

Hill Cipher

1st major cipher that really deals with blocks of data, beyond 2 characters.

based on matrix mult. (Square matrices)

$$\begin{matrix} n \times n & n \times 1 & n \times 1 \\ \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} & \begin{bmatrix} 6 \\ 4 \end{bmatrix} & = \begin{bmatrix} 3 \times 6 + 5 \times 4 \\ 2 \times 6 + 7 \times 4 \end{bmatrix} = \begin{bmatrix} 18 + 20 \\ 12 + 28 \end{bmatrix} = \begin{bmatrix} 38 \\ 40 \end{bmatrix} \end{matrix}$$

Key $\nearrow$

$\leftarrow$ HELLOX $\leftarrow$ Block size = 2

7, 4 || 11, 14, 23

$$\begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \cdot 7 + 5 \cdot 4 \\ 2 \cdot 7 + 7 \cdot 4 \end{bmatrix} = \begin{bmatrix} 41 \\ 42 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 16 \end{bmatrix} \pmod{26}$$

PQ

$$\begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 14 \\ 23 \end{bmatrix} \equiv \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 14 \\ -3 \end{bmatrix} = \begin{bmatrix} 3 \cdot 14 + 5(-3) \\ 2 \cdot 14 + 7(-3) \end{bmatrix} = \begin{bmatrix} 42 - 15 \\ 28 - 21 \end{bmatrix}$$

$$= \begin{bmatrix} 27 \\ 7 \end{bmatrix} \pmod{26} \rightarrow \begin{bmatrix} 1 \\ 7 \end{bmatrix} \text{ BH}$$

"CAT"

$$\begin{bmatrix} 2 & 1 & 0 \\ 3 & 1 & 5 \\ 4 & 2 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 19 \end{bmatrix} = \begin{bmatrix} 2 \cdot 2 + 1 \cdot 0 + 0 \cdot 19 \\ 3 \cdot 2 + 1 \cdot 0 + 5 \cdot 19 \\ 4 \cdot 2 + 2 \cdot 0 + 6 \cdot 19 \end{bmatrix} = \begin{bmatrix} 4 \\ 101 \\ 122 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 4 \\ 23 \\ 18 \end{bmatrix} \pmod{26} \rightarrow \begin{bmatrix} 4 \\ 23 \\ 18 \end{bmatrix} \text{ EXS}$$

3x3

How do I undo this?

9/23/19 (2)

Which ~~potenti~~ matrices are valid keys?

$$\begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} \quad \text{encrypt}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} \quad \text{decrypt}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} \quad \checkmark \quad (\text{known})$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

$$3a + 2b \equiv 1 \pmod{26} \quad \left. \begin{array}{l} 3a + 2b \equiv 1 \pmod{26} \\ 5a + 7b \equiv 0 \pmod{26} \end{array} \right\} \text{top row}$$

$$5a + 7b \equiv 0 \pmod{26}$$

$$3c + 2d \equiv 0 \pmod{26} \quad \left. \begin{array}{l} 3c + 2d \equiv 0 \pmod{26} \\ 5c + 7d \equiv 1 \pmod{26} \end{array} \right\} \text{bottom row}$$

$$5c + 7d \equiv 1 \pmod{26}$$

if orig matrix is $\begin{bmatrix} w & x \\ y & z \end{bmatrix}$

Inverse mat is $(wz - xy)^{-1} \pmod{26} \begin{bmatrix} z & -x \\ -y & w \end{bmatrix}$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \nearrow$$

$$\text{cur max} = \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} \text{inv} = (21 - 10)^{-1} \pmod{26} \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix}$$

$$\begin{aligned} &= (11^{-1} \pmod{26}) \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix} \\ &= 19 \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix} \\ &= -7 \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} -49 & 35 \\ 14 & -21 \end{bmatrix} \\ &\equiv \begin{bmatrix} 3 & 9 \\ 14 & 5 \end{bmatrix} \end{aligned}$$

9/23/19 (3)

$$\begin{bmatrix} 3 & 9 \\ 14 & 5 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 3 \cdot 3 + 9 \cdot 2 & 3 \cdot 5 + 9 \cdot 7 \\ 14 \cdot 3 + 5 \cdot 2 & 14 \cdot 5 + 5 \cdot 7 \end{bmatrix}$$

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

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

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

This exists IFF
 $\gcd(\text{Determinant}, 26) = 1$

* Under mod, the inverse of a matrix exists iff $\gcd(\det(m), \text{modulus}) = 1$.

~~Inv $\begin{bmatrix} 3 & 5 \\ 7 & 8 \end{bmatrix} = (-\frac{11}{4}) \pmod{26} \begin{bmatrix} 8 & -5 \\ -7 & 3 \end{bmatrix}$~~

$17^{-1} \pmod{26}$

(23)

$24 - 35$

49

~~$(-11)(9) \pmod{26}$~~

~~$(-11)^{-1} \pmod{26} =$~~

~~$\begin{bmatrix} 8 & -5 \\ -7 & 3 \end{bmatrix} \equiv \begin{bmatrix} -24 & 15 \\ 21 & -9 \end{bmatrix}$~~

$\equiv \begin{bmatrix} 2 & 15 \\ 21 & 17 \end{bmatrix}$

$$\text{inv}\left(\begin{bmatrix} 3 & 5 \\ 7 & 8 \end{bmatrix}\right) \equiv (3 \cdot 8 - 5 \cdot 7)^{-1} \bmod 26 \begin{bmatrix} 8 & -5 \\ -7 & 3 \end{bmatrix}$$

$$\equiv (-11)^{-1} \bmod 26 \begin{bmatrix} 8 & -5 \\ -7 & 3 \end{bmatrix}$$

$$\equiv 15^{-1} \bmod 26 \begin{bmatrix} 8 & -5 \\ -7 & 3 \end{bmatrix}$$

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

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

$$\equiv \boxed{\begin{bmatrix} 4 & 17 \\ 3 & 21 \end{bmatrix} \bmod 26}$$