمتع هذا التابع بإمكانية عكس ذاته، أي أن: $C = P \oplus K \rightarrow P = C \oplus K$

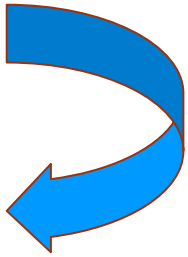


C = P ⊕ K	K	P must be:
1	1	0
1	0	1
0	1	1
0	0	0

تستخدم المشفرات الكتلية الحديثة التابع XOR للتشفير كما هو مبين في المثال التالي الذي يتعامل مع كتل مكونة من 8 خانات.

Encryption:

Plaintext:	10010101	00100110	01110101
Key:	10100110	10100110	10100110
Ciphertext:	00110011	10000000	01010011



Decryption:

Ciphertext:	00110011	10000000	01010011
Key:	10100110	10100110	10100110
Plaintext:	10010101	00100110	01110101

ملاحظة هامة: إذا جرى استخدام التابع XOR لوحده فإن عملية كسر التشفير تكون سهلة جداً ويمكن إيجاد المفتاح بواسطة أول نص غير مشفر معلوم وفقًا للمعادلة التالية :

$$K = P \oplus C$$

لذلك يجب اللجوء إلى إضافة أساليب تمويه أخرى والتي نذكر منها الأسلوبين:

البث (الانتشار) **Diffusion** والخلط **Confusion**

مشفرات الجداء Product Ciphers

وهي مشفرات معقدة مكونة من عدة مكونات للاستبدال والتدوير وغير ذلك من المكونات الأخرى. تعتمد هذه المكونات على أسلوبين للتمويه، هما:

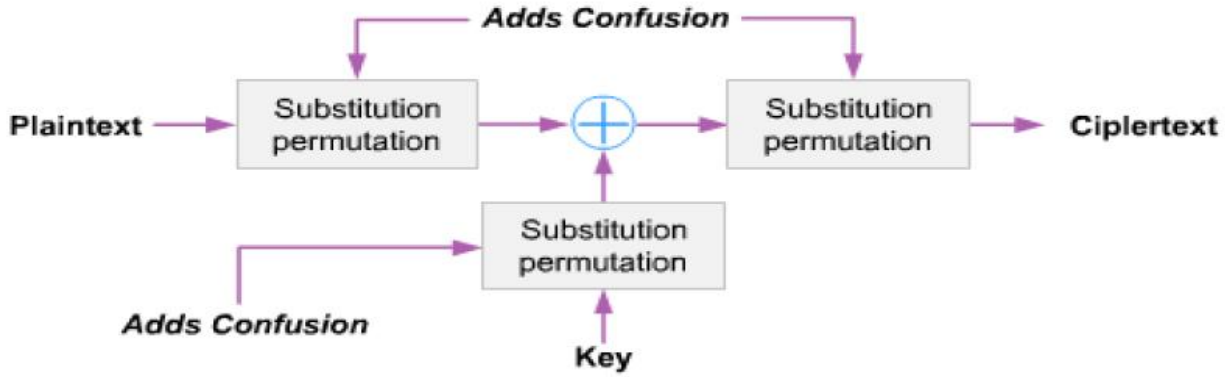
الانتشار **Diffusion** والخلط **Confusion**

نعرض فيما تعريفًا لهذين الأسلوبين ونوضح بالشكل مكونات مشفرات الجداء:

الانتشار **Diffusion**: تفيد هذه العملية في إخفاء العلاقة بين النص غير المشفر والنص المشفر حيث يمكن أن يؤدي تغيير خانة واحدة (بت) ضمن النص غير المشفر إلى تغيير عدة خانات ضمن النص المشفر.

الخلط **Confusion**: تفيد هذه العملية في إخفاء العلاقة بين النص المشفر ومفتاح التشفير حيث يمكن أن يؤدي تغيير خانة واحدة (بت) ضمن مفتاح التشفير إلى تغيير عدة حروف ضمن النص المشفر.

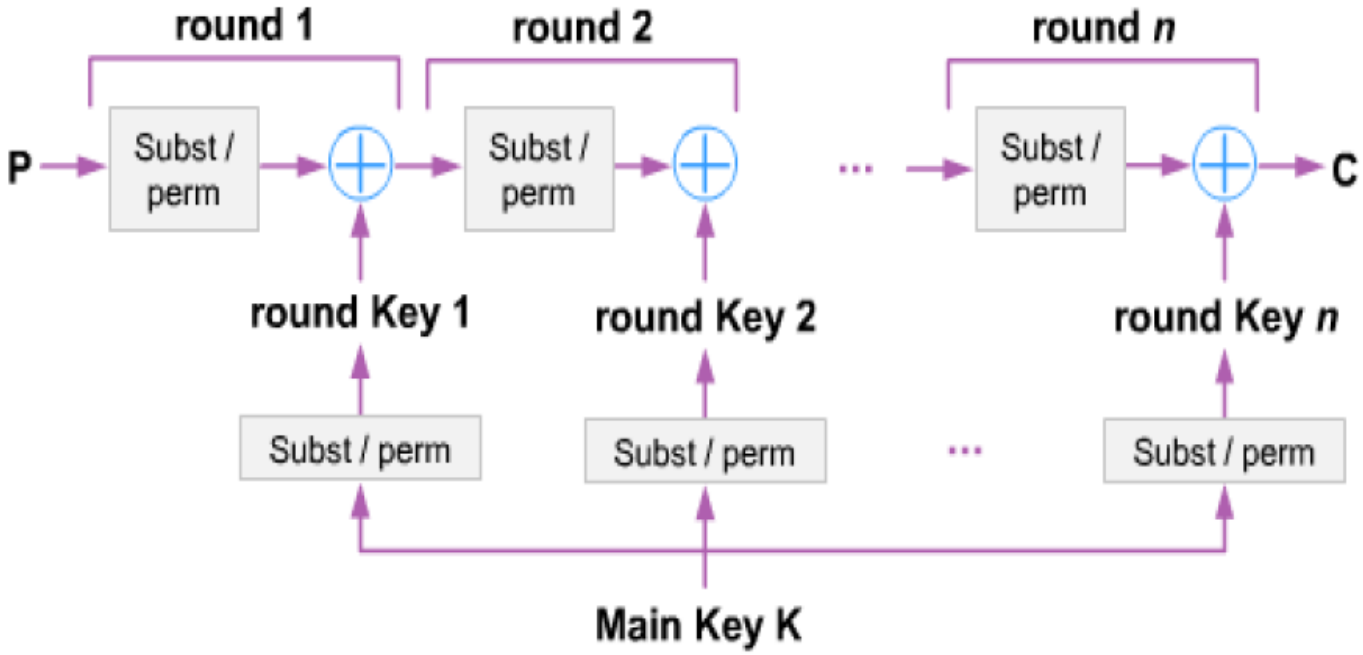
❖ يبين الشكل أماكن استخدام أسلوبي الانتشار والخلط.



الجولاتRounds:

يمكن أن تتكرر مشفرات الجداء المكونة من مكونات صناديق التدوير وصناديق الاستبدال المزودة بإمكانيات الانتشار والخلط أكثر من مرة وراء بعضهاالبعض. نسمي كل تكرار بالجولةROUND ويستخدم المشفر الكتلي عندها مجدول للمفاتيح **Key schedule** أو مولد لها **Key generator** لإنشاء مفاتيح مختلفة لكل جولة. يجري ضمن مشفر مؤلف من N جولة تشفر النص غير المشفر N مرة قبل توليد النص المشفر النهائي. نسمي النص المولد بين الجولات بالنص الوسيط **Middle text**

يوضح الشكل التالي بنية مشفر جداء مؤلف من عدة جولات.



صفوف مشفرات الجداء Classes of Product Ciphers

كافة المشفرات الكتلية الحديثة هي مشفرات جداء. ولكن يمكن تصنيف هذه المشفرات عموماً ضمن صفين:

- تتميز مشفرات الصف الأول باستخدام ضمن بنيتها مكونات قابلة للعكس وأخرى غير قابلة للعكس وتسمى بالمشفرات **Feistel Ciphers** وتعتبر المشفر DES أحد هذه المشفرات المعروفة والمستخدمة بكثرة.
- أما مشفرات الصف الثاني وتسمي بالمشفرات **Non-Feistel Ciphers** فهي تعتمد على استخدام مكونات قابلة للعكس فقط ضمن بنيتها ويعتبر المشفر AES مثالاً حقيقيًا لهذا الصف من المشفرات.

2. مشفرات دفق المعلومات الحديثة Modern Stream Ciphers

يجري التشفير مع هذه المشفرات على مستوى الخانات (بتات) وفقاً لما يلي:

$$P = P_1P_2P_3\cdots$$
$$C = C_1C_2C_3\cdots$$
$$K = (k_1, k_2, k_3, \cdots)$$
$$C_1 = E_{k1}(P_1)$$
$$C_2 = E_{k2}(P_2)$$
$$C_3 = E_{k3}(P_3)\cdots$$

يتوفر لدينا نوعين من مشفرات دفق المعلومات الحديثة، هما:

المشفرات المتزامنة Synchronous Stream Ciphers

وفيها يكون دفق معلومات المفتاح مستقلً لا عن دفق معلومات النص غير المشفر أو المشفر. يجري توليد دفق معلومات المفتاح واستخدامه دون وجود أية علاقة بين خاناته وخانات النص غير المشفر أو المشفر.

المشفرات غير المتزامنة Nonsynchronous Stream Ciphers: وفيها يكون دفق معلومات المفتاح مرتبطًا بالنص غير المشفر أو المشفر.