Codes and Ciphers	UNIT 10 *Public Key Cryptography* Lesson Plan 1	*Coding and Decoding*

Activity | | **Notes**

T: Teacher P: Pupil Ex.B: Exercise Book

1 **Introduction**

T: The RSA code, named after its inventors, Rivest, Shamir and Adleman, forms the basis of a method which continues to be extensively used for coding messages and information.

Notes: Interactive discussion on the need for coding in on electronic age, e.g. over the internet, building on what pupils already know, particularly with regard to providing internet security.

T: We'll go through the RSA coding method, using a simple example. The method is explained in this algorithm.

Notes: T shows **OS 10.1** on OHP and gives a copy to each P.

T: We start with two prime numbers – any suggestions (remember, we are aiming to make this easy)? *(2 and 3)*

T: That's too easy! Let's use 2 and 5 here. You can try other prime numbers for homework!

T: Who would like to show this on the board?

T: Let's complete the table together; you write on your sheet:
$p = 2,\ q = 5$

T: What is m ? $(m = 2 \times 5 = 10)$

T: What is A ? $(A = 1 \times 4 = 4)$

T: Choose E so that it is less than A and has no factors (except 1), in common with A. $(E = 3)$

Notes: T should make this as interactive as possible while guiding Ps in the correct direction. Ps (– less able where possible, chosen by T) answer T's questions; one P writes on the board and all Ps write on their copies of **OS 10.1**.

T: The next stage is not so easy. We need to find D so that $D \times E - 1$ is a multiple of A. $(D = 7)$

T: Why?

P: $3 \times 7 - 1 = 20 = 5 \times A$

T: Well done.

Notes: T gives Ps a few moments to calculate this, and then chooses P to give an answer and reason. Other Ps can help if necessary.

T: OK – we are ready now! Note that:

$E\ (= 3)$	is the encipher to be published
$m\ (= 10)$	is the modulus; we will use it for division when we will need to find the remainder)
$D\ (= 7)$	is the decipher and is <u>secret</u> (known only to the message sender and the message receiver)

T: To keep it simple, and because we cannot have more letters than the value of m, we will have just 9 letters in our alphabet.

Notes: T could allow Ps to choose the letters here, but should note that the letters chosen will need to make some meaningful words.

T: Here are our letters and their number values:

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

Notes: **OS 10.2** is shown on OHP, or written on board.

T: What shall we code? *(Pupils' suggestions, or DOOR)*

T: I need volunteers to work at the board.

T: We take each number to the power of $E\ (= 3)$.

Notes: P at board completes the first two lines of the table; other Ps pay attention.

(continued)

Codes and Ciphers	**UNIT 10** *Public Key Cryptography* Lesson Plan 1	*Coding and Decoding*
Activity		***Notes***
1 *(continued)*	<table><tr><td>Message</td><td>D</td><td>O</td><td>O</td><td>R</td></tr><tr><td>Number value</td><td>2</td><td>6</td><td>6</td><td>7</td></tr></table> T: Now we take each number to the power of $E\ (=3)$. P (on board): 2^3 6^3 6^3 7^3 8 216 216 343 T: Now work out the remainder on division by 10. That's easy! P (on board): 8 6 6 3 T: So the coded message is 8 6 6 3. T: We use a similar method to decode. You take each of the numbers to the power of $D\ (=7)$. P (on board): 8^7 6^7 6^7 3^7 2097152 279936 279936 2187 T: As before, we take the remainder on division by $m\ (=10)$. P (on board): D O O R T: Well done! *20 mins*	P at board, completes the first two lines of the table, with advice from class, if necessary. It might be useful for Ps to each have a copy of **OS 10.2** and quickly copy information from board. Other Ps help with the calculations and agree/disagree with what is written on board.
2	**Practice** Exercise 1, part b). *30 mins*	Ps work in pairs with T monitoring and helping. Ps have about 8 minutes for this before T interrupts and work is reviewed interactively.
3 *(continued)*	**Security** T: Why is our illustration not realistic? *(E and m are so small that m, p, q, etc. could easily be deduced)* T: Yes, in practice, p and q are very large so that it would be almost impossible to factor m. Of course, the process of deciphering and enciphering could be computerised. T: Can you find any other obvious flaws in the process? *(Letters repeated will have identical codes)* T: How could you overcome this? *(?)* T: One way is to work using pairs. So for DOOR, we have D O O R ↓ ↓ ↓ ↓ 2 6 6 7 i.e. 26 and 67 What is the problem here? *(You need the m value to be larger than 99)*	This part might need more clarification; remember that the number of possible numbers has to be less than m for the method to work.

Codes and Ciphers	**UNIT 10** *Public Key Cryptography* Lesson Plan 1	*Coding and Decoding*
Activity		***Notes***
3 *(continued)*	T: Yes; so here is a new choice of parameters: $\boxed{m = 115, \quad E = 83, \quad D = 35}$ T: What are p and q? *(5 and 23)* T: A ? $(A = 4 \times 22 = 88)$ T: Is $D \times E - 1$ a multiple of A ? *(Yes:* $D \times E - 1 = 2904 = 33A$*)* T: So this code will work. But what will cause problems? *(Calculating* 26^{83} mod 115*)*	T puts these on board. Depending on the class, T can ask Ps to investigate methods of calculating these modulo sums, or can ask Ps to design their own cipher code.
	45 mins	
	Homework Design a simple RSA code and check that it works.	