Shannon's Theorem in Cryptography

Introduction

Shannon's Theorem is a fundamental principle in cryptography, formulated by Claude Shannon in 1949. It establishes the condition for achieving perfect secrecy in an encryption scheme. According to Shannon, a cryptosystem provides perfect secrecy if the ciphertext gives no information about the plaintext, even if the attacker has unlimited computational power.

Shannon's Theorem (Perfect Secrecy Condition)

A cryptosystem (P, C, K, E, D) is perfectly secret if and only if the key space is at least as large as the message space and each key is used with equal probability.

Formally:

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

This means that observing a ciphertext does not change the probability of any plaintext being the original message.

Statement of Shannon's Theorem

Shannon's Theorem states that for a cipher to achieve perfect secrecy, the key must:

1. Be as long as the message.
2. Be chosen uniformly at random.
3. Never be reused.

This condition is both necessary and sufficient for achieving perfect secrecy.

Example: One-Time Pad (OTP)

The One-Time Pad (OTP) is the classic example of a cipher achieving perfect secrecy.

Encryption and decryption are performed using bitwise XOR ($\oplus$):

$C = M \oplus K$

$M = C \oplus K$

Where:
M = Plaintext
K = Key (random and same length as M)
C = Ciphertext

Numerical Example

Plaintext (M): 10101010
Key (K): 11001100 (random)
Ciphertext (C): $10101010 \oplus 11001100 = 01100110$

Decryption:
$C \oplus K = 01100110 \oplus 11001100 = 10101010 = M$

Since K is truly random and used only once, the ciphertext gives no information about M.

Implications of Shannon's Theorem

- To achieve perfect secrecy, the key must be as long as the plaintext.
- Key distribution becomes challenging as large, random keys must be securely shared.
- Key reuse compromises perfect secrecy (e.g., in OTP).
- Practical systems often use computational security instead of perfect secrecy.

Shannon's Theorem shows that perfect secrecy is theoretically achievable but impractical for most real-world applications due to key management challenges. The One-Time Pad is the only cipher known to achieve perfect secrecy when its strict requirements are met.

Shannon's Theorem – Confusion and Diffusion

Introduction

Claude Shannon introduced the principles of confusion and diffusion as key design criteria for creating secure cryptographic systems. These concepts form the foundation of symmetric key cryptography and are crucial in protecting data from statistical and structural attacks.

Confusion

Confusion refers to making the relationship between the ciphertext and the key as complex as possible. It ensures that a small change in the key produces a large and unpredictable change in the ciphertext. Confusion is typically achieved using substitution operations, where symbols or bits are replaced with others according to a non-linear mapping.

Example

Consider a simple substitution cipher where each letter in the plaintext is replaced by another letter based on a random mapping. Without knowing the mapping (key), it becomes extremely hard to deduce the original plaintext.

Diffusion

Diffusion ensures that the influence of each plaintext symbol spreads across many ciphertext symbols. This makes patterns in the plaintext (like repeated characters) less noticeable in the ciphertext. Diffusion is typically implemented using permutations or transposition operations.

Example

In a transposition cipher, the positions of characters in the plaintext are rearranged according to a key. A single character change in the plaintext affects the position of multiple characters in the ciphertext.

Shannon's Theorem on Confusion and Diffusion

Shannon proved that by combining confusion and diffusion repeatedly, a cipher can achieve a high level of security. This layered approach makes it difficult for attackers to perform cryptanalysis by hiding both the statistical

structure of the plaintext (diffusion) and the relationship to the key (confusion).

Importance

- Confusion hides the relationship between the key and the ciphertext.
- Diffusion spreads plaintext structure across the ciphertext.
- Together, they make cryptanalysis significantly harder.
- Modern ciphers rely on multiple rounds of both techniques for security.