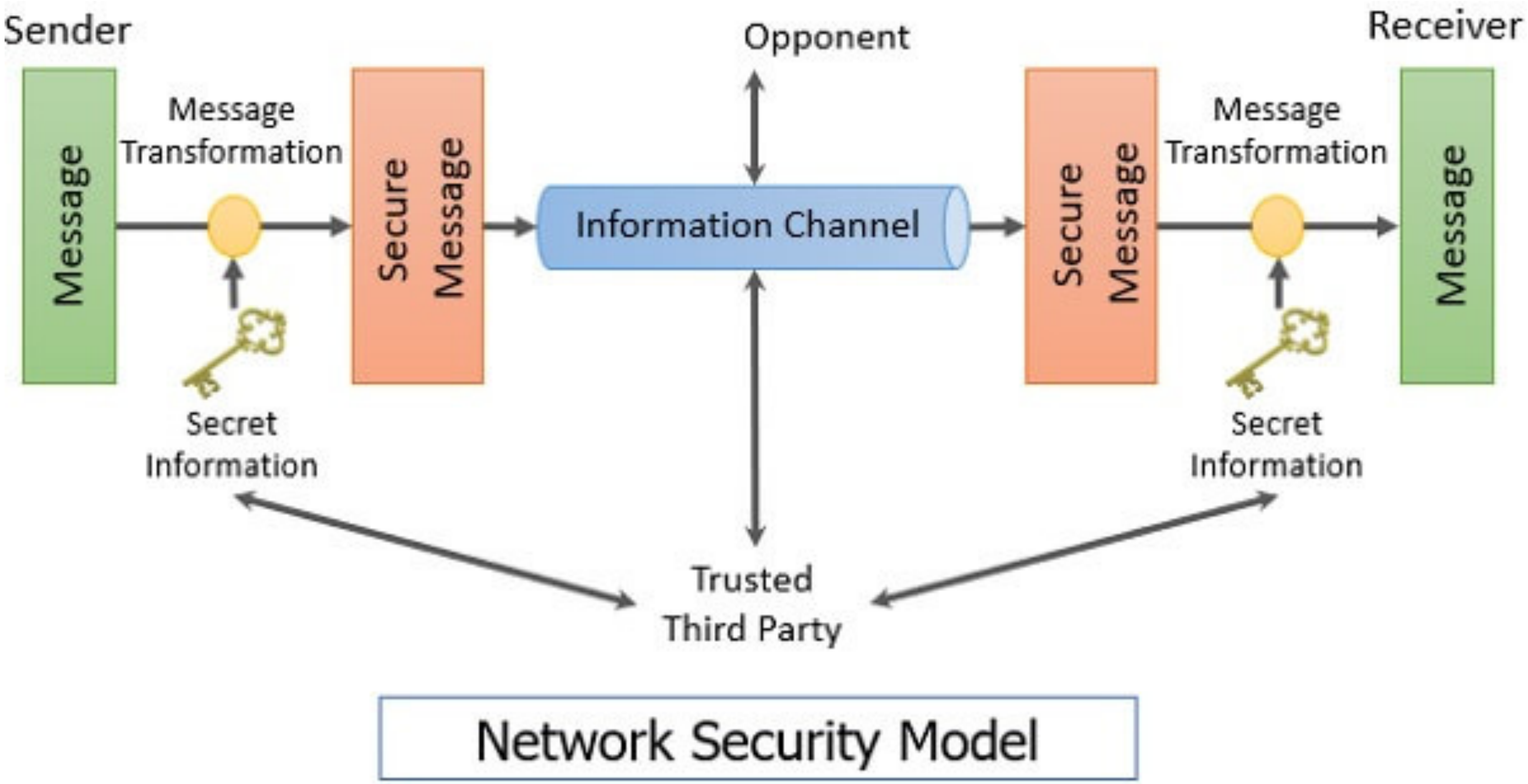
# Basic Concepts

- ***Plaintext*** The original intelligible message
- **Ciphertext** - the coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering ciphertext from plaintext

# Network Security model



# Symmetric Cipher Model

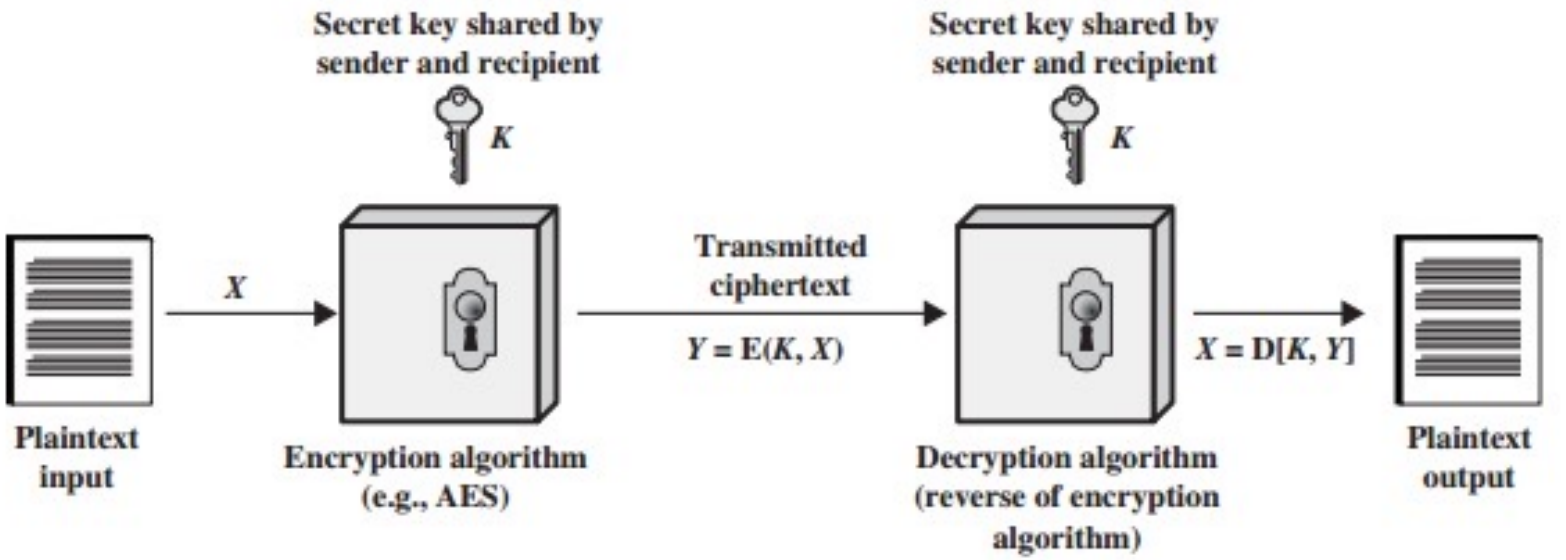

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2.1 Simplified Model of Symmetric Encryption

# Cryptography

Cryptographic systems are characterized along three independent dimensions:

**1. The type of operations used** for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: **substitution,** in which each element in the plaintext is mapped into another element, and **transposition,** in which elements in the plaintext are rearranged.

***2.* 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 encryp-tion. If the sender and receiver use different keys, the system is referred to as **asymmetric**, two-key, or public-key encryption.

3. **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, as it goes along.

# Types of Attacks

**Cryptanalysis:**

- This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

**Brute-force attack:**

The attacker tries every possible key on a piece of cipher-text until an intelligible translation into plaintext is obtained