10 Public Key Cryptography

For many centuries secret messages had to be transmitted by using a key and/or method known only to those who were meant to share in the contents of those messages. Clearly, with such systems, there were always difficulties in distributing these keys or systems so that they did not fall into the wrong hands.

A breakthrough was made (in 1977) by Rivest, Shamir and Adleman (which is why the initials RSA are often attached to this system), when they devised a system using two keys. One key is used to put the message into cipher, and this key can be broadcast to the world so there is no distribution problem: this key is known as the *public key*. In addition to the public key another number (known as the *modulus*) is also published. The key which is needed to decipher the message is kept secret by the individual(s) for whom the message(s) is, or are, intended.

The system, based on some relatively simple ideas in *modulo arithmetic*, will be explained here by means of a numerical example, using only the smallest numbers it is possible to use.

First of all it is necessary to set up the key numbers which will be used, by following this routine.

	General Routine	*Example*
1.	Choose two *prime numbers*, p, q	$p = 2, \quad q = 5$
2.	Let $m = p \times q$	$m = 2 \times 5 = 10$
3.	Let $A = (p-1) \times (q-1)$	$A = 1 \times 4 = 4$
4.	Choose a number E which is less than A and has no factors in common with A.	$E = 3$
5.	Find a number D so that $(D \times E) - 1$ is a multiple of A.	$D = 7$ since $(3 \times 7) - 1 = 20$

$E\ (=3)$ is used to *encipher* the message, and is published.

$m\ (=10)$ is the *modulus* and is used to do the division where a remainder is required, and is also published. In this very simple example, 10 is easy to use since the remainder on division by 10 must be the last digit of the number being divided.

$D\ (=7)$ is used to *decipher* the message, and is *not* published.

We will use these values to put a message into cipher.

The numbers we work with must be one less than the value of m. In this case $m = 10$ which means that we cannot use a number larger than 9. As we shall be working initially with the values of the individual letters, we cannot have more than 9 letters. Since the normal alphabet contains 26 letters, we need to use a subset of the alphabet.

So, being limited to a small 'alphabet' of only 9 letters, it makes good sense to choose those which are most commonly used, namely A, D, E, H, N, O, R, S and T. These will

take the corresponding numerical values, 1, 2, ..., 9, giving the code

Letter	A	D	E	H	N	O	R	S	T
Number	1	2	3	4	5	6	7	8	9

For our message we will use the single word 'DOOR'.

First write out the message in plain text:

D O O R

change all the letters to their corresponding values:

2 6 6 7

raise all values to the *power* of $E\ (=3)$:

2^3 6^3 6^3 7^3

which produces the values:

8 216 216 343

Finally find the remainder when each of those is divided by $m\ (=10)$:

8 6 6 3

So the final message in cipher is 8663, and this is the message sent.

To decipher, a similar process is used except that *D* is used in place of *E* in finding the power.

Write out the message in its cipher form:

8 6 6 3

raise all values to the power of $D\ (=7)$

8^7 6^7 6^7 3^7

which is within range of a calculator and produces the values

2097152 279936 279936 2187

Find the remainder when divided by $m\ (=10)$, giving

2 6 6 7

and change those values back into letters:

D O O R

Exercise 1

Using the same values of E, D and m as in the example above,

a) *decipher 5729,*

b) *cipher and decipher the word 'RODENT'.*

Activity 1

Using the same values of *E*, *D* and *m* as before, send a message in cipher to a friend and decipher the response from the friend (who is using the same cipher!).

Activity 2

Why does this cipher offer little security?

The values of *E* and *m* have to be made public and, in this case, they are so small that it would be easy to see that since $m = 10$, then *p* and *q* must be 2 and 5. From that the value of *A* could be found and, since *E* is also known, then *D* could be found.

However, this defect can be overcome by making *p* and *q* very, very large so that the factoring of *m* is almost impossible. This is what is done in practice.

A much bigger problem is that putting only one letter at a time into cipher must mean that each letter will always have the same value in its cipher form throughout the message. This immediately makes the final cipher message breakable by using a simple frequency count.

This defect is overcome by grouping letters (and their values) together and putting each complete group into cipher.

To provide an example of this grouping idea, we need to work with new values since, as we have already seen, *m* must be bigger than the largest value to be worked on, which will be 99 when putting numbers together in pairs.

So now we use

$$m = 115 \qquad E = 83 \qquad D = 35$$

Activity 3

What values of *p* and *q* were used? Find *A* and check that $D \times E - 1$ is a multiple of *A*.

Using the same message as before, 'DOOR', its letter values are 2667. Working on groups of two digits, this splits into 26 and 67 and it is those two numbers which are acted on by the ciphering process.

Each has to be raised to the power of $E\ (= 83)$ and then the remainder found after division by $m\ (= 115)$.

We write this as $26^{83} \bmod 115$ and $67^{83} \bmod 115$.

Your calculator is unlikely to be able to cope with this, but we do have a short-cut to work out these remainders. This is shown in the next activity.

Suppose we want to find the reminder when 7^{11} is divided by 9. (We can easily check this calculation by using a calculator.) First note that we write this as

$$7^{11} \bmod 9$$

and we can build up the result by starting with

$$7^1 \bmod 9 = 7$$

Also

$$7^2 \bmod 9 = 49 \bmod 9 = 4 \qquad (1)$$

In fact, we can write

$$7^2 = n \times 9 + 4 \qquad (\text{in fact, } n = 5)$$

and so

$$7^4 = (9n + 4)^2$$

$$= 81n^2 + 72n + 4^2$$

Since the first two terms are divisible by 9,

$$7^4 \bmod 9 = 4^2 \bmod 9$$

$$= 16 \bmod 9$$

$$7^4 \bmod 9 = 7 \qquad (2)$$

Similarly, noting that

$$7^2 \bmod 9 = 4$$

and

$$7^4 \bmod 9 = 4^2 \bmod 9$$

$$= 7$$

then

$$7^8 \bmod 9 = 7^2 \bmod 9$$

$$= 4$$

and so on.

Now

$$7^{11} = 7^{8+2+1} = 7^8 \times 7^2 \times 7^1$$

so

$$7^{11} \bmod 9 = 7^8 \times 7^2 \times 7^1 \bmod 9$$

$$= 4 \times 4 \times 7 \bmod 9$$

$$= 16 \bmod 9 \times 7$$

$$= 7 \times 7 \bmod 9$$

$$= 4$$

Exercise 2

Check that $7^{11} \bmod 9 = 4$ *on your calculator.*

Activity 4

Calculate $9^{13} \bmod 11$ by first evaluating, using the method above,

$$9^1 \bmod 11,\quad 9^2 \bmod 11,\quad 9^4 \bmod 11,\quad 9^8 \bmod 11$$

(Check your answer by actually calculating 9^{13} and then finding the remainder on division by 11.)

Now that we have a method for finding the remainder of large powers of numbers on division we can use this method to find

$$26^{83} \bmod 115$$

Activity 5

Show that $26^2 \bmod 115 = 101$

$26^4 \bmod 115 = 81$

$26^8 \bmod 115 = 6$

$26^{16} \bmod 115 = 36$

$26^{32} \bmod 115 = 31$

$26^{64} \bmod 115 = 41$

Noting that $83 = 64 + 16 + 2 + 1$, show that

$$26^{83} \bmod 115 = 41 \times 36 \times 101 \times 26 \bmod 115$$

Hence show that

$$26^{83} \bmod 115 = 16$$

Exercise 3

Find $67^{83} \bmod 115$.

Hence

$$26^{83} \bmod 115 \equiv 16$$

and

$$67^{83} \bmod 115 \equiv 28$$

and the final cipher message is 1628.

Notice how the clue of the doubled up letters in the middle has now gone.

Deciphering would require the evaluation of 16^{35} and 28^{35} using the same value of m for the divider.

Exercise 4

Decipher 1628 using $D = 35$ *and* $m = 115$.

Note that this is still an insecure system as

- $m = 115$ is easy to factorise
- taking every 2 letters at a time would still be vulnerable to a frequency count.

Both of these weaknesses can be overcome by using very large primes and much larger groups, but a computer is needed for this!

Exercise 5

Use the same ciphers ($D = 35$, $E = 83$, $m = 115$*) to send the message*

SEND TENT

and also to decipher it.

Activity 6

Choose a new cipher that can be used to code all letters and numbers. Show how it works in practice.