

Hill Cipher

evolution of ideas after Vigenere

- key for modern ciphers
- 1) Playfair - digraph easy to do by hand
 - 2) Transposition - really moving things around
 - 3) Compound Cipher w/ multiple stages
 - 4) ADFGVX $\nearrow$ uses both

5) Hill - localized and still still working w/ blocks, but extendable beyond digraphs.

Uses ^{square} matrices

Plain: KU|CF

$$\begin{pmatrix} 3 & 2 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 10 \\ 20 \end{pmatrix} = \begin{pmatrix} 3 \times 10 + 2 \times 20 \\ 5 \times 10 + 9 \times 20 \end{pmatrix} \pmod{26}$$

$$\begin{matrix} \text{key} & \text{plain} \end{matrix} = \begin{pmatrix} 30 + 2(-6) \\ 50 - 9 \times 6 \end{pmatrix} = \begin{pmatrix} 18 \\ -4 \end{pmatrix} = \begin{pmatrix} 18 \\ 22 \end{pmatrix} \begin{matrix} S \\ W \end{matrix}$$

$$\begin{pmatrix} 3 & 2 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 \times 2 + 2 \times 5 \\ 5 \times 2 + 9 \times 5 \end{pmatrix} = \begin{pmatrix} 16 \\ 55 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 3 \end{pmatrix} \begin{matrix} Q \\ D \end{matrix}$$

Add Matrices

$$\begin{pmatrix} \textcircled{1} & 2 \\ 3 & \boxed{4} \end{pmatrix} + \begin{pmatrix} \textcircled{6} & 9 \\ 2 & \boxed{3} \end{pmatrix} = \begin{pmatrix} 7 & 11 \\ 5 & 7 \end{pmatrix}$$

$2 \times 2 \qquad \qquad 2 \times 2 \qquad \qquad 2 \times 2$

$$\text{res}[i][j] = a[i][j] + b[i][j]$$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} - \begin{pmatrix} 6 & 9 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} -5 & -7 \\ 1 & 1 \end{pmatrix}$$

$$\text{res}[i][j] = a[i][j] - b[i][j]$$

row $\times$ col

$$\begin{pmatrix} \textcircled{1} & 2 \\ \boxed{3} & 4 \end{pmatrix} \begin{pmatrix} \textcircled{6} \\ \textcircled{11} \end{pmatrix} = \begin{pmatrix} 1 \times 6 + 2 \times 11 \\ 3 \times 6 + 4 \times 11 \end{pmatrix} = \begin{pmatrix} 28 \\ 62 \end{pmatrix}$$

$2 \times 2 \quad 2 \times 1 \quad \rightarrow \quad 2 \times 1 \quad 18$
 44

$$\begin{pmatrix} \textcircled{2} & 1 & 0 \\ \textcircled{-2} & -1 & 5 \\ 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \times 4 + 1 \times 2 + 0 \times 3 \\ -2 \times 4 + (-1) \times 2 + 5 \times 3 \\ 4 \times 4 + 1 \times 2 + 3 \times 3 \end{pmatrix}$$

$$= \begin{pmatrix} 10 \\ 5 \\ 27 \end{pmatrix}$$

M 's inverse is M^{-1} such that

$$M \times M^{-1} = I \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{cases} a_{[i][i]} = 1 \\ a_{[i][j]} = 0 \text{ if } i \neq j. \end{cases}$$

$I \times M = M$, that's why it's the identity matrix.

$$M = \begin{pmatrix} 3 & 2 \\ 5 & 9 \end{pmatrix}, \text{ What is } M^{-1}?$$

How to find?

When does M^{-1} exist???

(under mod) exists if and only if

$$\gcd(\det(M), 26) = 1.$$

← ALPHASIZE

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d - b \cdot c$$

$$\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh - gec - hfa - idb$$

Diagram illustrating the expansion of a 3x3 determinant using the rule of Sarrus. The first three columns are repeated to the right, forming a 3x5 grid of elements. Arrows indicate the positive terms (down-right diagonals) and negative terms (down-left diagonals).

Work to find inverse $\begin{pmatrix} 3 & 2 \\ 5 & 9 \end{pmatrix}$

$$\begin{array}{ccc|cc} 5 \times & 3 & 2 & : & 1 & 0 \\ 3 \times & 5 & 9 & : & 0 & 1 \end{array}$$

$$\rightarrow \begin{array}{ccc|cc} & 15 & 10 & : & 5 & 0 \\ - & 15 & 27 & : & 0 & 3 \end{array}$$

$$\begin{array}{ccc|cc} & 0 & -17 & : & 5 & -3 \\ & 0 & 17 & : & -5 & 3 \end{array}$$

New eqn

$$\begin{array}{ccc|cc} & 3 & 2 & : & 1 & 0 \\ & 0 & 17 & : & -5 & 3 \end{array}$$

mult 17^{-1}
= -3

$$\rightarrow \begin{array}{ccc|cc} & 0 & -51 & : & 15 & -9 \\ & 0 & 1 & : & 15 & -9 \end{array}$$

New eqn

$$\begin{array}{ccc|cc} & 3 & 2 & : & 1 & 0 \\ & 0 & 1 & : & 15 & -9 \end{array}$$

mult 2

$$\rightarrow \begin{array}{ccc|cc} & 0 & 2 & : & 30 & -18 \\ & 0 & 2 & : & 4 & 8 \end{array}$$

$$\begin{array}{ccc|cc} & 3 & 2 & : & 1 & 0 \\ - & 0 & 2 & : & 4 & 8 \end{array}$$

$$\begin{array}{ccc|cc} & 3 & 0 & : & -3 & -8 \end{array}$$

new eqn

$$\begin{array}{ccc|cc} & 3 & 0 & : & -3 & -8 \\ & 0 & 1 & : & 15 & -9 \end{array}$$

$$\begin{array}{ccc|cc} & 27 & 0 & : & -27 & -72 \\ & 0 & 1 & : & 15 & -9 \end{array}$$

$$\begin{array}{ccc|cc} & 1 & 0 & : & 25 & 6 \\ & 0 & 1 & : & 15 & 17 \end{array}$$

Is inverse!

Work to find inverse $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$:

$$\begin{array}{l} Cx \\ Cx \end{array} \begin{bmatrix} a & b & : & 1 & 0 \\ c & d & : & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} ac & bc & : & c & 0 \\ -ac & ad & : & 0 & a \end{bmatrix}$$

$$\times (-1) \quad 0 \quad bc-ad \quad c \quad -a$$

$$0 \quad (ad-bc) \quad -c \quad a$$

New eqn, let $m = ad-bc$

$$\begin{array}{l} \text{mult} \\ m^{-1} \end{array} \begin{bmatrix} a & b & : & 1 & 0 \\ 0 & m & : & -c & a \end{bmatrix}$$

New eqn

$$\begin{array}{l} \text{mult} \\ b \end{array} \begin{bmatrix} a & b & 1 & 0 \\ 0 & 1 & -cm^{-1} & am^{-1} \end{bmatrix}$$

$$a \quad b \quad 1 \quad 0$$

$$- \quad 0 \quad b \quad -bcm^{-1} \quad abm^{-1}$$

$$a \quad 0 \quad 1+bcm^{-1} \quad -abm^{-1}$$

new eqn

$$\begin{array}{l} \text{mult} \\ a^{-1} \end{array} \begin{bmatrix} a & 0 & 1+bcm^{-1} & -abm^{-1} \\ 0 & 1 & -cm^{-1} & am^{-1} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & : & +a^{-1}+a^{-1}bcm^{-1} & -bm^{-1} \\ 0 & 1 & : & -cm^{-1} & am^{-1} \end{bmatrix}$$

So this does
have 3 correct
entries:

$$m^{-1} \begin{bmatrix} ? & -b \\ -c & a \end{bmatrix}$$

My guess is that
a different method
shows that

$$a^{-1} + a^{-1}bcm^{-1} \equiv dm^{-1}$$

$$M = \begin{pmatrix} 3 & 2 \\ 5 & 9 \end{pmatrix}$$

$$= (17^{-1} \bmod 26) \begin{pmatrix} 9 & -2 \\ -5 & 3 \end{pmatrix}$$

$$= 23 \begin{pmatrix} 9 & -2 \\ -5 & 3 \end{pmatrix} \bmod 26$$

$$= -3 \begin{pmatrix} 9 & -2 \\ -5 & 3 \end{pmatrix} = \begin{pmatrix} -27 & 6 \\ 15 & -9 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 25 & 6 \\ 15 & 17 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 2 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 25 & 6 \\ 15 & 17 \end{pmatrix} = \begin{pmatrix} 3 \times 25 + 2 \times 15 & \boxed{3 \times 6 + 2 \times 17} \\ 5 \times 25 + 9 \times 15 & \boxed{5 \times 6 + 9 \times 17} \end{pmatrix}$$

$$= \begin{pmatrix} 75 + 30 & 18 + 34 \\ 125 + 135 & 30 + 153 \end{pmatrix}$$

$$= \begin{pmatrix} 105 & 52 \\ 260 & 183 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\bmod 26$$

$$\begin{aligned} 18a + 22b &\equiv 10 \pmod{26} \\ 16a + 3b &\equiv 2 \pmod{26} \end{aligned}$$

$$18a + 22b = 10 + 26n$$

$$9a + 11b = 5 + 13n$$

$$144a + 27b \equiv 18 \pmod{26}$$

$$4 \quad 14a + b \equiv 18 \pmod{26}$$

$$56a + 4b \equiv 72 \pmod{26}$$

$$4a + 4b \equiv 20 \pmod{26}$$

$$\rightarrow 18a + 22b \equiv 10 \pmod{26}$$

$$22a + 26b \equiv 30 \pmod{26}$$

$$22a \equiv 30 \pmod{26}$$

$$22a \equiv 4 \pmod{26}$$

$$\frac{22a}{2} = \frac{4}{2} + \frac{26n}{2}$$

$$11a = 2 + 13n$$

$$11a \equiv 2 \pmod{13}$$

$$\text{if } X \equiv Y \pmod{Z}$$

$$\text{and } d \mid X \wedge d \mid Y \wedge d \mid Z$$

$$\text{then } \frac{X}{d} \equiv \frac{Y}{d} \pmod{\frac{Z}{d}}$$

$$6 \cdot 11a \equiv 6 \cdot 2 \pmod{13}$$

$$a \equiv 12 \pmod{13} \rightarrow \boxed{12 \text{ or } 25}$$

$$16a + 3b \equiv 2 \pmod{26}$$

$$16 \times 12 + 3b \equiv 2 \pmod{26}$$

$$10 \text{ } \cancel{192} + 3b \equiv 2 \pmod{26}$$

$$9 \cdot 3b \equiv \cancel{10} \cdot 9 \pmod{26}$$

$$b \equiv \cancel{10} \cdot 9 \pmod{26}$$

$$-72$$

$$6$$

$$\begin{aligned} \text{if } a &= 12 \\ b &= \cancel{14} 6 \end{aligned}$$

$$\begin{aligned} 130 \\ 52 \end{aligned}$$

SW

$$\begin{pmatrix} 25 & 6 \\ 15 & 17 \end{pmatrix} \begin{pmatrix} 18 \\ 22 \end{pmatrix} = \begin{pmatrix} -1 & 6 \\ 15 & -9 \end{pmatrix} \begin{pmatrix} -8 \\ -4 \end{pmatrix}$$

$$= \begin{pmatrix} -1 \times (-8) + 6(-4) \\ 15 \times (-8) + (-9)(-4) \end{pmatrix}$$

$$= \begin{pmatrix} 8 - 24 \\ -120 + 36 \end{pmatrix}$$

$$= \begin{pmatrix} -16 \\ 10 + 10 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix} \begin{matrix} K \\ U \end{matrix}$$

Received ciphertext SWQD
and you think it maps to KUCF

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 18 \\ 22 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 16 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

$$\begin{aligned} 18a + 22b &\equiv 10 \pmod{26} \\ 18c + 22d &\equiv 20 \pmod{26} \\ 16a + 3b &\equiv 2 \pmod{26} \\ 16c + 3d &\equiv 5 \pmod{26} \end{aligned}$$

$\swarrow$ $\nwarrow$
 a, b c, d

$$\text{if } a=25, \\ b=6$$

$$16a + 3b \equiv 2 \pmod{26}$$

$$16(-1) + 3b \equiv 2 \pmod{26}$$

$$3b \equiv 18 \pmod{26}$$

$$9 \cdot 3b \equiv 10 \cdot 9 \pmod{26}$$

$$b \equiv 90 \pmod{26}$$

$$\cancel{12}$$

$$b \equiv 6 \pmod{26}$$

Note: Regardless of whether $a=12$ or $a=25$, we find $b=6$ is the only option.

Now do

$$9 \times \begin{cases} 18c + 22d \equiv 20 \pmod{26} \\ 16c + 3d \equiv 5 \pmod{26} \end{cases}$$

$$144c + 27d \equiv 45 \pmod{26}$$

$$4 \times \quad 14c + d \equiv 19 \pmod{26}$$

$$56c + 4d \equiv 76 \pmod{26}$$

$$4c + 4d \equiv -2 \pmod{26}$$

$$\rightarrow 18c + 22d \equiv 20 \pmod{26}$$

$$22c \equiv 18 \pmod{26}$$

$$6 \cdot 11c \equiv 9 \cdot 6 \pmod{13}$$

$$c \equiv 54 \equiv 2 \pmod{13}$$

$$c = 2 \text{ or } 15$$

Thus

$$d \equiv 17 \pmod{26}$$

$$16(2) + 3d \equiv 5 \pmod{26}$$

$$3d \equiv -27 \pmod{26}$$

$$9(3d) \equiv 9(-1) \pmod{26}$$

$$d \equiv -9 \equiv 17 \pmod{26}$$

FOUR
POSSIBLE
ANSWERS

$$\begin{pmatrix} 12 & 6 \\ 2 & 17 \end{pmatrix}$$

or

$$\begin{pmatrix} 12 & 6 \\ 15 & 17 \end{pmatrix}$$

or

$$\begin{pmatrix} 25 & 6 \\ 2 & 17 \end{pmatrix}$$

or

$$* \begin{pmatrix} 25 & 6 \\ 15 & 17 \end{pmatrix}$$