Exercise 5

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 6

The Martian alphabet has only 3 letters – ■ , ● and ▲ .

How many different substitution ciphers can you find for the Martian alphabet?

Exercise 7

The Venusian alphabet is similar, but has an extra letter – ⬟ .

(a) *How many different substitution ciphers can you find for the Venusian alphabet?*

(b) *Can you deduce how many ciphers there are for the Mercurian alphabet, which has 5 letters?*

In general, for an alphabet with n letters, there are

$$n \times (n-1) \times (n-2) \times \ldots \times 3 \times 2 \times 1$$

different substitution ciphers. This is sometimes written as $n!$, which is pronounced 'n factorial'.

For our English, 26-letter alphabet, there are $26!$ different substitution ciphers. This is an amazing 403 291 461 126 605 635 584 000 000, which is a little over 400 million million million million.

So it may seem that an arbitrary substitution cipher would be very hard to undo if you didn't know the order of the cipher alphabet.

However, we can use the same trick we used before. Remember, in English the most common letter is E. If we have an enciphered message, we can see which is the most common letter in the message, and guess that it is an E.

However, this time, we don't get the rest of the alphabet for free! So are we stuck? No – aside from E, some other letters of the alphabet appear more often than others. For example, T, O, N and A are fairly common, whilst J, X and Z are fairly rare.

Here is the alphabet in descending order of frequency for a typical passage of text in the English language:

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

A U H C M V K F C V B Y Z U G C V

I Z M C C J G U M B Z Y A Z D U K U V M.

V C H Z Z G Z B C J G Z V H C J J B

P D C F Z V Y J M K U C Z A Z U B V M K

C J C F Z B Y V W Z U M B O J Y U

I F V A Z V T J N A B M J C Z M C Z Y

O J Y C F Z I U D I U H P U Y Y Z B

C J G Z.

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?
