### UNIT 10 Public Key Cryptography

#### Lesson Plan 1

### Codes and Ciphers

#### Activity 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.

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

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:

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>5</td>
</tr>
</tbody>
</table>

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 \( A \). \( E = 3 \)

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.

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 secret (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.

T: Here are our letters and their number values:

<table>
<thead>
<tr>
<th>A</th>
<th>D</th>
<th>E</th>
<th>H</th>
<th>N</th>
<th>O</th>
<th>R</th>
<th>S</th>
<th>T</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

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).

(continued)
### Activity 1 (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>DOOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number value</td>
<td>2 6 6 7</td>
</tr>
</tbody>
</table>

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

P (on board): \[ \begin{array}{cccc} 2^3 & 6^3 & 6^3 & 7^3 \\ 8 & 216 & 216 & 343 \end{array} \]

T: Now work out the remainder on division by 10. That's easy!

P (on board): \[ \begin{array}{cccc} 8 & 6 & 6 & 3 \end{array} \]

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): \[ \begin{array}{cccc} 8^7 & 6^7 & 6^7 & 3^7 \\ 2097152 & 279936 & 279936 & 2187 \end{array} \]

T: As before, we take the remainder on division by $m (= 10)$.

P (on board): DOOR

T: Well done!

---

### Practice

Exercise 1, part b).

---

### 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

<table>
<thead>
<tr>
<th>D O O R</th>
</tr>
</thead>
<tbody>
<tr>
<td>↓ ↓ ↓ ↓</td>
</tr>
<tr>
<td>2 6 6 7</td>
</tr>
</tbody>
</table>

i.e. 26 and 67

What is the problem here?

*You need the m value to be larger than 99*

---

### Coding and Decoding

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.

Ps work in pairs with T monitoring and helping. Ps have about 8 minutes for this before T interrupts and work is reviewed interactively.

This part might need more clarification; remember that the number of possible numbers has to be less than $m$ for the method to work.
### Activity 3 (continued)

T: Yes; so here is a new choice of parameters:

\[ m = 115, \quad E = 83, \quad D = 35 \]

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 \( A \)?

\( \text{(Yes: } D \times E - 1 = 2904 = 33A) \)

T: So this code will work. But what will cause problems?

\( \text{(Calculating } 26^{83} \text{ mod } 115) \)

---

**Homework**

Design a simple RSA code and check that it works.

---

**Notes**

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.