UNIT I

Introduction: Basic Terminology

HILL CIPHER

- The Hill Cipher was invented by Lester S. Hill in 1929
- The Hill Cipher based on linear algebra
- Encryption
  - 2 x 2 Matrix Encryption
  - 3 x 3 Matrix Encryption

HILL CIPHER

- square matrix M by the equation $MM^{-1} = M^{-1}M = I$, where I is the identity matrix.

- C = P*K mod 26

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example

- Example of Key 2 x 2
- $K = \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$
- plaintext message "short example"
- $P =$ short example
- $P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$

Example

- $P = \binom{S}{h}\binom{o}{r}\binom{t}{e}\binom{x}{a}\binom{m}{p}\binom{l}{e} = \binom{18}{7}\binom{14}{17}\binom{19}{4}\binom{23}{0}\binom{12}{15}\binom{11}{4}$
- $C = K * P \ mod\ 26$
- $\begin{bmatrix} k_0 & k_1 \\ k_2 & k_3 \end{bmatrix} * \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} k_0 * p_0 + k_1 * p_1 \\ k_2 * p_0 + k_3 * p_1 \end{bmatrix}$
- $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} * \begin{bmatrix} 18 \\ 7 \end{bmatrix} = \begin{bmatrix} 7 * 18 + 8 * 7 \\ 11 * 18 + 11 * 7 \end{bmatrix} = \begin{bmatrix} 182 \\ 275 \end{bmatrix}$
- $C = \begin{bmatrix} 182 \\ 275 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} a \\ p \end{bmatrix}$

Example

- $P = \binom{S}{h}\binom{o}{r}\binom{t}{e}\binom{x}{a}\binom{m}{p}\binom{l}{e} = \binom{18}{7}\binom{14}{17}\binom{19}{4}\binom{23}{0}\binom{12}{15}\binom{11}{4}$

$$\begin{pmatrix}7 & 8\\11 & 11\end{pmatrix}\binom{14}{17}$$

$$7 \times 14 + 8 \times 17 = 234$$

$$11 \times 14 + 11 \times 17 = 341$$

$$\begin{pmatrix}7 & 8\\11 & 11\end{pmatrix}\binom{14}{17} = \binom{234}{341}$$

$$\begin{pmatrix}7 & 8\\11 & 11\end{pmatrix}\binom{14}{17} = \binom{234}{341} = \binom{0}{3} \; mod\ 26$$

$$\begin{pmatrix}H & I\\L & L\end{pmatrix}\binom{o}{r} = \begin{pmatrix}7 & 8\\11 & 11\end{pmatrix}\binom{14}{17} = \binom{234}{341} = \binom{0}{3} \; mod\ 26 = \binom{A}{D}$$

Example

- $P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix}$$

$$7 \times 19 + 8 \times 4 = 165$$

$$11 \times 19 + 11 \times 4 = 253$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix} = \begin{pmatrix} 9 \\ 19 \end{pmatrix} \mod 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix} = \begin{pmatrix} 9 \\ 19 \end{pmatrix} \mod 26 = \begin{pmatrix} J \\ T \end{pmatrix}$$

Example

- $P = \binom{S}{h}\binom{o}{r}\binom{t}{e}\binom{x}{a}\binom{m}{p}\binom{l}{e} = \binom{18}{7}\binom{14}{17}\binom{19}{4}\binom{23}{0}\binom{12}{15}\binom{11}{4}$

$$\begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}\binom{23}{0}$$

$$7 \times 23 + 8 \times 0 = 161$$

$$11 \times 23 + 11 \times 0 = 253$$

$$\begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}\binom{23}{0} = \binom{161}{253}$$

$$\begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}\binom{23}{0} = \binom{161}{253} = \binom{5}{19}\ mod\ 26$$

$$\begin{pmatrix}H & I\\ L & L\end{pmatrix}\binom{x}{a} = \begin{pmatrix}7 & 8\\ 11 & 11\end{pmatrix}\binom{23}{0} = \binom{161}{253} = \binom{5}{19}\ mod\ 26 = \binom{F}{T}$$

Example

- $P = \binom{S}{h}\binom{o}{r}\binom{t}{e}\binom{x}{a}\binom{m}{p}\binom{l}{e} = \binom{18}{7}\binom{14}{17}\binom{19}{4}\binom{23}{0}\binom{12}{15}\binom{11}{4}$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\binom{12}{15}$$

$$7 \times 12 + 8 \times 15 = 204$$

$$11 \times 12 + 11 \times 15 = 297$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\binom{12}{15} = \binom{204}{297}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\binom{12}{15} = \binom{204}{297} = \binom{22}{11} \; mod\ 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}\binom{m}{p} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}\binom{12}{15} = \binom{204}{297} = \binom{22}{11} \; mod\ 26 = \binom{W}{L}$$

Example

- $P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$7 \times 11 + 8 \times 4 = 109$$

$$11 \times 11 + 11 \times 4 = 165$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \ mod\ 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \ mod\ 26 = \begin{pmatrix} F \\ J \end{pmatrix}$$

Example

- $C = \binom{a}{p}\binom{a}{d}\binom{j}{t}\binom{f}{t}\binom{w}{l}\binom{f}{j}$
- This gives us a final ciphertext of "APADJ TFTWLFJ"

DECRYPTION

- $C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix}$
- This gives us a final ciphertext of "APADJ TFTWLFJ"
- $K = \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$
- We want to find K^{-1}

Example

- Step 1 $-$ *Find the Multiplicative Inverse of the Determinant*
  - $D(K) = 7 * 11 - 8 * 11 = -11 \ mod \ 26 = 15$
  - $DD^{-1} = 1 \ mod \ 26 = 15 * D^{-1}$
  - $15 * D^{-1} mod \ 26 = 1$
  - Try and Test $1 \ mod \ 26 = 105$
  - 105 mod 26 =1
  - $D^{-1} = 7$

Example

- *Step 2 — Find the Adjugate Matrix of Key*
  - $adj\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
  - $adj\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$

- *Step 3 Multiply the Multiplicative Inverse of the Determinant by the Adjugate Matrix*

- $7 * \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 105 & 49 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} = K^{-1}$

Example

- $C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$

$$\begin{aligned}
\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ P \end{pmatrix} &= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 15 \end{pmatrix} \\
&= \begin{pmatrix} 25 \times 0 + 22 \times 15 \\ 1 \times 0 + 23 \times 15 \end{pmatrix} \\
&= \begin{pmatrix} 330 \\ 345 \end{pmatrix} \\
&= \begin{pmatrix} 18 \\ 7 \end{pmatrix} \, mod\ 26 \\
&= \begin{pmatrix} s \\ h \end{pmatrix}
\end{aligned}$$

Example

- $C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ D \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 0 + 22 \times 3 \\ 1 \times 0 + 23 \times 3 \end{pmatrix}$$

$$= \begin{pmatrix} 66 \\ 69 \end{pmatrix}$$

$$= \begin{pmatrix} 14 \\ 17 \end{pmatrix} \, mod \; 26$$

$$= \begin{pmatrix} o \\ r \end{pmatrix}$$

Example

- $C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} J \\ T \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 9 + 22 \times 19 \\ 1 \times 9 + 23 \times 19 \end{pmatrix}$$

$$= \begin{pmatrix} 643 \\ 446 \end{pmatrix}$$

$$= \begin{pmatrix} 19 \\ 4 \end{pmatrix} \; mod\ 26$$

$$= \begin{pmatrix} t \\ e \end{pmatrix}$$

Example

- $C = \binom{a}{p}\binom{a}{d}\binom{j}{t}\binom{f}{t}\binom{w}{l}\binom{f}{j} = \binom{0}{15}\binom{0}{3}\binom{9}{19}\binom{5}{19}\binom{22}{11}\binom{5}{9}$

$$\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}F\\ T\end{pmatrix} = \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}5\\ 19\end{pmatrix}$$

$$= \begin{pmatrix}25 \times 5 + 22 \times 19\\ 1 \times 5 + 23 \times 19\end{pmatrix}$$

$$= \begin{pmatrix}543\\ 442\end{pmatrix}$$

$$= \begin{pmatrix}23\\ 0\end{pmatrix} \; mod\ 26$$

$$= \begin{pmatrix}x\\ a\end{pmatrix}$$

Example

- $C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} W \\ L \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 22 + 22 \times 11 \\ 1 \times 22 + 23 \times 11 \end{pmatrix}$$

$$= \begin{pmatrix} 792 \\ 275 \end{pmatrix}$$

$$= \begin{pmatrix} 12 \\ 15 \end{pmatrix} \; mod\ 26$$

$$= \begin{pmatrix} m \\ p \end{pmatrix}$$

Example

- $C = \binom{a}{p}\binom{a}{d}\binom{j}{t}\binom{f}{t}\binom{w}{l}\binom{f}{j} = \binom{0}{15}\binom{0}{3}\binom{9}{19}\binom{5}{19}\binom{22}{11}\binom{5}{9}$

$$\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\binom{F}{J} = \begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\binom{5}{9}$$

$$= \begin{pmatrix}25\times 5 + 22\times 9\\ 1\times 5 + 23\times 9\end{pmatrix}$$

$$= \binom{323}{212}$$

$$= \binom{11}{4}\ mod\ 26$$

$$= \binom{l}{e}$$

Example

- Using Hill Cipher how to implement 3x3 matrix encryption ? The key for a hill cipher is a matrix

$$\text{e.g. } \boldsymbol{k} = \begin{matrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{matrix}$$ and **message**= ATTACK AT DAWN

Thank You