Sudesh Pawar
BE Comp A
PRN: F17111037 (24)

ICS A 2

1) What do you mean by 'polygraphic substitution cipher? List types of it

→ Polygraphic substitution is a cipher in which as uniform substitution is performed on block of letters. When the length of the block is specifically known, more precise terms are used: for instance, a cipher in which pairs of letters are substituted is bigraphic.

Types:

i) Playfair Cipher: It replaces each pair of plaintext letters by another pair of letters, determined by single table.

ii) Two square cipher: It replaces each pair of plaintext letters by another pair of letters, determined by a single table

iii) Four-square cipher: It replaces each pair of plaintext letters by another pair of letters, determined by single table

iv) Hill Cipher: It is based on linear algebra. Each letter is represented by a no. modulo 26.

2) Discuss Hill Cipher in detail

Ans. i) When we use encryption algorithm, we take in successive plaintext letters & substitute for them in m cipher text letter.

ii) Hill Cipher is polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26.

iii) To encrypt a plaintext message, each block of m letters is multiplied by ~~inverse of the matrix~~ invertible used for encryption.

iv) To decrypt plaintext message, each block is multiplied by inverse of matrix used for encryption.

v) $C_{i1} = (K_{11} P_{i1} + K_{i2} P_{i2} + K_{i3} P_{i3}) \mod 26$

$C_{i2} = (K_{21} P_{i1} + K_{22} P_{i2} + K_{23} P_{i3}) \mod 26$

$C_{i3} = (K_{31} P_{i1} + K_{32} P_{i2} + K_{33} P_{i3}) \mod 26$

We can represent this technique like,

$$C_i = KP_i \bmod 26$$

Q.3. Find the key for decryption using Hill Cipher:

Ans. Encryption Key : DIMENSION.

∴ Key is $\begin{bmatrix} 3 & 4 & 8 \\ 8 & 13 & 14 \\ 12 & 18 & 13 \end{bmatrix}$

Decryption key is,

$$\begin{bmatrix} 3 & 4 & 8 \\ 8 & 13 & 14 \\ 12 & 18 & 13 \end{bmatrix}^{-1} = \frac{1}{89} \begin{bmatrix} 83 & -92 & 48 \\ -64 & 57 & -22 \\ 12 & 6 & -7 \end{bmatrix}$$

Q.4) Discuss choosen plaintext attack on Hill Cipher with Eg.

Ans. A choosen plaintext attack is an attack model for cryptoanalysts which presumes that the attacker can obtain the ciphertexts for arbitary plaintexts. The goal of the attack is to gain information that reduces security.

Let ciphertext be encrypted with an unknown matrix K with shape $2 \times 2 \bmod 251$.

$KP_1 = C_1 \pmod m$ & $KP_2 = C_2 \pmod m$

Each pair adds one eqn or two if we see them in a way.

$K_{1,1} P_{1,1} + K_{1,2} P_{1,2} = C_{1,1} \pmod m$

$K_{2,1} P_{1,1} + K_{2,2} P_{1,2} = C_{1,2} \pmod m$

$K_{1,1} P_{2,1} + K_{1,2} P_{2,2} = C_{2,1} \pmod m$

$K_{2,1} P_{2,1} + K_{2,2} P_{2,2} = C_{2,2} \pmod m$

Also, it can be written as

$$KP = C \pmod m$$