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:

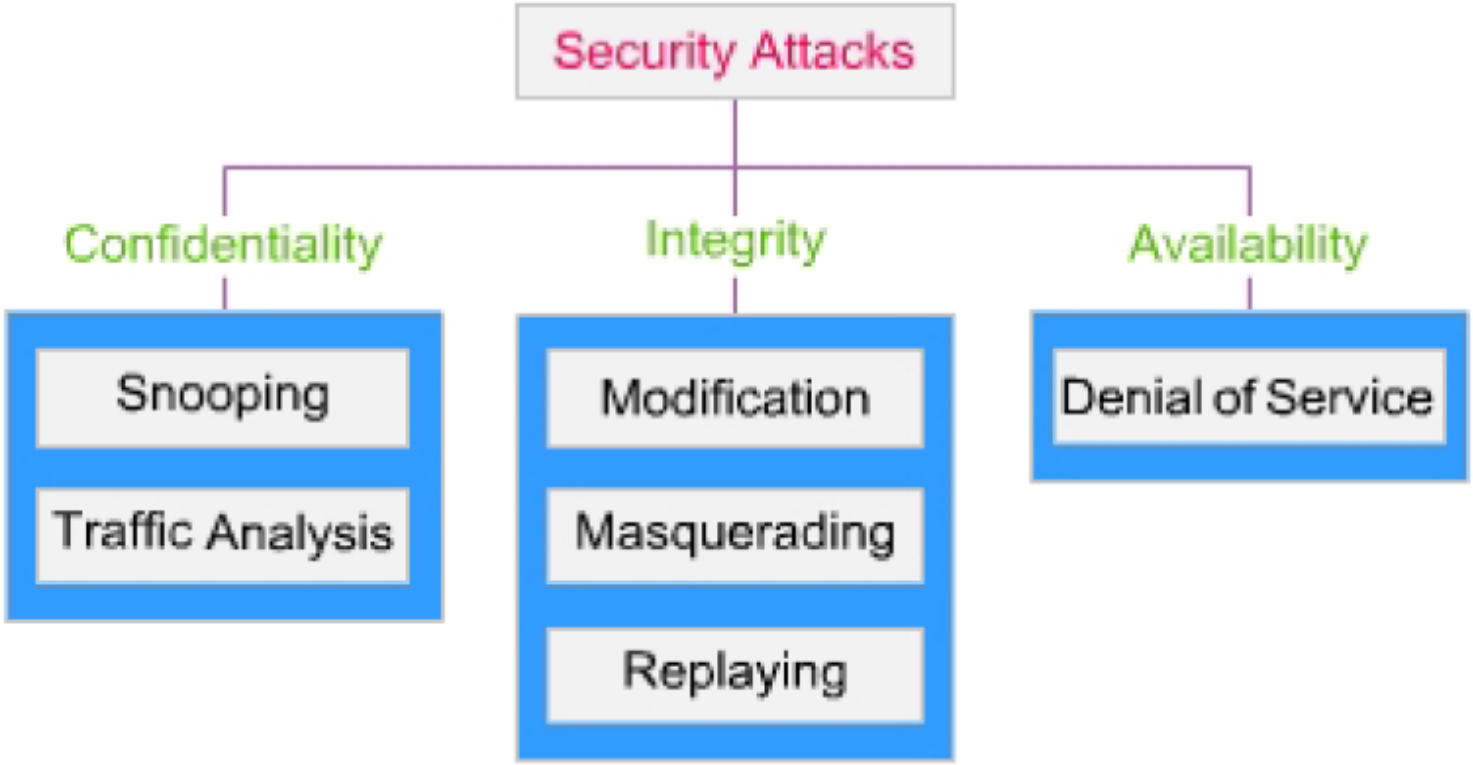
تعديلها يجب أن يتم حصرا من قبل الأشخاص المصرح لهم بذلك. يجب ملاحظة أن تعديل المعلومات لا يمكن أن يحدث بنتيجة فعل غير قانوني فقط، وإنما يمكن أن يؤدي انقطاع التيار الكهربائي في بعض الحالات إلى تعديل بعض المعلومات.

- **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) الخدمةDenial 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 |
|---|---|---|
| التصيدSnooping<br>المعطيات المتبادلة Traffic analysis | غير فعال | السرية Confidentiality |
| التغيير Modification<br>انتحال الصفة Masquerading<br>الإعادة Replaying<br>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.

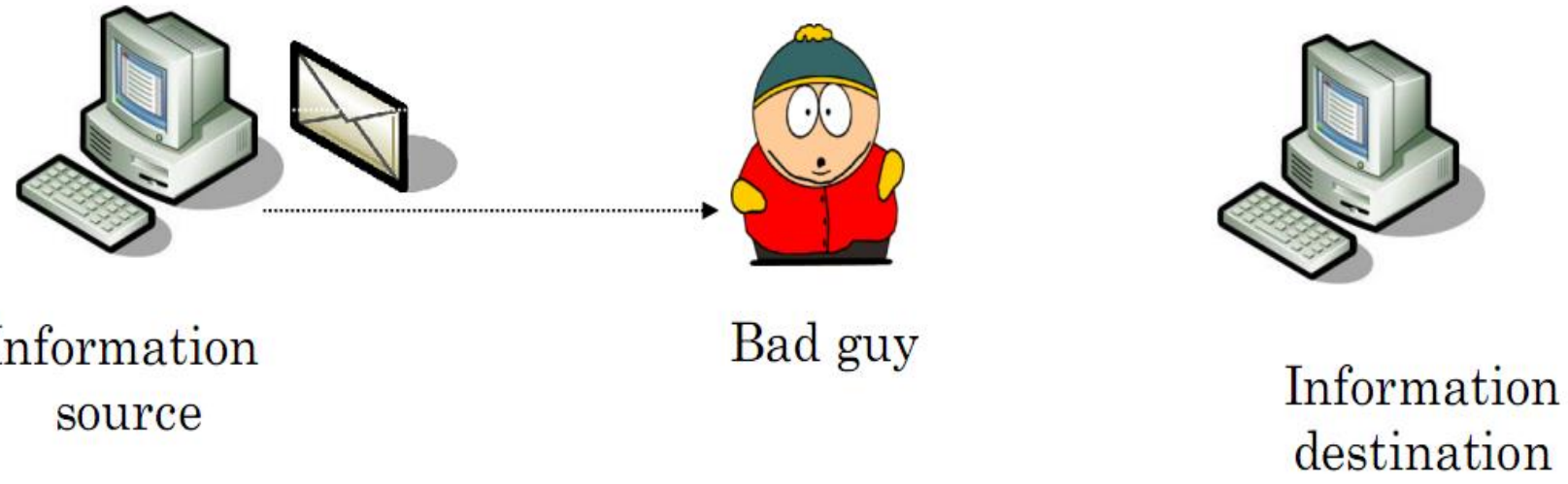
3- **هجوم التعديل Modification of Messages**: تغيير جزء من رسالة ما أو تغيير ترتيبها ومعناها.

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

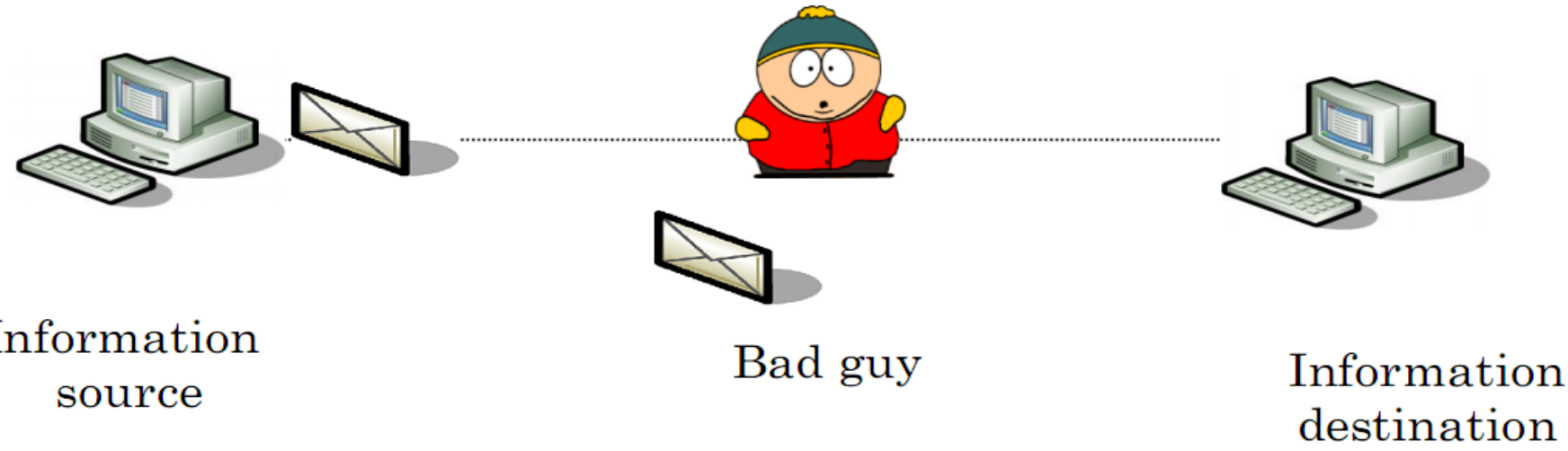
1. Interruption(المقاطعة)
2. Interception(الاعتراض)
3. Modification(التعديل)
4. Fabrication(التلفيق)

# 1. Interruption(المقاطعة)



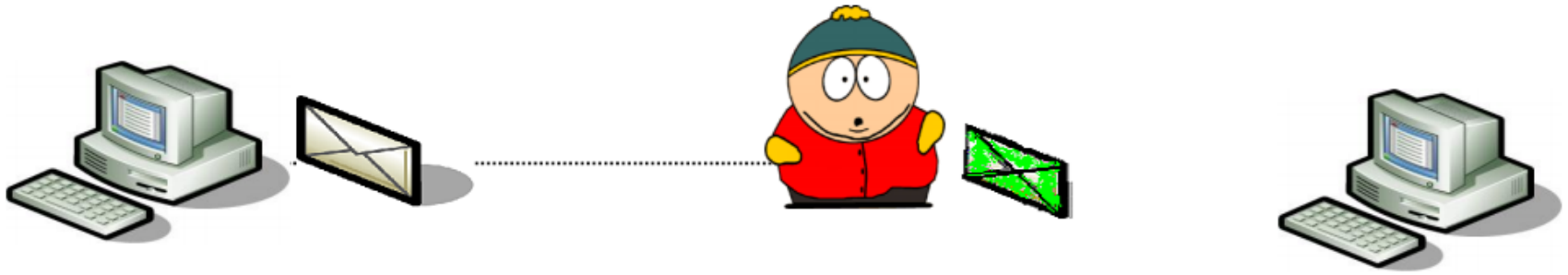

- The system becomes unavailable or unusable.
- Attack on the Availability.
- النظام يُصبحُ غير متوفرَ أَو غير صالح للإستعمالَ.
- الهجوم على التوفرِ.

# 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)




- 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 ( X. 800) ITU-T 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

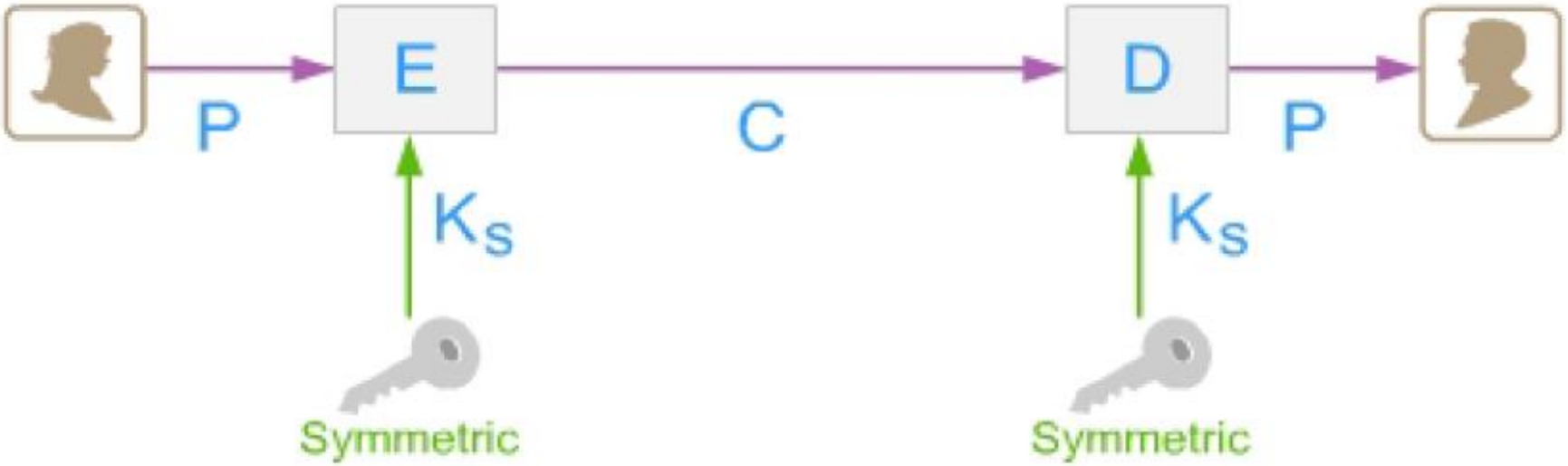
كتابة الأسرار أو الكتابة السرية **Secret writing**

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

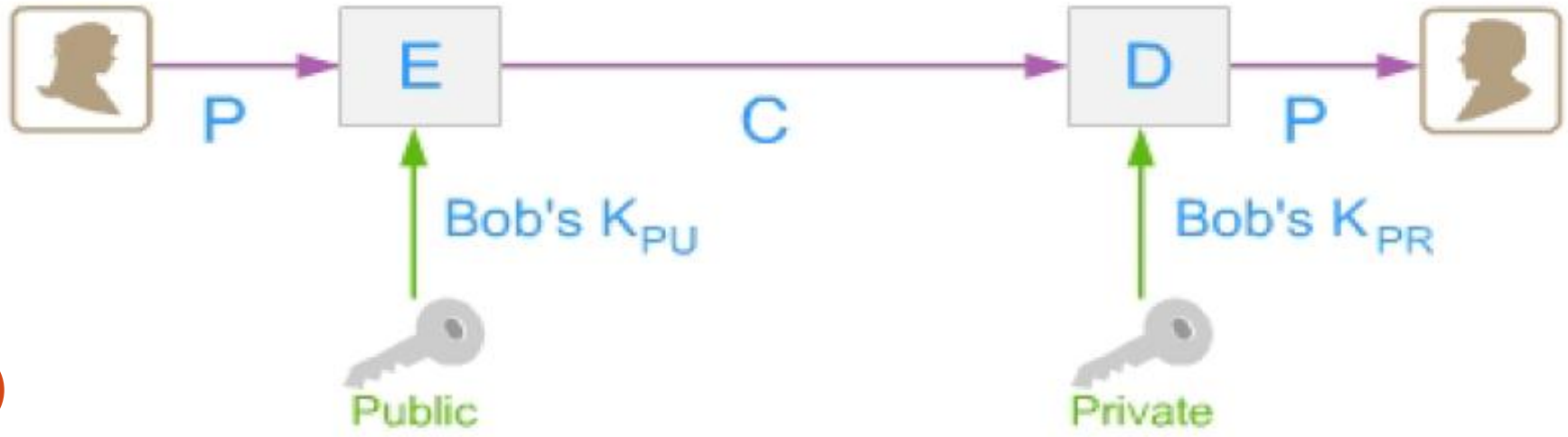
يجري التشفير وفقًا لهذه التقنية باستخدام مفتاح سري **Secret-key** مشترك من قبل الطرفين المتصلين كما هو مبين في الشكل التالي:



## التشفير بمفاتيح غير متناظرة Asymmetric-key encipherment

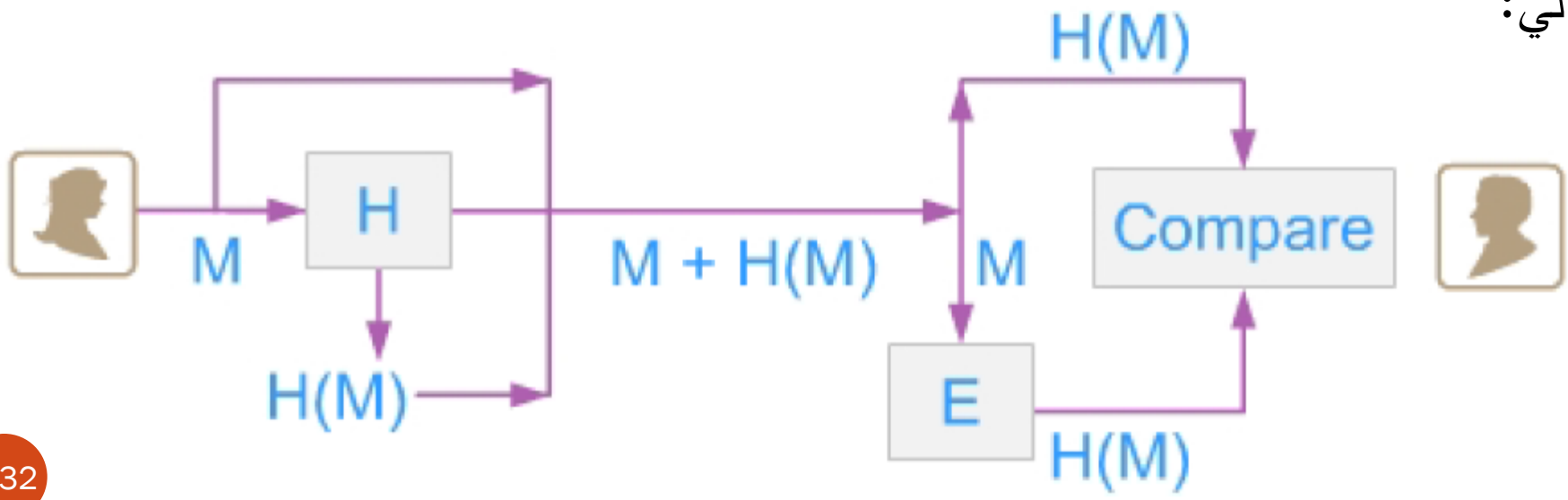
يجري التشفير وفقًا لهذه التقنية باستخدام مفتاحين أحدهما معلن وهو المفتاح العام **Public Key** والآخر سري وهو **Private key**

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:



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:



## 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.