Hill Cipher 9/12/25

Matrices

Plaintext: HOME
7, 14, 12, 4

key $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} \quad \\ \quad \end{pmatrix}$ Ciphertext

2×2

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 12 \\ 4 \end{pmatrix} = \begin{pmatrix} \quad \\ \quad \end{pmatrix}$ ciphertext

35
28

$\begin{pmatrix} 3 & 7 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 3\times7 + 7\times14 \\ 5\times7 + 2\times14 \end{pmatrix} = \begin{pmatrix} 119 \\ 63 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 15 \\ 11 \end{pmatrix} \begin{matrix} P \\ L \end{matrix}$

n×n n×1

key[i][j] * word[j][0]

$\begin{pmatrix} 3 & 7 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 12 \\ 4 \end{pmatrix} = \begin{pmatrix} 3\times12 + 7\times4 \\ 5\times12 + 2\times4 \end{pmatrix} = \begin{pmatrix} 10+2 \\ 8+8 \end{pmatrix} = \begin{pmatrix} 12 \\ 16 \end{pmatrix}$

M
Q

w/key $\begin{pmatrix} 3 & 7 \\ 5 & 2 \end{pmatrix}$ Plaintext: HOME → Ciphertext

PLMQ

What makes a valid key?

gcd (Determinant (KEY), 26) = 1

$\det\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right| = ad - bc$

$3\times2 - 5\times7$
$= 6 - 35$
$= -29$
$\equiv -3$
$\equiv 23 \pmod{26}$

Inverse $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\left[(ad-bc)^{-1} \bmod 26\right]$

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} 3 & 7 \\ 5 & 2 \end{pmatrix}^{-1} \text{ is } (23^{-1} \bmod 26)\begin{pmatrix} 2 & -7 \\ -5 & 3 \end{pmatrix} \qquad \begin{matrix} 104 \\ -85 \end{matrix}$$

$$= 17\begin{pmatrix} 2 & -7 \\ -5 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 34 & -119 \\ -85 & 51 \end{pmatrix} = \begin{pmatrix} 8 & 11 \\ 19 & 25 \end{pmatrix}$$

Prove $\begin{pmatrix} 3 & 7 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 8 & 11 \\ 19 & 25 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\begin{pmatrix} 3 & 7 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 8 & 11 \\ 19 & 25 \end{pmatrix} = \begin{pmatrix} 3\times8+7\times19 & 3\times11+7\times25 \\ 5\times8+2\times19 & 5\times11+2\times25 \end{pmatrix}$$

$25 \equiv -1$

$$= \begin{pmatrix} 24+133 & 33-7 \\ 40+38 & 55-2 \end{pmatrix}$$

$$= \begin{pmatrix} 157 & 26 \\ 78 & 53 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 26$$

P

$$\begin{pmatrix} 8 & 11 \\ 19 & -1 \end{pmatrix}\begin{pmatrix} 15 \\ 11 \end{pmatrix} = \begin{pmatrix} 8\times15+11\times11 \\ 19\times15-1\times11 \end{pmatrix}$$

$$= \begin{pmatrix} 120+121 \\ 285-11 \end{pmatrix}$$

$$= \begin{pmatrix} 241 \\ 274 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{matrix} H \\ O \end{matrix}$$

1) Cryptanalysis with H.11

2) Derive 3×3 inverse

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 15 \\ 11 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 12 \\ 4 \end{pmatrix} = \begin{pmatrix} 12 \\ 16 \end{pmatrix}$$

$$\begin{pmatrix} 7a+14b \\ 7c+14d \end{pmatrix} = \begin{pmatrix} 15 \\ 11 \end{pmatrix} \qquad \begin{pmatrix} 12a+4b \\ 12c+4d \end{pmatrix} = \begin{pmatrix} 12 \\ 16 \end{pmatrix}$$

$12 \quad 7a + 14b \equiv 15 \mod 26$

$7 \quad 12a + 4b \equiv 12 \mod 26$

$$84a + 168b \equiv 180 \mod 26$$
$$-\ 84a + 28b \equiv 84 \mod 26$$
$$140b \equiv 96 \mod 26$$

$$10b \equiv 18 \mod 26$$
$$10b = 18 + 26c, \quad c \in \mathbb{Z}$$
$$5b = 9 + 13c$$

Repeat Process for C and D

$$8(5b) \equiv (9)8 \pmod{13}$$
$$40b \equiv 72 \pmod{13}$$
$$b \equiv 7 \pmod{13}$$
$$b \equiv 7 \pmod{26} \longrightarrow a = 3$$
$$b \equiv 20 \pmod{26} \longrightarrow a = 3$$

$$7a + 14b \equiv 15 \mod 26$$
$$7a + 14(20) \equiv 15 \mod 26$$
$$7a + 280 \equiv 15 \mod 26$$
$$7a + 20 \equiv 15 \mod 26$$
$$15(7a) \equiv (-5)^{15} \mod 26$$
$$a \equiv -75 \mod 26 \equiv 3$$

$$\left[\begin{array}{ccc:ccc} 1 & 3 & 7 & 1 & 0 & 0 \\ 1 & 8 & 5 & 0 & 1 & 0 \\ 4 & 11 & 9 & 0 & 0 & 1 \end{array}\right]$$

$$\left[\begin{array}{ccc:ccc} 1 & 3 & 7 & 1 & 0 & 0 \\ 0 & 5 & -2 & -1 & 1 & 0 \\ 0 & -1 & 7 & -4 & 0 & 1 \end{array}\right] \begin{array}{l} \\ \rightarrow R2 - R1 \\ \rightarrow R3 - 4 \times R1 \end{array}$$

$$\left[\begin{array}{ccc:ccc} 1 & 3 & 7 & 1 & 0 & 0 \\ 0 & 5 & -2 & -1 & 1 & 0 \\ 0 & 0 & 7 & -21 & 1 & 5 \end{array}\right] \rightarrow 5R3 + R2$$

$$\left[\begin{array}{ccc:ccc} 1 & 3 & 7 & 1 & 0 & 0 \\ 0 & 5 & -2 & -1 & 1 & 0 \\ 0 & 0 & 1 & -3 & 15 & -3 \end{array}\right] \rightarrow 15R3$$

$$\left[\begin{array}{ccc:ccc} 1 & 3 & 0 & 22 & -1 & 21 \\ 0 & 5 & 0 & -7 & 5 & -6 \\ 0 & 0 & 1 & -3 & 15 & -3 \end{array}\right] \begin{array}{l} \rightarrow R1 - 7R3 \\ \rightarrow 2R3 + R2 \\ \\ \end{array}$$

$$\left[\begin{array}{ccc:ccc} 1 & 3 & 0 & 22 & -1 & 21 \\ 0 & 1 & 0 & 9 & 1 & 4 \\ 0 & 0 & 1 & -3 & 15 & -3 \end{array}\right] \rightarrow 21R2$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -5 & -4 & 9 \\ 0 & 1 & 0 & 9 & 1 & 4 \\ 0 & 0 & 1 & -3 & 15 & -3 \end{array}\right] \quad R1 - 3R2$$

$$= \begin{pmatrix} 21 & 22 & 9 \\ 9 & 1 & 4 \\ 23 & 15 & 23 \end{pmatrix}$$

Proof Correct

$$\begin{pmatrix} 1 & 3 & 7 \\ 1 & 8 & 5 \\ 4 & 11 & 9 \end{pmatrix}\begin{pmatrix} -5 & -4 & 9 \\ 9 & 1 & 4 \\ -3 & 15 & -3 \end{pmatrix} = \begin{pmatrix} 1(-5)+3(9)+7(-3) & 1(-4)+3(1)+7(15) & 1(9)+3(4)+7(-3) \\ 1(-5)+8(9)+5(-3) & 1(-4)+8(1)+5(15) & 1(9)+8(4)+5(-3) \\ 4(-5)+11(9)+9(-3) & 4(-4)+11(1)+9(15) & 4(9)+11(4)+9(-3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 104 & 0 \\ 52 & 79 & 26 \\ 52 & 130 & 53 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mod 26 \checkmark$$

WORKS!