Assignment Chapter 3

1) Describe the term:
i) Plaintext
ii) Ciphertext
iii) Cryptanalysis
iv) Cryptology

Plaintext:
Plaintext refers to readable data or message in its original form before any encryption is applied. It is the input provided to the encryption process. For example, the word *"HELLO"* is plaintext.

Ciphertext:
Ciphertext is the unreadable or scrambled form of data obtained after encryption. It ensures that unauthorized users cannot understand the information without the decryption key. For example, "IFMMP" (after Caesar shift +1) is ciphertext for "HELLO".

Cryptanalysis:
Cryptanalysis is the science of analyzing and breaking cryptographic systems without knowing the key. It involves studying ciphertexts, encryption algorithms, and possible weaknesses to recover plaintext. It is often referred to as "code breaking".

Cryptology:
Cryptology is the study of cryptography (creating secure communication methods) and cryptanalysis (breaking them). It is a broad field that covers designing encryption algorithms, analyzing their security, and developing ways to protect communication systems.

2) Explain Substitution techniques with an example.

Substitution techniques replace each element (letter, number, or symbol) of the plaintext with another element according to a defined rule.

Example – Caesar Cipher:
In Caesar Cipher, each letter in plaintext is shifted by a fixed number of positions down the alphabet.
Plaintext: *HELLO*
Key: Shift by 3
Ciphertext: *KHOOR*

Merits:
- Easy to implement and understand.
- Provides basic level of security.

Demerits:
- Can be broken easily using frequency analysis.
- Not suitable for modern cryptographic needs.

3) Explain Transposition techniques with an example.

Transposition techniques rearrange the positions of characters in plaintext without altering the actual characters themselves.

Example – Rail Fence Cipher:
Plaintext: *HELLO WORLD*
Key: 2 Rails
Arrangement:

H . L . O . W . R . D
. E . L . O . O . L .
Ciphertext: *HLOWRD ELOOL*

Merits:
- Stronger than substitution alone.
- Harder to break without knowing the key.

Demerits:
- Still vulnerable to pattern recognition.
- Needs to be combined with substitution for stronger security (product cipher).