Turing’s Treatise on Enigma

“Prof’s Book”

Chapter 4

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, © May 1999

Source:

National Archives and Records Administration (NARA), Record Group 457, NSA Historical Collection, Box 201, Nr. 964. The NARA copy has now been checked and verified against the copy in the Public Record Office (PRO) at Kew, London. The PRO copy is in HW 25/3.

COPYRIGHT

Updated: 8 May 2000

[65]

Chapter IV. Single-wheel processes. (Unsteckered Enigma)

We now suppose that we know the constatations of the machine, and that there are no Stecker. This practically presupposes that we have already read some of the traffic, and therefore that we know something of the probable word used, especially at the beginnings and ends of the messages. Suppose then what we think that a message starting FKSJTTQNYLBSCKVKX becomes when deciphered DANZIGVON... We shall have to take several independent hypotheses as to which wheel is in the R.H.W. position, unless other messages for the day have already been solved. Let us suppose that the purple wheel is on the right. We shall then have to make 26 separate hypotheses as to what rod position the message starts in. We write the message out in gauge with the rods, and when trying out the hypothesis that the pre-start position is at 26 on the rods we pick out the rods starting with F and D and lay them with $\frac{F}{D}$ under the $\frac{F}{D}$ of the message and crib as in Fig. 43. We find on the rods at position 4 $\frac{Z}{W}$ which implies that the Z of DANZIG should have been enciphered at W instead of J, or else that there was a turnover between the D and the Z. As we do not think this latter alternative very likely we go on to the hypothesis that the pre-start was at 1, and this also gives us a contradiction or else a T.O. So we go on until we try pre-start at 4. When we set up the pair of rods that gives $\frac{F}{D}$ we find that it also gives us V. This is known as a 'click', and when we set up the pair giving $\frac{T}{I}$ we get also $\frac{N}{O}$. This, together with the fact that there are no contradictions, makes it practically certain that we have found the right rod start. We can then decipher a few more letters of the message, assuming that there was no T.O. In this way we get DANZIGVON.ANNH..M[1] suggesting the decode DANZIGVONMANNHEIM... with a T.O. between the H and the E of

[1] Editors' Note: Turing has written DANZIGVON.ANNH.N but this must be wrong.

[65a][2]

```
F K S J T T Q N Y L B S C K V K X
D A N Z I G V O N
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
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
```

Fig. 43. Testing pre-start 26.

```
        F K S J T T Q N Y L B S C K V K X
        D A N Z I G V O N   A N N H   N
… 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
… 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

… 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
… 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

… 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
… 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

… 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 E I | O F N J [G] T W V R C [S] K D U P | A Z M Y D B   n

… 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
… G U P | H V S N E | R I [Y] S O | L B [K] N J | Z D U W D T   y

… 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
… 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

… 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
… 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
```

Fig. 44. Pre-start 4.

```
V K X U Z H E R B Z O Q V E T K V L D K S N R D B S
E I M   G               E   O   E R
```

Fig. 45. Consequences of EIM after T.O.

[2] Editors' Note: This page is not numbered in the PRO copy. As the first figure is referred to on page 65 we have decided to insert the page in between pages 65 and 66 and to label it 65a.

[66]

MANNHEIM. In order to decode more of the message we can try using the three couplings after the turnover to read a little more. This is shewn in Fig. 45. It is not possible to fill in the intermediate letters and we have to find some other method. One is to try decoding after the T.O. with various assumptions about which wheel is in the middle position, and what rod position the M.W. is in. We shall not actually need to do the decoding for each such position, as a very large proportion of the possibilities is immediately eliminated by the EIM known to occur after the T.O. In fact we have the seven couplings ku, ep, fq, xn, ay, td, vh, lw before the T.O. and sw, oa, le after it. We could treat those couplings with respect to the middle wheel in the same way as we treated the original crib with respect to the right hand wheel. However it is not really necessary to get out the rods. It is easiest to work with the rod square and for each possible position of the middle wheel look and see what coupling before the T.O. is a consequence of oa after the T.O. For example there are the bits of red rod

```
1 2
M A
V O
```

and therefore if the message starts in rod position 1 for the middle wheel the coupling mv must have occurred before the T.O. in order that oa may occur after it. Consequently this position & colour for the middle wheel is impossible. That the middle wheel rods can be used in this way amounts to nothing more than that they can be used in decoding in the way described on p. 14, 15. In this way we find that the only possible position for the middle wheel is red 11, and we have for couplings after the T.O. yg, uv, kt, nh, ws, cm, el, oa and the part of the message from the first to the second T.O. reads

```
V K X U Z H E R B Z C Q V E T K V L D K S N R D B S
E I M . G A N . A . M E E T O T E R . I T . . . E
```

[67]

```
                                                                  Prestart ↓
   5      10     15     20     25 26     5      10     15     20     25

        10     15     20     25 26 1    5      10     15     20     25
.. CNKDG BCRLT AMQFI XHJMY E OWZPU CNKDG BCRLT AMQFI XHJMY E F
.. ZXBJS FVXEM RONLD UYGHN P WIQTK ZXBJS FVXEM RONLD UYGHN P D

.. QMIRO GETKD NYXEB UFZAV S MWCJP QMIRO GETKD NYXEB UFZAV  K
.. HRPCG OSXPQ BWUVN ATKDF V JLZME HRPCG OSXPQ BWUVN ATKDF  A

.. YVHAD CYWNE IBMSZ PFGBK Q ULRJT YVHAD CYWNE IBMSZ PFGB  S
.. NYTLQ ARGXF KEPZO WBMIZ H SJCAD NYTLQ ARGXF KEPZO WBMI  N

.. NUEIF WRJSB PYWVZ DTOCA N QXHKL NUEIF WRJSB PYWVZ DTO J
.. CMSLG KATUJ GBYNE PXZQF I OPDVW CMSLG KATUJ GBYNE PXZ Z

.. XNAMF JORZH FVPBW KYTLD U IKSCQ XNAMF JORZH FVPBW KY T
.. WJYDU OPJMC LTXVI EHASX G NRBQF WJYDU OPJMC LTXVI EH I

.. NAMFJ ORZHF VPBWK YTLDU I KSCQX NAMFJ ORZHF VPBWK Y T
.. VTQZS LWGOC JKLXR AEUYI V MPFHN VTQZS LWGOC JKLXR A G

.. KBJXZ CODTL WSOPG YNFHQ V IERFU KBJXZ CODTL WSOPG  Q
.. ENMIW DPSHQ JRULC BZRFO G YIAVK ENMIW DPSHQ JRULC  V

.. ARGXF KEPZO WBMIZ HSJCA D NYTLQ ARGXF KEPZO WBMI  N
.. IAYKL VQZCB ORJSD CHMTN W GEKXF IAYKL VQZCB ORJS  O

.. GLCVT MOHID NFQRB PXEQA Z SJTUY GLCVT MOHID NFQ Y
.. RGXFK EPZOW BMIZH SJCAD N YTLQA RGXFK EPZOW BMI N
```

Fig. 46. Set up of Purple inverse rods for F K S J T T Q N Y[3]
D A N Z I G V O N

[68]

We can fill this in to read, for the whole message up to this point DANZIGVONMANNHEIMXGANZARMEETOTERBITTEBEFEHL. The other couplings bd, rf, jz, qi can soon be read off the filled-in letters, and altogether we now have the couplings of the M.W. rods qo, ev[4], ab, sx, wc, jm, pr, fi, yu, zl, hn so we can decode as described in Chap. II; the two remaining middle wheel couplings will soon be found.

We might of course use either the middle wheel couplings or the right hand wheel couplings to find the position of the L.H.W. and U.K.W. and we could then do the decoding on a machine instead of on the rods. Methods for doing this will be described in the next Chapter. The rest of this chapter will be devoted to methods of brightening up the first parts of the process.

[3] Editors' Note: Turing has written FKSJRMQXY, but elsewhere this has been corrected to FKSJTTQNY which are the correct letters.

[4] Editors' Note: Turing has written er instead of ev, and pv instead of pr. However, the example does not support this.

The inverse rods

Instead of picking out the R.H.W. rods and laying them against the crib as in Figs. 43, 44 we might write down the rod couplings which are consequences of each of the constatations, thus when testing pre-start 26

```
F K S J T T Q N Y
D A N Z I G V O N
o m u q l k i n s
w j s o n m y g y
```

The contradiction which we found before by setting up the pair ow now shows itself in the form of the contradictory couplings ow, oq. In the case of pre-start 4 we have

```
F K S J T T Q N Y
D A N Z I G V O N
u p t l q x u q y
k e d w f n k f a
```

and our confirmations (clicks) show up as repetitions of the couplings uk, qf. If we actually did this we should lose time in comparison with the original process, but we can actually get all the couplings in the different positions by a more mechanical method.

We have the lines of the inverse square (p. 10) written out on rods in double length, called ‘inverse rods’. We

[69 a][5]

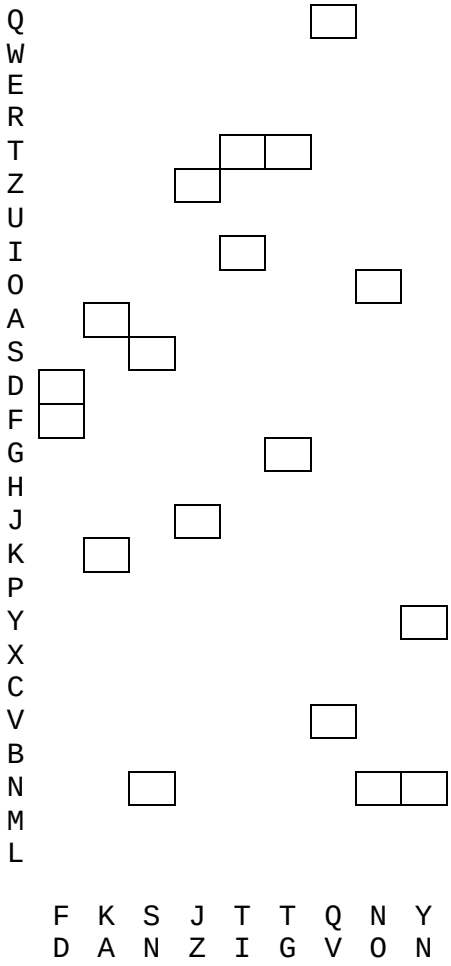

Fig. 47. Preparation of work for DANZIGVON crib.

[5] Editors' Note: In the original Fig. 47 and Fig. 48 are both drawn on page 69. To present these figures better we have split them and re-labeled the page to 69a and 69b.

[69 b]

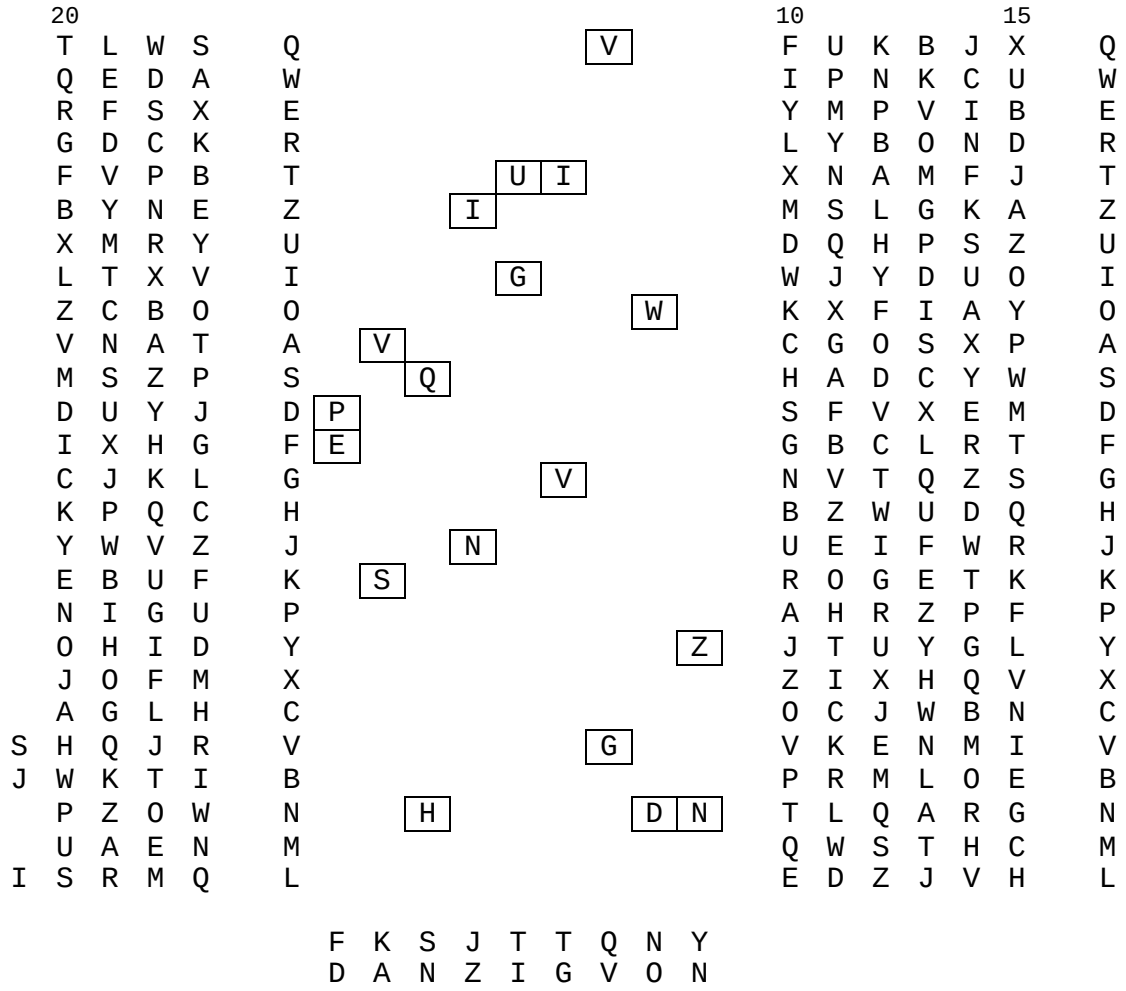

Fig 48. Mask in position. Text of pre-start 25.

[70]

pick out the inverse rods named after the letters in the crib, and lay them down in pairs, staggering them backwards. This is best seen in Fig. 46. The various columns in this set-up show us the various rod couplings which are consequences of the crib and various hypotheses as to the pre-start. In the figure the pre-starts have been written along the top, but this is not part of the normal routine. With this method we can easily see contradictions which are independent of where the T.O. occurs e.g. for pre-start 1 we have the couplings wi, wl, jl arising from the crib in that order. There must be a T.O. between the wi and the wl and also between the wl and jl which, apart from double T.O., is impossible.

Masks

There is another method which gives essentially the same result as the inverse rods and seems to be a little quicker and to require rather less permanent apparatus. We need to have the inverse squares written out with part of the beginning of the square repeated again at the end, and in rather small letters. In order to work a particular crib we take some paper in gauge with the inverse oblong and write the diagonal down the side of it, and write the crib along the bottom. Then for each letter of the crib (either code or decode) we punch a hole in the column in which it occurs, and in the line named after it (Fig. 47). We then move this mask over the inverse oblong. Each position of the mask corresponds to a different start on the rods. The pair of letters shewing through the two holes in a column gives the coupling which is a consequence of the constatation written in that column (Fig. 48).

Another advantage of this method is that we can test all colours with one mask. This advantage can however also be got by making inverse rods with all the colours on one rod.

[71]

Charts

When we want to try the same decode for a great many different messages, and perhaps for many different places in the same message it may be worth while to make special statistics for that crib. We can make statistics of the positions in which there will be ‘clicks’. There is quite a problem as to the form in which the statistics ought to be presented. I will describe two forms which have actually been used; named after the principal cribs for which they were made. First however I must explain the terminology I shall use. Let us take for example the crib XBRUESSELXX fitted onto a part of the message AEIRCMTWBZJ. There is a click as shown below

19	20	21	22	23	24	25	26	1	2	3	rod position
A	E	I	R	C	M	T	W	B	Z	J	message
X	B	R	U	E	S	S	E	L	X	X	crib
N	V	Y	L	C	O	T	W	B	P	U	rod
D	G	G	K	W	C	U	E	L	A	B	rod

Fig. 49[6]

As the constatations of the click are consecutive I shall say that the 'click distance' is I[7]. W is called the 'first cipher letter' and B the second cipher letter, E the first and L the second 'crib letters'. As the first letter of the crib comes at rod position 19 we say that the 'rod start' is 19. As the first crib letter E is the eighth letter of the crib we say that the crib position of the click is 8.

PERCOMMANDANTE type charts

This is the perfect form of chart for use when the position of the crib in the message is known exactly. The chart has several major divisions according to the different possible first crib letters. Each of these major divisions is further divided into lines labelled with the second crib letters, and columns labelled with the first cipher letters, in the resulting small

[72]

rectangles are written the second cipher letter and rod start. Thus the eighth major division of a PERCOMMANDANTE type chart made out for XBRUESSELXX would look like this

	A	B	C	…	W	…
E^2L					B 19	
E^2X^2						
E^2X^3						

all entries apart from the one corresponding to the click shown in Fig. 49 having been omitted. The numbers written above and to the right of the letters in the names of the rows distinguish between different occurrences of the same letter in the crib. By writing the message downwards in gauge with the lines of the chart it is very easy to see the possible clicks. We note down the rod starts, and, if we find one of them repeated try it out by the method described at the beginning of the chapter.

BRUESSEL type charts

These have the advantage over the PERCOMMANDANTE type charts that one can investigate all possible positions of the crib in the message without doing them all independently, but it has some counterbalancing disadvantages. In the form in which

[6] Editors' Note: The figure is showing rod V and O from the Green (III) Railway wheel.

[7] Editors' Note: For some obscure reason Turing has used Roman numerals to describe the click distance.

they were made for the Railway traffic all three colours were put together and there were separate sheets for the different click distances. I now think that it might be better to separate the colours and to have three or four click distances on a sheet. In any case the sheets are further divided into lines according to the different first cipher letters and the entries in the lines consist of the second cipher letter, the rod start and the crib position of the click. Thus the click shown in Fig. 49 would be represented on sheet I in line W by the entry B 19^8 in green. The chart is usually used one sheet at a time;

[73]

the message is written out with plenty of room for entries below it. Whilst using sheet I for each letter of the message take the corresponding line of the sheet and look in it for the letter which comes next in the message. For each such entry that we find we enter the rod start on the message under the letter which corresponds to the first letter of the crib. We know where this is because the entry on the chart gives the crib position. When we get the same number twice in a column we try out the corresponding rod position and position in the message.

A possible improvement of the layout which might combine the advantages of the PERCOMMANDANTE and BRUESSEL type charts would be to take a fairly wide column for each click distance, all the columns being the same width, instead of having separate sheets, and to make the lines fairly deep. The message could then be written out in gauge with the chart. However, I am afraid that this might make both chart and message unwieldy. An alternative possible improvement would be to have separate columns for the different second cipher letters. This would also mean having rather large charts, because of the great variation of the number of letters that would have to go into a rectangle.

[74]

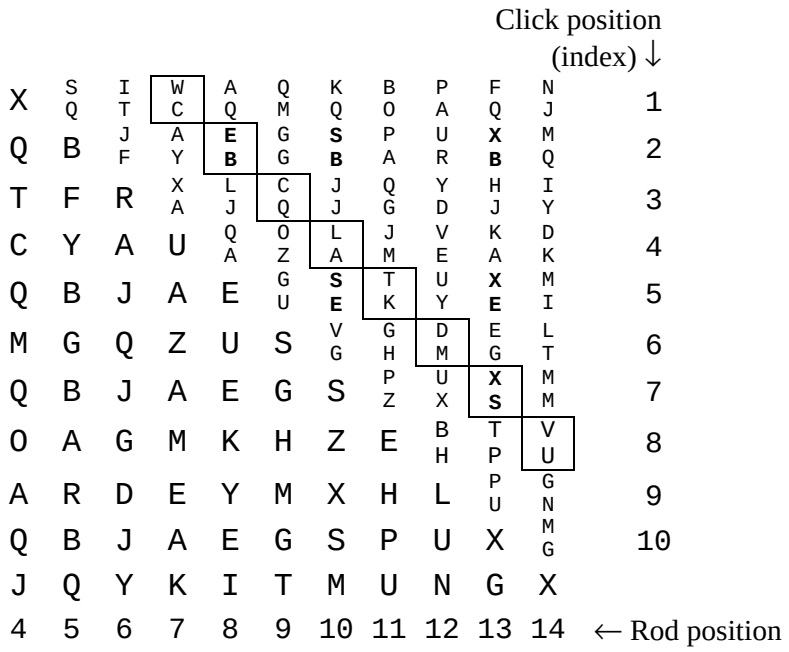

Fig. 50. Making a chart. Cross clicks with rod start 4.[8]

[75]

Making of charts

Although there is so much room for variation in the form in which a chart can take the manner in which they are made is fairly stereotyped. There are two kinds of click to be catalogued, called ‘direct’ and ‘cross’. Direct clicks are those in which both letters of the crib occur on the same rod. Both clicks in Fig. 44 are direct clicks. Cross clicks have one of the crib letters on one rod and the other on the other.

While cataloguing cross clicks we make 26 pictures like Fig. 50 by writing the crib diagonally and filling up a square with rods, and finally copying the left lower half into the right upper half symmetrically across the diagonal. The different pictures[9] correspond to different rod starts. Each square above the diagonal gives us an entry for the chart. The lower letter is the first cipher letter, and the upper is the second cipher letter. The row gives the click position, i.e. with a BRUESSEL type chart the number in the ‘index’ position. The click distance (i.e. the sheet, with BRUESSEL type) is determined by how far the square is from the central diagonal; in the figure the squares corresponding to click distance III are ringed in pencil. With a PERCOMMANDANTE type chart we should not use the diagonals but the columns.

[8] Editors’ Note: The squares with crossed out entries have their letters in **bold** type as the diagonal stoke is difficult to reproduce. The rods in the example are from the Purple (II) Railway wheel.

[9] Editors’ Note: Here there are a two lines from a tables corresponding to the first lines of Fig. 50. The lines have been stoked through and clearly are not meant to make part of the final text.

Some of the squares do not correspond to possible entries, as they could only arise from rods paired with themselves. Those squared have been crossed out in Fig. 50.

For cataloguing direct links we have to find all cases in which a pair of letters on a rod can fit with a pair of letters of the crib, e.g.

```
X  B  R  U  E  S  S  E  L  X  X
D  G  G  K  W  C  U  E  L  A  B
```

Each such case will give us 25 different entries in the chart,

[76]

all with the same click distance, rod start and crib positions. In cataloguing these either in a PERCOMMANDANTE or BRUESSEL chart it is sufficient if we put the second cipher letters all in similar positions and only once enter the remaining information for each set of 25.

X-charts

Sometimes one will find messages with about 30% of X's in the decode. These can be got out by a 'majority vote' method, looking for the R.H.W. starting position which gives the greatest number of clicks if we assume the message to say XXXXX all through. If there are actually 30% of X's there will be about 2.2 genuine clicks between X's per T.O.: there will also be an average of about 0.5 apparent clicks arising from letters which are not X, giving altogether 2.7 clicks per T.O. with the correct start. With the wrong start we have one bogus click per T.O. If we do not know where the T.O. is these figures have to be modified. In the right place we have 3.7 clicks per length of 26, and in the wrong place 2.0.

With X-charts there are less variables involved than with ordinary charts, as there is no question as to where the crib should be set against the message. The variables involved therefore are the first and second cipher letters, the click distance, and the rod position of the first constatation of the click. There are two ways of setting the chart out, one favoured by Kendrick and one by Turing.

With Turing's form of chart there are 26 lines named after the first cipher letters and 26 columns corresponding to the possible click distances. The second cipher letter and the rod position are entered in the square. The chart can be used by writing the message out in gauge with the chart, and putting each letter in turn over the corresponding letter in the left-hand

[77]

column which names the lines, and looking for each letter among the next 26 of the message in the square of the chart directly below it. In noting the click down we calculate the implied rod start of the message by subtracting the position in the message of the first cipher letter, i.e. the number in the square. We enter against this rod start the position in the message of the first cipher letter. The rod start with the greatest number of entries against it is presumed to be the right one. To read the message after we have found the R.H.W. rod start we can try setting up the rods

giving the clicks and see if this results in any further identifications, but this hardly ever gives the solution. The generally accepted method is to take the couplings giving the clicks and note down from a catalogue the places in which they could occur, and then take a ‘majority vote’.

In making an X-chart we can make a set-up like Fig. 50. This will measure 26x26 and only one of them will be needed. It will simply consist of a rod-square rearranged with X's down the diagonal. When making the entries for a particular value of rod position of the first constatation of the click (i.e. the entries where a particular number is written in pencil in the square) we copy down a line from the rearranged rod square, starting immediately after the X, across the top of the rod square, and also the column starting at the same X. The entry to be made in any column can then be seen by looking at the top. Having made these entries we rub out the lines at the top and replace them with others.

[78]

In Kendrick’s type of X-chart the names of the lines give the first of the cipher letters. The columns give the position of the other cipher letter, and the entry in the square is the second cipher letter and the position of the first cipher letter. This form of chart is particularly useful when we have a hunch about the rod start.

[79]

Consecutive tables

In the second part of the process, where we are finding the position of the middle wheel we can speed up the work by the use of consecutive tables. These are of two kinds, forward and backward, and look very much like rod squares. The letter in column 18, say and row R of the forward consecutive square is the letter which occurs in column 19 of the rod with R in Column 18. The letter in column 18 and row R of the backward consecutive square is that which occurs in column 17 of the same rod. Like rod squares and inverse squares these consecutive squares ‘have a diagonal’ i.e. can be filled in from a single upright by writing ‘the diagonal’ diagonally downwards to the left. In our DANZIGVON example we could have used the backward consecutives as soon as we had found the couplings ku, ep, fq, qx[10], ay, td, vh, lw before the T.O. and sw, oa, le after it. We should have laid rulers against the lines o,a of the backward consecutive square, and read off the consequences before the T.O. of having oa after it, in the various possible positions of the middle wheel, and would have looked to see whether these consequences were consistent with our data. We should then have repeated with ws looking only at the positions consistent with oa. The forward consecutives can be used when the place has been found for reading off the couplings after the T.O. (although this is only a small advantage), or in a case where we have started from the end of the message and worked backwards.

[10] Editors’ Note: Turing is confused here and writes fx, qn instead of fq, qx which are the correct constatations.