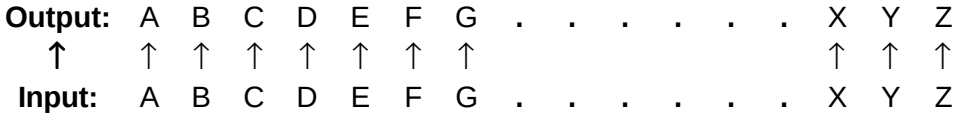
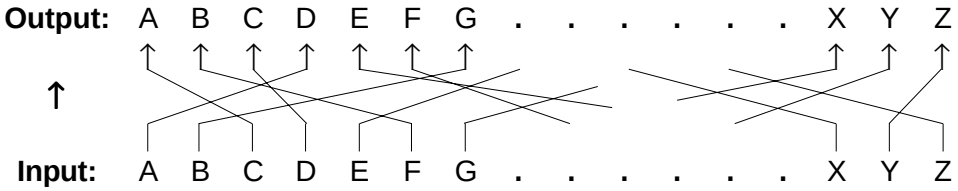
Rotor Ciphers ~ 1

Imagine how an electric typewriter or a computer works. When we press a letter on the keyboard (the input), a signal is sent along a wire and that letter appears as the output. It might appear on the screen, on paper or even be sent off as part of a message. There is a simple connection between the input and the output, and we can show it like this:-



Now suppose that the wiring was connected up in a different way, rather like this:-



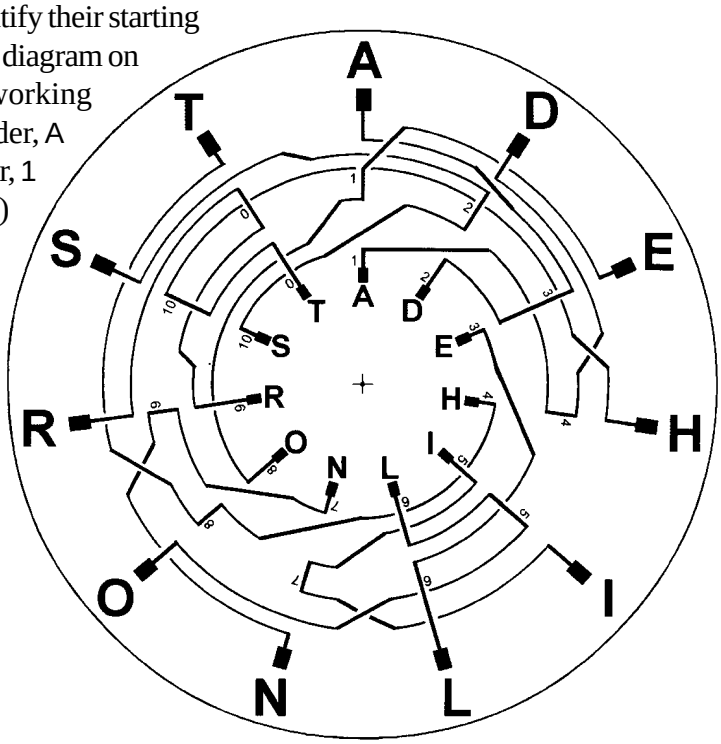
so that when key A was pressed the output was D, when B was pressed the output was G, and so on. In fact, our message would be put into cipher as it was being keyed in. It would be a simple cipher since every plain text letter would be enciphered in exactly the same way. But if the wiring could be readjusted quickly you would have the basis of a real ciphering machine.

Special ciphering machines which take advantage of this idea are made with several wheels, usually known as rotors. The electrical signal, from input to output, passes through all the rotors which contain the wiring. The rotors are able to turn independently (but always remain in contact with each other) so that many millions of different wiring systems, and hence ciphers, are possible. Usually it is arranged that one of the rotors is moved on one position every time an input key is struck, so that even a very long message has each plain text letter enciphered by a different cipher alphabet every time.

To see how such a machine works, and to attempt the exercise problems, the model needs to be made up. The template for the model is on Sheet 3.

Some points to note. The model uses an eleven letter alphabet for miniaturisation purposes only. The two alphabet wheels are not rotors since they carry no wiring, but represent only the input and output (whatever they are). Here we will designate the inner wheel as being the cipher and the outer wheel as the plain text. All movements are clockwise.

All rotor machines need to be able to identify their starting position. In the case of the settings shown in the diagram on the right we list them as (A 11 A). That is, working vertically up from the centre we read off, in order, A from the first (inner) wheel, 1 from the first rotor, 1 from the second rotor, A from the second (outer) wheel. Position (T 00 T) would also be valid. Remember it is done from the centre outwards, in case the first and last letters are not the same.



In that position, we see that cipher A (inner wheel) goes to plain D (outer wheel), cipher D goes to A, E goes to L and so on.

Set up position (A 22 A) and check that D, E, H, N, O, S go to I, S, H, D, O, E

Now set up position (A 56 A) and list the plain letters given by cipher letters A to T. Your list should start L, A, S, ...

© Frank Tapson 2003 [trolC7:1]

Deciphering

We will use the model rotor machine to decipher this message.

SLALD OHTST SLDDE ISRTS

The starting position is (A 35 A) and the outer wiring rotor is moved one position clockwise after every five letters.

With this starting position the first group SLALD can be changed into DONOT. This is a very encouraging start since it actually looks like English!

Now, having done five letters, it is necessary to move the outer wiring rotor round one positon clockwise. Care is needed, since it is necessary that none of the other three disks move. Assuming the move is made correctly, check that the position is (A 34 A). In that position OHTST can be changed into RESIS.

Another five letters done means another (clockwise) move of the outer wiring rotor. This should make the position (A 33 A). In that position SLDDE can be changed into TARRE.

Finally the last move should give the position (A 32 A) and ISRTS can be deciphered as STLRT.

To keep a check on things, in case there is a mistake, it could be set out like this

Rotor position	(A 35 A)					(A 34 A)					(A 33 A)					(A 32 A)				
Cipher text	S	L	A	L	D	O	H	T	S	T	S	L	D	D	E	I	S	R	T	S
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Plain text	D	O	N	O	T	R	E	S	I	S	T	A	R	R	E	S	T	L	R	T

No matter how it is done, the recovered message is

Do not resist arrest (LRT are nulls)

Exercise 17

Use the model rotor cipher machine to decipher these. The (starting position) is given and the outer wiring rotor is moved 1 position clockwise after every five letters.

1. (A 26 A) NSANE STIAO OODNS IRELD
2. (A 14 A) HLTAL NIOHI IDISN RDROD
3. (A 90 A) LRRIL EARLH TOSRH DNLHT
4. (A 56 A) DLTIO ALAIS RAATA HDOOL
5. (A 30 A) RENAE OIDRS ISRDO TDNOS
6. (S 93 E) NTDN SRSOI AIRSO LSHOS

In these, the outer wiring rotor is moved after every letter and, after it has made ten moves, the inner wiring rotor is moved on one position (and used) before continuing with the outer rotor again.

7. (A 45 A) EENLI SISEO OOEEN NNONO
8. (A 06 A) TTOLO IDESR SOLRS LTENT RTTAH

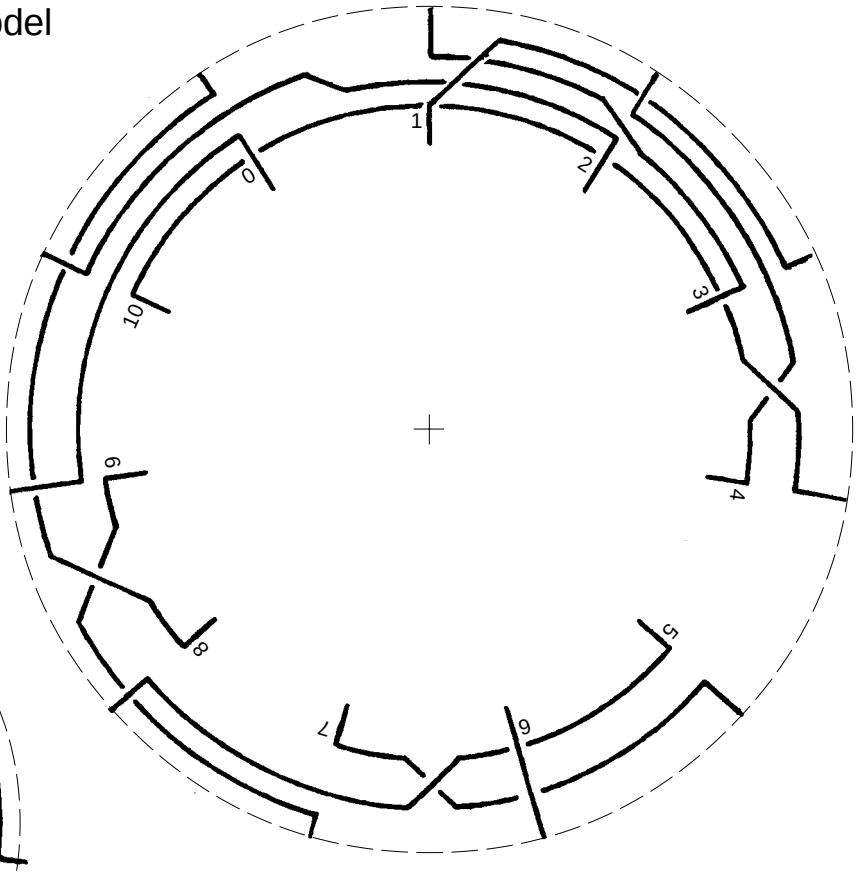
© Frank Tapson 2003 [trolC7:2]

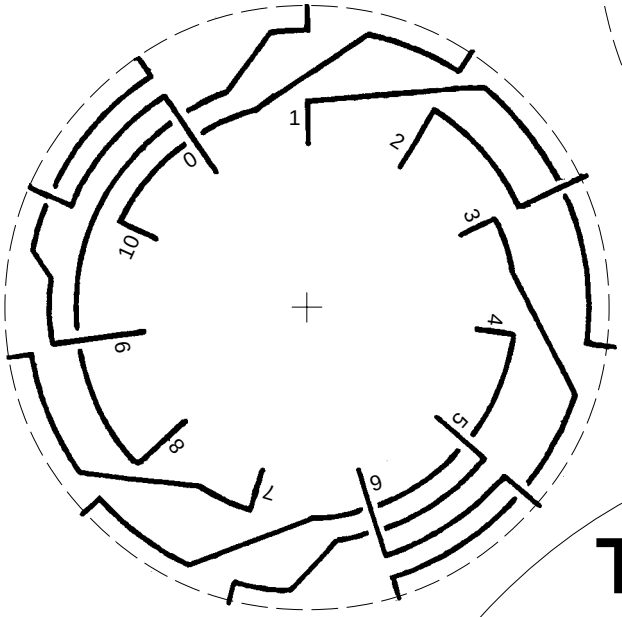
Rotor Ciphers ~ 4

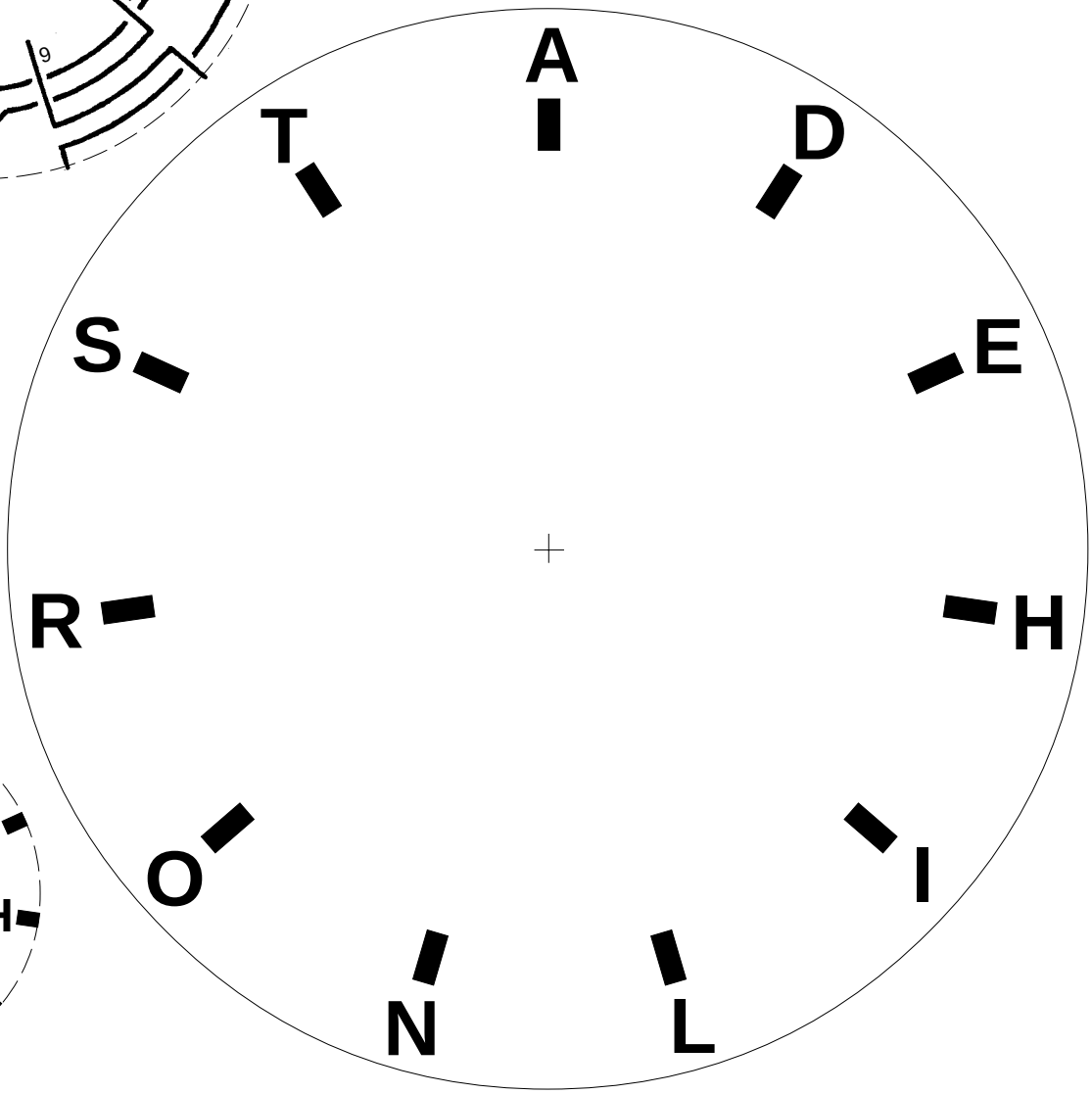
A Model

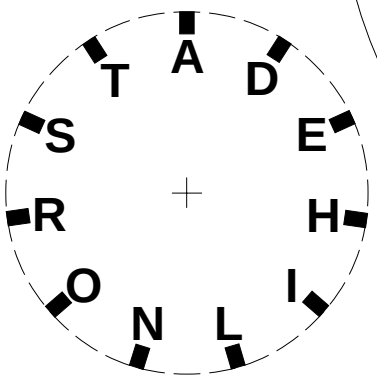
To make:

Cut out the 4 circles (rotors), pierce a hole in each of the marked centres, stack them in order (smallest to largest, face up, smallest on top) and fasten them together through their centres so that each one can be rotated separately from the others.









© Frank Tapson 2003 [trolC7:3]