Turing’s Treatise on Enigma

Chapter 2

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. Due a problem with the page layout, this chapter have also two end notes which are indicated by capital letters.

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

[10]

Chapter II. Elementary use of rods.

The rod square and inverse rod square.

It is convenient to have a table giving immediately the effect of a wheel in any position. We can make this out in the form of a square measuring 26×26 small squares, the columns being labelled with the numbers 1, …, 26, and the rows labelled with the letters of the diagonal, say qwertzu… If we want to know the output letter which is connected to a given rod point we look in the row named after the rod point and the column named after the rod position of the wheel. Thus in column 18 and row 'e' of the purple square, Fig. 15[A], we find R, and looking on the fixed comic strips (Fig. 11) where the purple wheel is in rod position 18 we find the rod point E connected to output point R.

Rod Pts				
Q	T	19	Y	Q
W	W	20	X	W
E	V	21	C	E
R	K	22	V	R

Rod pos 18

Rod Pts				
Q	W	20	X	Q
W	V	21	C	W
E	K	22	V	E

Rod pos 19

Fig. 12

This square is known as the 'rod square' for the wheel; its rows are known as 'rods' and its columns as 'uprights'. We can make out a rather similar square in which the rows are named after the output letters and the letters in the squares are the rod points. This is called the inverse square, Fig. 17[B].

It should be noticed that in both squares as one proceeds diagonally from top to bottom and from right to left the letters are in the order of the diagonal. Hence the name. That this must happen is obvious from the fact that if one proceeds steadily backwards round the E.W. as the wheel moves forward one will always be in contact with the same point of the R.H.W. and therefore connected to the same point on the left hand side of the R.H.W. This point is moving steadily round and therefore the rod points describing its position move backwards along the diagonal.

Encoding and decoding on the rods.

For the purpose of decoding without a machine, and in connection with many methods of finding keys it is convenient to have the

[11]

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	
	V Y R P S M A V T N	D M T K W T C W Z K	O		q o
	Z X F G Q J W C A E	U Y R J M K G M F Z	P M U		e v
	E V S R P S B Z M Z	H L G U I V E U P A	C		b a
	G M K H L A L U S V	S B J T N G D B I X	F		k g
	N U L U B P E G L Y	R I Y S O I Q H D B	X		s x
	X T Y D F R H Q X O	L Z P E H W J F N D	T		w c
	F Z X K W O F N J G	J O A B E M A V H R	H		m j
	H J E O C I Q I N T	Z P Q X Q O X D A C			t d
	L P J Q D C G H W I	N K Z M F X T K L Y	L		p r
	W O M Z A D N O C R	C F S V U B R X Q T	J		f i
	Y K W F M T S B I X	P U L G S E V E Y L			y u
	K R A V U U C P E K	Y W C W P A S N R J	M		z l
J W S R S N V U P R	Q I D B H B D T Y J	F N O C G Q H I O V	E V A U P W G M S X	Z M L F Y T F X A K C Z	h n

Set up of M.W. rods for U.K.W. rod pos 10 L.H.W (Green III) 14

Fig. 13[1]

[1] Editors' Note: The table is faint in many places and it has therefore been partly regenerated using the Railway Enigma rods.

[12]

12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
M	A	U	G	E	J	C	V	L	…						s
W	V	R	C	S	K	D	U	P	A	…					n
N	G	X	H	A	C	F	O	W	V	…					q
V	K	D	B	H	S	R	N	K	…						e
E	U	P	A	I	M	V	J	N	…						p
L	P	G	U	Q	X	T	W	O	…						z
Z	B	F	Y	G	O	X	D	I	Q	…					l
D	E	L	X	W	Y	O	H	A	…						v
R	Q	C	E	X	A	J	S	Z	K	O	…				b
I	Y	S	O	L	B	K	M	J	Z	…					y
O	J	T	P	B	N	W	F	T	E	X	…				f
A	R	B	I	T	D	Q	G	Y	X	…					o
H	C	J	S	V	G	A	E	B	…						w
K	Z	Y	N	M	E	G	Z	R	…						g
F	S	W	M	Y	Q	P	I	G	O	R	…				c
G	M	K	F	Z	L	Y	R	Q	…						t
S	I	H	R	K	V	B	Q	D	R	W	…				d
J	O	E	V	U	R	S	L	F	P	Y	…				i
T	N	O	Z	F	W	H	X	C	M	A	…				a
P	F	N	J	D	T	M	P	E	L	…					r
B	T	V	D	P	F	I	Y	S	U	L	…				m
X	D	A	Q	N	P	L	K	U	F	…					x
Y	H	I	W	C	Z	E	A	M	D	K	…				u
Q	W	Z	K	O	U	N	C	H	B	…					k
U	X	M	L	R	H	U	T	V	Y	F	…				h
C	L	Q	T	J	I	Z	B	X	G	…					j

First set up of R.H.W. rods.

Deciphering of message

					T.O.
14	15	16	17	18	19
	Q	S	Z	V	
	D	E	U	T	

Fig. 14[2]

[2] Editors' Note: The table is faint in many places and it has therefore been partly regenerated using the Railway Enigma rods.

[13]

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	
O	M	T	L	C	Z	N	X	F	U	L	S	I	H	R	K	V	B	Q	D	R	W	Y	J	A	P	d
T	B	C	D	O	E	S	W	P	N	Y	G	M	K	F	Z	L	Y	R	Q	I	B	A	H	J	X	t
B	G	S	T	F	R	X	L	C	J	Q	Y	H	I	W	C	Z	E	A	M	D	K	P	V	U	M	u
S	E	M	P	D	T	J	F	X	O	V	Q	W	Z	K	O	U	N	C	H	B	G	R	A	T	L	k
E	N	O	Q	B	J	A	E	G	S	P	U	X	M	L	R	H	U	T	V	Y	F	C	D	W	I	h
A	C	P	M	G	Q	Z	U	S	V	G	D	E	L	X	W	Y	O	H	A	T	J	I	R	B	K	v
K	I	N	R	M	X	T	B	Y	D	Z	M	A	U	G	E	J	C	V	L	S	E	Q	P	H	O	s
U	W	B	I	L	V	H	O	W	F	A	K	Z	Y	N	M	E	G	Z	R	C	P	D	X	S	Q	g
Y	R	V	X	S	I	W	A	Q	K	B	P	F	N	J	D	T	M	P	E	L	U	V	O	G	H	r
H	D	Z	G	T	C	Q	V	K	W	X	J	O	E	V	U	R	S	L	F	P	Y	B	I	L	N	i
P	T	A	S	H	L	P	J	U	R	N	Z	B	F	Y	G	O	X	D	I	Q	C	G	M	V	E	l
D	F	K	W	X	P	O	Z	L	I	M	H	C	J	S	V	G	A	E	B	J	Q	N	T	X	U	w
M	A	W	N	K	S	R	H	D	Y	I	C	L	Q	T	J	I	Z	B	X	G	V	F	E	O	R	j
W	K	R	O	A	G	M	K	H	Z	E	B	T	V	D	P	F	I	Y	S	U	L	X	F	N	C	m
N	V	F	A	R	D	E	Y	M	X	H	L	P	G	U	Q	X	T	W	O	N	S	J	K	C	Z	z
F	U	H	Z	V	W	B	P	E	C	K	A	R	B	I	T	D	Q	G	Y	X	N	O	Q	M	J	o
X	Q	J	E	I	O	F	N	J	G	T	W	V	R	C	S	K	D	U	P	A	Z	M	Y	D	B	n
C	H	I	Y	J	B	D	M	R	T	O	X	D	A	Q	N	P	L	K	U	F	I	E	G	Z	W	x
J	O	X	K	N	F	L	T	Z	A	C	F	S	W	M	Y	Q	P	I	G	O	R	H	U	E	V	c
V	Y	L	H	W	U	I	D	B	H	F	R	Q	C	E	X	A	J	S	Z	K	O	T	N	P	S	b
R	L	Y	F	Z	K	G	C	A	B	W	E	U	P	A	I	M	V	J	N	H	T	S	Z	Q	D	p
G	P	E	C	Y	A	U	Q	O	L	J	V	K	D	B	H	S	R	N	K	W	M	Z	C	I	F	e
Q	X	G	U	P	H	V	S	N	E	R	I	Y	S	O	L	B	K	M	J	Z	D	U	W	F	T	y
I	J	U	B	E	N	Y	R	V	P	S	T	N	O	Z	F	W	H	X	C	M	A	W	L	K	G	a
L	Z	Q	V	U	M	C	G	I	Q	D	O	J	T	P	B	N	W	F	T	E	X	K	S	Y	A	f
Z	S	D	J	Q	Y	K	I	T	M	U	N	G	X	H	A	C	F	O	W	V	H	L	B	R	Y	q

Second set up of R.H.W. rods.

First setup																	18	19	20	21	22	23	24	25	26	
														Q	S	Z	V	I	D	V	M	P	N	E	X	
																		S	Q	E	T	R	U	P	P	

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
A	C	M	R	W	W	X	U	I	Y	O	T	Y	N	G	V	V	X	D	Z	Third setup
E	N	S	I	N	D	J	E	T	Z	T	I	N	E	N	G	L	A			

Fig. 15[3]

[3] Editors' Note: The table is faint in many places and it has therefore been partly regenerated using the Railway Enigma rods.

[14]

rows of the rod square written out on actual cardboard rods, in gauge with squared paper. Let us suppose that we wish to decode a message beginning

QSZVI DVMPN EXACM RWWXU IYOTY NGVVX DZ…[4]

of not more than 30 groups, that we know the wheel order to be III, I, II (Green, Red, Purple), the Ringstellung to be 26 17 16 13, and the Spruchschluessel to be 10 5 26 1 i.e. that the machine should be set to the window position 10 5 26 1 and the deciphering then begun. We first work out the turnovers in terms of rod positions. Wheel II has window T.O. E–F i.e. 5–6, and since the Ringstellung for this wheel is 13 the rod T.O. is 18–19. The middle wheel window T.O. is N–O and the rod T.O. is 24–25. Next we transform the Spruchschluessel 10 5 26 1 into rod values by subtracting the Ringstellung. We obtain 10 14 10 14, and we can now write over the letters of the message the rod positions of the R.H.W. at which they are to be enciphered, remembering that the window position at which the first letter is enciphered is not the Spruchschluessel but its successor. We can also mark in the turnovers. Over each section between turnovers we can mark the position of the middle wheel. As the message is not more than 150 letters no double T.O. will be reached and the U.K.W. will be at 10 and the L.H.W. at 14 throughout. We can work out the effect of these two wheels for this message once and for all. We set up the comic strips for the U.K.W. and the L.H.W. to this position and read off the pairs of M.W. rod points which are connected through them. (The fixed comic strips Fig. 11 have the U.K.W. and M.W. set to this position) They are qo, ev, ba, kg, sx, wc, mj, td, pr, fi, yu, zl, hn. From these we wish to obtain the connections between the right hand wheel rod points for all relevant positions of the M.W. If we set up the red rods

		10								11				
14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3
	Q	S	Z	V	I	D	V	M	P	N	E	X	A	C	M

Fig.16. Message with rod position and T.O.s

[15]

according to the pairs qo, ev,… (see Fig. 13). In any column of the resulting set-up will be found the letters of the alphabet in pairs; these pairs are the R.H.W. rod points which are connected together through the U.K.W., L.H.W. and M.W. with the U.K.W. and L.H.W. in the position 10 14 and the M.W. in the position given at the head of the column in question: this can be verified from Fig. 11 in the case of column 10. In order to decipher the part of the message before the first turnover we set up the purple rods according to the pairs in column 10 of Fig. 13. This set of pairs is called the ‘coupling of the R.H.W. rods’ or simply the ‘coupling’. The pairs of letters in the various columns of the purple set-up are the possible constations when the U.K.W., L.H.W., and M.W. have the positions 10 14 10 and the R.H.W. has the positions given at the head of the column. We can therefore use the set-up for decoding up to the first

[4] Editors’ Note: There are several errors in the original message as given in the Treatise. The original is: QSZVI DMFPN EXACM RWWXU JYUTY NGVVX DZ… It appears correct in Fig. 15.

T.O. Afterwards we have to rearrange the rods with the coupling in the 11th column of the rod set-up (Fig. 15).

[A] Editors' Note: The original has Fig. 16 here which must be wrong.

[B] Editors' Note: Fig. 17 is missing in the archive copy.