Substitution Ciphers

A substitution cipher is one in which letters are represented by other letters; it can be deciphered by someone knowing the order of the cipher alphabet used.

One method of hiding messages in this way was invented by Julius Caesar, Roman Emperor over two thousand years ago. It is known as the Caesar cipher.

To encode a message, for example:

THIS CODE WAS INVENTED BY JULIUS CAESAR

take each letter, go three along the alphabet and use that letter instead (e.g. A goes to D).

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

So the message becomes

WKLV FRGH ZDV LQYHQWHG EB MXOLXV FDHVDU

EXERCISE 1

What does the following message say?

JRQH WR ZDWFK KDUOHTXLQV. EDFN DW VHYHQ.

EXERCISE 2

In a Caesar cipher, the coded alphabet is in order (it just starts in a different place). If the coded alphabet is not in order, then we have a *substitution cipher.* Here is an example:

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

What does this message say?

ZHCVHYP NYDCTG SJL GCMO

EXERCISE 3

One example of a secret code method is called a **Keyword Cipher**

With this secret code keyword is placed at the beginning and this shifts the remaining letters of the alphabet, not used in the keyword, to the right. The letters that are not used in the keyword are placed in line in alphabetical order.

For example if the keyword was JAMESBOND the code would read as follows:

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

To code the message: SEND HELP QUICKLY

The code for this is: RSIE NSGL PUDMFGY

Here is a challenge for you to try, use the JAMESBOND Keyword Cipher to break the code and find the answer to this question.

In the James Bond film **The Man With The Golden Gun**, how many shots does Scaramanga have with his Golden Gun?

Below is the coded answer to this question.

GDHDTSE TK CURT KIS AUGGST

Vigenere Square

The following message uses one of the shifted alphabets from the Vigenere square. What does it say?

BPQA PIA JMMV APQNBML JG MQOPB

SEE THE SQUARE ON THE NEXT PAGE

Going through all the possibilities one by one to see which makes sense is a tedious way of doing it! We can use the fact that in English, some letters occur more often than others. For instance, the most common letter in English is 'E'.

Exercise 4

Which letter occurs most often in the next coded message? What letter might this represent? How much of a shift is this? Can you use this fact to decode the message without trying every possibility?

VXKT BT RWTTHT EATPHT

Vigenere Square

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

Activity: Deciphering a substitution cipher

We are now going to put together everything we have learned so far to decipher the following passage, which uses yet another substitution cipher.

Your task is to decipher the passage and hence complete the substitution alphabet.

Fill in the table of cipher and plain letters as you find them and write the plain letters above the cipher letters on the lines of text.

Several hints are given to help you.

AUHC MVKFC V BYZUGC V

IZMC CJ GUMBZYAZD UKUVM.

VC HZZGZB CJ GZ V HCJJB

PD CFZ VYJM KUCZ AZUBVMK

CJ CFZ BYVWZ UMB OJY U

IFVAZ V TJNAB MJC ZMCZY

OJY CFZ IUD IUH PUYYZB

CJ GZ.

Plain	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
Cipher																										

Hint 1: The three most frequently occurring letters in the passage above concur with the list above (although this is not always the case in short English passages). Find the three most commonly occurring letters in the cipher and substitute the letters you think they could represent.

Hint 2: Note that there are some one-letter words; one of these you should already have found. What would the other one be? Use this information to find a fourth letter.

Hint 3: The next most frequently occurring letter in the cipher can now be assigned its real letter. So you now have a fifth letter.

Hint 4: If you have done everything correctly, you should have a couple of words that look like T?E, where ? is an unknown letter. What common three-letter word starts with T and ends with E? Use this information to find the fifth letter.

Hint 5: Look at the word ?ATE. There are a few possibilities for this – DATE, FATE, GATE, LATE, MATE, RATE, SATE. Note that whatever the letter K stands for, it stands for the same thing in the second word – ?I?HT. Which letter would make this look like an English word?

Hint 6: What word could this be? Note that M is a fairly common letter, and that it occurs in word 20, which (if you've got everything right so far!) has a very common ending. By now you should have enough to work out/guess (both are very important skills in cipher analysis) to decipher the whole message!

Once you have deciphered the whole message, are you able to give the complete substitution table? If not, why not? What would you need to finish the task?