المحاضرة الأولى:

علم التشفير Cryptography

Is the science of designing cipher system by mathematical to encrypt and decrypt data.

أو هو العلم الذي يتناول سرية المعلومات وأمنية البيانات ويمثل علم بناء نظم التشفير.

Terms of Cryptography:

1- Encryption [or Encoding; Enciphering]: التشفير

Is the process of encoding a data or a message so that the meaning of the data or the message is unobvious (غامض).

إذاً هو عملية تحويل بيانات أو رسالة معينة مفهومة إلى بيانات أو رسالة غامضة

2- Decryption [Decoding or Deciphering]: فك التشفير

Is the reverse (عكس)of encryption, transforming an encrypted message back into its normal form.

اذا يمثل عكس عملية التشفير ويعني إعادة البيانات أو الرسالة الغامضة وغير المفهومة إلى شكلها الطبيعي قبل التشفير.

Cryptosystem: نظام التشفير

Is a system for encryption and decryption.

هو النظام الذي يشمل التشفير وفك الشفرة.

Cryptograph: **النص المشفر**

Means hidden writing the practice of using encryption to conceal a text. In another meaning, is the study of secret (cryptography) writing.

إذاً هو علم دراسة الكتابة السرية.

Cryptoanalysis: علم كسر الشفرات

Is a science of analyzing and breaking secure data or communication.

Terms in encryption:

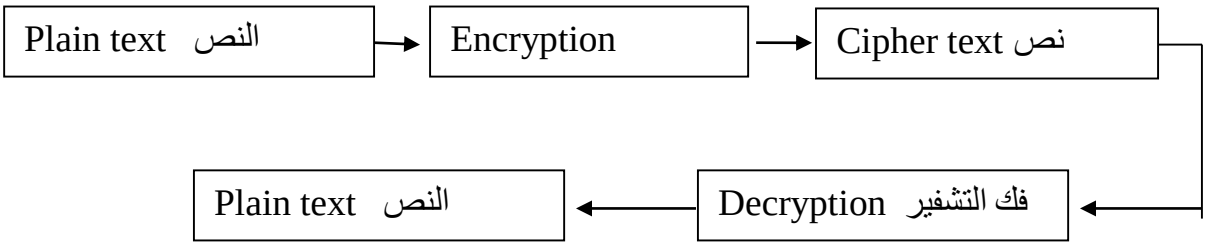
Cryptanalyst: محلل او كاسر للشفرة

Sender: المرسل

Receiver: المستقبل

Plain text: النص الصريح (المفهوم)

How Does Cryptography Work?



شكل رقم (1): يمثل مخطط لعملية التشفير

Diagram Represent [Encryption Process]

Plain Text: The Original form of data represented as:

$$P = \{p_1, p_2, ..., p_n\}.$$

Cipher Text: Encrypted form of data represented as:

$$C = \{c_1, c_2, ..., c_n\}$$

The **mathematical model** for the encryption is:

$$C = E(p) \quad \text{and} \quad P = D(C)$$

Where:

E: represent encryption algorithm (set of transformation operation).

D: represent decryption algorithm.

Then:

Crypto system $P = D(E(p))$.

Some encryption algorithm use a key $C = E(k, p)$ and sometimes the encryption and decryption keys are the same so that:

$P = D(k, E(k, p))$,

Other times the keys come in pairs.

خطوات التشفير:

1- Encryption التشفير: يمثل عملية تحويل بيانات نصية مفهومة الى نص مشفر(Cipher text) باستخدام مفتاح.

2- Decryption فك التشفير: يمثل عملية فك الشفرة إذ تقوم بتحويل النص المشفر الى النص الأصلي (Plain text) باستخدام مفتاح

3- Key المفتاح: عبارة عن رموز متكونة من رقم أو مجموعة أرقام أو حروف وقد يكون جملة Phrase أو Code (0,1).

4- Key Space فضاء المفتاح: يمثل مجموعة كل المفاتيح والتي نختار منها مفتاح معين.

5- Message Space فضاء الرسالة: مجموعة كل الرسائل المراد تشفيرها.

6- Cipher text Space فضاء النص المشفر: يحول النصوص الداخلة للتشفير والتي تكون واضحة ومفهومة الى كلمات غير مفهومة.