CRYPTOGRAPHY

LECTURE THREE (CONT.)

Classical (Traditional) Encryption Techniques

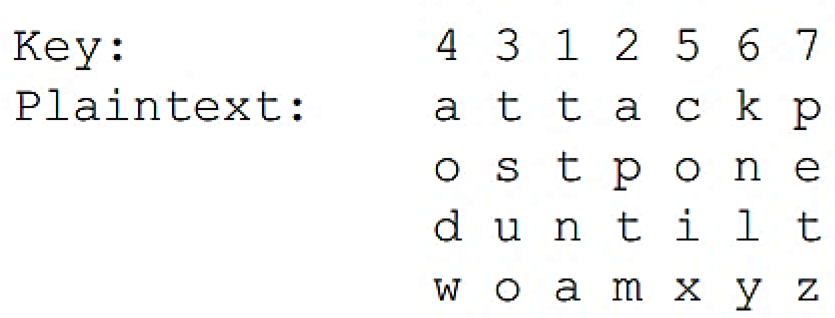
Assist prof. Dr. Saja J. Mohammed

2. Columnar Transposition Technique

The columnar transposition cipher is more complex **as compared to** the rail fence. The steps to obtain cipher text using this technique are as follow:

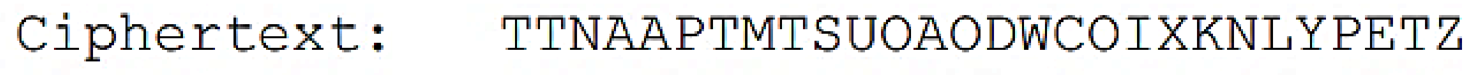
- **Step 1:** The plain text is written in a matrix of the initially defined size in a row by row pattern.
- **Step 2:** To obtain the cipher text read the text written in a matrix column by column. But you have to permute the order of column before reading it column by column. The order of the columns then becomes the key to the algorithm. For example,

- **Plain text: Attack postponed until two Am**
- KEY = 4 3 1 2 5 6 7



```
Key:           4 3 1 2 5 6 7
Plaintext:     a t t a c k p
               o s t p o n e
               d u n t i l t
               w o a m x y z
```

- Now, to obtain the cipher text we have to read the plain text column by column as the sequence of permuted column order.

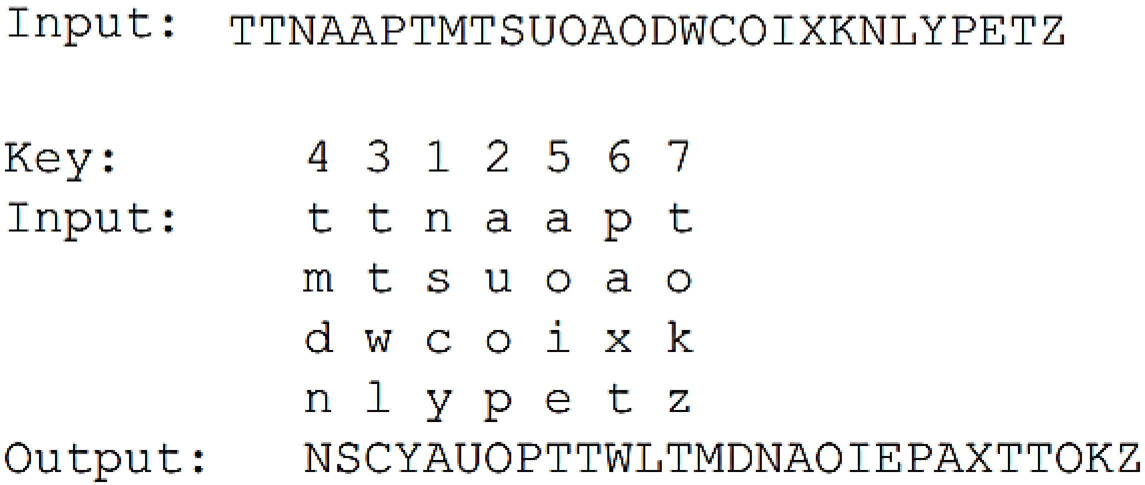


```
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

- Similar to the rail fence cipher, the columnar cipher can be easily broken. The cryptanalyst only has to try few permutation and combination over the order of column to obtain the permuted order of column and the get the original message. So, a more sophisticated technique was required to strengthen the encryption.

Double transposition cipher

The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is re-encrypted using the same algorithm,



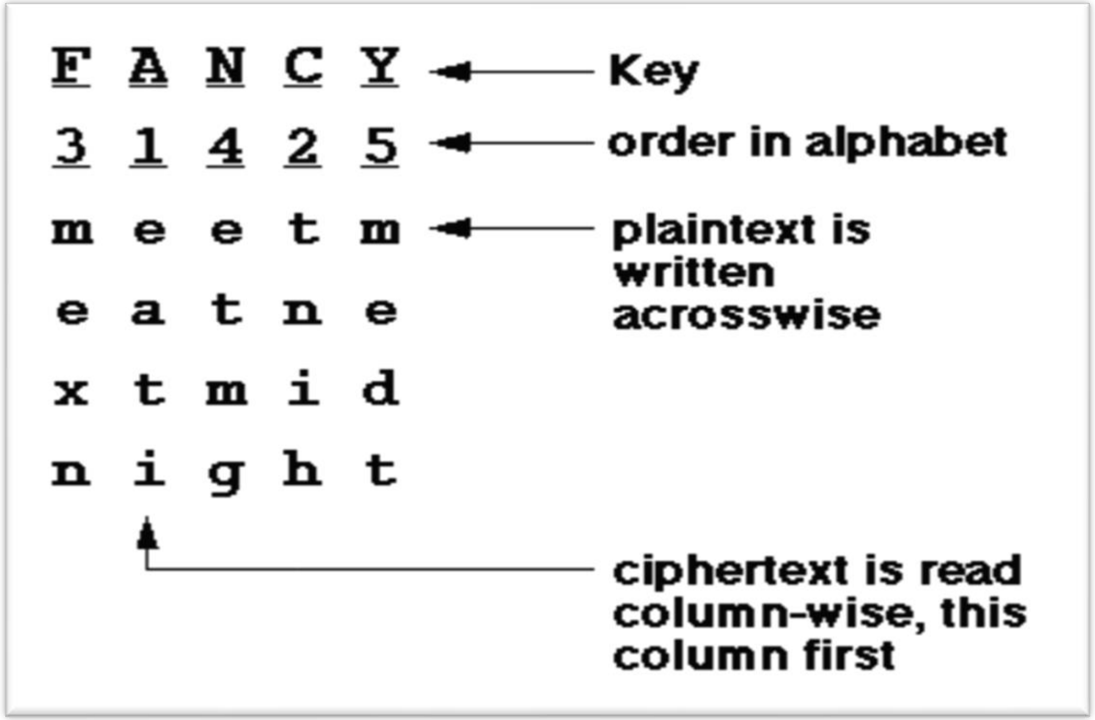
```
Input:  TTNAAPTMTSUOAODWCOIXKNLYPETZ

Key:       4 3 1 2 5 6 7
Input:     t t n a a p t
           m t s u o a o
           d w c o i x k
           n l y p e t z
Output:    NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

This is a much less structured permutation and is much more difficult to cryptanalyze.

Note:

The key may be written as English characters . i.e.



F	A	N	C	Y
3	1	4	2	5
m	e	e	t	m
e	a	t	n	e
x	t	m	i	d
n	i	g	h	t

Key

order in alphabet

plaintext is written acrosswise

ciphertext is read column-wise, this column first

Attack->>>> atck->>>>> 1423

Other transposition Ciphers: Route transposition cipher

Route cipher has two phases:

Phase 1:

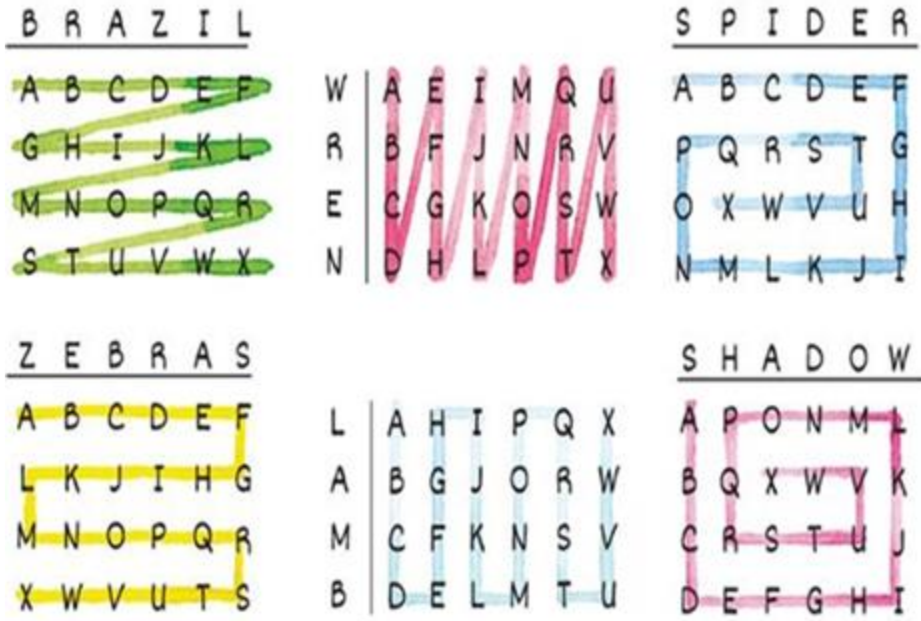
Write message into block with a specific route (on – by route) determined by a key (route).

Phase 2:

Write cipher out using column/ row route (off-by route).

We'll depend on **column direction** to get ciphertext.

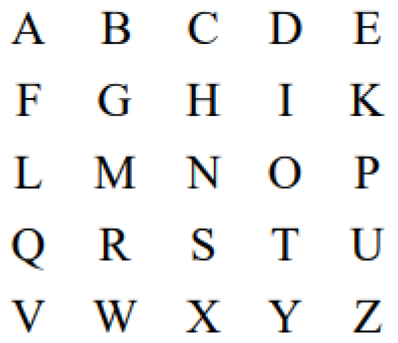
Note : the key will be here the route of writing the message into specified block



Route Cipher has six basic patterns. Many routes are found from each of these patterns. The other routes are obtained from the pattern by reflection or transposition (interchanging rows and columns).

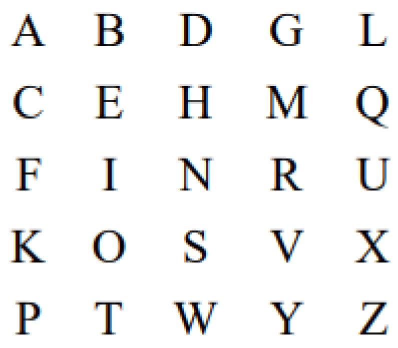
Such of the basic patterns of route transposition patterns:

Orthogonal



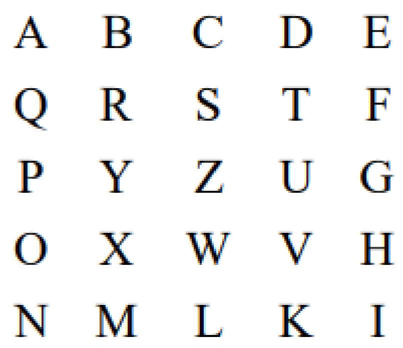
A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Diagonal



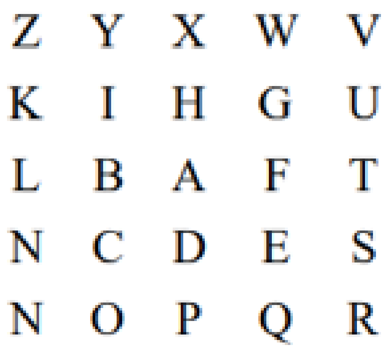
A	B	D	G	L
C	E	H	M	Q
F	I	N	R	U
K	O	S	V	X
P	T	W	Y	Z

Spiral



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

Crab Spiral (Reverse Spiral)



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

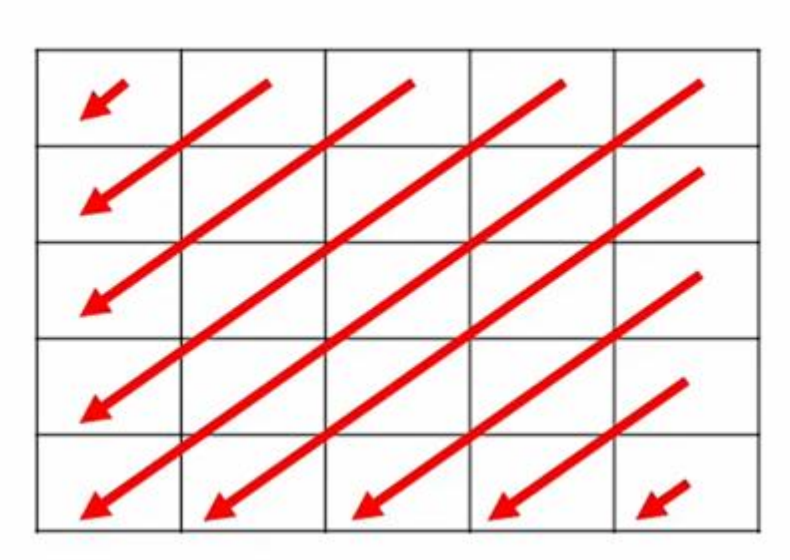
Example : use route cipher to encrypt the message (To run in circles, not in places)

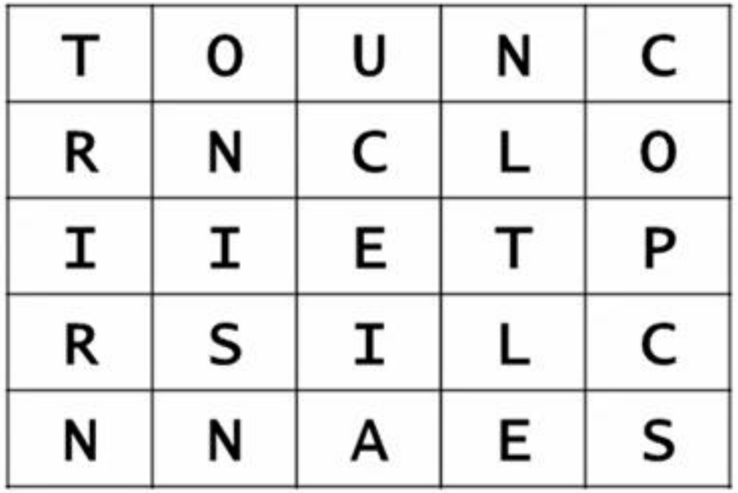
TORUNINCIRCLESNOTINPLACES

To run in circles no in places

25 letters: 5x5 block

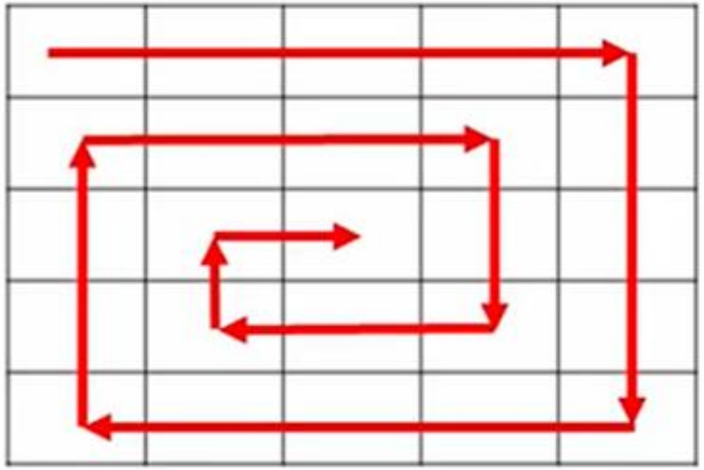
1. Diagonal route





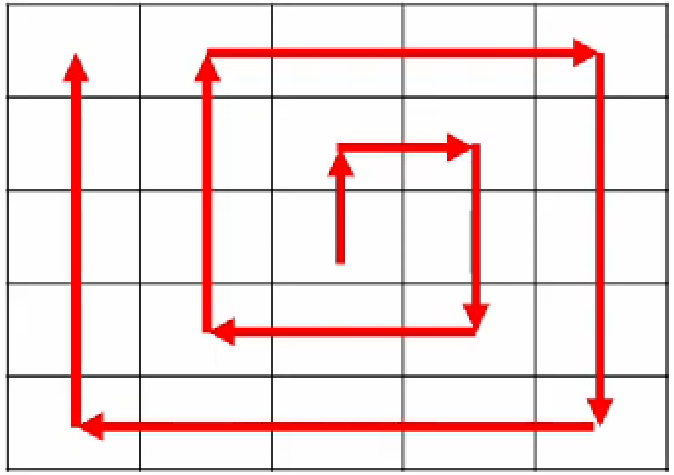
T	O	U	N	C
R	N	C	L	O
I	I	E	T	P
R	S	I	L	C
N	N	A	E	S

2. Spiral route

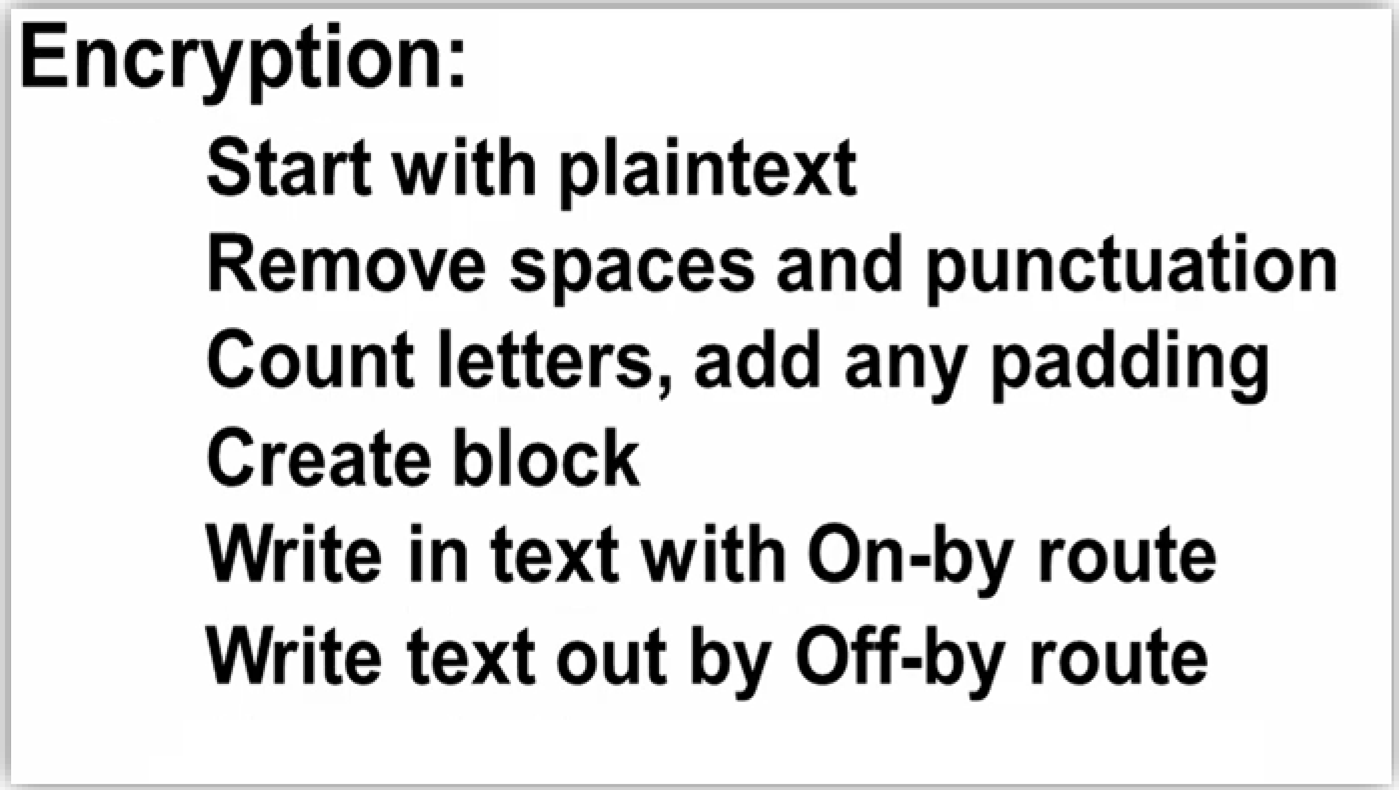


T	O	R	U	N
O	T	I	N	I
N	E	S	P	N
S	C	A	L	C
E	L	C	R	I

3. Reverse spiral route:



S	R	C	L	E
E	I	o	R	S
C	C	T	U	N
A	N	I	N	O
L	P	N	I	T



Encryption:

Start with plaintext

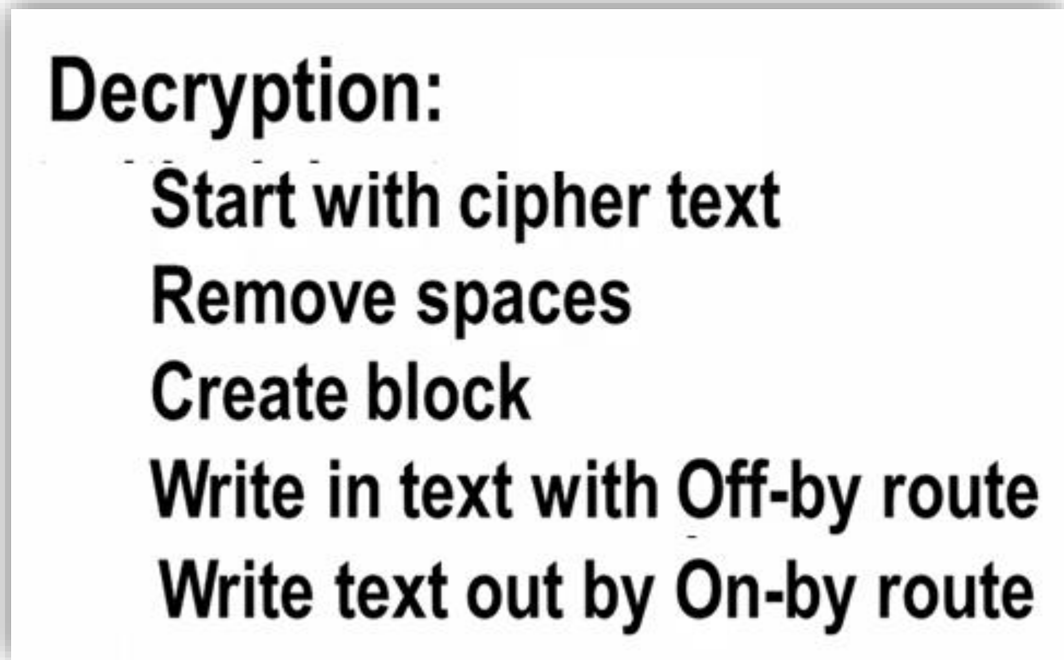
Remove spaces and punctuation

Count letters, add any padding

Create block

Write in text with On-by route

Write text out by Off-by route



Decryption:

Start with cipher text

Remove spaces

Create block

Write in text with Off-by route

Write text out by On-by route

H.W.

- Get the ciphertext of each pattern in the example.
- Decrypt the ciphertext for each pattern.

Note:

In route transposition cipher there are **two** way to get ciphertext from the block (using column route):

1. normally, begin with the first column towards the last one.

2. Depending on key, we can use the same way of (column transposition cipher) by using key which determined the order of getting ciphertext from block.

Note:

In reverse spiral route examples we ‘ll based on square matrix of odd dimension (i.e. 3*3, 5*5, 7*7, and so)

H.w. Encrypt the text “ be careful” using all of the given routs with key “312”, then decrypt the produced cipher.