CLASSICAL ENCRYPTION TECHNIQUES

Symmetric encryption : is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption or single-key encryption.

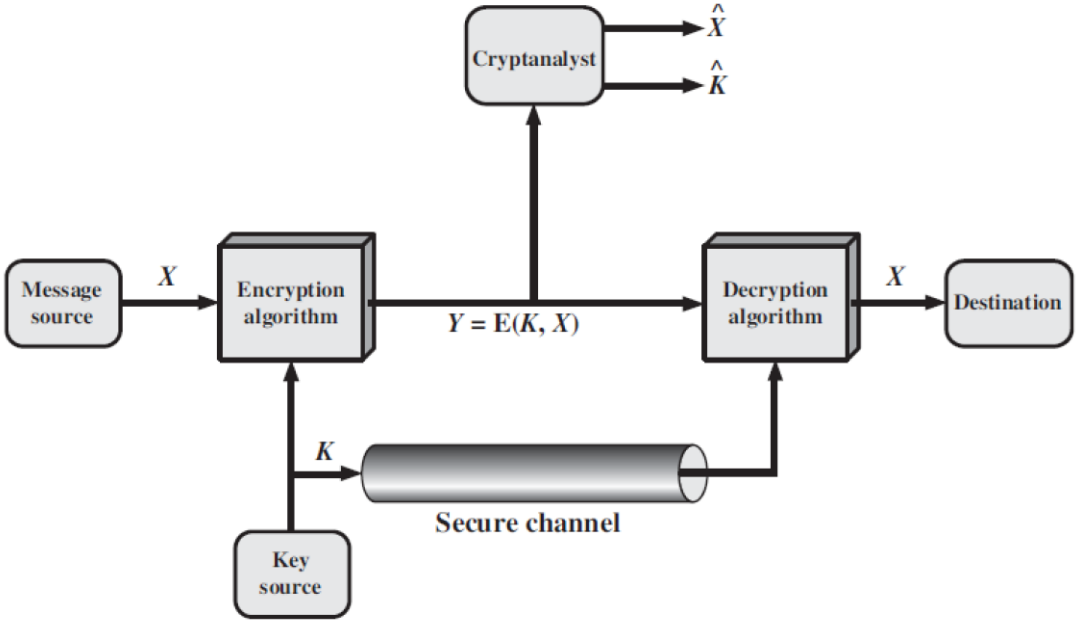

Figure 2.2 Model of Symmetric Cryptosystem

There are two requirements for secure use of conventional encryption (symmetric encryption):

• A strong encryption algorithm

• A secret key known only to sender / receiver

Mathematically:

C = EK(X) or C = E (K, X)

X = DK(C) or X = D (K, C)

X = plaintext, C = ciphertext, K = secret key, E = encryption algorithm, D = decryption

algorithm

Cryptanalysis

- Objective: to recover the plaintext of a ciphertext or, more typically, to recover the secret key.

- Kerkhoff's principle: the adversary knows all details about a cryptosystem except the secret key.
- Two general approaches:

  – brute-force attack

  – non-brute-force attack (cryptanalytic attack)

Brute-Force Attack

– Try every key to decipher the ciphertext.

– On average, need to try half of all possible keys

– Time needed proportional to size of key space

Key Size (bits)	**Number of Alternative Keys**	**Time required at 1 decryption/μs**	**Time required at 10^6 decryptions/μs**
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Non-brute-force attack (Cryptanalytic Attacks)

•summarizes the various types of cryptanalytic attacks based on the amount of information

known to the cryptanalyst.

1. ciphertext only : only know algorithm / ciphertext, statistical, can identify plaintext
2. known plaintext : know/suspect plaintext & ciphertext to attack cipher
3. chosen plaintext : select plaintext and obtain ciphertext to attack cipher

4. chosen ciphertext : select ciphertext and obtain plaintext to attack cipher
5. chosen text : select either plaintext or ciphertext to en/decrypt to attack cipher

Classical Ciphers

• Plaintext is viewed as a sequence of elements (e.g., bits or characters)

• There are three basic building blocks of all encryption techniques:

1. Substitution cipher: replacing each element of the plaintext with another element.

(Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Polyalphabetic Ciphers, Vegenere table, One-Time Pad)

2. Transposition (or permutation) cipher: rearranging the order of the elements of the plaintext. (Rail fence cipher, Row Transposition Ciphers)
3. Product cipher: using multiple stages of substitutions and transpositions.