



Transposition Cipher

GERAMI M. BENEDICTO
instructor

**College of Engineering and
Information Technology**

Transposition Ciphers

- **Transposition cipher technique** - the plaintext remains the same, there is no text replacement of alphabets or numbers occurs but the order of characters are changes or reorder to produce to cipher



Columnar Transposition Encryption Technique

1. Count the number of characters in the message and the key.
 - Example: Common sense is not so common.
 - 30 characters
2. Draw a row of a number of boxes equal to the Key.
 - 8 boxes
 - key of 8

1	2	3	4	5	6	7	8



Columnar Transposition Encryption Technique

3. Start filling in the boxes from left to right, entering one character per box.

1	2	3	4	5	6	7	8
C	o	m	m	o	n	_	s

4. When you run out of boxes but still have more characters, add another row of boxes.

1	2	3	4	5	6	7	8
C	o	m	m	o	n	_	s
e	n	s	e	_	i	s	_
n	o	t	_	s	o	_	c
o	m	m	o	n	.		



Columnar Transposition Encryption Technique

The steps for encrypting are:

1. Count the number of characters in the message and the key.
2. Draw a number of boxes equal to the key in a single row. (For example, 12 boxes for a key of 12.)
3. Start filling in the boxes from left to right, with one character per box.
4. When you run out of boxes and still have characters left, add another row of boxes.
5. Shade in the unused boxes in the last row.
6. Starting from the top left and going down, write out the characters. When you get to the bottom of the column, move to the next column to the right. Skip any shaded boxes. This will be the ciphertext.



Columnar Transposition Encryption Technique

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

- The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
- Width of the rows and the permutation of the columns are usually defined by a keyword.
- For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be “3 1 2 4”.
- Any spare spaces are filled with nulls or left blank or placed by a character (Example: _).
- Finally, the message is read off in columns, in the order specified by the keyword.



Encryption

Given text = Geeks for Geeks

Keyword = HACK

Length of Keyword = 4 (no of rows)

Order of Alphabets in HACK = 3124

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4

Encrypted Text = e kefGsGsrekeo_

