CIS 3362 - 9/13/23

Hill cipher

key $n \times n$ matrix [split input into blocks of n letters each]

example 2×2

msg: HOME

7, 14, 12, 4

$$\text{key} = \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix}$$

col 1 $n \times 1$ matrix

row 1

$$\begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \times \begin{bmatrix} 7 \\ 14 \end{bmatrix} = \begin{bmatrix} 3*7 + 5*14 \\ 2*7 + 7*14 \end{bmatrix}$$

$$= \begin{bmatrix} 91 \\ 112 \end{bmatrix} \% 26 = \begin{bmatrix} 13 \\ 8 \end{bmatrix} \begin{matrix} N \\ I \end{matrix}$$

14
98

24
28

$$\begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \times 12 + 5 \times 4 \\ 2 \times 12 + 7 \times 4 \end{bmatrix}$$

$$= \begin{bmatrix} 56 \\ 52 \end{bmatrix} \% 26 = \begin{bmatrix} 4 \\ 0 \end{bmatrix} \begin{matrix} E \\ A \end{matrix}$$

HOME → NIEA

Are all possible matrices w/entries in btw 0 and 25 valid keys?

NO $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \longrightarrow$ AAAA

What are the criteria that makes a key valid?

Process for finding an inverse of a matrix

$$\left[\begin{array}{cc|cc} 3 & 5 & 1 & 0 \\ 2 & 7 & 0 & 1 \end{array}\right]$$

In this process "row operations" until LHS looks like $\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$, A lot like solving a sys of eqns.

Sometimes: $0x + 0y = 5$? IMPOSSIBLE

In real #s matrices, m are invertible iff $\det(m) \neq 0$.

Only invertible if $\gcd(\det(m), 26) = 1$.

Def of $\left|\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right| = ad - bc$

$$\begin{vmatrix} 3 & 5 \\ 2 & 7 \end{vmatrix} = 3 \times 7 - 2 \times 5 = 11 \checkmark$$

$\gcd(11, 26) = 1 \checkmark$

Determinant 3×3

$$\left|\begin{array}{ccc|cc} a & b & c & a & b \\ d & e & f & d & e \\ g & h & i & g & h \end{array}\right| = aei + bfg + cdh - ceg - afh - bdi$$

For 2×2 if $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is key

Inverse is $(ad-bc)^{-1} \bmod 26 \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

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

$\begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix}$ $\quad$ $\det = 3\times7-2\times5 = 11$

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

$$19\begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 133 & -95 \\ -38 & 57 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3 & 9 \\ 14 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 9 \\ 14 & 5 \end{bmatrix}\begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 3\cdot3+9\cdot2 & 3\cdot5+9\cdot7 \\ 14\cdot3+5\cdot2 & 14\cdot5+5\cdot7 \end{bmatrix}$$

row i x col j gives entry in row i, col j

$$= \begin{bmatrix} 27 & 78 \\ 52 & 105 \end{bmatrix} \bmod 26$$

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

$$[ad-bc]^{-1} \bmod 26 \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= [ad-bc]^{-1} \bmod 26 \begin{bmatrix} ad-bc & bd-bd \\ -ac+ac & -bc+ad \end{bmatrix}$$

$$= [ad-bc]^{-1} \bmod 26 \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix}$$

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

$$\begin{matrix} 3 & 5 \\ 7 & 8 \end{matrix}$$

$24-35$

-11

-19

$$-19 \begin{bmatrix} 8 & -5 \\ -7 & 3 \end{bmatrix} = 7 \begin{bmatrix} 8 & -5 \\ -7 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 56 & -35 \\ -49 & 21 \end{bmatrix}$$

$$= \boxed{\begin{bmatrix} 4 & 17 \\ 3 & 21 \end{bmatrix}}$$