Turing’s Treatise on Enigma

Chapter 1

Dr. Alan M. Turing

Editors' Preface

This document was written by the late Dr. Alan M. Turing while he worked as a cryptanalyst at Bletchley Park during the Second World War. The document has been obtained from the US National Archives and permission has been obtained from the Controller of Her Majesty's Stationery Office to publish the paper on the personal Web Page of Frode Weierud. The document has been faithfully retyped by the three editors, Ralph Erskine, Philip Marks and Frode Weierud. The original document was typed and had the style and layout of a typewritten document of that period. To make the re-edited presentation more pleasing the document has been both left and right justified and a more modern type font has been used. The page numbers of the original are given as numbers in square brackets. Apart from these modifications to the layout the document has the appearance of the original.

Where there are obvious typing errors these have been corrected in square brackets. In a few cases a superfluous letter(s) has been removed by putting the letter(s) in square brackets preceded by a slash, e.g. [/s]. The Editors' comments are in square brackets and in italic. Longer and more detailed comments are in numbered footnotes.

The Editors,

Ralph Erskine,
Philip Marks,
Frode Weierud, © February 1999

Source:

National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 201, Nr. 964.

COPYRIGHT

Updated: 26 September 1999

[1]

I. A description of the machine.

We begin by describing the ‘unsteckered enigma’. The machine consists of a box with 26 keys labelled with the letters of the alphabet and 26 bulbs which shine through stencils on which letters are marked. It also contains wheels whose function will be described later on. When a key is depressed the wheels are made to move in a certain way and a current flows through the wheels to one of the bulbs. The letter which appears over the bulb is the result of enciphering the letter on the depressed key with the wheels in the position they have when the bulb lights.

To understand the working of the machine it is best to separate in our minds

The electric circuit of the machine without the wheels.
The circuit through the wheels.
The mechanism for turning the wheels and for describing the position of the wheels.

The circuit of the machine without the wheels.

[*The figure contains a drawing of the Eintrittwalze.*]

Fig.1

The machine contains a cylinder called the Eintrittwalze (E.W.) on which are 26 contacts C_1, ..., C_{26}. The effect of the wheels is to connect these contacts up in pairs, the actual pairings of course depending on the positions of the wheels. On the other side the contacts C_1, C_2, ..., C_{26} are connected to one of the keys. For the moment we will suppose that the order is QWERTZUIOASDFGHJKPYXCVBNML, and we will say that Q is the letter associated with C_1, W that [is] associated with C_2 etc. This series of letters associated with C_1, C_2, ..., C_{26} is called the diagonal, for reasons which will appear in Chap. ??

[2]

The particular order we have chosen is known as QWERTZU order.

The diagram shews[1] the connections when the key Q is depressed and supposing that C_1 is connected to C_3 through the wheels

[1] Editors’ Note: This is not a typing mistake. Alan Turing consistently wrote ‘shew’ and ‘shewn’ for show and shown. We have decided to maintain this spelling throughout the text.

[*The figure contains a simplified electrical drawing of the lamp and key connections.*]

Fig.2

The only outlet for the positive of the battery is through the Q key to C_1 hence to C_3 and then through the E bulb. The result is that the E bulb lights. More generally we can say:

If two contacts C, $C^{'}$ of the Eintrittwalze are connected through the wheels then the result of enciphering the letter associated with C is the letter associated with $C^{'}$.

Notice that if P is the result of enciphering G, then G is the result of enciphering P at the same place, also that the result of enciphering G can never be G.

Henceforward we may neglect all of the machine except what affects the connections between the contacts of the E.W. and the turnover mechanism which affects the positions of the wheels.

Connections through the wheels.

The wheels include one which is seldom removed from the machine, and which may or may not be rotatable. It is called the Umkehrwalze (U.K.W.). This wheel has 26 spring contacts which are connected together in pairs. There are three or more other wheels which are removable and rotatable; they have 26 spring contacts on the right side and 26 plate contacts on the left (left and right with positions when in the machine). Each spring

[3]

contact is connected to one and only one plate contact. On the wheels are rings or tyres carrying alphabets, and rotatable with respect to the rest of the wheel; more about this under ‘turnovers’. When the machine is being used three of the wheels are put in between the U.K.W. and the E.W. in some prescribed order. The way the current might flow from the E.W. through the wheels and back is shewn below.

[*Figure 3 shows a drawing of the Umkehrwalze. Figure 5 shows the assembly of the Umkehrwalze (U.K.W.), the three wheels (L.H.W., M.W., and R.H.W.) and the Eintrittwalze (E.W.). Figure 4 shows the left- and right-hand faces of a wheel.*]

Fig.3 Fig.5 Fig.4

Turnovers, Ringstellung, Window position, Rod position.

From the point of view of the legitimate decipherer, the position of the wheels is described by the letters on the tyres which shew through the three (or 4 if the U.K.W. rotates) windows in the casing of the machine. This sequence of letters we call the ‘window position’. When a key is depressed the window position changes, but does not change further when the key is allowed to rise. We will say that the position changes into the ‘following’ position. The position which follows a given one depends only on the order of the wheels and on the original window position. This is because the mechanism for changing the positions is carried on the tyres.

The turning mechanism consists of

> Three pawls operated by the keys, one lying just to the right of the right hand wheel, one between the R.H.W. and M.W. and one between the M.W. and the L.H.W.
>
> 26 catches fixed on each wheel on the right.
>
> One (or possibly more, here we will always assume it is only one) catch on each tyre [on] the left.

The effect of the right hand pawl is to move the R.H.W. forward one place every time a key is depressed. The middle pawl

[4]

normally comes into contact with the smooth surface of the tyre of the R.H.W. which prevents it from engaging with the catches of the M.W. If however it is able to slip in to the catch on the tyre of the R.H.W. it will reach the catch on the M.W. and will push both R.H.W. and M.W. forward: of course the R.H.W. is being pushed forward by the right hand pawl in any case. The occurrence of such a movement of the M.W. is called a ‘turnover’. Owing to the fact that the catch is on the tyre the position at which the turnover occurs depends only on what wheel is in the right hand position, and on the window position of that wheel. For instance with German service wheels, wheel I turns over between Q and R, i.e. if I is in the R.H. position then the M.W. will move forward whenever the window position of the R.H.W. changes from Q to R. The left hand pawl operates similarly to the middle pawl, but in this case it is essential to remember that both M.W. and L.H.W. move forward.

Typical examples of consecutive window positions with middle wheel turnover E-F, R.H.W. T.O. Q-R

```
AWO          BDO          MEW          PEQ
AWP          BDP          NFX          QFR
AWQ          BDQ          NFY          QFS
AXR          BER          NFZ          QFT
AXS          CFS
AXT          CFT
```

Fig. 6

The effect of enciphering a letter depends only on the wheel order (Walzenlage) and the position (i.e. amount rotated) of the wheel proper (i.e. not the tyre). To describe this position we could imagine that there was a set of letters attached to the business part of each wheel, and that these letters could be seen through the windows as well as the letters on the tyres. The letters seen would give the ‘absolute’ or ‘rod’ position of the wheel (the point of the expression ‘rod position’ will be seen in Chap

??). The position of the tyre relative to the business part is fixed by means of a clip on the business part which can drop into holes near the letters. When the clip is in the

[5]

hole near the letter C we say that the Ringstellung is C for that wheel. It is clear that some equation of the form

Window position = Rod position + Ringstellung + a constant

must hold (it being understood that A, B, C, ... are regarded as interchangeable with 1, 2, 3, ...). Normally one arranges that this is zero (see also ………..).

The Steckered Enigma.

In some Enigmas the association of the contacts of the Eintrittwalze with the keys and bulbs can be varied. There are 26 pairs of sockets labelled with the letters of the alphabet one of each pair leading to a contact of the Eintrittwalze and the other to one of the keys. Normally two sockets are connected together by a hidden spring, if however a ‘Stecker’ is plugged into two pairs of sockets, W and R say, these springs are forced away and new connections are made through the Stecker, the W key being connected to the contact which would otherwise be connected to the R key, and vice-versa. That W and R are connected by such a plug is expressed in the form ‘W/R’ or ‘R/W’. The effect of the Stecker on the encipherment is quite simple. If at a certain position of the wheels A enciphered gives N, (abbreviated to AN) then at the same position with Stecker A/V, N/O, and perhaps others, we have VO; if instead we have the Stecker A/V but none involving N, we should have VN (or as we sometimes say the ‘constatation’ VN). Thus if a possible encipherment without any Stecker were

```
DIESERBE
KYMVKEYO
```

then a possible encipherment starting from the same positions of the wheels (or as we say, from the same place) with the Stecker D/S, R/N, B/K, V/Y would be

```
SIEDENKE
BVMYBEVO
```

[*The figure is a drawing of one of the Stecker connections, a cable with a two-pronged plug at each end.*]

Fig. 7

[6]

[*unreadable heading*]

For the purpose of describing the wiring of wheels to electricians one works from a ‘spot’ on the right hand (spring contact bearing) side of the wheel, or if there is no spot, from the contact which is uppermost when any writing on the face is horizontal.

[*The figure shows the upper half of a wheel. The contact pins are numbered and the core of the wheel is marked with the neutral reference point, the wheel number (II) and the serial number, 13579.]*

Fig. 8

The contact which is uppermost or nearest to the spot is called 1 and then the numbering is continued in a clockwise direction. One makes out a scheme like this

Spring contacts	1	2	3	4	5	6	7	8	…
Fixed contacts	6	3	16	14	…				

Fig. 9

From the point of view of the cryptographer the most natural way of naming the contacts is rather different. One would put the Ringstellung to zero, then put zero (Z) in the window, and name any contact on the right of the R.H.W. after the letter associated with the contact of the E.W. which it touches, there being assumed to be no Stecker. To connect these two notations it would be necessary to take into consideration the relative positions of the contact C_{26} of the E.W. and the windows, and also the positions of the clip and spot on the wheel. Here is a rule of thumb for obtaining electricians data from the cryptographic data, illustrated by Railway Wheel I. [W]

Write down the first upright of the inverse square for the wheel and above it the unsteckered diagonal. Use the two top lines to ‘transpose’

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
Z	E	J	G	B	X	P	W	L	D	I	T	K	C	Y	H	F	R	V	A	Q	S	M	N	U	O
6	3	16	14	23	20	18	2	26	12	8	5	17	21	19	15	13	4	22	10	1	11	25	24	7	9

Fig. 10

[7]

the third line into numbers. Then rub out the second and third lines.

This rule is not absolutely reliable because of possible variations of design of wheels and machines.

The comic strips.

For demonstration purposes it is best to replace the machine by a paper model. We replace each wheel by a strip of squared paper 52 by 5 squares. The squares in the right hand column of the strip represent the spring contacts of the wheel in natural order (to make the squares of the strip agree with the contacts of the wheel one must wrap the strip round the wheel with the writing on the strip inwards. The squares on the left represent the plate contacts. In the right hand column is written the diagonal twice over, these being the 'cryptographers names' of the contacts as explained in the last section; in the left hand column letters are also written, and in such a way that the squares containing the same letter represent contacts which are connected together. Down the centre column may be written the numbers 1,...,26,1,...,26. These numbers serve to describe the position of the wheel, either the rod position or the window position according to how they are used. The Umkehrwalze is represented by a strip three squares wide, containing in one column the diagonal repeated (this is not entirely essential) in another the numbers 1,...,26 repeated. The third column represents the contacts; and squares representing contacts which are connected contain the same number (which does not exceed 13). The machine itself is represented by a sheet of paper with slots to hold the 'wheels'. In a column on the right is written the unsteckered diagonal to represent the Eintrittwalze. It is convenient to repeat this alphabet between each pair of wheels. The square bearing the letter Q between the R.H.W and the M.W. will be called R.H.W. 'rod point Q' or M.W. 'output point Q'. Between the wheels we also write 1,...,26 repeated. These are used for describing the position of the wheel when the Ringstellung is given. To understand how this can be done we need only notice that the same effect as a movable tyre

[8]

U	K	W			III					I					II				
7	U	10			D	11	S			W	7	U			I	15	H		
8	I	8			L	12	D			L	8	I			R	16	J		
9	O	2			B	13	F			D	9	O			L	17	K		
10	A	12			C	14	G			Q	10	A			D	18	P		
11	S	1	1	Q	K	15	H	1	Q	C	11	S	1	Q	T	19	Y	Q	1
12	D	6	2	W	J	16	J	2	W	B	12	D	2	W	W	20	X	W	2
13	F	13	3	E	G	17	K	3	E	S	13	F	3	E	V	21	C	E	3
14	G	11	4	R	V	18	P	4	R	P	14	G	4	R	K	22	V	R	4
15	H	9	5	T	P	19	Y	5	T	T	15	H	5	T	S	23	B	T	5
16	J	12	6	Z	U	20	X	6	Z	K	16	J	6	Z	B	24	N	Z	6
17	K	7	7	U	R	21	C	7	U	R	17	K	7	U	C	25	M	U	7
18	P	4	8	I	W	22	V	8	I	G	18	P	8	I	E	26	L	I	8
19	Y	3	9	O	N	23	B	9	O	I	19	Y	9	O	Y	1	Q	O	9
20	X	13	10	A	X	24	N	10	A	J	20	X	10	A	U	2	W	A	10
21	C	1	11	S	A	25	M	11	S	U	21	C	11	S	F	3	E	S	11
22	V	2	12	D	H	26	L	12	D	H	22	V	12	D	H	4	R	D	12
23	B	3	13	F	S	1	Q	13	F	X	23	B	13	F	X	5	T	F	$\boxed{13}$
24	N	4	14	G	T	2	W	14	G	Z	24	N	14	G	Z	6	Z	G	14
25	M	5	15	H	I	3	E	15	H	M	25	M	15	H	M	7	U	H	15
26	L	6	16	J	O	4	R	16	J	N	26	L	$\boxed{16}$	J	N	8	I	J	16
1	Q	7	17	K	F	5	T	$\boxed{17}$	K	A	1	Q	17	K	J	9	O	K	17
2	W	5	18	P	M	6	Z	18	P	V	2	W	18	P	G	10	A	P	18
3	E	8	19	Y	Y	7	U	19	Y	O	3	E	19	Y	O	11	S	Y	19
4	R	9	20	X	Z	8	I	20	X	E	4	R	20	X	P	12	D	X	20
5	T	10	21	C	E	9	O	21	C	Y	5	T	21	C	A	13	F	C	21
6	Z	11	22	V	Q	10	A	22	V	F	6	Z	22	V	Q	14	G	V	22
7	U	10	23	B	D	11	S	23	B	W	7	U	23	B	I	15	H	B	23
8	I	8	24	N	L	12	D	24	N	L	8	I	24	N	R	16	J	N	24
9	O	2	25	M	B	13	F	25	M	D	9	O	25	M	L	17	K	M	25
10	A	12	$\boxed{26}$	L	C	14	G	26	L	Q	10	A	26	L	D	18	P	L	26
11	S	1			K	15	H			C	11	S			T	19	Y		
12	D	6			J	16	J			B	12	D			W	20	X		
13	F	13			G	17	K			S	13	F			V	21	C		
14	G	11			V	18	P			P	14	G			K	22	V		
15	H	9			P	19	Y			T	15	H			S	23	B		
16	J	12			U	20	X			K	16	J			B	24	N		
17	K	7			R	21	C			R	17	K			C	25	M		
18	P	4			W	22	V			G	18	P			E	26	L		
19	Y	3			N	23	B			I	19	Y							

Fig. 11[2]

Set up of Railway Comic Strips for the wheel order III, I, II with Ringstellung 26, 17, 16, 13 and with window positions 10, 5, 26, 5. As the turnover point is just below the Ringstellung mark to R.H.W the next window position will be 10, 5, 1, 6. In the position shewn the result of enciphering Y is P: the path of the current is ?? … ?? In the column [beside the] letters [we shew the effect of the ??] [*unreadable*]

[2] Editors' Note: The Railway Comic Strip figure is very faint at places and it has been partly regenerated. The explanation below the figure is in Alan Turing's handwriting which is at times hard to decipher.

[9]

could be obtained by having windows and pawls which could be rotated round the wheel in step. To use this Ringstellung device on the comic strips we make pencil marks against the numbers on the fixed sheet and read off the window positions on the strips opposite these marks. We also make permanent lines on the strips to shew where the turnover occurs. When these lines pass the Ringstellung marks a turnover occurs.

If the machine has Stecker, we may leave a column on the right for the keys to which the contacts of the E.W. are connected through the Stecker.

The rule of thumb for the making of comic strips is to take the last upright of the rod square for the left hand columns of the strips.

It may appear rather strange that the letters written on the fixed sheet between the strips should be in the order of the diagonal, rather than say ABCD... ; the point of writing the letters in this order is that wherever a strip is put into the machine there is the same arrangements of letters on either side of it. If this were not so it would be necessary to have one ‘rod square’ for the wheel when in the R.H. position and another for the other positions.