DS Substitution Cipher

A substitution cipher is a method of encryption in which each letter of the plaintext is replaced with another letter or symbol. This creates a ciphertext that can only be decrypted with knowledge of the original substitution rule. The Caesar cipher, which involves shifting the letters of the alphabet a certain number of places, is one type of substitution cipher.

DS Give a simple example of encryption/decryption

Here is a simple example of a substitution cipher:

Plaintext: HELLO

Encryption:

- Choose a substitution rule, for example, shifting each letter 3 places to the right in the alphabet:
  H -> K
  E -> H
  L -> O
  L -> O
  O -> R

Ciphertext: KHOOR

Decryption:

- Apply the inverse of the substitution rule to obtain the original plaintext:
  K -> H
  H -> E
  O -> L
  O -> L
  R -> O

Plaintext: HELLO