Components of Modern Block Ciphers

Block Cipher

A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size.
The size of block is fixed in the given scheme.
The choice of block size does not directly affect to the strength of encryption scheme.
The strength of cipher depends up on the key length.

Components of Modern Block cipher

There are two common techniques used to construct ciphers:
substitution and permutation.

Permutation/Transposition Technique: uses the plaintext message letters but rearranges their order.

Substitution replaces plaintext letters or strings of letters by letters or numbers or symbols.

Permutation Cipher

- The Permutation Cipher is another form of Transposition Cipher.
- The Permutation Cipher acts on blocks of letters (the lengths of the keyword), rather than the whole ciphertext.

NOTE:
Mathematically, a permutation is a rule that tells you how to rearrange a set of elements. **For example, the permutation shown to the left (this is how we write a permutation mathematically), tells us that the first element is moved to the third position, the second element is moved to the first position and the third element is moved to the second position.**

A simple permutation

EXAMPLE:
If our set was the {Monday, Tuesday, Wednesday}, then after the permutation is applied we get {Tuesday,Wednesday,Monday}.

Substitution Cipher

Substitution technique is a classical encryption technique where the characters present in the **original message** are **replaced** by the **other characters or numbers or by symbols.**

Note:
Substitution Technique:
1.Caesar Cipher
2.Monoalphabetic Cipher
3.Playfair Cipher
4.Hill Cipher
5.Polyalphabetic Cipher
6.One-Time Pad

Substitution Cipher Example

Caesar Cipher
This the simplest substitution cipher by Julius Caesar. In this substitution technique, to encrypt the plain text, each alphabet of the plain text is replaced by the alphabet three places further it. And to decrypt the cipher text each alphabet of cipher text is replaced by the alphabet three places before it.

Let us take a simple example:
Plain Text: meet me tomorrow
Cipher Text: phhw ph wrpruurz

Look at the example above, we have replaced, ‘m’ with ‘p’ which occur three places after, ‘m’. Similarly, ‘e’ is replaced with ‘h’ which occurs in three places after ‘e’.

Note: If we have to replace the letter ‘z’ then the next three alphabets counted after ‘z’ will be ‘a’ ‘b’ ‘c’. So, while counting further three alphabets if ‘z’ occurs it circularly follows ‘a’.

Components of Modern Block cipher

NOTE: In block ciphers, the S-boxes and P-Boxes are used to make the relation between the plaintext and the ciphertext and the ciphertext difficult to understand.

Most important components are:

- **PBOX**:It is a key-less fixed transposition cipher
- **SBOX**: It is a key-less fixed substitution cipher

They are used to provide:

- **CONFUSION:**It hides the relationship between the ciphertext and the key

EXAMPLE: ABC ⟶ XYZ

- **DIFFUSION:**It hides the relationship between the ciphertext and the plaintext.

EXAMPLE: ABC ⟶ CAB

NOTE: **Confusion and diffusion** also Known as **frustrate statistical cryptanalysis.**

TASK:

Difference Between confusion and diffusion