CIS 3362 9/15/21 – Hill Cipher

(1) H3 is now posted.

(2) Hill cipher

↳ Another polyalphabetic cipher

More mathematics!!

Key is a k by k matrix

Example 2×2 matrix

$$\text{Key} = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}$$

3 14 13 20 19 18

Plain = "DONUTS"

$$\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}\begin{pmatrix} 3 \\ 14 \end{pmatrix} = \begin{pmatrix} 3\times3 + 5\times14 \\ 3\times4 + 7\times14 \end{pmatrix}$$

$$= \begin{pmatrix} 9+70 \\ 12+98 \end{pmatrix} = \begin{pmatrix} 79 \\ 110 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 1 \\ 6 \end{pmatrix} = \begin{matrix} B \\ G \end{matrix}$$

$$\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}\begin{pmatrix} 13 \\ -6 \end{pmatrix} = \begin{pmatrix} 3\times13 + 5(-6) \\ 4\times13 + 7(-6) \end{pmatrix} = \begin{pmatrix} 9 \\ 10 \end{pmatrix} \begin{matrix} J \\ K \end{matrix}$$

$$\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}\begin{pmatrix} -7 \\ -8 \end{pmatrix} = \begin{pmatrix} 3\times(-7) + 5(-8) \\ 4\times(-7) + 7(-8) \end{pmatrix} = \begin{pmatrix} -61 \\ -84 \end{pmatrix} \equiv \begin{pmatrix} 17 \\ 20 \end{pmatrix} \begin{matrix} R \\ U \end{matrix}$$

28
56

DONUTS ⟹ BGJKRU

Inverse of a 2x2 Matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad M^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$ad-bc$ ← DETERMINANT

for real numbers

M^{-1} DOES NOT EXIST IF ~~$ab-bc$~~ $ad-bc = 0$.

for mod math

$\gcd(ad-bc, 26) = 1$ for the M^{-1} to exist.

$$M^{-1} = \begin{pmatrix} d \times (ad-bc)^{-1} \bmod 26 & -b \times (ad-bc)^{-1} \bmod 26 \\ -c \times (ad-bc)^{-1} \bmod 26 & a \times (ad-bc)^{-1} \bmod 26 \end{pmatrix}$$

$$M = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix} \quad M^{-1} = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \equiv \boxed{\begin{pmatrix} +7 & 21 \\ 22 & 3 \end{pmatrix}}$$

$$\begin{pmatrix} 7 & 21 \\ 22 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 6 \end{pmatrix} = \begin{pmatrix} 7 \cdot 1 + 21 \cdot 6 \\ 22 \cdot 1 + 3 \cdot 6 \end{pmatrix} = \begin{pmatrix} 133 \\ 40 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 14 \end{pmatrix} \begin{matrix} D \\ O \end{matrix}$$

Prove $\begin{pmatrix} 7 & 21 \\ 22 & 3 \end{pmatrix}$ (BG) is decryption key:

$$\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix} \begin{pmatrix} 7 & 21 \\ 22 & 3 \end{pmatrix} = \begin{pmatrix} 3 \cdot 7 + 5 \cdot 22 & 3 \cdot 21 + 5 \cdot 3 \\ 4 \cdot 7 + 7 \cdot 22 & 4 \cdot 21 + 7 \cdot 3 \end{pmatrix}$$

$$= \begin{pmatrix} 131 & 78 \\ 182 & 105 \end{pmatrix} \equiv$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \checkmark$$

154
28

$$M = \begin{pmatrix} 7 & 4 \\ 6 & 5 \end{pmatrix}$$

$ad - bc = 35 - 24$
$= 11$

$11^{-1} \bmod 26 = 19$

$$M^{-1} = \begin{pmatrix} 19 \cdot 5 & (-4)19 \\ 19(-6) & (7)19 \end{pmatrix} = \begin{pmatrix} 95 & -76 \\ -114 & 133 \end{pmatrix}$$

$$= \begin{pmatrix} 17 & 2 \\ 16 & 3 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 14 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 14 \\ 10 \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \end{pmatrix}$$

$a \cdot 1 + b \cdot 14 \equiv 0 \mod 26$
$a \cdot 14 + b \cdot 10 \equiv 24 \mod 26$
$14a + 196b \equiv 0 \mod 26$

$a + 20 \cdot 14 \equiv 0 \mod 26$
$a \equiv -280 \mod 26$
$\equiv 6$

$a + 7 \cdot 14 \equiv 0 \mod 26$
$a \equiv -98 \equiv 6 \mod 26$

$186b \equiv -24 \mod 26$
$4b \equiv -24 \mod 26$
$4b = -24 + 26n, \quad n \in \mathbb{Z}$
$2b = -12 + 13n$
$7 \cdot 2b \equiv -12 \cdot 7 \mod 13$
$b \equiv -84 \equiv 7 \mod 13$

$b \equiv 7 \mod 26$
or $b \equiv 20 \mod 26$

6
6