جامعة حماة

الكلية التطبيقية

قسم تقنيات الحاسوب

- المقرر: أمن المعلومات
- المحاضرة : الثانية

Dr. Mohammed AL-Mohammed

Chapter 2

التعمية وأمن المعلومات

مبادئ وتطبيقات

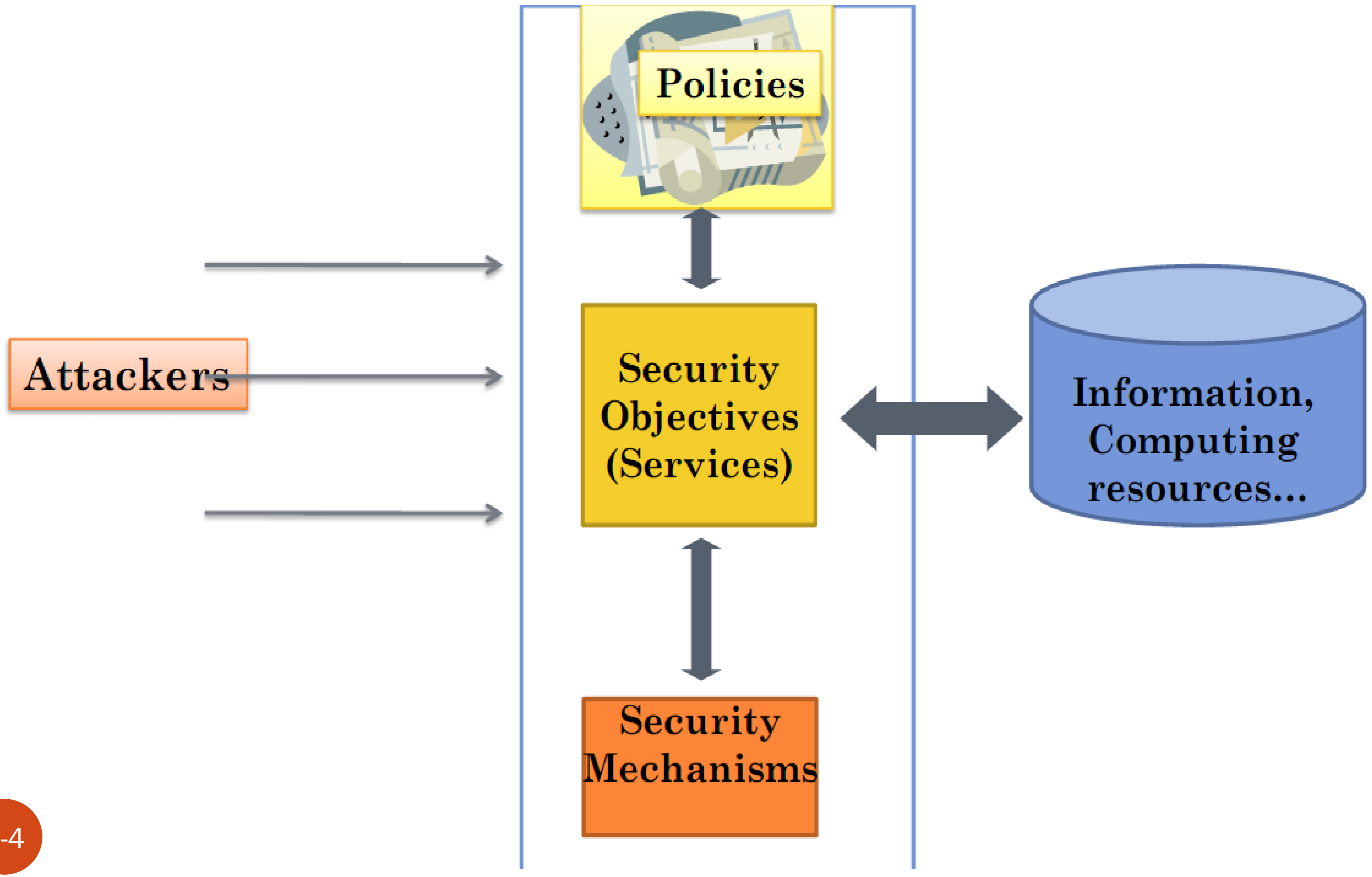
Introduction to Information Security

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 :

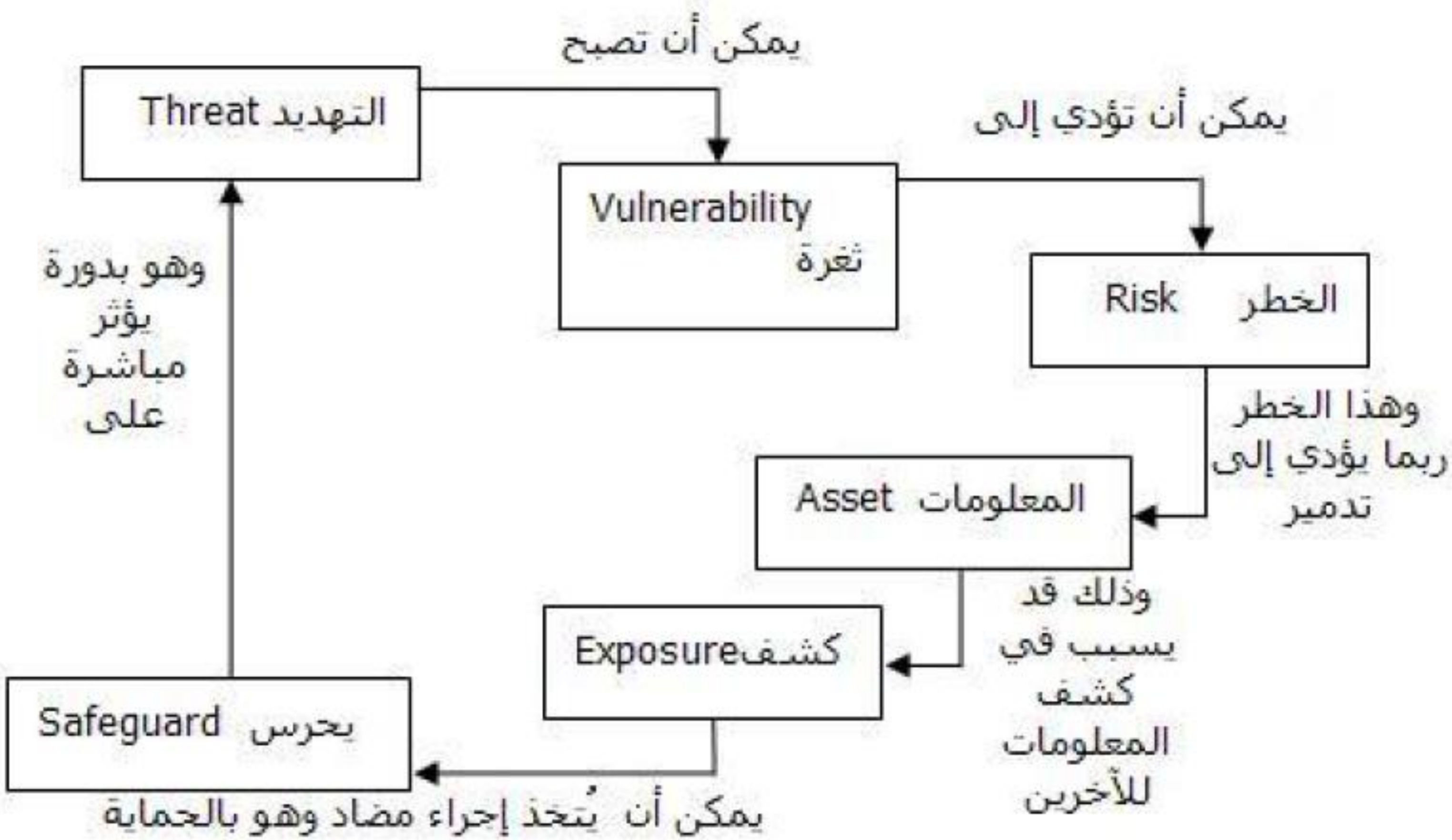
- التهديد Threat: وهو عملية المحاوله الى الوصول إلى المعلومات السرية الخاصة بالمنظمة.
- الثغرات Vulnerabilities وهي أنه يوجد ضعف في المنظمة يستطيع المهاجم Attacker الدخول من خلالها

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 :



أولاَ: 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. الهدف Target : 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 الأحداث Events 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 و هما:

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

  التحصين التقني: استخدام الأجهزه للحمايه مثل أجهزة التشفير.

- تحصين غير تقني Administrative Vulnerability:و هو 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 للتهديد Threats 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 الخطر Risk Analysis

ثانيا: اتخاذ قرار بشأن هذا الخطر Decision Management

ثالثا: تطبق ذلك القرار Implementation

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.

CRYPTOGRAPHY علم التعمية

CRYPTOLOGY

مصطلح إغريقي:الكتابة السرية=إخفاء الكلمات
kryptos = إخفاء,
logos = كلمات

- CRYPTOGRAPHY

تشفير=encryption
(فك تشفير)إظهار=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 أنواعِ 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 معلوماتِ 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 التعمية

Encyption

عملية الإظهار

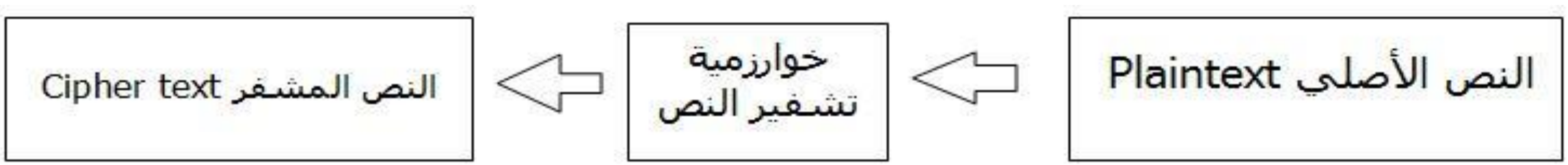
Decryption

مفاتيح التعمية والإظهار

.(Cryptographic Keys)

علم التعمية Cryptography

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



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

Cryptography علم التعمية

<u>**Cryptography:**</u> Many schemes used for encryption.
<u>**Encryption:**</u> Process of converting from plaintext to ciphertext
<u>**Decryption**</u>: Process of restoring plaintext from ciphertext.
<u>**Cryptanalysis:**</u> 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:

$$e_k : p \to c$$

$$d_k : c \to p$$

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

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

علم التعمية Cryptography

يصدر المبلغ رسالة على شكل نص صريح هو $X=\{x_1,x_2,....x_m\}$ إن العناصر Mمن 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 $K=\{k_1,k_2,k_3.........k_j\}$.

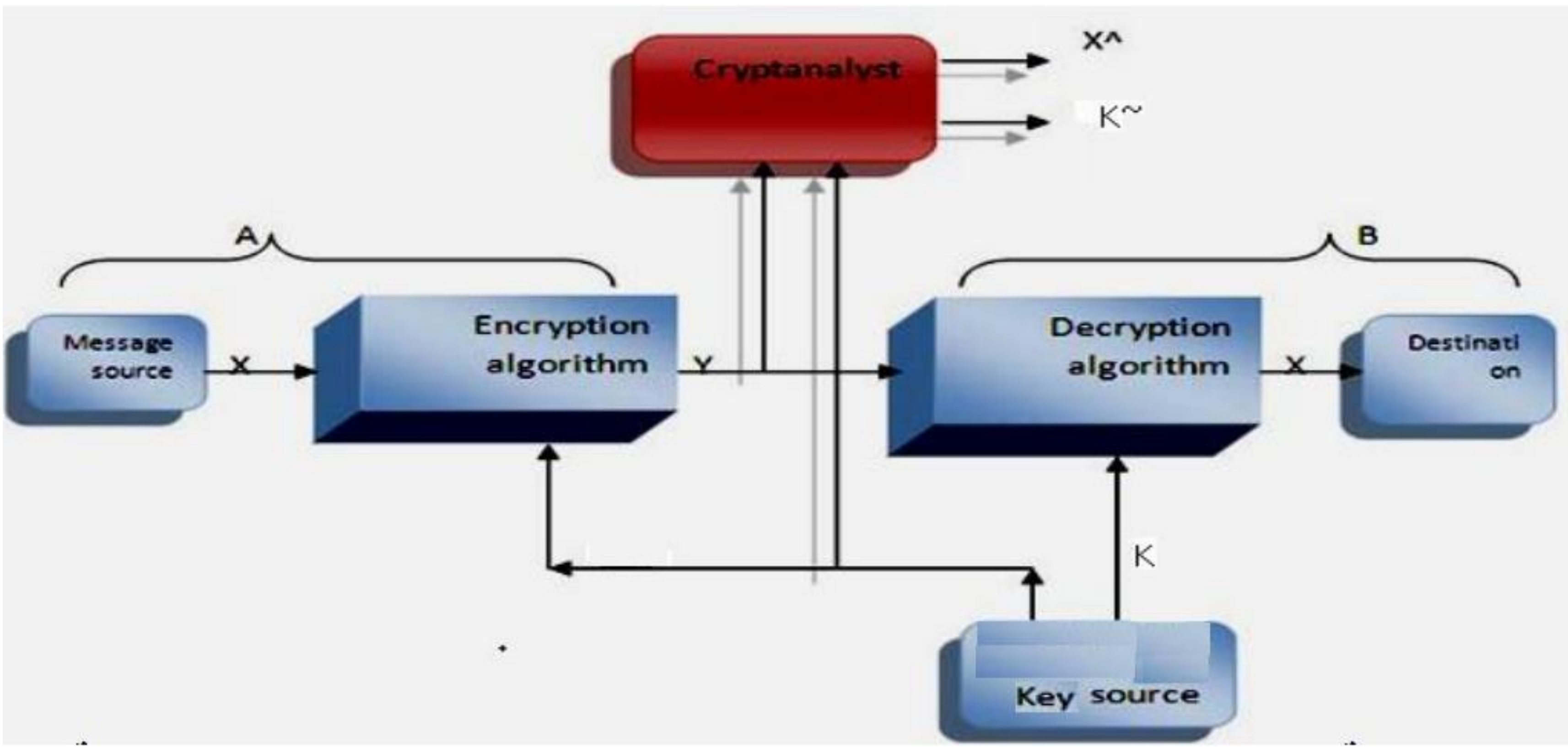
إذا ولد المفتاح عند مصدر الرسالة يجب نقله إلى وجهة الهدف عبر قناة آمنة للطرف الآخر.

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

Cryptography علم التعمية



علم التعمية Cryptography

أثناء سير النص للوصول إلى الوجهة سيحاول المعتدي الحصول على Y
ولكن لا يمكنه الوصول إلى X وK
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~.