Symmetric Key Ciphers

Part III: Transposition Ciphers

Priyank Kalla
Professor
Electrical & Computer Engineering

Keyless Transposition Ciphers

- Transposition Ciphers do not substitute one symbol for another
- Transposition Ciphers reorder the symbols
- Simple transposition ciphers can be keyless: the ***rail fence cipher***
    - Create a $m \times n$ matrix: insert P either column-wise or row-wise
    - Transmit C conversely

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

C = "MMTAEEHREAEKTTP"

Keyless Transposition Cipher

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

"MMTAEEHREAEKTTP"

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
01	05	09	13	02	06	10	13	03	07	11	15	04	08	12

- Transposition: 2nd char moves to 5th position
- 3rd char to the 9th position

- Pattern: (1, 5, 9, 13) (2, 6, 10, 13), …
- Easy to break

Keyed Transition Cipher

e n e m y a t t a c k s t o n i g h t z

Encryption ↓

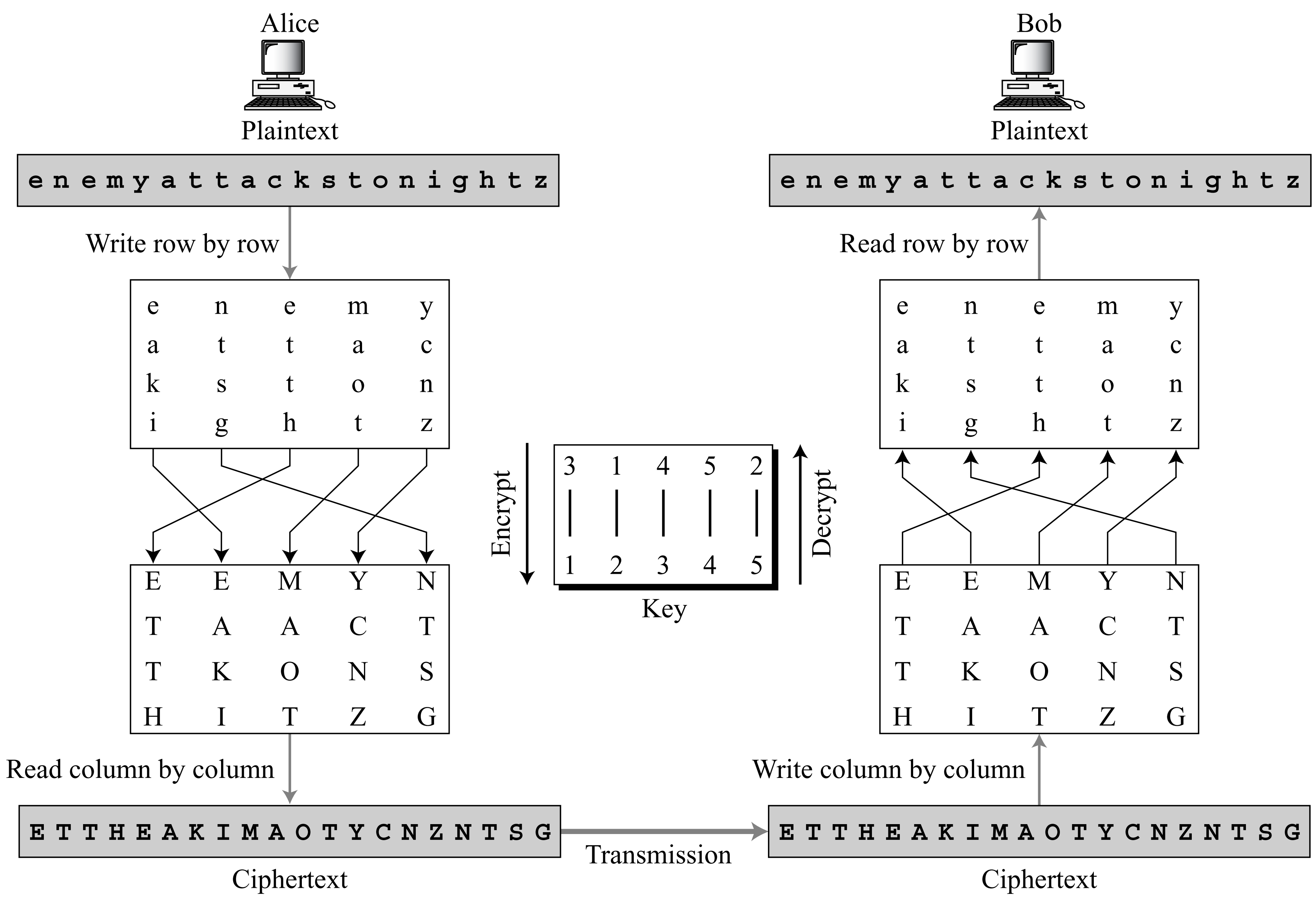
3	1	4	5	2
1	2	3	4	5

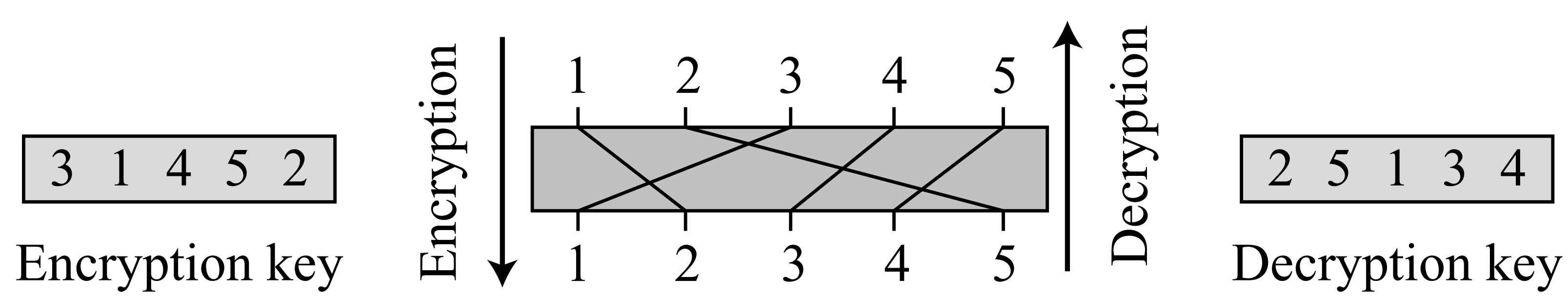
↑ Decryption

E E M Y N T A A C T T K O N S H I T Z G

- Combine keyless + keyed ciphers

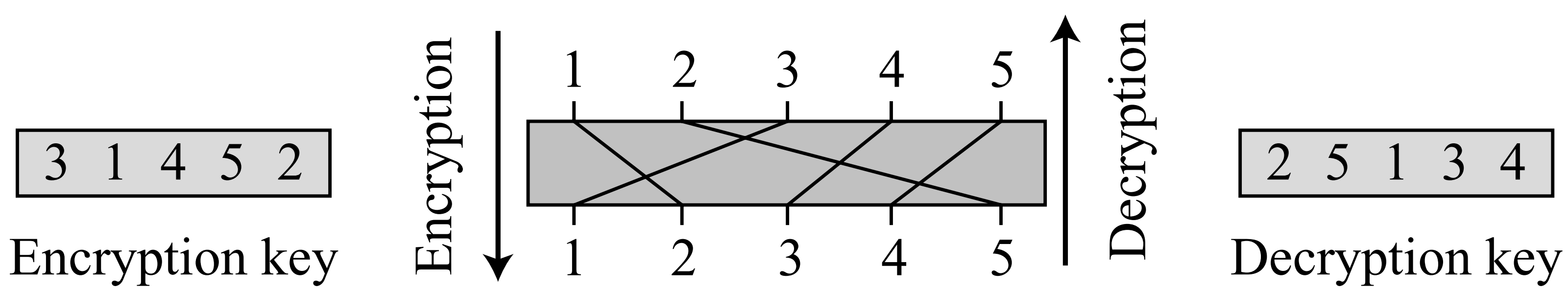
Keyless + Keyed Transpose





Using Matrices for Transposition

- Use matrices to represent P, C and K
- $C_{l\times m} = P_{l\times m} \cdot K_{m\times m}$ and $P_{l\times m} = C_{l\times m} \cdot K^{-1}_{m\times m}$
- Use permutation matrices as keys: A permutation matrix has only 1 entry as “1” in any row or column, and 0s everywhere else
- Inverse(K) = Transpose (K)



$$\underbrace{\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 00 & 19 & 19 & 00 & 02 \\ 10 & 18 & 19 & 14 & 13 \\ 08 & 06 & 07 & 19 & 25 \end{bmatrix}}_{\text{Plaintext}} \cdot \underbrace{\begin{array}{c} \begin{array}{ccccc} 3 & 1 & 4 & 5 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}}_{\text{Encryption key}} = \underbrace{\begin{bmatrix} 04 & 04 & 12 & 24 & 13 \\ 19 & 00 & 00 & 02 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 07 & 08 & 19 & 25 & 06 \end{bmatrix}}_{\text{Ciphertext}}$$