Playfair

(1) Pick a keyword
"KNIGHTS"

K	N	I/J	G	H
T	S	A	B	C
D	E	F	L	M
O	P	Q	R	U
V	W	X	Y	Z

MISSISSIPPI

M	I	S	P	

To encrypt:
"TODAYWEENTERED"
(X)

TO → DV (same col more down one spot, with wrap around.)

DA → FT (opposite corners of rectangle - each letter encrypts to a letter on its same row)

YW → ZX (same row more right one spot with wrap around)

EX → FW (rectangle)

EN → PS (same column)

TE → SD (rect)

RE → PL (rect)

col ⇒ up
box ⇒ same

Strategies to cryptanalyze

no double letter pairs in ciphertext.
because of construction, later letters tend to be on bottom row.
Try to make some basic guesses about matching plain ↔ cipher pairs

---

Hill Cipher

Matrix Multiplication

$$\begin{bmatrix} 2 & 6 \\ 9 & 11 \end{bmatrix} \begin{bmatrix} 4 \\ 9 \end{bmatrix} = \begin{bmatrix} 2\times4+6\times9 \\ 9\times4+11\times9 \end{bmatrix}$$

$2\times2 \quad 2\times1$

$= \quad =$

Size of ans

$$= \begin{bmatrix} 8+54 \\ 36+99 \end{bmatrix} = \begin{bmatrix} 62 \\ 135 \end{bmatrix}$$

$X \times Y$

$$A[i][j] = \sum_{k=1}^{n} x[i][k] * y[k][j]$$

$$\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}\begin{bmatrix} 3 & 4 \\ 2 & 6 \end{bmatrix} = \begin{bmatrix} 2\cdot 3+3\cdot 2 & 2\cdot 4+3\cdot 6 \\ 1\cdot 3+4\cdot 2 & 1\cdot 4+4\cdot 6 \end{bmatrix}$$

$$= \begin{bmatrix} 12 & 26 \\ 11 & 28 \end{bmatrix}$$

Hill Cipher

Key square nxn matrix, all entries 0-25.

$K = \begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix}$ Plain = "PAPERS" Cipher = TIRKDM

PA

$$\begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix}\begin{bmatrix} 15 \\ 0 \end{bmatrix} = \begin{bmatrix} 3\times15 + 6\times0 \\ 4\times15 + 7\times0 \end{bmatrix} = \begin{bmatrix} 45 \\ 60 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 19 \\ 8 \end{bmatrix} \boxed{TI}$$

$$\begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix}\begin{bmatrix} 15 \\ 4 \end{bmatrix} = \begin{bmatrix} 3\times15 + 6\times4 \\ 4\times15 + 7\times4 \end{bmatrix} = \begin{bmatrix} 45+24 \\ 60+28 \end{bmatrix} = \begin{bmatrix} 69 \\ 88 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 17 \\ 10 \end{bmatrix} \boxed{RK}$$

$$\begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix}\begin{bmatrix} 17 \\ 18 \end{bmatrix} = \begin{bmatrix} 3\times17 + 6\times18 \\ 4\times17 + 7\times18 \end{bmatrix}$$

$$= \begin{bmatrix} 51 + 108 \\ 68 + 126 \end{bmatrix} = \begin{bmatrix} 159 \\ 194 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3 \\ 12 \end{bmatrix} \boxed{DM}$$

First cipher where multiple plaintext letters affect ciphertext in a significant way.

M^{-1} M

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\left(\begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix}\begin{bmatrix} P_1 \\ P_2 \end{bmatrix}\right) = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

In general our goal is find w, x, y, z such that → are known

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

$$wa + xc = 1 \pmod{26}$$
$$ya + zc = 0 \pmod{26}$$
$$wb + xd = 0 \pmod{26}$$

Determinant

Inverse exists iff $\gcd(ad-bc, 26) = 1$

d $\quad wa + xc \equiv 1 \pmod{26}$

$-c$ $\quad wb + xd \equiv 0 \pmod{26}$

$$wad + xcd \equiv d \pmod{26}$$
$$-wbc - xcd \equiv 0 \pmod{26}$$

$$w(ad-bc) \equiv d \pmod{26}$$

$$w \equiv (ad-bc)^{-1} \cdot d \pmod{26}$$

$$x \equiv (ad-bc)^{-1} \cdot (-b) \pmod{26}$$

$y \equiv (ad-bc)^{-1}(-c) \bmod 26$

$z \equiv (ad-bc)^{-1}(a) \bmod 26$

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

$$M = \begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix} \quad \det(m) = 3\times 7 - 4\times 6$$

$$= -3 \bmod 26$$

$$\equiv 23 \bmod 26$$

$$23^{-1} \bmod 26 = \boxed{17}$$

$$M^{-1} = 17 \begin{bmatrix} 7 & -6 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 119 & -102 \\ -68 & 51 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 2 \\ 10 & 25 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 6 \\ 4 & 7 \end{bmatrix}\begin{bmatrix} 15 & 2 \\ 10 & 25 \end{bmatrix} = \begin{bmatrix} 3\times 15 + 6\times 10 & 3\times 2 + 6\times 25 \\ 4\times 15 + 7\times 10 & 4\times 2 + 7\times 25 \end{bmatrix}$$

$$= \begin{bmatrix} 105 & 156 \\ 130 & 183 \end{bmatrix}$$

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

$$\begin{bmatrix} 15 & 2 \\ 10 & 25 \end{bmatrix}\begin{bmatrix} 19 \\ 8 \end{bmatrix} = \begin{bmatrix} 15\times 19 + 2\times 8 \\ 10\times 19 + 25\times 8 \end{bmatrix}$$

$$= \begin{bmatrix} 285+16 \\ 190+200 \end{bmatrix} = \begin{bmatrix} 301 \\ 390 \end{bmatrix}$$

$$= \begin{bmatrix} 15 \\ 0 \end{bmatrix} \begin{matrix} P \\ A \end{matrix}$$

$\leq 26^4$