CIS 3362 9/11/24

(1) Finish Hill

(2) Start ADFGVX

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

Inverse matrix (corresponding dec key

$$M \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$$

$$M^{-1} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

$$\left(M^{-1} M \right) \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

$$M^{-1} \times M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 1 \times P_1 + 0 \times P_2 \\ 0 \times P_1 + 1 \times P_2 \end{pmatrix} = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

Identity Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$ row1: $\begin{pmatrix} d & -b \end{pmatrix}$ row2: $\begin{pmatrix} -c & a \end{pmatrix}$ col1: $\begin{pmatrix} a \\ c \end{pmatrix}$ col2: $\begin{pmatrix} b \\ d \end{pmatrix}$

$2 \times 2 \quad 2 \times 2$

$$= \begin{pmatrix} ad-bc & bd-bd \\ -ac+ac & -bc+ad \end{pmatrix}$$

$$= \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

$$(ad-bc)^{-1} \bmod 26 \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} V$$

(ad-bc): Determinant

easily scales to larger "block sizes".

In modern ciphers, they usually now give directions to extend the keysize if necessary.

AES → 128 bit → 192 bits → 256 bits

One other idea about Hill

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 4a+0b \\ 4c+0d \end{pmatrix} = \begin{pmatrix} 12 \\ 14 \end{pmatrix} \bmod 26$$

cipher — plain

In theory 2 pairs of matching plain/cipher text will give you a total of 4 equations:

$4a \equiv 12 \bmod 26$] 2 solution valid

$4c \equiv 14 \bmod 26$] 2 solution valid

2 with a and b } If you're lucky these equations
2 with c and d } will have a unique sol.

$4a \equiv 12 \mod 26$

$\Rightarrow 26 \mid (4a-12)$ def mod

$4a-12 = 26n, \quad n \in \mathbb{Z}$ (integer)

$2a-6 = 13n \Rightarrow 13 \mid (2a-6)$

$\Rightarrow 2a \equiv 6 \mod 13$

$a \equiv 3 \mod 13$

$a \equiv 3$ or $16 \mod 26$

$4c \equiv 14 \pmod{26}$

$26 \mid (4c-14)$

$4c-14 = 26n$

$2c-7 = 13n$

$2c \equiv 7 \mod 13$

$7(2c) \equiv 7(7) \mod 13$

$c \equiv 49 \equiv 10 \mod 13$

$c \equiv 10$ or $23 \mod 26$

ADFGVX

Cipher Germans used during WWI.

Initially it was ADFGX.

ADFGVX are the only letters in the ciphertext. They were chosen because they are less likely to be confused for each other when transmitted as Morse code.

A = ·—

G = ——·

F = ··—·

D = —··

X = —··—

V = ···—

R\C	A	D	F	G	V	X
A	~~0~~	O	H	9	T	A
D	E	C	W	Z	V	5
F	R	8	4	G	2	1
G	K	J	U	X	P	Y
V	6	S	B	N	D	Q
X	F	3	M	I	7	L

→ KEY

map char → loc

Plain: GOKNIGHTS2024

Step 1: FG AD GA VG FG FF

Use grid, for each char, find its row label and col label and write text down in order.

Step 2: Second key (key word) used for transposition cipher.

K	E	Y	W	O	R	D
3	2	7	6	4	5	1
F	G	A	D	G	A	V
G	X	G	F	G	A	F
A	V	V	D	F	V	~~A~~
A	F	F				

~~A~~ for repeated PAPER (3 1 4 2 5) letters

Ciphertext: VFAGXVFFGAAGGFAAVDFOAGVF

read columns down in order

c1 c2 c3 c4 c5 c6 c7

CLAUDE SHANNON

CONFUSION + DIFFUSION

(1) SUBSTITUTE

(2) MOVE AROUND