CS553 Cryptography

BitBees

Question 5

Part A

$k_1 = \begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix}$ and $k_2 = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$

We are given the message $m = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$

The encryption algorithm is $e_k(m) \equiv k_1.m + k_2 \pmod p$

The ciphertext is $\begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \end{bmatrix} + \begin{bmatrix} 5 \\ 4 \end{bmatrix} \pmod{11} = \begin{bmatrix} 10 \\ 10 \end{bmatrix}$

The matrix k_1^{-1} used for decryption is $\begin{bmatrix} 1 & 3 \\ 2 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & 6 \\ 4 & 5 \end{bmatrix}$

We are given ciphertext $\begin{bmatrix} 3 \\ 5 \end{bmatrix}$

The decryption algorithm is $d_k(m) \equiv k_1^{-1}.(c - k_2) \pmod p$

Hence the decryption of the ciphertext is

$$\begin{bmatrix} 3 & 6 \\ 4 & 5 \end{bmatrix} \cdot \left(\begin{bmatrix} 3 \\ 5 \end{bmatrix} - \begin{bmatrix} 5 \\ 4 \end{bmatrix} \right) \pmod{11} = \begin{bmatrix} 0 \\ 4 \end{bmatrix}$$

Part B

Let $M = (x_1, x_2, ..., x_m)$

Hill Cipher is vulnerable to Known Plaintext Attack(KPA) because the ciphertext is a linear combination of x_i where $x_i \in M$. This means that given enough linearly independent equations, one could solve the system of linear equations to get back the keys k_1 and k_2.

Part C

We are given with three (m, c) pairs.

$m_1 = \begin{bmatrix} 5 \\ 4 \end{bmatrix}$, $c_1 = \begin{bmatrix} 1 \\ 8 \end{bmatrix}$, $m_2 = \begin{bmatrix} 8 \\ 10 \end{bmatrix}$, $c_2 = \begin{bmatrix} 8 \\ 5 \end{bmatrix}$, $m_3 = \begin{bmatrix} 7 \\ 1 \end{bmatrix}$, $c_3 = \begin{bmatrix} 8 \\ 7 \end{bmatrix}$
Using the encryption algorithm $e_k(m) \equiv k_1.m + k_2 \pmod p$
We are given that $p = 11$

Let $k_1 = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$ and $k_2 = \begin{bmatrix} k_1^1 \\ k_2^1 \end{bmatrix}$

Therefore, we get a system of linear equations in 6 variables.

Using (m_1, c_1)

$$\begin{bmatrix} 5k_{11} + 4k_{12} + k_1^1 \mod 11 \\ 5k_{21} + 4k_{22} + k_2^1 \mod 11 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 8 \end{bmatrix}$$

Using (m_2, c_2)

$$\begin{bmatrix} 8k_{11} + 10k_{12} + k_1^1 \mod 11 \\ 8k_{21} + 10k_{22} + k_2^1 \mod 11 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 5 \end{bmatrix}$$

Using (m_3, c_3)

$$\begin{bmatrix} 7k_{11} + k_{12} + k_1^1 \mod 11 \\ 7k_{21} + k_{22} + k_2^1 \mod 11 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 7 \end{bmatrix}$$

Solving the above system of linear equation in six variables.

$$X = \begin{bmatrix} 5 & 4 & 0 & 0 & 1 & 0 \\ 0 & 0 & 5 & 4 & 0 & 1 \\ 8 & 10 & 0 & 0 & 1 & 0 \\ 0 & 0 & 8 & 10 & 0 & 1 \\ 7 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 7 & 1 & 0 & 1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} 1 \\ 8 \\ 8 \\ 5 \\ 8 \\ 7 \end{bmatrix} = \begin{bmatrix} 3 \\ 7 \\ 4 \\ 3 \\ 2 \\ 9 \end{bmatrix}$$

$k_1 = \begin{bmatrix} 3 & 7 \\ 4 & 3 \end{bmatrix}$ and $k_2 = \begin{bmatrix} 2 \\ 9 \end{bmatrix}$

Part D

Substitution cipher can be thought as a special case of Hill Cipher as we can represent permutations in the form of a matrix. This special form of matrix called permutation matrix is defined as a square binary matrix that has exactly one entry of 1 in each row and each column and 0s elsewhere. Each such matrix, say P, represents a permutation of m elements and, when used to multiply another matrix, say A, results in permuting the rows (when pre-multiplying, to form PA) or columns (when post-multiplying, to form AP) of the matrix A.

For example, permuatation P_π, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$ can be represented in the form of a matrix.

$$P_\pi = \begin{bmatrix} \mathbf{e}_{\pi(1)} \\ \mathbf{e}_{\pi(2)} \\ \mathbf{e}_{\pi(3)} \\ \mathbf{e}_{\pi(4)} \\ \mathbf{e}_{\pi(5)} \end{bmatrix} = \begin{bmatrix} \mathbf{e}_1 \\ \mathbf{e}_4 \\ \mathbf{e}_2 \\ \mathbf{e}_5 \\ \mathbf{e}_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$