V. Columnar Transposition Cipher

We arrange the message as an array of 2-dimensions. The number of rows and columns depends on the length of the message, if the length of the message equal to 30 (**including the spaces**) then the probability of the numbers of rows and columns are: **15X2, 2X15, 10X3, 3X10, 5X6, or 6X5.**

Note that if the length of the message is 29, we must add a dummy letter in the end of the message.

Example: if the message is: “the attack will start sunday”, then the length of the message is 28, we will add dummy letters x and x to the end of the message and the length will be 30. We can say that **30=10X3** and If the **key is (2,3,1)** then we arrange the columns as the following:

Plaintext is: “the attack will start sunday”

The Ciphertext: “HAA LSRSDXETCWLTTUAXT TKI A NY”, the Ciphertext comes from the reading on the table by columns: to make the key easy to remember we take a keyword like TWO and rearrange its letters alphabetically. So (2,3,1) is the key that will use to rearrange the array columns.

T	W	O
2	3	1

1	2	3
t	h	e
	a	t
t	a	c
k		w
i	l	l
	s	t
a	r	t
	s	u
n	d	a
y	x	x

2	3	1
h	e	t
a	t	
a	c	t
	w	k
l	l	i
s	t	
r	t	a
s	u	
d	a	n
x	x	y

Vi. Double Transposition

Double Transposition consists of two applications of columnar transposition to a message. The two applications may use the same key for each of the two steps, or they may use different keys.

Example: Columnar transposition works like this: First pick a keyword, such as describe, then write the message under it in rows, Then number the letters in the keyword in alphabetical order.

The plaintext: “the german army surprise the allies with a swift attack”

d	e	s	c	r	i	b	e
t	h	e		g	e	r	m
a	n		a	r	m	y	
s	u	r	p	r	i	s	e
	t	h	e		a	l	l
i	e	s		w	i	t	h
	a		s	w	i	f	t
	a	t	t	a	c	k	x

3	4	8	2	7	6	1	5
d	e	s	c	r	i	b	e
t	h	e		g	e	r	m
a	n		a	r	m	y	
s	u	r	p	r	i	s	e
	t	h	e		a	l	l
i	e	s		w	i	t	h
	a		s	w	i	f	t
	a	t	t	a	c	k	x

Then read the cipher off by columns, starting with the lowest-numbered column Column 1 is **Ciphertext1:**

R	Y	S	L	T	F	K		A	P	E		S	T	T	A	S		I			H	N	U	T	E	A	A	M		E	L	H	T	X	E	M	I	A	I	I	C	G	R	R		W	W	A	E		R	H	S		T

This completes the first columnar transposition. Next, select and number **a second keyword (coastline),** and write this intermediate Ciphertext under it in rows:

2	7	1	8	9	5	4	6	3
c	o	a	s	t	l	i	n	e
R	Y	S	L	T	F	K		A
P	E		S	T	T	A	S	
I			H	N	U	T	E	A
A	M		E	L	H	T	X	E
M	I	A	I	I	C	G	R	R
	W	W	A	E		R	H	S
	T							

Finally, take it off by columns again. **Ciphertext2:**

S				A	W		R	P	I	A	M			A		A	E	R	S		K	A	T	T	G	R		F	T	U	H	C				S	E	X	R	H		Y	E		M	I	W	T	L	S	H	E	I	A	

T	T	N	L	I	E	

The Steps of Columnar Transposition Technique

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

Step 1: The plaintext is written in the rectangular matrix of the initially defined size in a row by row pattern.

Step 2: To obtain the ciphertext read the text written in a rectangular matrix column by column. But you have to permute the order of column before reading it column by column. The obtained message is the ciphertext message.

The Steps of Columnar Transposition Technique with Multiple Rounds (Double)

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

Step 1: The plaintext is written in the rectangle of predetermined size row by row.

Step 2: To obtain the ciphertext, read the plaintext in the rectangle, column by column. Before reading the text in rectangle column by column, permute the order of columns the same as in basic columnar technique.

Step 3: To obtain the final ciphertext repeat the steps above multiple time.

Example: Encrypt the message (plaintext) is “battle of berlin”, using a columnar transposition for the given key (3,1,4,2).

Ans. : The key have 4 columns, while the message have 16 characters (including spaces), then the number of rows = 16/4 = 4

1	2	3	4
b	a	t	t
l	e		o
f		b	e
r	l	i	n

3	1	4	2
t	b	t	a
	l	o	e
b	f	e	
i	r	n	l

Ciphertext round 1:

“T BIBLFRTOENAE L”

Example: Encrypt the plaintext “battle of berlin”, using a multiple rounds columnar transposition cipher for the given keyword round1= (3,1,4,2), keyword round2= (2,3,1,4).

Ans. :

1	2	3	4
t	b	t	a
	l	o	e
b	f	e	
i	r	n	l

2	3	1	4
b	t	t	a
l	o		e
f	e	b	
r	n	i	l

Ciphertext round 2:

“ BLFRTOENT BIAE L”

Example : Encrypt the message “success is not final failure is not fatal” using a columnar transposition cipher for the given **keyword** “**battle**”. Then, using the same keyword again to obtain the double transposition ciphering.

b	a	t	t	l	e
2	1	5	6	4	3
s	u	c	c	e	s
	i	s		n	o
t		f	i	n	a
l		f	a	i	l
u	r	e		i	s
	n	o	t		f
a	t	a	l	x	x

b	a	t	t	l	e
2	1	5	6	4	3
u	i			r	n
t	s		t	l	u
	a	s	o	a	l
s	f	x	e	n	n
i	i		x	c	s
f	f	e	o	a	c
	i	a		t	l

Ans. : We have written the keyword above the grid of the plaintext, and also the numbers telling us which order to read the columns in. Notice that the first “t" is 5 and the second “t" is 6. The numbers represent the alphabetical order of the keyword, and so the order in which the columns will be read.

The Ciphertext-round 1: UI RNTS TLU ASOALSFXENNII XCSFFEOAC IA TL

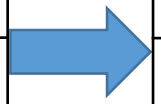
The Ciphertext-round 2: ISAFIFIUT SIF NULNSCLRLANCAT SX EA TOEXO-

Example : Decrypt the Ciphertext "UI RNTS TLU ASOALSFXENNII XCSFFEOAC IA TL" using a columnar transposition cipher for the given keyword battle.

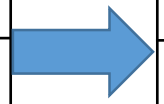
Ans. : There are 42 letters in the Ciphertext, and the keyword has six letters, so we need 42 ÷ 6 = 7 rows.

We have the keyword and the order of the letters in the keyword. We also know there are 7 rows. Now we start by filling in the columns in the order given by the alphabetical order of the keyword, starting with the column headed by "U". Then, we continue to add columns in the order specified by the keyword.

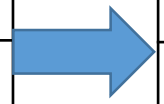
b	a	t	t	l	e
2	1	5	6	4	3
	U				
	I				
	R				
	N				
	T				



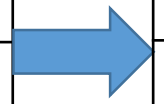
b	a	t	t	l	e
2	1	5	6	4	3
S	U				
	I				
T					
L					
U	R				
	N				
A	T				



b	a	t	t	l	e
2	1	5	6	4	3
S	U				S
	I				O
T					A
L					L
U	R				S
	N				F
A	T				X



b	a	t	t	l	e
2	1	5	6	4	3
S	U			E	S
	I			N	O
T				N	A
L				I	L
U	R			I	S
	N				F
A	T			X	X



b	a	t	t	l	e
2	1	5	6	4	3
S	U	C		E	S
	I	S		N	O
T		F		N	A
L		F		I	L
U	R	E		I	S
	N	O			F
A	T	A		X	X

b	a	t	t	l	e
2	1	5	6	4	3
s	u	c	c	e	s
	i	s		n	o
t		f	i	n	a
l		f	a	i	l
u	r	e		i	s
	n	o	t		f
a	t	a	l	x	x

Now we read off **the plaintext** row at a time to get "**success is not final failure is not fatal**".

Example : Decrypt the Ciphertext "**ELI TRTWITD ESSAEHVE ASIT B YSWHY E FIE--**" using a columnar transposition cipher for the given keyword "battle".

Ans. : we start similarly to the last example, by heading the columns with the keyword battle. This time, to find how many rows we need, we do 38 ÷ 6 = 6.3333. We round this up to the next number, which is 7, so we need 7 rows. When we multiply 6 x 7 we get 42, and 42 - 38 = 4. Hence we need 4 placeholders in the last row. We get the grid below to the left. After plugging the Ciphertext letters in, in the same way as previous example, we get the grid on the right.

b	a	t	t	l	e
2	1	5	6	4	3

b	a	t	t	l	e
2	1	5	6	4	3
w	e		e	a	s
i	l	y		s	a
t	i	s	f	i	e
d		w	i	t	h
	t	h	e		v
e	r	y		b	e
s	t				

Finally, we read off the **plaintext** in rows, to reveal the same plaintext as the other example,

"**we easily satisfied with the very best**".

Conventional (Classical or Traditional) Ciphering Systems

In general we can classify the classical ciphering systems as the following:

- **1. Substitution**
  - i. Monoalphabetic.
    - (a) Direct stander (Caesar or Shift)
    - (b) Standard reverse.
    - (c) Multiplicative cipher.
    - (d) Affine cipher.
    - (e) Mixed alphabet.
    - (f) Keyword mixed.
    - (g) Transposed keyword mixed.
  - ii. Polyalphabetic.
    - Vigenere
    - Beaufort
  - iii. Vernam Cipher (Stream)
  - iv. One Time Pad
  - v. Ploygraphic
    - Playfair
    - Hill Cipher
- **2. Running Key**
- **3. Rotor Machines**
- **4. Transposition (Permutation)**
  - i. 1D Transposition.
  - ii. Message reversal.
  - iii. Rail Fence (Zig-Zag).
  - iv. Route.
  - v. Columnar Transposition.
  - vi. Double Transposition.