Name - Shubham Solanki
UID - 2022301015
Batch - CSS Batch VIII
Comps A (BE)

Report on Substitution Ciphers.

Cipher

→ A process of writing a secret pattern of a particular set of letters or symbols used to represent other letter symbols.

Types

1. Caesar Cipher
→ A classical substitution cipher that shifts each letter of plaintext by a fixed number of positions in the alphabet.
Eg. Shift of 3 A becomes 'D' etc.

2. Hill Cipher
→ A polygraphic substitution cipher based on linear algebra. Uses matrix multiplication to encode blocks of text. A key matrix is chosen, plaintext is converted into vectors.

3. Playfair Cipher
→ encrypts of pair of letters using a 5×5 grid of letters derived from a keyword. It replace each pair of letter with letters from different corners of the grid.

4. Monoalphabetic Cipher
→ it substitution cipher where each letter of the plaintext is replaced by a fixed unique letter of the ciphertext alphabet.
Eg: A might become M

5. Poly alphabetic cipher
→ Uses multiple substitution alphabets to encode a message making it a harder to break monoalphabetic ciphers. This ensures and enhances security by obscuring letter frequency pattern.