Network and Information Security
Lecture 12

B.Tech. Computer Engineering
Sem. VI.

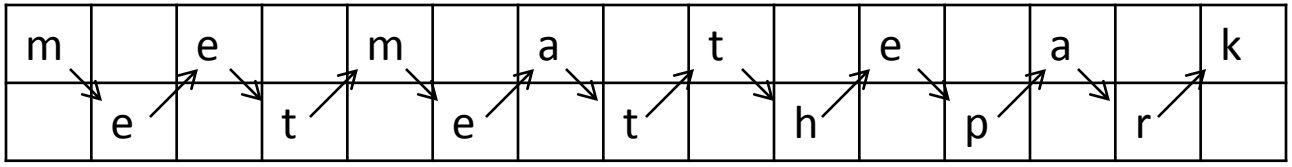
Prof. Mrudang T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

Transposition Ciphers

- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- A symbol in the first position of the plaintext may appear in the tenth position of the cipher text.
- A symbol in the eighth position in the plaintext may appear in the first position of the cipher text.
- A transposition cipher reorders (transposes) the symbols.

Keyless transposition ciphers

- There are two methods
- One: the text is written into a table column by column and then transmitted row by row.
- Second: the text is written into the table row by row and then transmitted column by column
- Example 1: Rail fence cipher
- Plain text is arranged in two lines as a zig zag pattern



- Plain text: Meet me at the park
- Cipher text: MEMATEAKETETHPR
- Bob receives the cipher text and divides it into half.
- First half forms the first row,
- Second half forms the second row
- Bob reads the result in zig zag.
- Cryptanalysis is easy. No key is used.

- Example 2: Alice and Bob can agree on the number of columns and use the second method. Alice writes the same plaintext, row by row, in a table of four columns.

	1	2	3	4
1	m	e	e	t
2	m	e	a	t
3	t	h	e	p
4	a	r	k	

- She then creates the cipher text MMTAEEHREAEKTTP by transmitting the characters column by column.
- Bob receives the cipher text and follows the reverse process.
- He writes the received message, column by column, and reads it row by row as the plaintext.
- Eve can easily decipher the message if she knows the number of columns.

- Length of the plaintext = 15
- Number of comumns = 4 (known to both alice and bob)
- Number of rows = $\lceil$ length/number of column $\rceil$

  = 15/4 = 4
- Write text column by column
- Read it row by row

- Example 3
- The following shows the permutation of each character in the plaintext into the cipher text based on the position. (Example2)
-

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	5	9	13	2	6	10	14	3	7	11	15	4	8	12

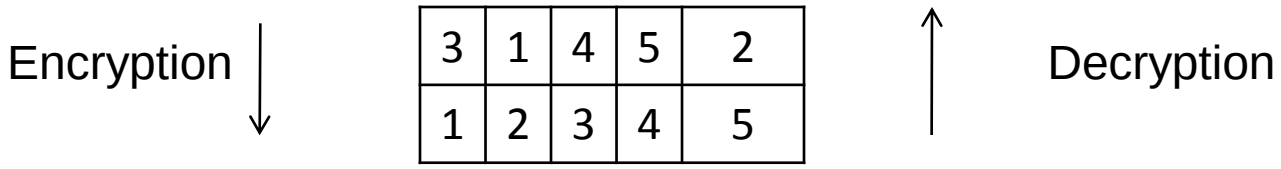
- The second character in the plaintext has moved to the fifth position in the cipher text
- The third character has moved to the ninth position, and so on.
- The pattern in the permutation (1,5,9,13), (2,6,10,14), (3,7,11,15), (8,12)
- In each section, the difference between the two adjacent numbers is 4.

Keyed transposition ciphers

- Divide the plaintext into groups of predetermined size, blocks, and then use a key to permute the characters in each block separately.
- Example 4
- Alice and Bob have agreed to divide the text into groups of five characters and then permute the characters in each group .

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

- The key used for encryption and decryption is a permutation key,



- The third character in the plain text block becomes the first character in the cipher text block;
- The first character in the plain text block becomes the second character in the cipher text block

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

- Bob divides the cipher text into 5- character groups and, using the key in the reverse order, finds the plain text.

Encryption Key: 3,1,4,5,2

e	n	e	m	y
E	E	M	Y	N

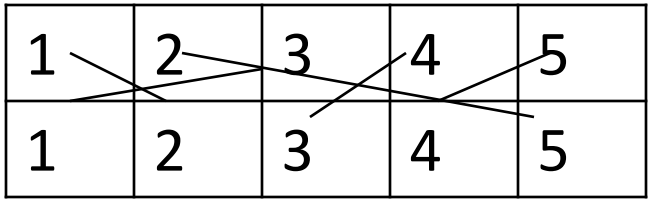
a	t	t	a	c
T	A	A	C	T

k	s	t	o	n
T	K	O	N	S

i	g	h	t	z
H	I	T	Z	G

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

3	1	4	5	2



2	5	1	3	4

Decryption Key: 2,5,1,3,4

E	E	M	Y	N
e	n	e	m	y

T	A	A	C	T
a	t	t	a	c

T	K	O	N	S
k	s	t	o	n

H	I	T	Z	G
i	g	h	t	z

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

- Combining Two Approaches:

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

Encryption

Write Row by Row (Step1)

(Assume key = number of columns = 5)

	1	2	3	4	5
1	e	n	e	m	y
2	a	t	t	a	c
3	k	s	t	o	N
4	i	g	h	t	z

- Step 2 Use key to permute columns
- 3 1 4 5 2

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

- Step 3 Read column by column

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

- At decryption side, number of columns are known
- Length=20, Number of columns are 5
- Number of rows = 20/5 = 4
- Step 1 Write column by column

	1	2	3	4	5
1	E	E	M	Y	N
2	T	A	A	C	T
3	T	K	O	N	S
4	H	I	T	Z	G

- Step 2: Use key 2,5,1,3,4 to permute the columns

	1	2	3	4	5
1	e	n	e	m	y
2	a	t	t	a	c
3	k	s	t	o	N
4	i	g	h	y	z

- Step 3: Read row by row
- e n e m y a t t a c k s t o n i g h t z

Transposition Cipher Cryptanalysis

- Assume cipher text length is L
- We don’t know the length of the key
- So, we can assume key length and then proceed
- Plain text: enigma
- Key 312
- PT: e n i g m a
- 3 1 2 3 1 2
- CT: I E N A G M

- Given, IENAGM
- We want to apply Bruteforce:
- Assume key length is 1
  - It is not possible because character is permuted by itself
  - No permutation
- Key length is 2
  - (1,2), (2,1) {two possibilities }
  - (1,2) does not do any permutation
  - Apply (2,1) after dividing CT into blocks of 2 characters each, E I A N MG <= Does not mean anything

- Next guess is Key length is 3.
- 3 ! = 6
- 1,2,3
- 1,3,2
- 2,3,1
- 2,1,3
- 3,1,2
- 3,2,1

Try 1, 3, 2

i	e	n	a	g	m
1	3	2	1	3	2

Try
2, 3, 1

e n i g m a

So, (2,3,1) is correct one for decryption.
Note (3,1,2) is the encryption key but (2,3,1) is used for decryption because both can be obtained easily provided one is given.

- Brute force trials required
- 2! + 3! + 4 ! + 5!+.....+L!
- Where L = cipher text length
- $\sum i!$ (for i=2 to L)