Cryptography Worksheet — Transposition Ciphers 1

One way to encipher a message is to jumble the order that the letters are written in.
What does this message say: "KCATTA"*? How has it been enciphered?*

What is bad about this method of enciphering?

Can you think of any other ways to reorder the letters of a message?

Ciphers that use a method of jumbling the order that the letters of the plaintext are written are called *Transformation Ciphers.*

A *Scytale* was an ancient tool used for encrypting messages, and is the earliest known "machine" used for cryptography. It was used by the Ancient Greeks, and specifically the Spartans, to send secret messages during military campaigns. Both the sender and receiver would need identical rods (the same length and diameter). The sender of the message would wrap a long thin piece of leather around his Scytale, and write the message in rows. When the leather was removed from the Scytale, it had a long list of letters running down it, it no particular order. When the message was delivered, the recipient would once again wrap the leather around his Scytale, revealing the original message.

What is the cipher key when using a Scytale?

The Scytale has been adapted into a written cipher called *Columnar Transposition*. For this, you need a grid with 5 columns, and you write the message horizontally across the grid, moving to the next row when you reach the end of the row. So for the plaintext "Meet me at the fountain at nine", we get the table shown. *Complete the table with the rest of the plaintext.*

m	e	e	t	m
e				

We then read off the ciphertext from the table by reading down each column in order. *What is the ciphertext for this encryption?*

How is this the same as the Scytale?

How secure is Columnar Transposition? Could we make it more secure? How?

Cryptography Worksheet — Transposition Ciphers 2

You receive the following message from a friend, that you know has been encrypted using Columnar Transposition, with 5 columns. *Decipher it. Explain how you do it.*

"ANYLD TRTIO LMHKM GUFEE XIHWI IPXDT INNAX"

(HINT: How many rows will there be in the grid?)

What do you notice about the last few letters of the plaintext? Why do you think this is?

Does this cause any problems to the security of the cipher?

Choose a key (a number of columns), and encipher a short message using this key. Give the key and the ciphertext to a friend to decode.

There are lots of different types of Transposition Cipher. One of the more famous ones is called the *Rail-fence Cipher*. In this cipher we write the plaintext diagonally across two lines. For example, given the plaintext "Life should be simple" we write it out as shown below. *Complete the table*.

L		**F**		**S**		**O**											
	I		**E**		**H**												

We then read across the top row, and then across the bottom row. *What is the ciphertext?*

How can we introduce a key to the Railfence Cipher to make it more secure?

How would we use a Railfence Cipher with 4 rows? Encipher the same message this way.

Choose a key, and encipher a message of your own. Pass it to a friend for them to decipher.

Can you think of any other ways of transposing the letters of a message? Explain you cipher to the person next to you, and give them and enciphered message to decipher.

What happens if you apply a Transposition Cipher twice? Is the same true for Substitution Ciphers?

Teacher's Notes — Transposition Ciphers 1

If this is coming after a discussion of Frequency Analysis, then introducing these types of ciphers as ways of getting round the problem of Frequency Analysis will probably be beneficial. Due to the fact that letters are not replaced, but rather just moved within the plaintext, the frequency of the letters will remain the same as for the original language.

How could we reorder the letters in word to create a ciphertext? Suggestions will probably include writing it backwards, swapping pairs of letters, etc. The first question has had the order of the letters reversed, so "KCATTA" becomes "attack". Discuss that this is a very simplistic method of enciphering, and that it is easily breakable, even by someone who has not come across cryptography.

Note that, when they are giving ideas for how to reorder the letters, that it must be easy to use for both the person enciphering, and the person intended to decipher the message (so a list of numbers for where to put the letters is impractical).

All ciphers which reorder the letters of the Plaintext are called Transposition Ciphers. Discuss what transposition means (to move something).

When discussing the use of the Scytale, it would be very useful to have a model prepared before the lesson. To make this, all you need is a cylinder (or preferably 2 identical cylinders) of any size (any prism will work as well). Then cut a long strip of paper out, that wraps round the cylinder. To demonstrate its use in class, write a short message on the paper whilst it is wrapped around the cylinder, and then unwrap it. Pass it round the room, to show that the message has been scrambled. Then ask a pupil to wrap the strip around the cylinder, to recover the original message. *(As a practical activity, making their own Scytale to use would be pleasant with some groups, and involves careful measuring and nets).* The key for a Scytale is the rod itself, and the size of the rod.

Columnar Transposition is the formal way of writing out how the Scytale works. Shown is the completed table. The ciphertext is "MEETT EAFAN ETOII TTUNN MHNAE".

m	e	e	t	m
e	a	t	t	h
e	f	o	u	n
t	a	i	n	a
t	n	i	n	e

Columnar is the same as the Scytale since we write the plaintext in the same order, and when you unwrap the leather on the Scytale, you have moved the letters by the same rule as using this method.

Columnar Transposition is not very secure as in this form it has no key. It can be made more secure by using a key. In this case, the key would be how many columns to use in the grid. This is equivalent to the length of the Scytale used.

Another method used for making the cipher more secure is to read the columns off in a different order, given by a list of numbers perhaps (where "25134" means **either** read the third column first, then the first column, then the fourth, fifth and finally second columns **or** read the second first, then the fifth, first, third and fourth). Another common way for doing this is using a keyword, where the alphabetical order of the letters gives the order (so "bread" would give the order "25413").

Teacher's Notes — Transposition Ciphers 2

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

The plaintext reads: "At midnight, you will find me in the park".

The method to decipher is to first work out how many rows are needed. This is easy to calculate as the number of rows times by the number of columns equals the numbers of letters. Since there are 5 columns, and 35 letters, there must be 7 rows. (How did the fact that the ciphertext is grouped into blocks of 5 help us here). Now you just need to write out the ciphertext down the columns, revealing the plaintext horizontally across the rows.

In the grid, we have inserted the letter "X" to fill in any empty squares in the last row. This is done to make the deciphering easier. It does not have to be the letter "X" that is used, sometimes punctuation marks are used, or other infrequent letters. Unfortunately, doing this can actually help somebody who intercepts the message to break the cipher, since the "X"'s in the cipher text are 7 apart, they can work out that there are seven rows without knowing the key. This can be avoided by adding the "X"'s randomly in the grid, rather than all at the end, and removing them when deciphering.

In the Railfence Cipher you write the first letter in the top left box, then the second letter in the box diagonally down to the right. When you reach the bottom row, you move right one box, but back up to the top. The completed table is shown, and the ciphertext is: "LFSOLBSMLIEHUDEIPE".

L		**F**		**S**		**O**		**L**		**B**		**S**		**M**		**L**	
	I		**E**		**H**		**U**		**D**		**E**		**I**		**P**		**E**

The key in the Railfence Cipher is provided by the number of rows down that you go. Using 4 rows, we get the ciphertext "LSLSLIHDIEFOBMEUEP".

L				**S**				**L**				**S**				**L**	
	I				**H**				**D**				**I**				**E**
		F				**O**				**B**				**M**			
			E				**U**				**E**				**P**		

Other methods for transposing the letters of the message could include: writing them in a spiral in a given grid size (starting in the centre or top left) and a direction.

If you apply a transposition cipher twice, then it just mixes the letters up even more. This make it harder for someone who intercepts it to break the code, but it also makes it a bit harder to decipher the message. This is not true for substitution ciphers. If you encipher "a" to "F", and then "F" to "W", then this is the same as just mapping "a" to "W". What is more secure, however, is to perform a substitution, followed by a transposition.