

**Transposition Ciphers:**

A **transposition** cipher is a rearrangement of the letters in the plaintext according to some specific system & key (i.e. a permutation of the plaintext). They are generally insecure.

Simple example:

A **route** cipher:

we arrange the plaintext in a geometrical figure, then copy it out following a different route.

e.g. P/T: Now is the time for all good men . . .

We arrange this in a rectangle of K columns and extract the ciphertext by the columns:

```
N O W I S
T H E T I
M E F O R
A L L G O
O D M E N
```

Ciphertext: NTMAO OHELD WEFLM ITOGE SIRON

How do we detect this? Well, the character frequency should be the same as English.

More generally, we deal with:

**Rectangular Columnar Transposition:**

- 1) Arrange horizontally in a rectangle.
- 2) Use a key to generate a permutation of the columns
- 3) Read vertically.

Key: SCHMID  
613542

Plaintext: sell all stock on Monday

```
6 1 3 5 4 2
s e l l a l
l s t o c k
o n M o n d
a y
```

Ciphertext: ESNYL KDLTM ACNLO OSLOA

**Analysis of columnar transposition ciphers:**

Since these represent permutations of the plaintext, we can detect such a cipher by using the frequency distribution for plaintext.

Note that since it is customary to pad the rectangle out so all columns are the same size, the number of letters usually suggests the size of the rectangle.

Example:

```
EOEYE GTRNP SECEH
HETYH SNGND ODDT
OCRAE RAEMH TECSE
USIAR WKDRI RNYAC
ANUEY ICNTT CEIET
US
```

Note that this ciphertext has 77 letters. This suggests a block 7x11 or 11x7, although it could be a ragged rectangle 8x10 with the last 3 letters missing. To determine the correct number of rows, we look at all possible values. Since the correct number of rows will tend to keep letters from the same word clumping together, we expect that the variance in vowel/consonant ratios per row will be lower with the correct number of rows.

E	E	G	A	E	R	C
O	C	N	E	U	N	N
E	E	D	R	S	Y	T
Y	H	D	A	I	A	T
E	H	D	E	A	R	C
G	E	D	M	R	A	E
T	T	E	H	W	N	I
R	Y	T	T	K	U	E
N	H	O	E	D	E	T
P	S	C	C	R	Y	U
S	N	R	S	I	I	S

Once this is done, take a test column. Pair each other column with it on its right-hand side. Look at the digrams thus created. Sum them for each column. Assuming you have not chosen the rightmost column in the first place, the digram sum should be highest for the correct pairing of columns.

To do this, we first need to analyze the frequency of digrams: (Based on 50,000 letters of governmental telegrams in plaintext, reduced to 5,000 digraphs)

First	Second Letter																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	3	6	14	27	1	4	6	2	17	1	2	32	14	64	2	12		44	41	47	13	7	3		12	
B	4			18			2	1	6	1		6	1		4			2	1	1	2					7
C	20		3	1	32	1		14	7		4	5	1	1	41			4	1	14	4		1		1	
D	32	4	4	8	33	8	2	2	27	1		3	5	4	16	5	2	12	13	15	5	3	4		1	
E	35	4	32	60	42	18	4	7	27	1		29	14	111	12	20	12	87	54	37	3	20	7	7	4	1
F	5		2	1	10	11	1		39			2	1		40	1		9	3	11	3		1		1	
G	7		2	1	14	2	1	20	5	1		2	1	3	6	2		5	3	4	2		1			
H	20	1	3	2	20	5			33			1	2	3	20	1	1	17	4	28	8		1		1	
I	8	2	22	6	13	10	19				2	23	9	75	41	7		27	35	27		25		15		2
J	1				2										2						2					
K	1		1		6				2			1		1				1								
L	28	3	3	39	37	3	1	1	20			27	2	1	13	3		2	6	8	2	2	2		10	
M	36	6	3	1	26	1		1	9				13	10	8		2	4	2	2					2	
N	26	2	19	52	57	9	27	4	30	1	2	5	5	8	18	3	1	4	24	82	7	3	3		5	
O	7	4	8	12	3	25	2	3	5	1	2	19	25	77	6	25		64	14	19	37	7	8	1	2	
P	14	1	1	1	23	2		3	6			13	4	1	17	11		18	6	8	3	1	1		1	
Q													1					1				15				
R	39	2	9	17	98	6	7	3	30	1	1	5	9	7	28	13		11	31	42	5	5	4		9	
S	24	3	13	5	49	12	2	26	34		1	2	3	4	15	10		5	19	63	11	1	4		1	
T	28	3	6	6	71	7	1	78	45			5	6	7	50	2	1	17	19	19	5		36		41	1
U	5	3	3	3	11	1	8		5			6	5	21	1	2		31	12	12		1				
V	6				57				12						1											
W	12				22			4	13			1		2	19			1	1						1	
X	2		2	1	1	1		1	2					1	1	2		1	1	7						
Y	6	2	4	4	9	11	1	1	3			2	2	6	10	3		4	11	15	1		1			
Z	1				2				1																	

Frequency of di-grams formed by putting columns 1, 2, 3, ..., 6 to the right of column 7:

E	32	E	32	G	0	A	20	E	32	R	4
O	18	C	19	N	8	E	57	U	7	N	8
E	71	E	71	D	6	R	17	S	19	Y	41
Y	41	H	78	D	6	A	28	I	45	A	28
E	32	H	14	D	1	E	32	A	20	R	4
G	4	E	42	D	6	M	14	R	87	A	35
T	27	T	27	E	13	H	0	W	0	N	75
R	87	Y	4	T	37	T	37	K	0	U	3
N	7	H	78	O	50	E	71	D	6	E	71
P	2	S	12	C	3	C	3	R	31	Y	0
S	19	N	4	R	5	S	19	I	34	I	34
	340		381		189		298		281		303

We conclude that column 2 (with 381) is the most **probable** right-hand neighbour of column 7.