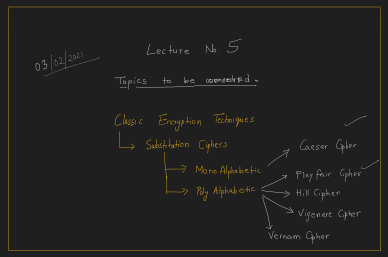

Pg. 64 Stallings

3. Hill Cipher

This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1,c, z = 25).

For m = 3, the system can be described as:

$$c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$$
$$c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$$
$$c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$$

This can be expressed in terms of row vectors and matrices:[6]

$$(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3)\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

or

$$\mathbf{C} = \mathbf{PK} \bmod 26$$

where C and P are row vectors of length 3 representing the plaintext and ciphertext, and K is a 3 * 3 matrix representing the encryption key. Operations are performed mod 26. For example, consider the plaintext "paymoremoney" and use the encryption key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

ENCRYPTION :-

The first three letters of the plaintext are represented by the vector (15 0 24).

Then(15 0 24)K = (303 303 531) mod 26 = (17 17 11) = RRL.

Continuing in this fashion, the ciphertext for the entire plaintext is RRLMWBKASPDH

DECRYPTION :-

Decryption requires using the inverse of the matrix K.

We can compute det K = 23, and therefore,

$(\det K)^{-1} \bmod 26$ needs to be calculated

Here $(\det K \times n) \bmod 26 = 1$

$(\det K)^{-1}$

So, $K^{-1} = \frac{1}{(\det K)} \times (K^{adj})$

$= (\det K)^{-1} \times (K^{adj})$

Know?

Mathematics is Everywhere ☺

Calculate the determinant of the matrix.

$$M = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$$

$\det(M) = 1(0-24) - 2(0-20) + 3(0-5) = 1$

Transpose the original matrix.

$$M = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \quad M^T = \begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}$$

Find the determinant of each of the 2x2 minor matrices

$$M^T = \begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}$$

$\begin{vmatrix} 1 & 6 \\ 4 & 0 \end{vmatrix} = -24$ $\quad \begin{vmatrix} 2 & 6 \\ 3 & 0 \end{vmatrix} = -18$ $\quad \begin{vmatrix} 2 & 1 \\ 3 & 4 \end{vmatrix} = 5$

$\begin{vmatrix} 0 & 5 \\ 4 & 0 \end{vmatrix} = -20$ $\quad \begin{vmatrix} 1 & 5 \\ 3 & 0 \end{vmatrix} = -15$ $\quad \begin{vmatrix} 1 & 0 \\ 3 & 4 \end{vmatrix} = 4$

$\begin{vmatrix} 0 & 5 \\ 1 & 6 \end{vmatrix} = -5$ $\quad \begin{vmatrix} 1 & 5 \\ 2 & 6 \end{vmatrix} = -4$ $\quad \begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} = 1$

Create the matrix of cofactors.

$$Adj(M) = \begin{bmatrix} -24 & -18 & 5 \\ -20 & -15 & 4 \\ -5 & -4 & 1 \end{bmatrix} \times \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

$$Adj(M) = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$$

Divide each term of the adjugate matrix by the determinant

$Adj(M) = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$; $\det(M) = 1$

$$M^{-1} = \frac{1}{\det(M)} \times Adj(M)$$

$$M^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$$