Perfect Secrecy and Its Limitations

Introduction

Perfect secrecy is a theoretical model of absolute confidentiality, introduced by Claude Shannon. **A cryptosystem achieves perfect secrecy if the ciphertext reveals no additional information about the plaintext. In other words, knowing the ciphertext does not change the probability of any plaintext being the original message.**

Formal Definition

A cryptosystem (P, C, K, E, D) provides perfect secrecy if for all plaintexts M and ciphertexts C:

$$P(M \mid C) = P(M)$$

where:

- P(M) = Probability of message M
- P(M|C) = Probability of message M given ciphertext C

Meaning: Knowing C does not give any clue about M

This means that even after observing the ciphertext, the probability of a message being the plaintext remains unchanged.

One-Time Pad (OTP)

The One-Time Pad is a cipher that achieves perfect secrecy. It uses a random key K of the same length as the plaintext M. Encryption and decryption are performed using the bitwise XOR (⊕) operator:

Encryption: $C = M \oplus K$

Decryption: $M = C \oplus K$

⊕ (XOR) outputs 1 when the bits differ, and 0 when they are the same.

XOR (⊕) Truth Table (single bit):

M bit	K bit	M ⊕ K
0	0	0
0	1	1
1	0	1
1	1	0

Numerical Example

Plaintext (M): 10101010

Key (K): 11001100 (random)

Ciphertext (C): 10101010 ⊕ 11001100 = 01100110

Decryption: 01100110 ⊕ 11001100 = 10101010 = M

Since K is truly random and used only once, each possible plaintext is equally likely for a given ciphertext — achieving perfect secrecy.

Limitations of Perfect Secrecy

- Key length must be equal to the message length, which is impractical for large messages.
- Secure key distribution is difficult and costly.
- Key cannot be reused — otherwise, security is compromised (two-time pad attack).
- Storing large, random keys securely is challenging.
- Not efficient for large-scale or real-time communications.