UID: 2021800101 Batch - CSS Batch V
Name: Adwait Purao BE-COMPS B

PAGE NO.:

→ Report on substitution ciphers:

Introduction

In this technique each letter in plaintext is systematically replaced with another letter.

Types:

→ Caesar Cipher → Hill cipher
→ Monoalphabetic cipher → Polyalphabetic cipher
→ Playfair cipher

→ Caesar Cipher: Each letter in plaintext is shifted by fixed no. of positions in the alphabet. Its simple but not secure.

→ Hill Cipher: It encrypts blocks of plaintext using matrix multiplication with a key matrix. It requires key matrix to be invertible for decryption. Offers enhanced security over simple substitution ciphers.

→ Monoalphabetic cipher:
It replaces each letter in the plaintext with a fixed letter from a substitution alphabet. Vulnerable to frequency analysis.

→ Playfair cipher
Encrypts a pair of letters using 5X5 matrix derived from a keyword. More secure than

simple substitution methods due to use of digraphs & matrix based encryption.

Polyalphabetic cipher:
Uses multiple substitution alphabets determined by a key, encrypting each letter with a different alphabet. Enhances security by reducing susceptibility to frequency analysis.