UNIT 10 *Public Key Cryptography* Teacher Resource Material

Key Stage: *4 or A-level*

Target: *High achieving GCSE students*

Teaching Notes

This is a really important topic, now very relevant for internet security. The values used here for the parameters are not realistic but are chosen so that students can see how the method works. Despite this, the more complex examples do require extensive use of modulo arithmetic and some introduction or revision of this subject may be needed before pupils are ready to tackle this unit. Only the bare bones of the subject are presented here.

Solutions and Notes

Exercise 1 a) 5 7 2 9 $\Rightarrow$ 5 3 8 9, i.e. N E S T

b) Code: R O D E N T i.e. 7 6 2 3 5 9 $\Rightarrow$ 3 6 8 7 5 9

Decode: 3 6 8 7 5 9 $\Rightarrow$ 7 6 2 3 5 9 i.e. R O D E N T

Activity 3 $p = 5,\quad q = 23;\quad A = 4 \times 22 = 88;\quad D \times E - 1 = 33A$

Activity 4

$9^1 \bmod 11 = 9$

$9^2 \bmod 11 = 4$

$9^4 \bmod 11 = 4^2 \bmod 11 = 5$

$9^8 \bmod 11 = 5^2 \bmod 11 = 3$

$$\begin{aligned} 9^{13} \bmod 11 &= 9^{8+4+1} \bmod 11 \\ &= 3 \times 5 \times 9 \bmod 11 \\ &= 135 \bmod 11 \\ &= 3 \end{aligned}$$

Exercise 3 Noting that $83 = 64 + 16 + 2 + 1$, we need to calculate

$67^1 \bmod 115 = 67$

$67^2 \bmod 115 = 4$

$67^4 \bmod 115 = 4^2 \bmod 115 = 16$

$67^8 \bmod 115 = 16^2 \bmod 115 = 26$

$67^{16} \bmod 115 = 26^2 \bmod 115 = 101$

$67^{32} \bmod 115 = 101^2 \bmod 115 = 81$

$67^{64} \bmod 115 = 81^2 \bmod 115 = 6$

UNIT 10 *Public Key Cryptography* Teacher Resource Material (continued)

Thus

$$67^{83} = 67^{64+16+2+1} = 67^{64} \times 67^{16} \times 67^{2} \times 67^{1}$$

and

$$\begin{aligned} 67^{83} \bmod 115 &= 6 \times 101 \times 4 \times 67 \bmod 115 \\ &= 162\,408 \bmod 115 \\ &= 28 \end{aligned}$$

Exercise 4 We need to find

$$16^{35} \bmod 115 \quad \text{and} \quad 28^{35} \bmod 115$$

Calculating in the same way gives

$$16^{35} \bmod 115 = 26 \quad \text{and} \quad 28^{35} \bmod 115 = 67$$

Hence message was, as expected,

2	6	6	7
↓	↓	↓	↓
D	O	O	R

Exercise 5

S	E	N	D	T	E	N	T
↓	↓	↓	↓	↓	↓	↓	↓
8	3	5	2	9	3	5	9

and, in pairs (except for the last digit)

83 52 93 59

We now need to calculate each number to the power $83 \bmod 115$,

e.g. $83^{1} \bmod 115 = 83$

$$\begin{aligned} 83^{2} \bmod 115 &= 104 \\ 83^{4} \bmod 115 &= 104^{2} \bmod 115 \\ &= 6 \\ 83^{8} \bmod 115 &= 6^{2} \bmod 115 \\ &= 36 \\ 83^{16} \bmod 115 &= 36^{2} \bmod 115 \\ &= 31 \\ 83^{32} \bmod 115 &= 31^{2} \bmod 115 \\ &= 41 \end{aligned}$$

UNIT 10 *Public Key Cryptography* Teacher Resource Material (continued)

$$83^{64} \bmod 115 = 41^2 \bmod 115$$
$$= 71$$

So

$$83^{64} \bmod 115 = 83^{64+16+2+1} \bmod 115$$
$$= 71 \times 31 \times 104 \times 83 \bmod 115$$
$$= 112$$

Calculating in the same way we obtain

112 58 47 29

For decoding, there is a potential problem here. If no spaces were left in the code there would be 9 digits. So how does the decoder know which 3 to take? It has to be less than 115, and there is only one possibility, i.e. the first three digits, 112.