**Columnar Transposition Instruction Sheet**

Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns. Columnar Transposition builds in a keyword to order the way we read the columns, as well as to ascertain how many columns to use.

## Encryption

First, pick a keyword for the encryption. Write the plaintext out in a grid where the number of columns is the number of letters in the keyword. Then title each column with the respective letter from the keyword. Take the letters in the keyword in alphabetical order, and read down the columns in this order. If a letter is repeated, we do the one that appears first, then the next and so on.

As an example, let's encrypt the message "The tomato is a plant in the nightshade family" using the keyword *tomato*. We get the grid given below. The X's at the end are called nulls and are used to pad out the message (finish the grid) in the encryption process.

| T | O | M | A | T | O |
|---|---|---|---|---|---|
| 5 | 3 | 2 | 1 | 6 | 4 |
| T | H | E | T | O | M |
| A | T | O | I | S | A |
| P | L | A | N | T | I |
| N | T | H | E | N | I |
| G | H | T | S | H | A |
| D | E | F | A | M | I |
| L | Y | X | X | X | X |

The plaintext is written in a grid beneath the keyword. The numbers represent the alphabetical order of the keyword, and so the order in which the columns will be read.

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 "O" is 3 and the second "O" is 4, and the same thing for the two "T"s.

Starting with the column headed by "A", our ciphertext begins "TINESAX" from this column. We now move to the column headed by "M", and so on through the letters of the keyword in alphabetical order to get the ciphertext "TINESAX / EOAHTFX / HTLTHEY / MAIIAIX / TAPNGDL / OSTNHMX" (where the / tells you where a new column starts). The final ciphertext is rewritten in 5 letter groupings and is thus "TINES AXEOA HTFXH TLTHE YMAII AIXTA PNGDL OSTNH MX".

## Decryption

Start by writing out the keyword and the alphabetical order of the letters of the keyword. You must then divide the length of the ciphertext by the length of the keyword. The answer to this is the number of rows you need to add to the grid. You then write the ciphertext down the first column until you reach the last row. The next letter becomes the first letter in the second column (by the alphabetical order of the keyword), and so on.

As an example, we shall decrypt the ciphertext "ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX" given the keyword *potato*. We start by writing out the keyword and the order of the letters. There are 42 letters in the ciphertext, and the keyword has six letters, so we need 42 ÷ 6 = 7 rows.

| P | O | T | A | T | O |
|---|---|---|---|---|---|
| 4 | 2 | 5 | 1 | 6 | 3 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

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 "A". After the first column is entered we have the grid shown to the right.
We continue to add columns in the order specified by the keyword.

| P | O | T | A | T | O |
|---|---|---|---|---|---|
| 4 | 2 | 5 | 1 | 6 | 3 |
| | | | A | | |
| | | | R | | |
| | | | E | | |
| | | | S | | |
| | | | A | | |
| | | | S | | |
| | | | X | | |

| P | O | T | A | T | O |
|---|---|---|---|---|---|
| 4 | 2 | 5 | 1 | 6 | 3 |
| | O | | A | | |
| | S | | R | | |
| | T | | E | | |
| | H | | S | | |
| | E | | A | | |
| | Y | | S | | |
| | L | | X | | |

After inserting the second column.

| P | O | T | A | T | O |
|---|---|---|---|---|---|
| 4 | 2 | 5 | 1 | 6 | 3 |
| | O | | A | | O |
| | S | | R | | I |
| | T | | E | | I |
| | H | | S | | A |
| | E | | A | | I |
| | Y | | S | | E |
| | L | | X | | X |

After inserting the third column.

| P | O | T | A | T | O |
|---|---|---|---|---|---|
| 4 | 2 | 5 | 1 | 6 | 3 |
| P | O | T | A | T | O |
| E | S | A | R | E | I |
| N | T | H | E | N | I |
| G | H | T | S | H | A |
| D | E | F | A | M | I |
| L | Y | A | S | W | E |
| L | L | X | X | X | X |

The completely reconstructed grid.

Now we read off the plaintext row at a time to get "potatoes are in the nightshade family as well".