CIS 3362 9/9/24

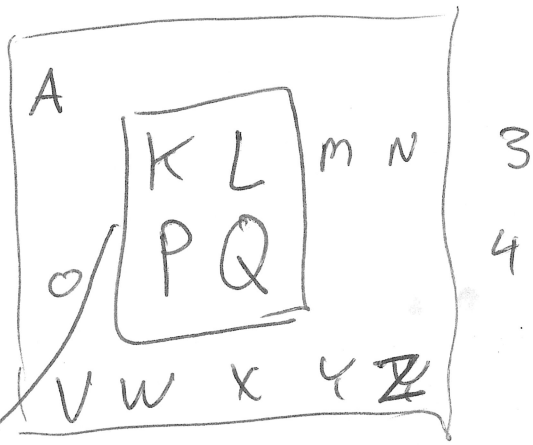
(1) Playfair decryption

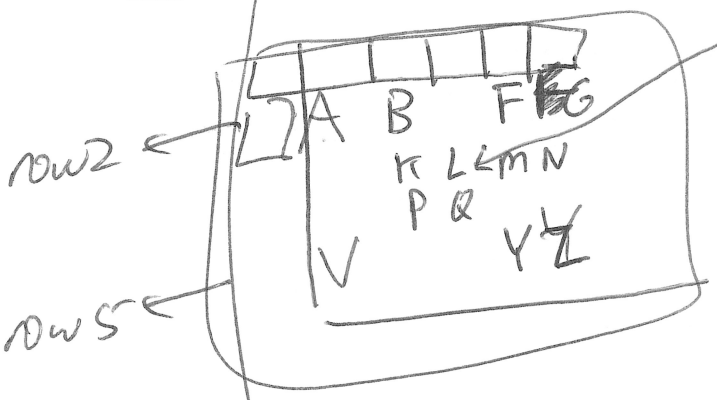
(2) Hill Cipher

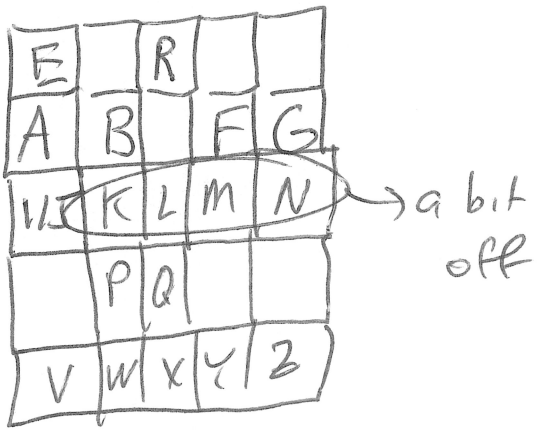
(3) Hand back Q1

→ With a little matching plain/cipher text

Plain		CIPHER
PL	↔	QK
AY	↔	FV
FA	↔	GB
IR	↔	LE







Valid

DESSERT

SECRET

Box and likely E, R are in the keyword

Hill Cipher

Lester Hill 1920s

"HOME"

7, 14, 12, 4

H O

$$\begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 3\times 7 + 5\times 14 \\ 2\times 7 + 7\times 14 \end{pmatrix} = \begin{pmatrix} 21+70 \\ 14+98 \end{pmatrix}$$

$$= \begin{pmatrix} 91 \\ 112 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} = \begin{pmatrix} 13 \\ 8 \end{pmatrix} \to \begin{matrix} N \\ I \end{matrix}$$

$2\times 2 \quad 2\times 1 \quad \to \quad 2\times 1$

$$\begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix}\begin{pmatrix} 12 \\ 4 \end{pmatrix} = \begin{pmatrix} 3\times 12 + 5\times 4 \\ 2\times 12 + 7\times 4 \end{pmatrix} = \begin{pmatrix} 36+20 \\ 24+28 \end{pmatrix} = \begin{pmatrix} 56 \\ 52 \end{pmatrix}$$

$$= \begin{pmatrix} 4 \\ 0 \end{pmatrix} \begin{matrix} E \\ A \end{matrix}$$

"HOME" → "NIEA".

Question #1: Are all possible matrices valid keys?

Question #2: For all the valid keys what is the corresponding decryption key?

Q1: No, consider $\begin{pmatrix} 13 & 0 \\ 8 & 4 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 13x+0y \\ 8x+4y \end{pmatrix}$

These can't be "repeats"

Q2: A key can be valid iff a decryption key exists

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix}\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right] = \begin{pmatrix} x \\ y \end{pmatrix}$$

must exist — key CIPHER — PLAIN

Answers to both: Valid keys are one such that $M^{-1} \pmod{26}$ exists.

$\text{Inv}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ in real #s

for mod, we have $((ad-bc)^{-1} \bmod 26)\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$19 \equiv -7 \pmod{26}$

$M = \begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix}$, $M^{-1} = 19\begin{pmatrix} 7 & -5 \\ -2 & 3 \end{pmatrix} = -7\begin{pmatrix} 7 & -5 \\ -2 & 3 \end{pmatrix}$

$= \begin{pmatrix} -49 & 35 \\ 14 & -21 \end{pmatrix}$

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

$ad-bc = 3\cdot 7 - 2\cdot 5$

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

17 | 11 | 187 | -130 | 57 | 26 | 21 | -21 | 31

Corresponding decryption matrix is

$$\begin{pmatrix} 3 & 9 \\ 14 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 9 \\ 14 & 5 \end{pmatrix}\begin{pmatrix} 13 \\ 8 \end{pmatrix} = \begin{pmatrix} 3\times13+9\times8 \\ 14\times13+5\times8 \end{pmatrix} = \begin{pmatrix} 39+72 \\ 182+40 \end{pmatrix} \rightarrow \begin{pmatrix} 7 \\ 14 \end{pmatrix}$$

$$= \begin{pmatrix} 111 \\ 222 \end{pmatrix} = \begin{pmatrix} 7 \\ 14 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 9 \\ 14 & 5 \end{pmatrix}\begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 3\times4+9\times0 \\ 14\times4+5\times0 \end{pmatrix} \rightarrow \begin{pmatrix} 12 \\ 4 \end{pmatrix}$$

$$= \begin{pmatrix} 12 \\ 56 \end{pmatrix} = \begin{pmatrix} 12 \\ 4 \end{pmatrix} \bmod 26$$