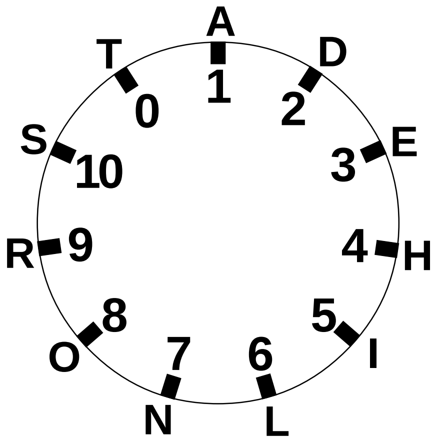
Messages can be put into cipher using a multiplication process, again working with modulo arithmetic. However, working 'by hand' is rather tedious since the numbers soon become very large and always have to be reduced by the modulus. It is no quick mental process to find that 485 is 17 (modulo 26). So, we shall work with a reduced alphabet of only 11 letters and do all our arithmetic modulo 11. The 11 letters we shall use are

A D E H I L N O R S T

These with their matching numbers are shown on the 'clock' on the right.

Notice the number 0 appears in place of 11.



The next problem is to know the results, in modulo 11 arithmetic, of all the possible multiplications that could be done. To avoid any long explanation and keep it simple we will use a multiplication table written in modulo 11 AND shown below.

Multiplication Table - Modulo 11

×	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

It certainly looks different to the normal multiplication table to which we are accustomed.

Two points to be aware of.

Multiplication by 1 is not shown. This is because multiplying by 1 leaves the number unchanged regardless of the modulus.

Multiplication by 0 is not shown. This is because multiplication by 0 produces an answer of 0 regardless of the modulus.

With those facts and the multiplication table, we can put a plain message into cipher.

We will encipher the message

RAIDER LOST

using the multiplication key

(7, 4, 2, 9)

All the working is shown in this table

Plain message	R	A	I	D	E	R	L	O	S	T
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Change to numbers	9	1	5	2	3	9	6	8	10	0
MULTIPLY by key	7	4	2	9	7	4	2	9	7	4
Result (from table)	8	4	10	7	10	3	1	6	4	0
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Change to letters	O	H	S	N	S	E	A	L	H	T

Then the cipher message to be sent is

OHSNS EALHT

Multiplication Ciphers ~ 2

Deciphering

Deciphering is also done by multiplication but using a different key. The deciphering key is derived from the enciphering key by use of this table.

If enciphering multiplier is	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**0**
Deciphering multiplier is	**1**	**6**	**4**	**3**	**9**	**2**	**8**	**7**	**5**	**10**	**0**

The connection between the two keys becomes apparent if corresponding numbers are multiplied together and then divided by 11 (with the exception of the 0)

So, in the previous example, where the Enciphering key was (7, 4, 2, 9) the deciphering key would need to be (8, 3, 6, 5)

Of course the key can always be put into its equivalent letter form

Exercise 15

Put these plain messages into cipher using the (multiplication key) given.

1. Tell Hilda to hide (4, 5, 2, 3, 6)
2. Lads lost in hills (5, 8, 7, 7)
3. Rations are short (2, 3, 4, 5, 6, 7)
4. Are shells sent on train (9, 8, 7, 6, 5, 4, 3, 2)

Decipher these messages using the (multiplication key) given.

5. NNRAR SAISH TARLN (4, 2, 5, 2)
6. AEHRS HHTON HNHST (1, 2, 3, 2, 1)
7. ORONR EIOHO TILSS (7, 8, 9, 4, 5, 6)
8. TEAOT NNNAE DSLHD (LEADER)

Decipher these messages knowing it is the (enciphering key) which is given.

9. RLOHO ERSEO NNOIT (1, 6, 4, 3)
10. DAEIH OIOIO RHEIN (3, 5, 7, 9, 9)

Increasing Security

So far we have only used addition or multiplication on their own. Neither is very secure. Addition only produces a 'shift' similar to that done by Cipher Wheels or their equivalent. Multiplication only ensures that the cipher alphabet is 'mixed up'. The use of a key steps up the security a little, but not very much if the message is a long one. Inevitably there will be repetition and patterns will emerge that are fatal flaws in any ciphering system.

A big increase in security is offered by combining addition and multiplication and also using the message itself as a part of the ciphering process. One of doing this is to use a matrix and matrix multiplication.

A suitable matrix could look like this $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

The process for carrying out the multiplication requires that the plain message (in its number form) is written on two lines, in some organised manner, and the numbers are worked on in pairs, using the number from the top and the bottom to create another pair for the top and the bottom of the cipher message. Remember that all the arithmetic is done modulo 11.

When adding**:** any number greater than 10 must have 11 subtracted from it.

When multiplying**:** the Modulo 11 multiplication table must be used.

The method of carrying out the process is summarised here

$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

Multiply TOP number by this number (1)
Multiply BOTTOM number by this number (2)
and ADD these together to make Cipher TOP number

Multiply BOTTOM number by this number (4)
Multiply TOP number by this number (3)
and ADD these together to make Cipher BOTTOM number

Using that same matrix as our key we will encipher the message

RAID IN EAST

First change it into numbers

9 1 5 2 5 7 3 1 10 0

and put the second under the first to get

$$\begin{pmatrix} 9 & 1 & 5 & 2 & 5 \\ 7 & 3 & 1 & 10 & 0 \end{pmatrix}$$

then carry out the above instructions like this

$$\begin{array}{lc} \mathbf{1}\times & \left(\begin{array}{ccccc} 9 & 1 & 5 & 2 & 5 \\ 7 & 3 & 1 & 10 & 0 \end{array}\right) \\ \mathbf{2}\times & \end{array} \begin{array}{l} = 9\ \ 1\ \ 5\ \ 2\ \ 5 \\ = \underline{3\ \ 6\ \ 2\ \ 9\ \ 0} \end{array} \qquad \begin{array}{lc} \mathbf{3}\times & \left(\begin{array}{ccccc} 9 & 1 & 5 & 2 & 5 \\ 7 & 3 & 1 & 10 & 0 \end{array}\right) \\ \mathbf{4}\times & \end{array} \begin{array}{l} = 5\ \ 3\ \ 4\ \ 6\ \ 4 \\ = \underline{6\ \ 1\ \ 4\ \ 7\ \ 0} \end{array}$$

$$\begin{array}{llcccccclccccc} \text{ADD} & \textit{(Remember mod 11)} & = & 1 & 7 & 7 & 0 & 5 & \qquad = & 0 & 4 & 8 & 2 & 4 \\ & & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \text{Change to letters} & & = & A & N & N & T & I & \qquad = & T & H & O & D & H \end{array}$$

and the cipher message is

ANNTI THODH

Deciphering

Deciphering is done in a similar way to enciphering but using a different matrix. We will not concern ourselves here with how it is derived from the original matrix. (For those interested, it depends upon forming the inverse of the enciphering matrix using modulo arithmetic.)

We will decipher the message

NDERL SNDSA RSRRI RHENO

using the deciphering matrix $\begin{pmatrix}3&2\\5&1\end{pmatrix}$

Change the message into numbers

7 2 3 9 6   10 7 2 10 1   9 10 9 9 5   9 4 3 7 8

Stack 1st group over 2nd group, 3rd group over 4th group

$$\begin{pmatrix}7&2&3&9&6\\10&7&2&10&1\end{pmatrix}\qquad\qquad\begin{pmatrix}9&10&9&9&5\\9&4&3&7&8\end{pmatrix}$$

Carry out multiplication and addition (mod 11) as before, and change back into letters

$$\begin{array}{l}\mathbf{3}\times\\\mathbf{2}\times\end{array}\begin{pmatrix}7&2&3&9&6\\10&7&2&10&1\end{pmatrix}\begin{array}{cccccc}=&10&6&9&5&7\\=&9&3&4&9&2\\\hline\end{array}$$

$$\begin{array}{lcccccc}\text{ADD } \textit{(Remember mod 11)}&=&8&9&2&3&9\\&&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\\text{Change to letters}&=&O&R&D&E&R\end{array}$$

$$\begin{array}{l}\mathbf{5}\times\\\mathbf{1}\times\end{array}\begin{pmatrix}7&2&3&9&6\\10&7&2&10&1\end{pmatrix}\begin{array}{cccccc}=&2&10&4&1&8\\=&10&7&2&10&1\\\hline=&1&6&6&0&9\\&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\=&A&L&L&T&R\end{array}$$

$$\begin{array}{l}\mathbf{3}\times\\\mathbf{2}\times\end{array}\begin{pmatrix}9&10&9&9&5\\9&4&3&7&8\end{pmatrix}\begin{array}{cccccc}=&5&8&5&5&4\\=&7&8&6&3&5\\\hline\end{array}$$

$$\begin{array}{lcccccc}\text{ADD } \textit{(Remember mod 11)}&=&1&5&0&8&9\\&&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\\text{Change to letters}&=&A&I&T&O&R\end{array}$$

$$\begin{array}{l}\mathbf{5}\times\\\mathbf{1}\times\end{array}\begin{pmatrix}9&10&9&9&5\\9&4&3&7&8\end{pmatrix}\begin{array}{cccccc}=&1&6&1&1&3\\=&9&4&3&7&6\\\hline=&10&10&4&8&0\\&\downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\=&S&S&H&O&T\end{array}$$

and the recovered message is

ORDER ALL TRAITORS SHOT

Exercise 16

Recover the plain text from these using the (deciphering key) given.

1. HOOES ATTHO LNSTI ATDLO $\begin{pmatrix}1&2\\3&4\end{pmatrix}$

2. ELREN TTSOT IEEDA OILHD $\begin{pmatrix}2&5\\4&3\end{pmatrix}$

3. HTNEI INRHA HNEIA DNODD $\begin{pmatrix}3&2\\5&1\end{pmatrix}$

4. ATANO DOEOO SSALD TLNES $\begin{pmatrix}7&8\\8&7\end{pmatrix}$

5. LRINN NSTNL IODEL HADNA NLLAS ATOIA $\begin{pmatrix}9&1\\6&4\end{pmatrix}$

Decipher this given only the (enciphering key)

6. SLRTS IINEN AEOIL HONEO $\begin{pmatrix}5&7\\8&6\end{pmatrix}$