Other Transposition (Permutation) Ciphers

In transposition ciphers the letters of the original message (plaintext) are arranged in a different order to get the ciphertext.

Plaintext → Rearrange characters → Ciphertext

It uses different kinds of mapping and is achieved by performing some sort of permutation on the plaintext letters.

ii. Message Reversal Cipher

In such procedure the plaintext will be written backward to produce the ciphertext.

Example: If the message is: almansour university college, then

Plaintext = almansour university college

Ciphertext = EGELLOC YTISREVINU RUOSNAMLA

Mathematically if L is the length of the message then **C=E(k)=L+1-k**, where k is the position of the letter in the plaintext.

iii- Rail Fence (Zig-Zag) Cipher

The Rail Fence cipher is the simplest transposition cipher.

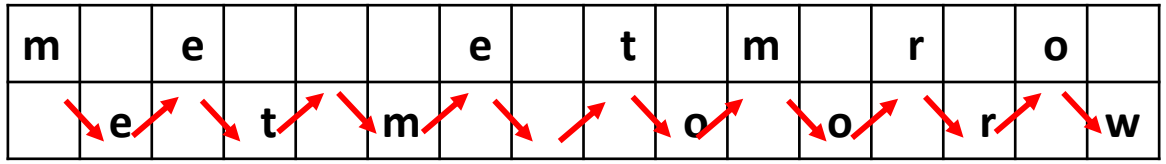
Encryption Steps for Rail Fence Method:

The steps used to obtain the ciphertext using this technique are as follows:

Step 1: The plaintext is written as a sequence of diagonals (zigzag pattern).

Step 2: Then, to obtain the ciphertext the text is read as a sequence of rows (Row-wise writing).

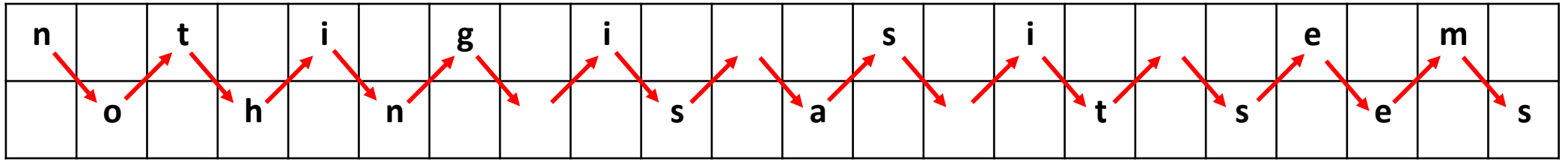
Example: Encrypt the Plaintext**:** "meet me tomorrow", using Rail fence cipher method



Looking at the image, you would get it why it is named rail fence because it appears like the rail fence. To obtain the ciphertext out of it you have to read it as a sequence of rows. So, reading the first row the first half of Ciphertext will be: **ME ETMRO,** reading the second row of the rail fence, we will get the second half of the Ciphertext: **ETM OORW** , now, to obtain the complete ciphertext combine both the halves of ciphertext and the complete ciphertext will be:

Ciphertext: ME ETMROETM OORW

Example: Encrypt the message: “nothing is as it seems” using Rail Fence method



Ciphertext: “NTIGI SI EMOHN SA TSES”

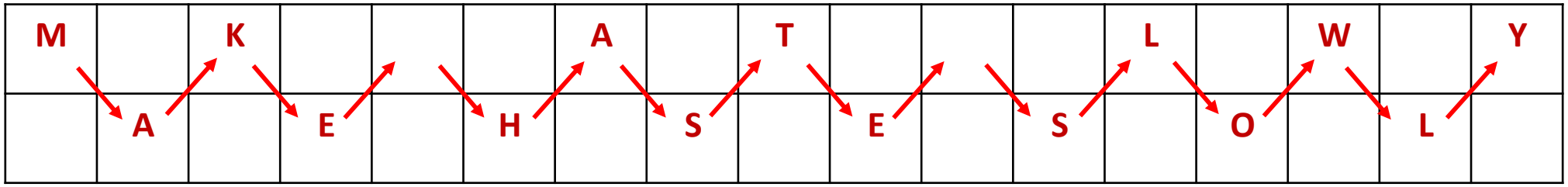
Example: Decipher the message: “**MK AT LWYAEHSESOL**” using Rail Fence method

Decryption Steps for Rail Fence Method:

Step1: Mark the boxes in a zigzag pattern

Step2: Fill in the top marked boxes with the ciphertext.

Step3: Fill in the remaining marked bottom boxes with the rest of the ciphertext.



Plaintext: “make haste slowly”

Note:

It is also possible to use zig-zag pattern with more than two rows as shown below

Example: Encrypt the Plaintext: “put that phone away” using Rail Fence method,

Key: 4 rows

Ans. : Ciphertext: “PANYUHTOEATT H W PA”.

p						a						n					y
	u				h		t				o		e			a	
		t		t				----		h				----		w		
			----						p						a			

iv- Route Cipher:

The Route cipher is a transposition cipher where the key is which route to follow when reading the Ciphertext from the block created with the plaintext.

- Plaintext is written as a grid of a particular size.
- Then read off using a predetermined pattern called “Route”.
- This pattern is the key used in Route cipher.
- The size of the grid is also passed with the key.

Some examples of routes could be: spiral inwards counter-clockwise from the top right, zig-zagging up and down, spiral inwards clockwise from bottom left, spiral inwards counter-clockwise from top left and etc.

Encryption:

The steps for encryption are as follows:

Step 1: Choose a block sized properly for the message. Let’s say that your message was 28 letters long. You might want to use a 5x6 block to fit the message with your desired route.

Step 2: Place your message in the block with desired route.

Decryption:

Step 1: You need to know the route chosen and either the length or width of the block

Step 2: Then build a block that size and place the jumbled text into the block as the route specifies

Example : Encrypt the message “the battle of lepanto happened in fifteen seventy one” using a Route transposition cipher, Key: spiral inwards, counterclockwise, starting from the top left.

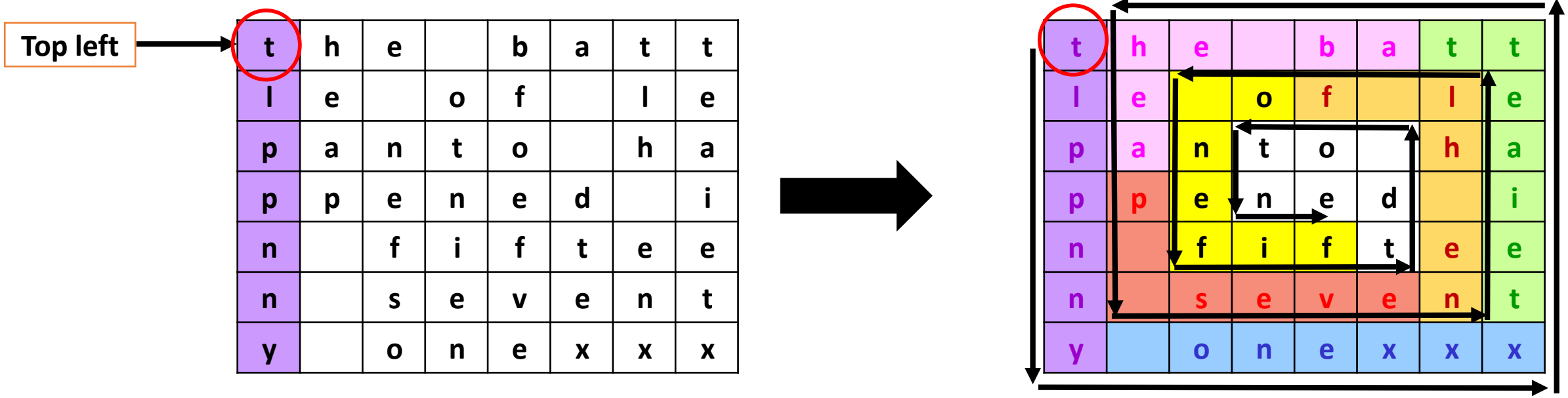
Use grid size 7 x 8.

Ans. :

Step 1: The plaintext is arranged in a grid with 8 columns and 7 rows.

Step 2: The key is applied. Starting from the top left letter, T, the ciphertext will be determined as the letters spiral toward the center from counterclockwise.

Step 3: The ciphertext is written out horizontally.



The Ciphertext:

TLPPNNY ONEXXXTEIAETTAB EHEAP SEVENE HL FO NEFIFTD OTNE

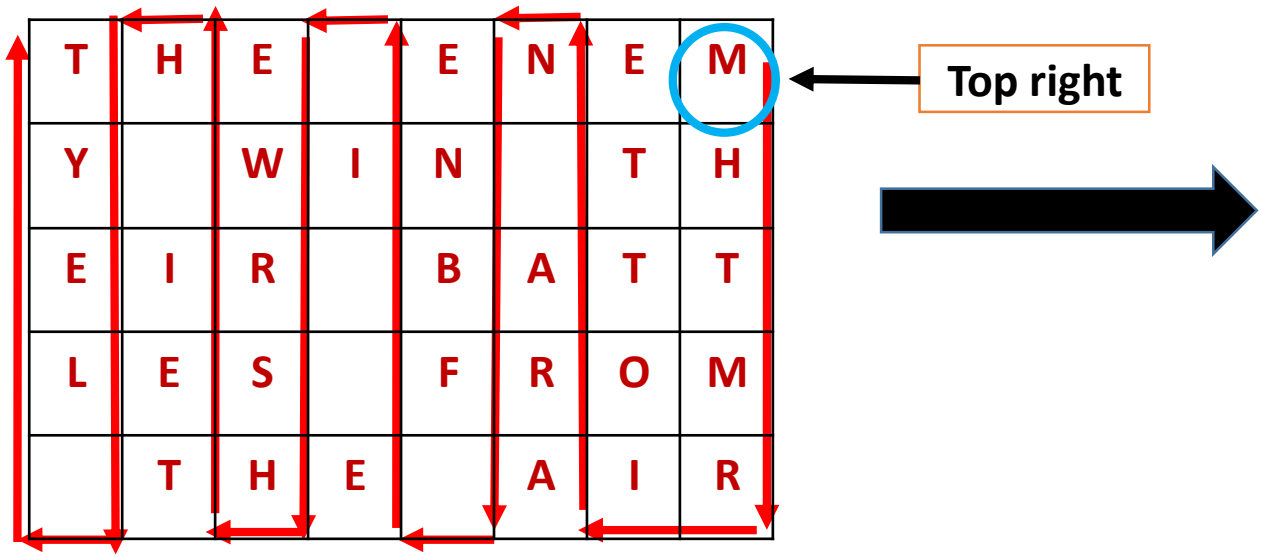
Example : Decrypt the Ciphertext "**MHTMRIOTTEN ARA FBNE I EHSRWEH IET LEYT**" using a Route transposition cipher, Key: zigzag up and down, starting from the top right. Use grid size 5 x 8.

Ans. :

Step 1: The ciphertext and the key is given.

Step 2: Write the ciphertext in the pattern the key specifies.

Step 3: The plaintext can then be read from left to right, starting from the top row.



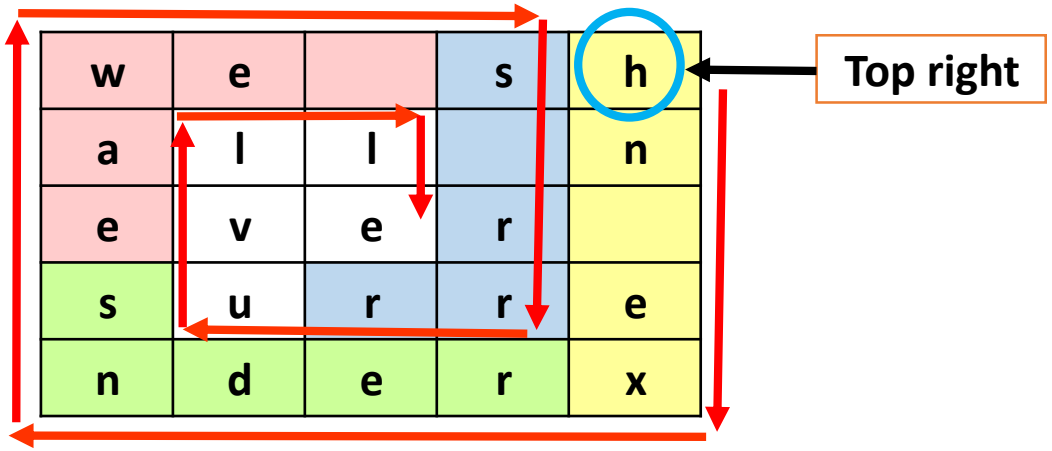
T	H	E		E	N	E	M
Y		W	I	N		T	H
E	I	R		B	A	T	T
L	E	S		F	R	O	M
	T	H	E		A	I	R

Plaintext: "The enemy win their battles from the air".

Example : Encrypt the plaintext "we shall never surrender" using a Route transposition cipher, Key: Spiral inwards, clockwise, from the top right. Use grid size 5 x 5.

w	e		s	h
a	l	l		n
e	v	e	r	
s	u	r	r	e
n	d	e	r	x

Top right



Ans. : Ciphertext: "HN EXREDNSEAWE S RRRUVLLE "

Example : Decrypt the **Ciphertext "EDXXTS EHTWITAR RAS"** using a Route transposition cipher,

Key: Spiral inwards, counterclockwise, from the bottom left. Use grid size 5 x 4.

Ans. : Plaintext: "the war is started"