12 One-Time Pads

A *one-time pad* is a random collection of letters, e.g. FXIPUF, which can be used to encrypt messages with complete security (i.e. it is impossible to recover the message without knowing the key).

Suppose we wish to encrypt the message SECRET. There are three main methods for doing this, all of which involve a slightly different arithmetic from normal.

The arithmetic is called *modular arithmetic*. If the result of a sum is bigger than or equal to 26, we only consider the remainder after division by 26.

Thus $16 + 11 = 27 = 1 \pmod{26}$

and $11 \times 5 = 55 = 3 \pmod{26}$

Negative numbers follow the same rule, but we add 26 repeatedly rather than subtract.

So $11 - 16 = -5$

$= -5 + 26 = 21 \pmod{26}$

26 is known as the *modulus* of the arithmetic. Note that $26 = 0 \pmod{26}$.

You should already be familiar with this type of arithmetic when telling time:

for example, three hours after 11 o'clock is

$11 + 3 = 14$

$= 2$ o'clock

which is the same as saying

$11 + 3 = 14$

$= 2 \pmod{12}$

For this reason, modular arithmetic is also known as 'clock arithmetic'.

We treat each letter of the alphabet as a number between 0 and 25. We can use any order we like, but a sensible one would be $A = 1,\ B = 2,\ ...,\ Y = 25,\ Z = 0$. We ignore spaces between words.

So using numbers our message becomes

S	E	C	R	E	T
19	5	3	18	5	20

We do the same to our one-time pad,

F	X	I	P	U	F
6	24	9	16	21	6

Method 1: **Additive key**

Here we just *add* modulo 26 each letter of the message (plaintext) with its corresponding key.

Hence

$$S + F \Rightarrow 19 + 6 = 25 \pmod{26} \Rightarrow Y$$

$$E + X \Rightarrow 5 + 24 = 3 \pmod{26} \Rightarrow C, \text{ etc.}$$

This gives the message Y C L H Z Z, which without the one-time pad is very difficult to decrypt (decode).

If you have the one-time pad, i.e. the key, decryption is relatively simple; you just reverse the process by taking the key from the coded messages.

Here, we have

	Y	C	L	H	Z	Z			25	3	12	8	0	0
–	F	X	I	P	U	F	⇒	–	6	24	9	16	21	6
	S	E	C	R	E	T	⇐		19	5	3	18	5	20

Note

The encrypted letters are arranged in groups of five rather than with the spacing of the plaintext words they represent.

Exercise 1

Use the one-time pad PJKVA RJGME BWJBH *to encrypt the following messages:*

a) NICE ONE CYRIL

b) KEEP BRITAIN TIDY

Method 2: **Subtractive key**

This works in a similar way to Method 1, but here the value of the key is *subtracted* modulo 26 from the value of the plaintext.

For the message, SECRET, we have

$$S - F \Rightarrow 19 - 6 = 13 \pmod{26} \Rightarrow M$$

$$E - X \Rightarrow 5 - 24 = 7 \pmod{26} \Rightarrow G, \text{ etc.}$$

This gives the message M G T B J N.

Again, with the one-time pad, decryption is straightforward. This time you add the key, giving

	M	G	T	B	J	N			13	7	20	2	10	14
+	F	X	I	P	U	F	⇒	+	6	24	9	16	21	6
	S	E	C	R	E	T	⇐		19	5	3	18	5	20

Exercise 2

Repeat Exercise 1, using the one-time pad as a subtractive key.

Activity 1 (Method 3: **Minuend)**

There is a third method, namely 'minuend', which is the reverse of subtraction. Here the value of the plaintext is *subtracted* from the key.

Use this method to encrypt and decrypt SECRET. (Hint: to decrypt, you again *subtract* from the key.)

Exercise 3

Use the one-time pad PJKVA RJGME BWJBH *to decrypt the following messages:*

a) IXLLD JKJXQ GMYR *(additive key)*

b) CJDTK WEDYD QWUL *(subtractive key)*

c) SBVRZ ZENPV ND *(minuend)*

From now on we will just work with the 'additive key' method.

Exercise 4

a) *Use the one-time pad* DNCRG ZBQCS PQRXZ GNPI *to decrypt the message*

CCXFL VGIKT TZLQO NCEM.

b) *Now decrypt the same message using pad* WXABC QFUGF ELGYJ UTXY.

The one practical problem with this method is that if you are sending a message to someone, that someone has to know what the key is. How do you distribute keys in such a way that they are not made public?

The usual method is to physically deliver key on paper, floppy disk, etc. Another way round the problem is not to use totally random letters, but rather letters from some known scheme. This has its problems too as you will see in the next activity.

Activity 2

You intercept the following message:

TGFVJ ZFWDB ATBBT XRKUY ZJQYO PFF

You know that the sender always begins his encrypted messages with the word SECRET.

a) *What are the first six letters of the key?*

b) *How do you think the key might continue? Use this to decrypt the message.*

It can be helpful when deciphering the plaintext if you know, for example, that a message has been padded with dummy letters, e.g. XXX, or that each message begins with today's date.

Activity 3

You intercept another message from the same person:

IJBLW ZKJDI CXYUY UTVCF PQQDQ XJAPT LSGKK GUVJF FOCFK CCG.

a) *What are the first six letters of the key?*

b) *Does this help you recover the rest of the message?*