Concepts of Encryption and Decryption

- **Encryption**: The process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and a key.
- **Decryption**: The reverse process, where ciphertext is converted back into plaintext using a decryption algorithm and a key.
- **Symmetric Encryption**: The same key is used for both encryption and decryption (e.g., AES, DES).
- **Asymmetric Encryption**: Different keys are used for encryption and decryption (e.g., RSA, ECC). One key is public and the other is private.
- **Key**: A secret value used in encryption and decryption algorithms, which ensures data confidentiality.
- **Ciphertext**: The scrambled output produced after encryption.
- **Plaintext**: The original, readable input data.

Shannon's Characteristics of a Good Cipher

1. **Confusion**: The relationship between the plaintext, ciphertext, and the key should be complex. This makes it hard for an attacker to deduce the key from the ciphertext.
    - Achieved by complex substitution (e.g., S-boxes in AES).
2. **Diffusion**: The plaintext should be spread out across the ciphertext, so that changing one bit of plaintex affects many bits of ciphertext. This reduces patterns that could be exploited.
    - Achieved by techniques like permutation and mixing in algorithms.
3. **Avalanche Effect**: A small change in the plaintext or key should result in a completely different ciphertext. This makes it difficult to predict the effect of minor changes.
    - Example: In AES, a single bit change in the input causes significant changes in the output.
4. **Resistance to Known-Plaintext Attacks**: The cipher should be resistant to attacks where the attacker knows both the plaintext and corresponding ciphertext. This ensures that knowing plaintext doesn't reveal key information.
5. **Key Space**: The size of the key should be large enough to make brute-force attacks computationally infeasible. For modern ciphers, key sizes typically range from 128 bits to 256 bits.
6. **No Shortcut to Decryption**: There should be no faster method to decrypt the message than trying all possible keys, ensuring the security of the system even against advanced techniques.

Shannon's Theory of Confusion and diffusion

Shannon's Theory of confusion and Diffusion

1) The terms confusion and diffusion were introduced by Claude Shannon.

2) Shannon's concern was to prevent cryptanalysis, based on statistical analysis. The reason is as follows:

Assume attacker has some knowledge of the statistical characteristics of the plaintext (eg in a msg, the frequency distribution of the various letters may be known.
If these statistics are in any way reflected in the ciphertext, the cryptanalyst i.e attacker may be able to deduce the encryption key.

Assume attacker has some knowledge of the statistical characteristics of the plaintext (eg in a msg, the frequency distribution of the various letters may be known.
If these statistics are in any way reflected in the ciphertext, the cryptanalyst i.e attacker may be able to deduce the encryption key.

Thus Shannon suggested 2 methods for frustating the attackers:

1) Confusion } properties for creating
2) Diffusion } a secure cipher

DIFFUSION → In simple words, if a symbol in the plaintext is changed, several or all symbols in the ciphertext will also change.

BOOK ↓

reflected in the ciphertext, the cryptanalyst
i.e attacker may be able to deduce the
encryption key.

Thus Shannon suggested 2 methods for frustating the attackers:

1) Confusion
2) Diffusion

} properties for creating a secure cipher.

BOOK

DIFFUSION → In simple words, if a symbol in the plaintext is changed, several or all symbols in the ciphertext will also change.

→ The idea of diffusion is to hide the relationship between the ciphertext and plaintext.

a/c to wikipedia

Diffusion means that if we change a single bit of the plaintext, then (statically) half of the bits in the ciphertext should change, and similarly,

if we change 1 bit of ciphertext, then atleast one half of the plaintext bits should change.

Diffusion implies that each symbol in the ciphertext is dependent on some or all the symbols in the plaintext.

is maintained as complex

In short

diffusion

if change 1 bit of

then half or

confu

the symbols in the plaintext.

2) CONFUSION → is maintained as complex as possible.

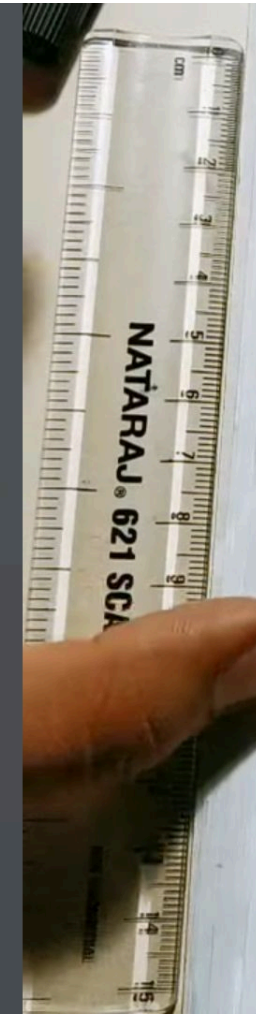
→ It hides the relationship b/w ciphertext and the key.

→ If a single bit in the key is changed then most/all bits of the ciphertext will also be changed.

A/c To wikipedia,

Confusion means that each bit of the ciphertext should depend on several parts of the key, obscuring the connection b/w the two.

obscuring → make under or difficult to understand.



In short,

diffusion → make statistical relation b/w plaintext and ciphertext as complex as possible

↓

if change 1 bit of plain then half or more bits of cipher should change.

confusion → makes relation b/w key & cipher text as complex as possible.

↓

each bit of ciphertext should depend on key.