CLASSICAL ENCRYPTION TECHNIQUES

INTRODUCTION

- **Plaintext**: original message
- **Cipher text**: coded message
- **Enciphering** or **encryption**: the process of converting from plaintext to cipher text
- **Deciphering** or **decryption:** the process of restoring the plaintext from the cipher text

The many schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cipher**. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls **"breaking the code".** The areas of cryptography and cryptanalysis together are called **cryptology**.

SYMMETRIC CIPHER MODEL

A symmetric encryption scheme has **five ingredients**

Plain text

This is the original intelligible message or data that is fed into the algorithm as input.

Encryption Algorithm

The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key

The secret key is also input to the encryption algorithm. The algorithm will produce a different output depending on the specific key begin used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

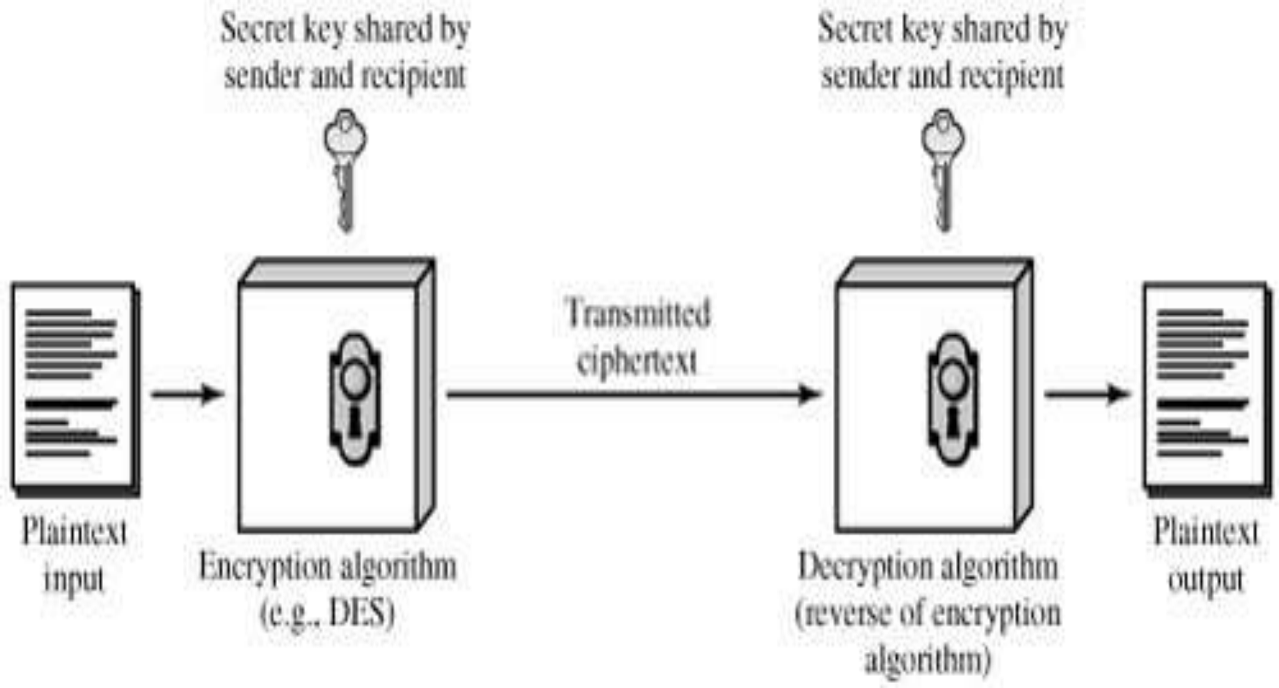
Cipher text

This is the scrambled message produced as output. It depends on the plaintext and Secret key. Two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data.

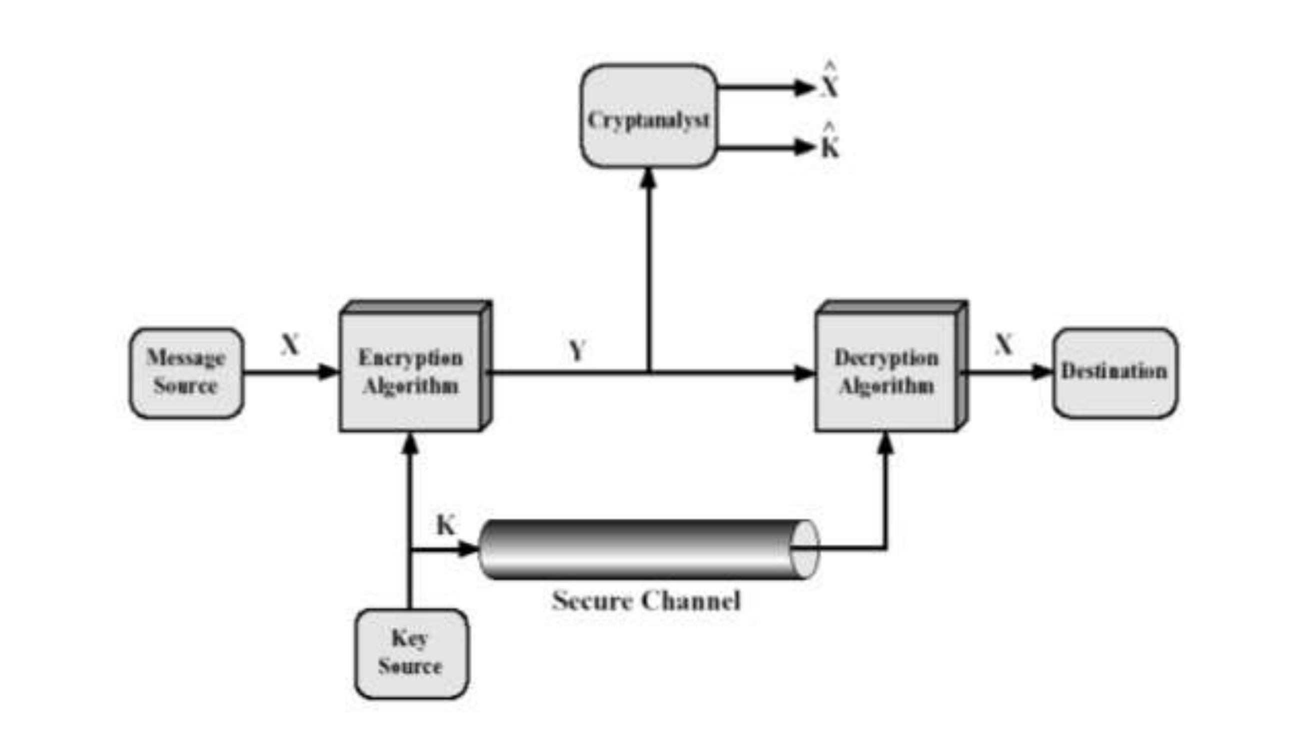
Decryption Algorithm

This is essentially the encryption algorithm run is reverse. It takes the cipher text and the secret key and produces the original plain text.

SIMPLIFIED MODEL OF CONVENTIONAL MODEL


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

MODEL OF CONVENTIONAL CRYPTOSYSTEM



Symmetric cipher model has two types. There are:

- Cryptography
- Cryptanalysis

CRYPTOGRAPHY

Cryptographic system are characterized along three independent dimensions:

The type of operations used for transforming plaintext to cipher text

All encryption algorithms based on **two principles**: substitution , in which each element in the plaintext (bit , letter , group of bits or letters) is mapped into another element and transposition , in which elements in the plain text are rearranged. Most systems , referred to as product systems multiple stages of substitutions and transpositions.

The number of keys used

If both sender and receiver use the same key , the system is referred to as symmetric , single-key , secret-key or conventional encryption. If the sender and receiver use different keys , the system is referred to as asymmetric , two-key or public-key encryption.

The way in which the plaintext is processed

A block cipher processes the input one block of elements at a time , producing an output block for each input block. A stream cipher processes the input elements continuously , producing output one element at a time.

CRYPTANALYSIS

There are two general approaches to attacking a conventional encryption scheme:

Cryptanalysis

Cryptanalysis attack rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-cipher text pairs.

Brute-force attack

The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained. All possible keys must be tried to achieve success.