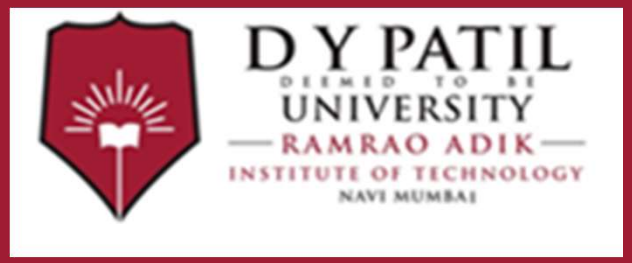


Subject Name: Cryptography and Network Security

Unit No: 01 Unit Name: Introduction to Cryptography

Faculty Name:

Dr. Sangita Chaudhari
Dr.Pallavi Sapkale

Index

Unit No: 1 Unit Name: Introduction & Number Theory

Lecture No: 1
Playfair cipher, Hill cipher

Playfair Cipher

- Playfair Key Matrix
  - A 5X5 matrix of letters based on a keyword
  - fill in letters of keyword
  - fill rest of matrix with other letters
  - eg. using the keyword MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Playfair Cipher

M	O	N	A	R
C	H	Y	B	D
E	G	F	I/J	K
L	P	Q	S	T
U	V	W	X	Z

- Break the plaintext into pairs of two consecutive letters
- If a pair is a repeated letter, insert a filler like 'X‘ in the plaintext.
- If both letters fall in the same row of the key matrix, replace each with the letter to its right (wrapping back to start from end), eg. “AR" encrypts as "RM"
- If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. “MU" encrypts to "CM"
- Otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. “HS” encrypts to “BP”, and “EA” to “IM” or “JM” (as desired)

Playfair Cipher

Encrypt the plaintext "HELLO"

Secret Key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

he → EC lx → QZ lo → BX

Plaintext: hello Ciphertext: ECQZBX

Playfair Cipher

- Example

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

- Plaintext: meet me after the party
  - Make a pair of letters from plaintext

    me et me af te rt he pa rt yx
  - Apply encryption using matrix

    CL KL CL OI LK CF SO DZ BW

  Ciphertext : CLKLCLOILKCFSODZBW

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Security of Playfair Cipher

- Security much improved over monoalphabetic since have 26 x 26 = 676 combinations
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext
- was widely used for many years (eg. US & British military in WW1)
- it can be broken, given a few hundred letters since still has much of plaintext structure

Hill Cipher

- By Lester Hill in 1929.
- Key is matrix
- The key matrix in the Hill cipher needs to have a multiplicative inverse.
- [c]=[p][k] and [p]=[c][k]

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

$$C_1 = P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1}$$
$$C_2 = P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2}$$
$$\cdots$$
$$C_m = P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm}$$

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Hill Cipher

$$k = \begin{bmatrix} 3 & 7 \\ 15 & 12 \end{bmatrix}$$

P= HI = [7 8]

$$c = [7 \;\; 8] * \begin{bmatrix} 3 & 7 \\ 15 & 12 \end{bmatrix} = [11 \;\; 15] = [\, L \;\; P]$$

How to do decryption ?

D Y PATIL DEEMED TO BE UNIVERSITY — RAMRAO ADIK — INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Hill Cipher

- plaintext “code is ready”
- Key Matrix is 4x4
- Make a 3 × 4 matrix when adding extra bogus character “z” to the last block and removing the spaces.
- Ciphertext is “OHKNIHGKLISS”.

$$\underset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} = \underset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} \underset{K}{\begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}}$$

a. Encryption

$$\underset{P}{\begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix}} = \underset{C}{\begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix}} \underset{K^{-1}}{\begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}}$$

b. Decryption

D Y PATIL DEEMED TO BE UNIVERSITY — RAMRAO ADIK — INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Unit No: 1 Unit Name: Introduction & Number Theory

Lecture No: 2
Transposition techniques: keyed and keyless transposition ciphers

Transposition Cipher

- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- A transposition cipher reorders symbols

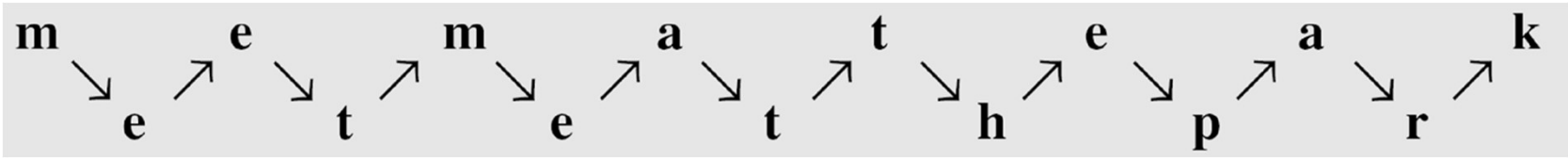
  - Keyless Transposition Ciphers
    - Keyed Transposition Ciphers
    - Combining Two Approaches

Keyless Transposition Ciphers

Simple transposition ciphers, which were used in the past, are keyless.

Rail fence cipher

The ciphertext is created reading the pattern row by row. Plaintext = "Meet me at the park"



Ciphertext = "MEMATEAKETETHPR".

Rail Fence Cipher

m	e	e	t
m	e	a	t
t	h	e	p
a	r	k	

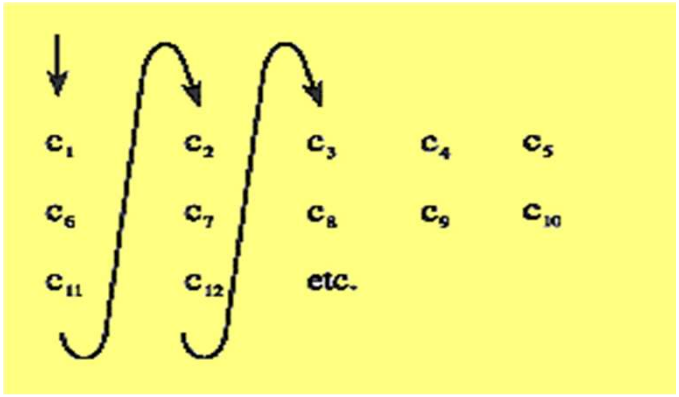
Ciphertext = "MMTAEEHREAEKTTP"

Keyed Transposition Ciphers

- The keyless ciphers permute the characters by using writing plaintext in one way and reading it in another way.
- The permutation is done on the whole plaintext to create the whole ciphertext.
- Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

Columnar Transposition (Keyed)

Plaintext: THIS IS CNS
CLASS

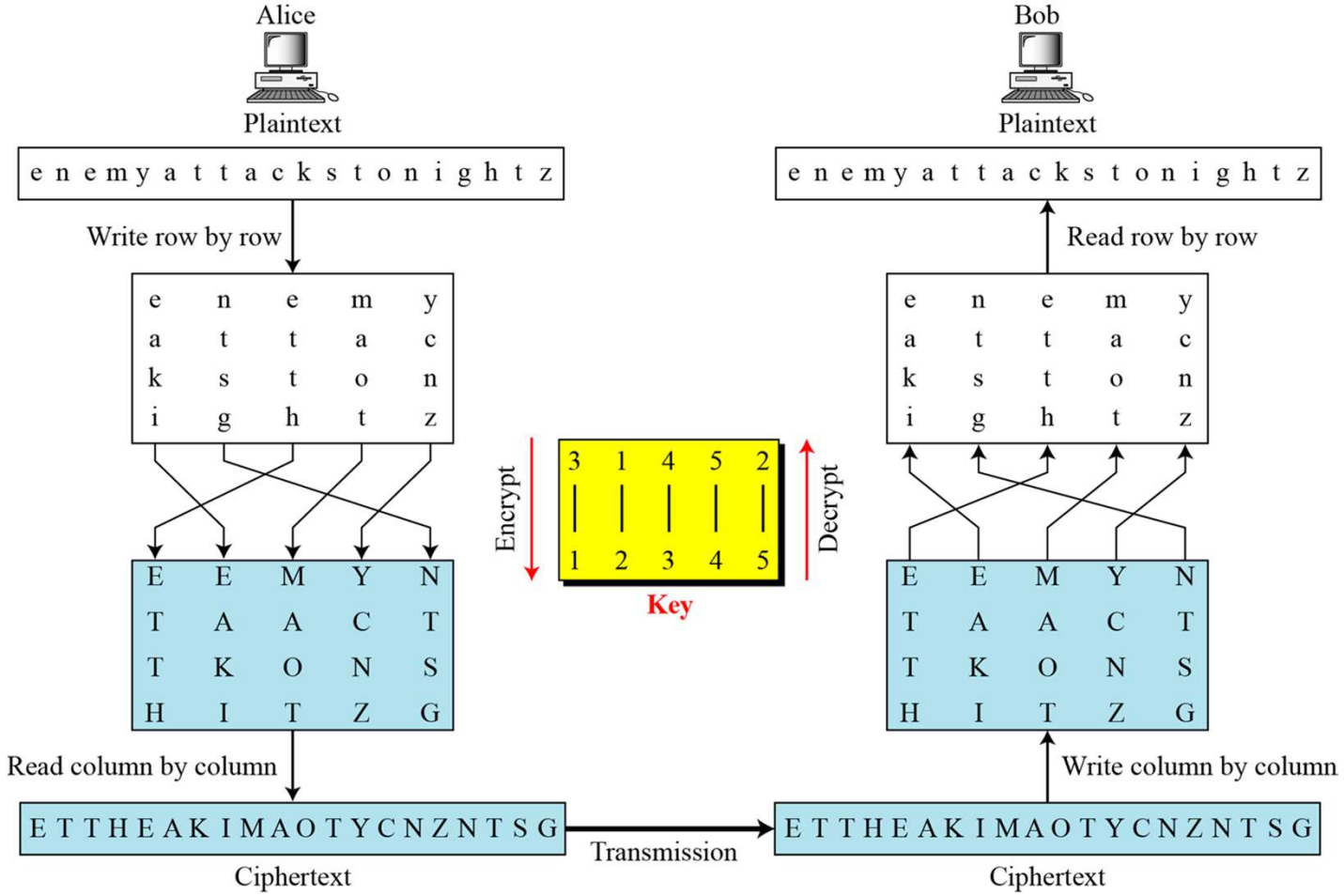


T	H	I	S	I	S
C	N	S	C	L	A
S	S	-	-	-	-
1	2	3	4	5	6

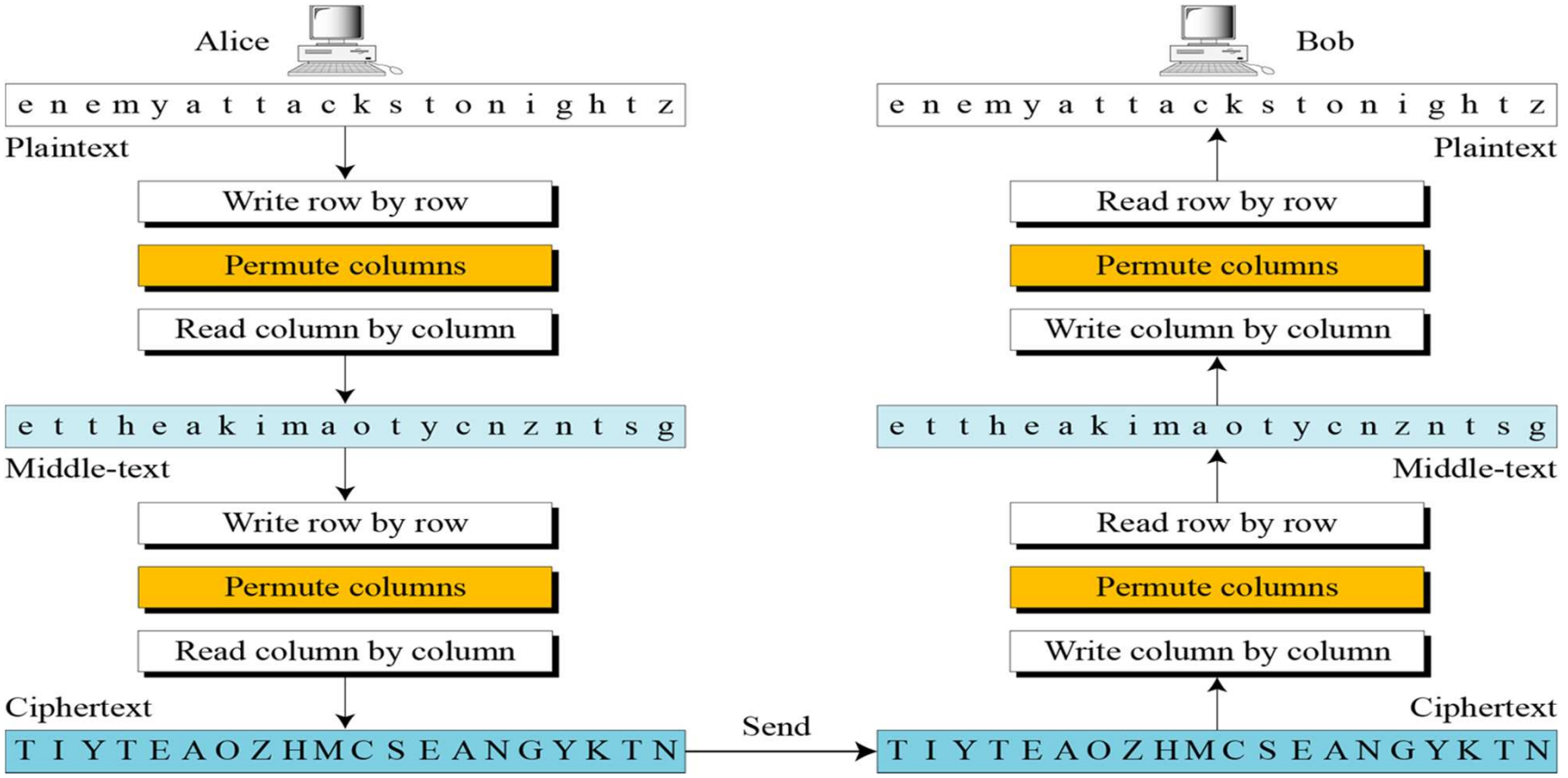
Order : 3 6 1 4 5 2

Ciphertext: ISSATCSSCILHNS

Columnar Transposition (Keyed)



Double Transposition



Confusion and Diffusion

- Confusion: No clue regarding the relationship between ciphertext and the key

- Diffusion: Hides relationship between plaintext and corresponding ciphertext

- Strong substitution function enhances confusion while transposition is used to enhance diffusion

D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You

D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI