

# Network and Information Security

## Lecture 11

B.Tech. Computer Engineering  
Sem. VI.

Prof. Mrudang T. Mehta  
Associate Professor  
Computer Engineering Department  
Faculty of Technology,  
Dharmsinh Desai University, Nadiad

# Hill Cipher

- Polyalphabetic cipher
- Invented by Lester S. Hill
- The plain text is divided into equal-size blocks.
- The blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block.
- For this reason, the Hill cipher belongs to a category of ciphers called block ciphers.

- In a Hill cipher, the key is a square matrix of size  $m \times m$  in which  $m$  is the size of the block.
- If we call the key matrix  $K$ , each element of the matrix is  $K_{i,j}$

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

- How one block of the ciphertext is encrypted.
- If we call the  $m$  characters in the plaintext block  $P_1, P_2, \dots, P_m$ , the corresponding characters in the cipher text block are  $C_1, C_2, \dots, C_m$ .

$$C_1 = P_1 K_{11} + P_2 K_{21} + \dots + P_m K_{m1}$$

$$C_2 = P_1 K_{12} + P_2 K_{22} + \dots + P_m K_{m2}$$

$$C_m = P_1 K_{1m} + P_2 K_{2m} + \dots + P_m K_{mm}$$

- Note- Not all square matrices have multiplicative inverse in  $Z_{26}$
- Bob will not be able to decrypt the cipher text sent by Alice if the matrix does not have a multiplicative inverse.

# Example

Plain text: code is ready

Matrix representation of plain text can make 3 x 4 matrix when adding extra bogus character z to the last block and removing the spaces.

$$\begin{pmatrix} c & o & d & e \\ i & s & r & e \\ a & d & y & z \end{pmatrix} \quad \begin{pmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{pmatrix}$$

P

$$\begin{pmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{pmatrix}$$

K

$$\begin{pmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{pmatrix}$$

C

$$\begin{pmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 07 \\ 05 & 08 & 18 & 18 \end{pmatrix}$$

$$C_1 = P_1 K_{11} + P_2 K_{21} + P_3 K_{31} + P_4 K_{41}$$

$$C_1 = (2)(9) + (14)(4) + (3)(2) + (4)(3)$$

$$= 18 + 56 + 6 + 12$$

$$= 92 \bmod 26$$

$$= 14$$



$C_1$	$2*9 + 14*4 + 3*2 + 4*3 = 92 \% 26 = 14$
$C_2$	$2*7 + 14*7 + 3*21 + 4*23 = 267 \% 26 = 7$
$C_3$	$2 * 11 + 14*5 + 3*14 + 4*21 = 10$
$C_4$	$2*13 + 14*6 + 3*9 + 4*8 = 13$
$C_5$	$8*9 + 18*4 + 17*2 + 4*3 = 8$
$C_6$	$8*7 + 18*7 + 17*21 + 4*23 = 7$
$C_7$	$8*11 + 18*5 + 17*14 + 4*21 = 6$
$C_8$	$8*13 + 18*6 + 17*9 + 4*8 = 7$
$C_9$	$0*9 + 3*4 + 24*2 + 25*3 = 5$
$C_{10}$	$0*7 + 3*7 + 24 * 21 + 25*23 = 8$
$C_{11}$	$0*11 + 3*5 + 24*14 + 25*21 = 18$
$C_{12}$	$0*13 + 3*6 + 24*9 + 25*8 = 18$

- Decryption

$$\begin{array}{cccc}
 \left( \begin{array}{cccc} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{array} \right) & = & \left( \begin{array}{cccc} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 07 \\ 05 & 08 & 18 & 18 \end{array} \right) & \left( \begin{array}{cccc} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 03 & 23 & 21 & 08 \end{array} \right) \\
 P & & C & K^{-1}
 \end{array}$$

- $A^{-1} = 1/|A| * \text{adj}(A)$

- Example

- $K = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \quad 2 \times 2$

- $\text{Det}(K) = 2 \times 2 - 1 \times 1 = 4 - 1 = 3$

- $K^{-1} = 1/\text{Det}(K) \text{ adj}(K)$

- $= (3)^{-1} \text{ adj}(K)$

- $(3)^{-1} \bmod 26$

q	r1	r2	r	t1	t2	t
8	26	3	2	0	1	-8
1	3	2	1	1	-8	9
2	2	1	0	-8	9	-26
	1	0		9	-26	

$$(3)^{-1} \bmod 26 = 9$$

$$K^{-1} = 9 * \text{adj}(K)$$

- Cofactor matrix
- Cofactor of  $K_{11}$  [ 2] =  $(-1)^{1+1} \times 2 = 2$
- Cofactor of  $K_{12}$  [ 1] =  $(-1)^{1+2} \times 1 = -1$
- Cofactor of  $K_{21}$  [ 1] =  $(-1)^{2+1} \times 1 = -1$
- Cofactor of  $K_{22}$  [ 2] =  $(-1)^{2+2} \times 2 = 2$

- Cofactor matrix = 
$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

- Adjoint = transpose of cofactor matrix

- $\text{Adj}(K) = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$
- $K^{-1} = 9 * \text{adj}(K) = \begin{pmatrix} 18 & -9 \\ -9 & 18 \end{pmatrix} \pmod{26}$

- $K^{-1} = \begin{pmatrix} 18 & 17 \\ 17 & 18 \end{pmatrix}$

- Encryption

- $C = (P \times K) \bmod 26$

- Plain text = abcd

- Plain text block =  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$

- $C = (P \times K) \bmod 26$

- $\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \times \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}$



- Decryption

- $P = (C \times K^{-1}) \bmod 26$

$$= \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix} \times \begin{pmatrix} 18 & 17 \\ 17 & 18 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 52 & 53 \\ 262 & 263 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$$

$$= P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

# Cryptanalysis

- Brute force is not possible
- Each entry in the matrix can have one of the possible 26 values
- (at first glance)
- Number of keys =  $26^{m * m} = 26^{m^2}$
- Not all of the matrices have multiplicative inverses (Smaller key domain but huge)
- Statistical attack is not possible as one Cipher Text depends on many plain text characters

- Possible attacks
  - Known plain text attack
  - Chosen plain text attack
- $K = (C \times P^{-1}) \bmod 26$
- Eve can choose Invertible  $P$  and can obtain  $C$  using chosen plain text attack
- Using received  $C$  and  $P^{-1}$  , Eve can guess the key.
- Difficulty: Value of  $m$  not known
- Chosen plain text attack is difficult to launch

# One Time Pad Cipher

- Goal of Cryptography is perfect secrecy.
- Shannon - It can be achieved if each plaintext symbol is encrypted with a key randomly chosen from a key domain
- Additive cipher can become a perfect cipher if the key that is used to encrypt each character is chosen randomly from the key domain i.e.  $\{0,1,2,\dots,25\}$
- If the first character is encrypted with key 4, the second character is encrypted with key 2, the third character is encrypted with key 21.

- Invented by Vernam
- The key has the same length as the plain text and is chosen completely in random.
- Difficulty:
- It is a perfect cipher but it is impossible to implement commercially.
- If the key must be newly generated each time, how can Alice tell the new key each time she has a message to send?