Gary Hobson

Module 3 Homework

May 19, 2023

5.4 - 5

$$x_{n+2} = c_0 x_n + c_1 x_{n+1} \pmod 3$$

this gives:

$$1, 1, 0, 2, 2, 0, 1, 1$$

n	x_n	x_{n+1}	x_{n+2}	Equation
0	1	1	0	$0 = c_0(1) + c_1(1) \pmod 3$
1	1	0	2	$2 = c_0(1) + c_1(0) \pmod 3$

$$c_0 + c_1 \equiv 0 \pmod 3$$

$$c_0 \equiv 2 \pmod 3$$

So,

$$c_0 = 2$$

Substitute,

$$2 + c_1 \equiv 0 \pmod 3 \quad \Rightarrow \quad c_1 \equiv -2 \equiv 1 \pmod 3$$

$$c_0 = 2, \quad c_1 = 1 \pmod 3$$

6.6 - 2

$$\det(A) = (1)(1) - (1)(1) = 0$$

So,

$$\det(A) \equiv 0 \pmod{26}$$

If $\det(A) \equiv 0 \pmod{26}$, then:

$$\gcd(0, 26) = 26 \neq 1$$

Since the GCD is not 1, the matrix is not invertible modulo 26.

So, decryption is impossible.

6.6 - 6

- aaa $\rightarrow$ vector $(0, 0, 0)$
- baa $\rightarrow$ vector $(1, 0, 0)$
- aba $\rightarrow$ vector $(0, 1, 0)$
- aab $\rightarrow$ vector $(0, 0, 1)$

The last three are needed to form a 3×3 identity matrix when stacked:

$$P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Then, the corresponding ciphertext blocks will become the rows of the matrix M:

$$C = \begin{bmatrix} ? & ? & ? \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \quad \Rightarrow \quad M = C$$

Choose three plaintexts:

"baa", "aba", "aab" $\rightarrow$ these convert to vectors $(1, 0, 0), (0, 1, 0),$ and $(0, 0, 1)$.

Encrypt each using the unknown Hill cipher.
Stack the resulting ciphertexts as rows to obtain the matrix M.

6.6 - 8

$$M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \pmod{26}$$

$$M \cdot P_1 \equiv M \cdot P_2 \pmod{26} \quad \Rightarrow \quad M \cdot (P_1 - P_2) \equiv 0 \pmod{26}$$

Set $v = \begin{bmatrix} x \\ y \end{bmatrix}$, and solve:

$$M \cdot v = \begin{bmatrix} x + 2y \\ 3x + 4y \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{26}$$

So,

$$x \equiv -2y \pmod{26}$$

Substitute

$$3(-2y) + 4y = -6y + 4y = -2y \equiv 0 \pmod{26} \quad \Rightarrow \quad y \equiv 0 \pmod{13}$$

Try $y = 13$, then:

$$x = -2y = -2 \cdot 13 = -26 \equiv 0 \pmod{26}$$

So:

$$v = \begin{bmatrix} 0 \\ 13 \end{bmatrix}$$

So, for any plaintext P, $P + v$ will encrypt to the same ciphertext.

Let:

$$P_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 1 \\ 15 \end{bmatrix}$$

Compute the ciphertexts:

$$M \cdot P_1 = \begin{bmatrix} 1 \cdot 1 + 2 \cdot 2 \\ 3 \cdot 1 + 4 \cdot 2 \end{bmatrix} = \begin{bmatrix} 1 + 4 \\ 3 + 8 \end{bmatrix} = \begin{bmatrix} 5 \\ 11 \end{bmatrix}$$

$$M \cdot P_2 = \begin{bmatrix} 1 \cdot 1 + 2 \cdot 15 \\ 3 \cdot 1 + 4 \cdot 15 \end{bmatrix} = \begin{bmatrix} 1 + 30 \\ 3 + 60 \end{bmatrix} = \begin{bmatrix} 31 \\ 63 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 11 \end{bmatrix} \pmod{26}$$

So, $P_1 = (1, 2)$ and $P_2 = (1, 15)$ encrypt to the same ciphertext under matrix $M \pmod{26}$.