11. Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages. First of all, we assign each letter of the alphabet a number: $A = 1$, $B = 2$, $\ldots$, $Z = 26$. We’ll need some punctuation: period = 27, comma = 28, $? = 29$, and blank = 30. It is convenient to put our conversion values in a table, for easy referral.

<table>
<thead>
<tr>
<th>A</th>
<th>1</th>
<th>K</th>
<th>11</th>
<th>U</th>
<th>21</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>2</td>
<td>L</td>
<td>12</td>
<td>V</td>
<td>22</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>M</td>
<td>13</td>
<td>W</td>
<td>23</td>
</tr>
<tr>
<td>D</td>
<td>4</td>
<td>N</td>
<td>14</td>
<td>X</td>
<td>24</td>
</tr>
<tr>
<td>E</td>
<td>5</td>
<td>O</td>
<td>15</td>
<td>Y</td>
<td>25</td>
</tr>
<tr>
<td>F</td>
<td>6</td>
<td>P</td>
<td>16</td>
<td>Z</td>
<td>26</td>
</tr>
<tr>
<td>G</td>
<td>7</td>
<td>Q</td>
<td>17</td>
<td></td>
<td>27</td>
</tr>
<tr>
<td>H</td>
<td>8</td>
<td>R</td>
<td>18</td>
<td></td>
<td>28</td>
</tr>
<tr>
<td>I</td>
<td>9</td>
<td>S</td>
<td>19</td>
<td></td>
<td>29</td>
</tr>
<tr>
<td>J</td>
<td>10</td>
<td>T</td>
<td>20</td>
<td>b</td>
<td>30</td>
</tr>
</tbody>
</table>

This is a rather crude code. It doesn’t allow for lower case letter, the digits, or many other punctuation symbols. But it will serve our purpose and the calculations are not too long. Our modulus (clock number) is $p = 31$.

The **31-code** requires an encoding number $e$ between 2 and 30. Say we choose the encoding number $e = 7$. Using this value of $e$, we can encode our messages in a simple way. Suppose we wish to encode the message $HELP$. We first convert each of the four letters $H, E, L, P$ into its numerical equivalent, using the above table. Since $H \rightarrow 8$, $E \rightarrow 5$, etc., our message becomes

$$8, \ 5, \ 12, \ 16.$$ 

Multiply each of these four numbers by the encoding number $e = 7$ to get

$$56, \ 35, \ 84, \ 112.$$
Now reduce each number using the 31-clock: 56 mod 31 = 25, 35 mod 31 = 4, 84 mod 31 = 22, and 112 mod 31 = 19 to get the remainders 25, 4, 22, 19.

Convert these four numbers back to letters and you have the encoded message \(YDVS\).

Now suppose you receive the scrambled message \(YDVS\). How can you decode this message to get the original message? The answer is surprisingly simple: apply the same procedure as when encoding, except you must use the decoding number \(d\) that corresponds to the number \(e\) used to encode the original message. In our case, it turns out that the number \(d = 9\) corresponds to the encoding number \(e = 7\). To decode, first convert the letters to numbers:

\[(Y, D, V, S) \rightarrow (25, 4, 22, 19).\]

Multiply each number by \(d = 9\):

\[(225, 36, 198, 171).\]

Reduce these four numbers on a 31-clock, using 225 mod 31 = 8, etc., to obtain

\[(8, 5, 12, 16).\]

So our original message was \(HELP\).

Two questions arise: (1) How do we find the decoding number \(d\) if we know the encoding number \(e\)? (2) Why does this work?

To answer the first question, solve the POW problem with the numbers \(d = 7\) and \(p = 31\). Since 31 = 4 \(\times\) 7 + 3, we have the reduction \((7, 31) \rightarrow (3, 7)\) and we can easily solve POW with 3 and 7: \(7 - 2 \times 3 = 1\). Working backwards, we have

\[
1 = 7 - 2 \times 3 \quad \text{solution for 5 and 7} \\
= 7 - 2(31 - 4 \times 7) \quad \text{substituting } 3 = 31 - 4 \times 7 \\
= 7 - 2 \times 31 + 8 \times 7 \quad \text{expand the parentheses} \\
= 9 \times 7 - 2 \times 31 \quad \text{gather the 7's together}
\]

The decoding number \(d\) is the 9 in this last equation.

Why does this work? The key equation is \(1 = 9 \times 7 - 2 \times 31\), or equivalently, \(de = 9 \times 7 = 1 + 2 \times 31\). Suppose we start with the letter ‘H’, the first letter of our message. Since
the ‘H’ has value 8, the encoding process multiplies 8 by $e$. The decoding process multiplies the result by $d$, giving

$$d(e8) = (de)8 = (1 + 2 \times 31)8 = 8 + 16 \times 31.$$ 

It is clear that this last number reduces to 8 mod 31.

The state of the art encryption method, called RSA, uses a much larger clock size consisting of hundred of digits and uses exponentiation rather than multiplication. But the basic principle of RSA encryption is much the same as the code described here.

**Exercise #44.** Given $d = 13$, decode the following message, to discover the number one security issue of the White House: AYMOEL

**Exercise #45.** If $e = 17$, find $d$.

**Exercise #46.** Given $e = 10$, encode the word: URANUS. Insert joke here.

**Exercise #47.** A message of advice for passing this course was encoding using $e = 10$. If the scrambled message is DNXIB, what was the original message.

**Exercise #48.** What happens if you use encoding number $e = 1$?