

<p><i>Codes and Ciphers</i></p>	<p><b>UNIT 10</b> <i>Public Key Cryptography</i> Lesson Plan 1</p>	<p><i>Coding and Decoding</i></p>																		
<p><b>Activity</b></p> <p><b>1</b></p> <p><i>(continued)</i></p>	<p><b>Introduction</b></p> <p>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.</p> <p>T: We'll go through the RSA coding method, using a simple example. The method is explained in this algorithm.</p> <p>T: We start with two prime numbers – any suggestions (remember, we are aiming to make this easy)? <i>(2 and 3)</i></p> <p>T: That's too easy! Let's use 2 and 5 here. You can try other prime numbers for homework!</p> <p>T: Who would like to show this on the board?</p> <p>T: Let's complete the table together; you write on your sheet:</p> $p = 2, q = 5$ <p>T: What is <math>m</math> ? <i>( <math>m = 2 \times 5 = 10</math> )</i></p> <p>T: What is <math>A</math> ? <i>( <math>A = 1 \times 4 = 4</math> )</i></p> <p>T: Choose <math>E</math> so that it is less than <math>A</math> and has no factors (except 1), in common with <math>A</math>. <i>( <math>E = 3</math> )</i></p> <p>T: The next stage is not so easy. We need to find <math>D</math> so that <math>D \times E - 1</math> is a multiple of <math>A</math>. <i>( <math>D = 7</math> )</i></p> <p>T: Why?</p> <p>P: <math>3 \times 7 - 1 = 20 = 5 \times 4</math></p> <p>T: Well done.</p> <p>T: OK – we are ready now! Note that:</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><math>E (= 3)</math> is the encipher to be published</p> <p><math>m (= 10)</math> is the modulus; we will use it for division when we will need to find the remainder)</p> <p><math>D (= 7)</math> is the decipher and is <u>secret</u> (known only to the message sender and the message receiver)</p> </div> <p>T: To keep it simple, and because we cannot have more letters than the value of <math>m</math>, we will have just 9 letters in our alphabet.</p> <p>T: Here are our letters and their number values:</p> <table border="1" style="margin: 10px auto;"> <tr> <td>A</td><td>D</td><td>E</td><td>H</td><td>N</td><td>O</td><td>R</td><td>S</td><td>T</td> </tr> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td> </tr> </table> <p>T: What shall we code? <i>(Pupils' suggestions, or DOOR)</i></p> <p>T: I need volunteers to work at the board.</p> <p>T: We take each number to the power of <math>E (= 3)</math>.</p>	A	D	E	H	N	O	R	S	T	1	2	3	4	5	6	7	8	9	<p style="text-align: center;"><b>Notes</b></p> <p>T: Teacher P: Pupil Ex.B: Exercise Book</p> <p>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.</p> <p>T shows <b>OS 10.1</b> on OHP and gives a copy to each P.</p> <p>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 <b>OS 10.1</b>.</p> <p>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.</p> <p>T could allow Ps to choose the letters here, but should note that the letters chosen will need to make some meaningful words.</p> <p><b>OS 10.2</b> is shown on OHP, or written on board.</p> <p>P at board completes the first two lines of the table; other Ps pay attention.</p>
A	D	E	H	N	O	R	S	T												
1	2	3	4	5	6	7	8	9												



<b>Codes and Ciphers</b>	<b>UNIT 10</b> <i>Public Key Cryptography</i> Lesson Plan 1	<i>Coding and Decoding</i>
<b>Activity</b> <b>3</b> <i>(continued)</i>	<p>T: Yes; so here is a new choice of parameters:</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <math>m = 115, \quad E = 83, \quad D = 35</math> </div> <p>T: What are <math>p</math> and <math>q</math>? <span style="float: right;"><i>(5 and 23)</i></span></p> <p>T: <math>A</math> ? <span style="float: right;"><i>(A = 4 × 22 = 88)</i></span></p> <p>T: Is <math>D \times E - 1</math> a multiple of <math>A</math> ?  <span style="float: right;"><i>(Yes: D × E - 1 = 2904 = 33A)</i></span></p> <p>T: So this code will work. But what will cause problems?  <span style="float: right;"><i>(Calculating <math>26^{83} \bmod 115</math>)</i></span></p> <p style="text-align: right;"><i>45 mins</i></p>	<p style="text-align: center;"><b>Notes</b></p> <p>T puts these on board.</p> <p>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.</p>
	<p><b>Homework</b></p> <p>Design a simple RSA code and check that it works.</p>	