INTRODUCTION

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission.
- **Internet Security**- measures to protect data during their transmission over a collection of interconnected networks.

Basic Concepts

Cryptography: The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

Plaintext: The original intelligible message.

Cipher text: The transformed message.

Cipher: An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods.

Key: Some critical information used by the cipher, known only to the sender& receiver.

Encryption (Encipher or encode): The process of converting plaintext to cipher text using a cipher and a key.

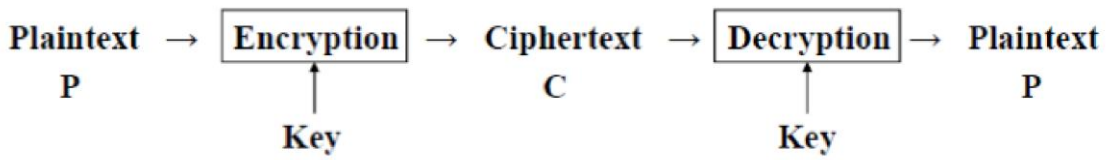
Decryption (Decipher or decode): The process of retrieving the plaintext from the ciphertext using a cipher and a key.

Cryptanalysis (code breaking): The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the proper key.

Cryptology: Both cryptography and cryptanalysis.

Cryptographer: is person who does cryptography.

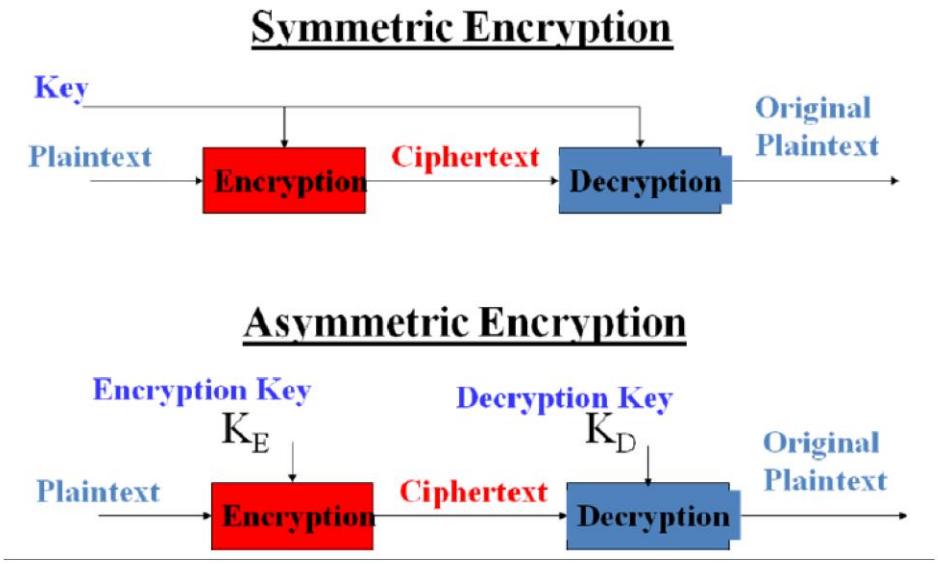
Cryptanalyst: is a person practitioner of cryptanalysis.



Cryptography

Cryptographic systems are generally classified along 3 independent dimensions:

- Type of operations used for transforming plain text to cipher text
  All the encryption algorithms are based on two general principles:
  - ✓ **Substitution**, in which each element in the plaintext is mapped into another element.
  - ✓ **Transposition**, in which elements in the plaintext are rearranged.
- The number of keys used
  - ✓ If the sender and receiver uses same key then it is said to be symmetric key (or secret-key or single key or conventional encryption).
  - ✓ If the sender and receiver use different keys then it is said to be asymmetric (or public key) encryption.



- The way in which the plain text is processed
  - ✓ A block cipher processes the input as block of elements at a time, producing output block for each input block.
  - ✓ A stream cipher processes the input elements continuously, producing output element one at a time, as it goes along.