DECLASSIFIED
Authority NND 963016

TOP SECRET

TOP SECRET

TURING'S TREATISE ON THE ENIGMA

A Photographic Copy of a Paper Prepared in GCCS,

Written ca. 1939-1942

DO NOT REMOVE. Return to the
N.A. Technical Library when no longer needed
S-3363 TL Copy No. 3

TOP SECRET

Filed: M.C. - Enigma (21)

TOP SECRET

N.B.

Pages missing in film of Turing's Treatise

38-40, 47-59

68 (but there are two "67"'s)

74, 81-83, 90

100? (but there is an empty 26 x 26 square instead)

113-114

119? (But there is an unnumbered page instead)

124-128 (but there are two "129"'s)

131

DECLASSIFIED
Authority NND 963016

TOP SECRET

Filed: Machine Cipher - Enigma (21)

DECLASSIFIED
Authority NND 363016

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 positions of the wheels.

The circuit of the machine without the wheels.

Fig 1

Eintrittswalz

The machine contains a cylinder called the Eintrittswalz (E.W) on which are 26 contacts $C_1, \ldots, C_{26}$. 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 $C_1, C_2, \ldots, C_{26}$ are connected each 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 associated with C_2 etc. This series of letters associated with $C_1, C_2, \ldots, C_{26}$ is called the diagonal, for reasons which will appear in Chap

The particular order we have chosen is now an UNRELATED order.

The diagram shows the connections when the key Q is depressed and supposing that C_1 is connected to C_3 through the wheels

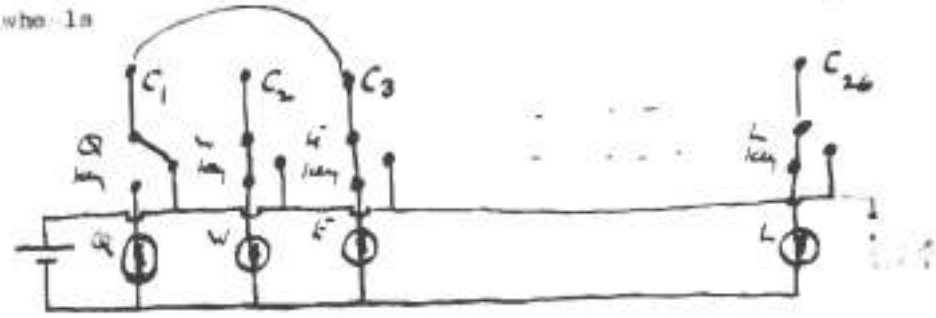


Fig 2

The only outlet for the positive of the battery is through the Q keyt o 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 Eintrittswalz are connected throughthe wheels th en 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 the what effects the connections between the contacts of the E.W. , and the turnover mechanism which effects 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 Umkehrwalz (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 theright and 26 plate contacts on the left(left and right with xxxxx positions when in the machine). Each spring

DECLASSIFIED
Authority NND 363046

DECLASSIFIED
Authority NND 363016

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

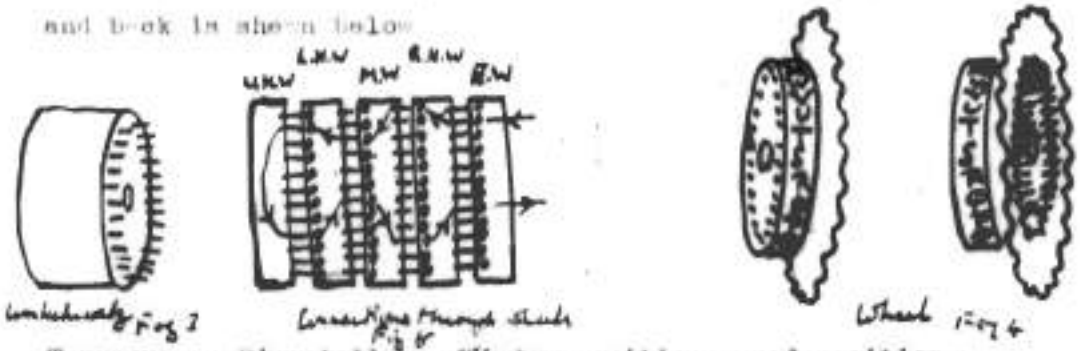


Fig 2 Fig 3 Fig 4

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 ~~of the wheels~~ which show 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 ~~as~~ 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 bells 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 ~~the right~~ each wheel on the right .

One (or ~~in the exxxxxx~~ possibly more, here we will always assume it is only one) catch on each tyre the left.

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

DECLASSIFIED
Authority NND 363016

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 occurence 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 positionof 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	[illegible]	[illegible]
AwP	BDP	NFX	[illegible]
AWQ	BDQ	NFY	[illegible]
AXR	DER	NFZ	[illegible]
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 throughthe 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

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,...). ~~xxxxxxx~~ Normally ~~xxxxxxxxxxx~~ ~~the~~ one arranges that this constant is zero (see also)

The steckered enigma.

In some enigmas the association of the con tacts of the Eintrittswalz withthe 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 Eintrittswalz and the other to one of the keys. Normally the 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 ~~xx~~ 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 'constellation' VN). Thus if a possible encipherment without any Stecker were

~~XXXXXXXXXXXXX~~ ~~XXXXXXXXXXXX~~ [redacted]

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

SIEDENKE
BVMYBENYO

Each short plug is connected to a long one

DECLASSIFIED
Authority NND 963016

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

Upper half of wheel

Fig 8

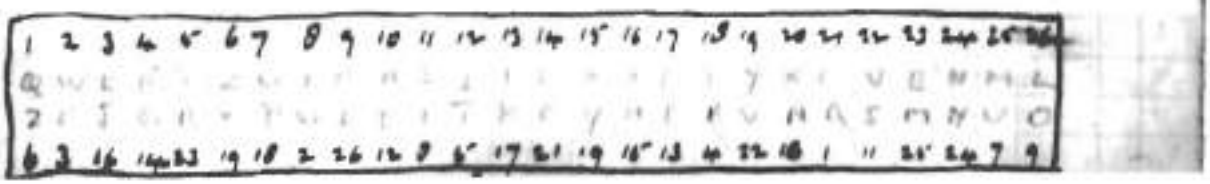
The contact which is uppermost or nearest to the spot is called 1 and then the numbering is continued in clockwise direction. One then makes out a scheme like this

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 top two lines to 'transpose' the



DECLASSIFIED
Authority NND 763016

DECLASSIFIED
Authority NND 363046

third line into numbers, then rub out the second and third lines.

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

The conic strips.

For demonstration purposes it is best to replace the machine by a paper model. We replace each wheel by a ~~xxxxxxxxxxxxxx~~ strip of squared paper 52 squares 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 squares containing the same letter ~~xxx~~ 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 Umkehrwalz 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 unstackered diagonal ~~xxxxxx~~ to represent the Eintrittswalz. It is convenient to repeat ~~xxxxxx~~ 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 ~~xxxxxxxxxxxxxxxxxx~~ ~~xxxxxxx~~ 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 type

DECLASSIFIED
Authority NND 963016

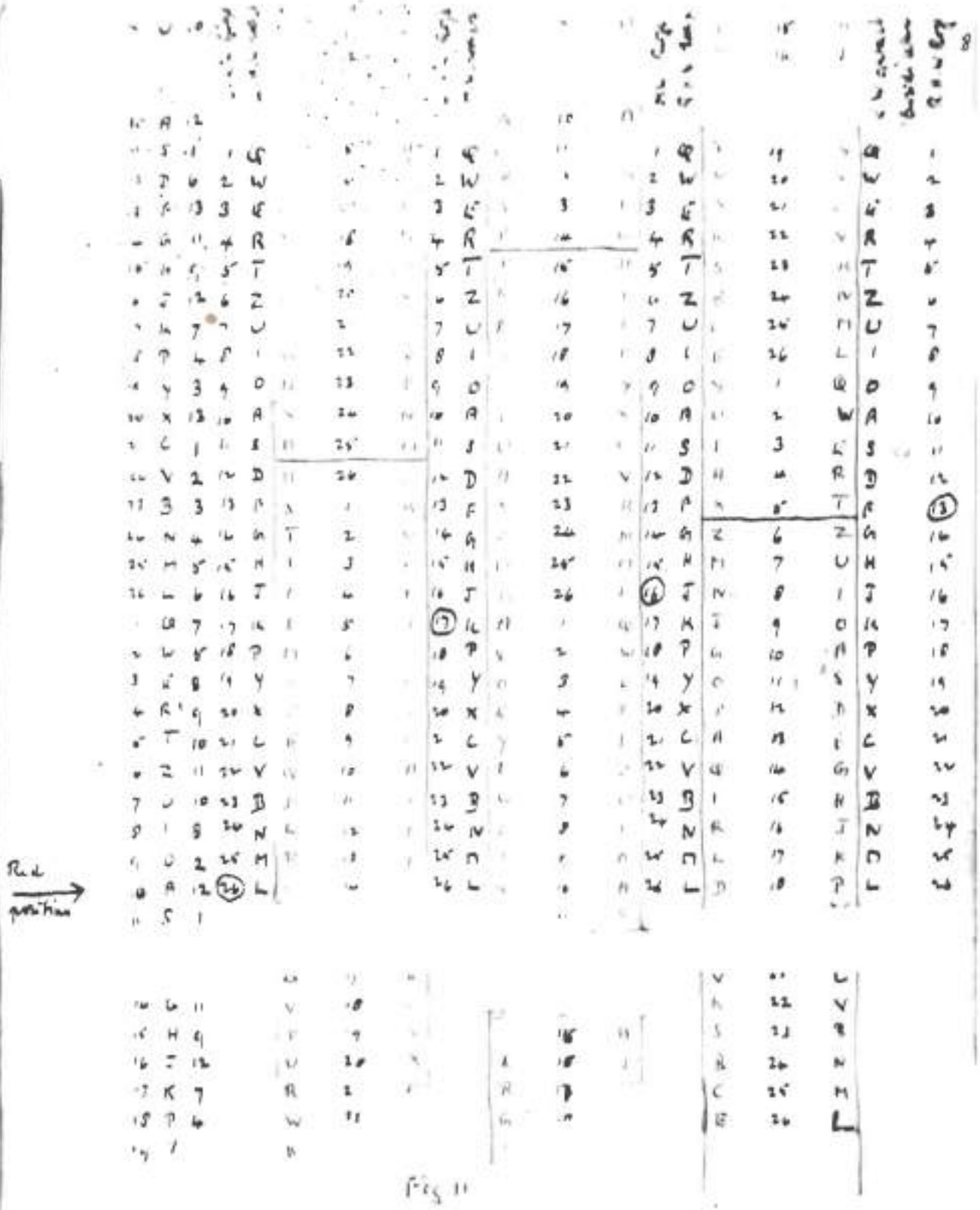


Fig 11

Set up of Rawlway Cover Stripe for the wheel order III I II with Ringstellung 26 17 16 18 and wheel position 10 5 26 5. As the keyboard unit is just below the Ringstellung circle & R H L the rest wheel position will be 10 5 1 0. In the position shown the result of encipherment of Y is P: the path of the current is [illegible] In the column [illegible] the letters we read the wheel [illegible] position [illegible]

could be obtained by having windows and pawls which could be rotated round the wheels 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 show 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 R.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 arrangement 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.

DECLASSIFIED
Authority NND 963016

DECLASSIFIED
Authority NND 363046

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 one position. We can make this out in the form of a square measuring 26x26 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 for the wheel. Thus in column 18 and row e of the purple square Fig 16 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

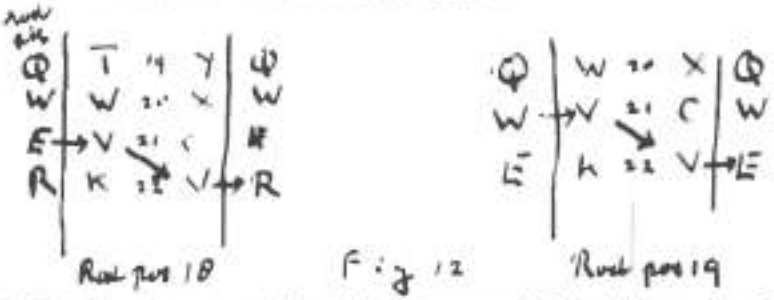


Fig 12

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 smaller 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

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 round the K.W. as the wheel moves forward one will always be in contact with the same point of the K.H.W. and therefore connected to the same point on the left hand side of the K.H.W. This point is moving steadily round and therefore the rod points describing its position move backward along the diagonal.

Encoding by rods

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

DECLASSIFIED
Authority NND 363016

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

[illegible]

DECLASSIFIED
Authority NND 363016

12 13 14 15 16 17 18 19 20 21 22 23 24 25 26	
M A V G K J C V L . . .	s
W V R C S F D V P A .	n
N G X H A C F O W V . .	q
V K D A H S R N K . . .	l
C U P A I M V J N . .	p
K P G U G X T W O . .	z
Z R C Y G O X D I Q . .	l
D C 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 I 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 A Q . .	t
S I H R K V B Q D R W . .	d
J O E V U R S L P P Y .	i
T N O Z F W H X C M A . .	a
P F N J D I 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 R . . .	k
U X M L R H U T V Y F . . .	h
C L Q T J I Z B X G . . .	j

Decipherment of message 10

16	17	18	19
Q	S	Z	V
D	E	U	T

First attempt of R.H.W code.

DECLASSIFIED
Authority NND 363066

O M T L C P N I U E J I P R E V F U D H W J V . . . —
T R C D O E S W T N Y G M K I Z L Y M Q I B A H V X L

B G S T F R X I C J Q Y H I W C Z E A M D K P V U M m
S C H P D T J F X O V Q W Z K O U N C H B U R A T L k

E N O Q B J H 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 K 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 U F A K Z Y N M E G Z R C P D I 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 w
H I Z G T C Q V K W X J O E Y U R S L A P Y B I L N i

P T A S H L P J U R N Z D F Y G O X D I Q C G M V E l
D F K U 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 J 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 D T V D P F I Y S U L X F N C m

N V F H R D E Y M X H L P G U Q X T W O N S J K C Z z
P 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 a
C H I Y S B D M R T O X D A Q N P L K U F I E G Z W e

J O X K N F E T Z A C F S U M Y Q P I G O R H U E V c
V Y L H W U I D B H A 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 N 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 T H V S N E F 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 C 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 V G X H A C F O W V H L B R Y q

Second set up of A.H.W rocks.

First set up.

																		18	19	20	21	22	23	24	25	26
																Q	S	Z	V	I	D	W	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	. . .
E	N	S	I	N	D	J	E	T	Z	T	B	N	E	N	G	L	A			

Think along.

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

~~xqxxx~~ GSZVI DMFFN KXACM RWWXU JYUFY NGVVX DZ...

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 Spruch schluessel to be 10 5 26 1 i.e. that the ~~windowxxxxxxxxxx~~ machine should be set to the window position 10 5 26 1 ~~xxxxin~~ 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 ~~Mt~~ 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 ~~thexrodxpositionxxxxxof thexNxNxNx~~ over the letters of the message the rod positions of the R.H.W. at which they are to be enciphered, remembering that the ~~xxxxxxx~~ 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 ~~only~~ 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 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 L.W. set to this position) They are qo, ev, bn, kc, sx, wc, mj, td, pr, fi, yu, zl, hw. 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					
1	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3
	Q	S	[illegible]	V	I	D	V	F	P	N	E	X	A	C	M ...

Fig 16

Rings = rod position + T.O.s

DECLASSIFIED
Authority NND 363046

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. . have the positions 10 14 10 and the R.H.W.has the positions given at the head of the dolumn. We can therefore use the set up for decoding up to the first T.O. Afterwards we have to rearrange the rods with the coupling inthe 11th column of the red rod set-up (Fig 15)

DECLASSIFIED
Authority NND 363016

Chapter III. Methods for finding the connections of a machine. Alphabets and boxes. cf. 504 paper on Friedman figure

For any position of the wheels of a machine the letters of the alphabet can be put into 13 pairs so that the result of enciphering one member of a pair is the other member. These pairs are usually written one under the other and called 'the alphabet' at the position in question. Thus the alphabet for the wheel order Green Red Purple and rod position 10 14 11 17 is

Y
MS
VL
ZU
HY
JE
TR
OG
IF
XD
KC
AQ
BW
NP

The order in which these are written is immaterial.

When we have two alphabets to deal with it is sometimes helpful to describe both alphabets simultaneously in the form of a 'box'. Take for instance the two alphabets

α	β
VM	VU
ZJ	ON
ES	JW
GA	HI
NP	TM
XR	FG
OF	EZ
HI	LR
LB	QB
DW	XP
YT	YK
UK	AC
QC	SD

To form a box from these we choose a letter at random, say T, and ~~xxxxxxxxxxxx~~ write it down with its partner in the first alphabet, Y, following it, thus TY; we then look for Y in the second alphabet and find it in YK; we write the K diagonally downwards to the left from Y, thus TY / K ; now we look for K in

DECLASSIFIED
Authority NND 363016

the first and finding it in KU write TY/KU. From this we get to

TY/KU/V and TY/KU/VM, but now if we were to continue the process we should

get TY
KU
VM
TY
KU
VM
TY
.
.

We therefore draw a line, select a new letter, Rmay, and start again, writing our results below what we have already written. Thus we get

TY
KU
VM
RX
PN
OF
GA
CQ
BL

Eventually when there are no letters left we stop with the completed 'box' (α/β box)

TY
KU
VM
RX
PN
OF
GA
CQ
BL
SE
ZJ
WD
HI

There are various remarks to be made about boxes. A box completely determines the alphabets from which it was made. Also it can be written in various forms depending on the choices of letter which are made during the process, but two different boxes made from the same alphabets can always be transformed into one another by a combination of the processes

DECLASSIFIED
Authority NND 363046

i) Rearranging the order of the compartments

ii) Moving a number of lines from the top of the compartment to the bottom, the order of the lines remaining the same

iii) Rotating a compartment through 180° about its centre, and then rotating each letter through 180° about its centre.

At first sight it would seem possible that in making a box one might reach a state of affairs like this

AB
CD
E.

and that EA occurs in the first alphabet, and one would not then know what to do. This is not actually possible as EA in the first alphabet would contradict AB, For the same reason it is notpossible to have E coupled with any other letter which has already occured.

If we think of the columns in a compartment of a box we see that the effect of going down the left hand column of a compartment, or up the right hand column gives the result of enciphering aletter with the first alphabet and then enciphering the result with the second. Consequently if ~~xxxxxxxxxxxxxxxx~~ instead of being given the alphabets we have the result of this double encipherment we shall almost have the box. We shall not know how much to slide the opposit sides of a compartment relative to one another, and in the case of compartments of equal size we shall not know how to pair off the sides.

The effect of enciphering first with α then with β I shall call 'the permutation $\beta\alpha$ ', likewise the effect of enciphering with α then β then γ will be called $\gamma\beta\alpha$. For these permutations there is a notationsimilar to the boxes. However this kind of 'general box' does not enable one to recover the original alphabets. It is also more convenient to write them horizontally (the same applies to ordinary boxes, but the tradition there is firmly established). As an example of the notation

$\gamma\beta\alpha$ = (KLAIYSUHPP)(TCWMZB)(DEXVRN)(J)(O)(Q)

DECLASSIFIED
Authority NND 363016

This means that G enciphered at α (giving A), and then at β (giving C) and then at γ gives K, likewise K enciphered with $\gamma\beta\alpha$ gives L, P enciphered gives G, and J enciphered gives J. With the same notation the alphabet α could be expressed in the form (VM)(ZJ)(ES)(GA)(NP)(XR)(OF)(HI)(LB)(DW)(YT)(UK)(QC).

If the letters of a pair of alphabets are subjected to a substitution, and a new box is made up from the resulting alphabets the sizes of the compartments of this box will be the same as in the original box: in fact this box can be obtained from the first box by subjecting it to the same substitution, (except possibly for order of compartments etc.): e.g. if we subject the alphabets α, β to the substitution

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	P	G	Y	T	N	R	H	F	I	K	O	L	U	E	M	S	B	Q	C	J	A	V	X	W	P

(Z to replace A etc.) then we get the alphabets

α'	β'		ρ, σ
AL	AJ	and the box	CW
PI	EU		KJ
TQ	IV		AL
BZ	~~MKEF~~ HF		RX
XR	NB		MU
EN	TP		EN
HF	OR		BZ
OD	SD		GS
YV	XM		DO
WC	WK		QT
JK	ZG		PI
SG	QY		VY
UM	~~MX~~		HF

Conversely if we are given two pairs of alphabets λ, μ and ρ, σ such that the sizes of the compartments in the $\lambda\mu$ box are the same as in the $\rho\sigma$ box, then it is possible to find a substitution which will transform λ into ρ and μ into σ (in fact usually a great many such substitutions). We have only to write the boxes in decreasing compartment size(say), and then a substitution with the required property will be the one which transforms letters in corresponding positions into one another.

DECLASSIFIED
Authority NND 363016

The sizes of the compartments in a box, and the lengths of the ~~xy xxinx~~ brackets (cycles) are important, as they remain the same if all the letters involved are subjected to the same substitution,(which might be a Steckering). ~~Xxxxxx~~ If we write down the lengths of the cycles of a substitution~~x~~ in decreasing order we obtain what we call the 'class' or the 'shape' of th substitution. e.g. the class of $\gamma\beta\alpha$ above is 11,6,6,1,1,1; with boxes there are two ways of describing the shape, either by the lengths of the compartments or by the numbers of letters in them. ~~It~~ It is always obvious enough which is being used. The following information about frequencies of box shapes may be of interest.

26	25%
24,2	13%
22,4	7.3%
20,6	5.4%
18,8	4.5%
16,10	4.0%
14,12	3.9%
22,2,2	3.7%
	[illegible]

DECLASSIFIED
Authority NND 363016

The phenomena involved

Before trying to explain the actual methods used in finding the connections of a machine it will be as well to show the kind of phenomena on which the solution depends.

The most important of the phenomena is this. Suppose we are given the alphabets at the positions ~~XXXXXXXXX~~ REA FKA WMA and also at REB FKB WMB then there is a substitution which will transform the alphabet REA into REB, FKA into FKB etc. The substitution is that which transforms letters of the column of the rod square corresponding to position A into the letters on the same rod in column B. When we are given complete alphabets we can box REA with FKA and REB with FKB, and the substitution will have to be one which transforms the first box into the second. As an example of this phenomenon we may take the alphabets and boxes

REA	REB	FKA	FKB	WMA	WMB	REA FKA	REB FKB	REA WMA	REB WMB
EX	RO	KH	ZJ	TW	XI	EX	RO	EX	RO
UL	FU	JQ	NI	QD	PG	UL	FU	UL	FU
HG	JM	NL	EU	ZF	HB	NK	EZ	KN	ZE
CD	AG	GC	MA	RN	VE	HG	JM	HT	VX
YV	KL	ZR	HV	VZ	IN	CD	AG	WI	ID
FJ	BY	IO	DC	OC	CA	MQ	SP	PB	TW
RT	VX	PA	TQ	KL	[illegible]	JZ	NH	YV	KL
QZ	FJ	BW	WI	GT	MY	RT	VX	JZ	NH
WI	ID	TV	XL	BY	WK	VY	LK	FJ	BY
BP	WT	SY	YX	IP	ZT	SP	YB	OH	MJ
AO	QC	MD	SG	HN	JU	WI	ID	MQ	SP
JZ	NH	EF	KB	AU	QF	OA	CQ	DC	GA
NK	EZ	UX	FO	AE	OA	PB	TW	OA	CQ

The substitution which will transform REA into REB, FKA into FKB, WMA into WMB, the box REA FKA into REB FKB and REA WMA into REB WMB is

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	A	G	R	H	M	J	D	N	Z	U	J	E	C	T	P	V	Y	X	F	L	I	O	K	H

In this example the alphabets have been written out in such a way that the letter and the result of applying the substitution occupy corresponding positions. Of course if our alphabets were data from which the substitution was to be found this would not generally be the case. Our problem would be to arrange them ~~in xxxxxxxxxxxxx~~ order or the boxes made from them, in such an order.

DECLASSIFIED
Authority NND 363046

It might for instance be the alphabets in the more or less alphabetical order

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	RKA	RKB	RKA	RKB
						EKA	FKB	WMA	WMB
AO	AG	AP	AN	AU	AC	AO	AG	AO	AG
BT	BY	BW	BK	BY	BH	IW	SP	CD	PS
CD	CQ	CG	CD	CO	DT	BP	NH	QM	JM
EX	DI	DM	EU	DQ	EV	CD	VX	HG	YB
FI	AZ	EF	FO	AX	FZ	MQ	LK	SF	HN
GH	FU	HK	GS	FZ	GP	JZ	YB	ZJ	LK
IW	HN	IO	HV	GS	[illegible]	RT	RO	VY	WT
JZ	JX	JQ	IW	HM	IX	VY	FU	BY	DI
KN	KL	LN	JZ	IP	JS	SF	EZ	IW	XV
LU	OR	RZ	KY	JV	KW	KX	JM	TR	EZ
MQ	PS	SY	LX	KL	LN	UL	CQ	NK	UF
RT	TW	TV	NP	NR	MY	NK	TW	LU	QC
VY	VX	UX	QT	TW	OR	HG	ID	EX	OR

and then make from the boxes on the right. From the right hand pair of boxes we see that E must become either O or R in the substitution, and we can try both hypotheses out by arranging the first two boxes correspondingly. If the first box is left as it is, the corresponding rearrangements of the second are

..	..
..	..
..	..
RT	AC
PS	SP
MJ	VX
ZE	LK
UF	YB
OR	RO
BY	FU
KL	EZ
XV	JM

The first of these arrangements is impossible. It implies for instance that in the substitution C becomes H and M becomes P but in the third box C and M occur on opposite sides of a compartment while in the fourth they are on the same side. Actually we have in the six alphabets rather an embarras de richesse. It would really be easier to work with say the first five alphabets and the two constatations , AC and BH say of the remaining one. Since B and H occur three apart in the same column of RKB the pair of letters of WMA from which BH arises by the substitution must occur three apart in one of the columns of the large compartment of RKA . The only possibility is that BH arises from FZ, and we can check the result with the AG.

4 complete

DECLASSIFIED
Authority NND 363016

We make use of a third phenomenon when we have found some parts of of the rod . Suppose we find the substitution which transforms the first column of the purple rods into the third

L	SY	Q
[illegible]	[illegible]	Y
D	KW	P
G	EC	A
Y	VX	I
T	CD	E
N	FA	D
B	ST	R
H	ZG	C
F	HE	W
I	UB	N
K	NR	X
O	TL	Z
L	QV	M
U	BI	V
E	OQ	J
M	WN	S
S	MP	T
R	YF	K
Q	[illegible]	[illegible]
C	[illegible]	[illegible]
J	XE	F
[illegible]	[illegible]	Q
V	[illegible]	[illegible]
X	[illegible]	O
W	RS	G
[illegible]	[illegible]	L

It is

(ZDEWFH)(GEOTCIUBSIWRYVLQ)(JX)(AP)

and the substitution which transforms the third column into the fourth is

(JYBNSLZWPTRXIVMQ)(CADKOG)(HU)(FE)

These two substitutions are of the same shapes, and if we write them like this

(YVLQGEOTCIUBSIWR)(NFIZDE)(PA)(JX)
(JYBNSLZWPTRXIVMQ)(CADKOG)(HU)(FE)

each letter in the lower line is below the letter which is three places further on along the (QGEWNZU) diagonal. We can see that this must happen because if we replace the letters of the first and third columns of the rod square by those which are three places further along the diagonal and then move the result three places to the right and three upwards we get the fourth and sixth columns.

DECLASSIFIED
Authority NND 363016

A rather similar phenomenon is useful when we do know the diagonal of the machine. In such a case we can make a correction to our constations transforming them into connections between the contacts on the right of the R.H.W. instead of between contacts of the Eintrittswalz. The constatations when so transformed are described as 'added up' or 'buttoned up'. The process can be carried out with two strips of cardboard with the diagonal written on them, and in one case repeated. As an example to make quite clear what this adding up process is take the fixed comic strips Fig 11. The alphabet for this position of the machine is (CB)(FR)(TV)(XO)(JK)(WZ)(AG)(PY)(BZ)(HS)(IL)(EM)(US) The added up alphabet can be obtained either by tracing through the wheels from the purple column on the right back to this column again, or by applying the substitution

[illegible]	[illegible]	K	R	T	Z	[illegible]	I	O	A	[illegible]	D	F	[illegible]	H	J	[illegible]	P	Y	X	C	V	B	N	M	L
Y	X	C	V	[illegible]	N	[illegible]	[illegible]	[illegible]	E	[illegible]	[illegible]	Y	Z	[illegible]	I	O	A	J	D	F	[illegible]	H	J	K	P

to the ordinary alphabet. It is

~~(XR)(TV)(BG)(DZ)(IO)(XY)(WZ)(AS)(EN)(UK)(LP)(CJ)(MK)~~

(FR)(TV)(BG)(DZ)(IO)(XY)(WZ)(AS)(EN)(UK)(LP)(CJ)(MK)

Instead of tracing the current through from the right hand purple column in Fig 11 we can of course trace it through from the left hand purple column back to this column again. ~~[illegible]~~ This gives us a very simple picture of how the added up alphabets between turnovers are related; one is obtained from another simply by a slide on this left hand purple column, i.e. a slide on the ~~[illegible]~~ last upright of the rod square. For instance ~~the~~ if on the ~~fixed~~ comic strips Fig 11 we move the R.H.W. to rod position 15 we have the added up alphabet

(EA)(RD)(VM)(IO)(PN)(UB)(LF)(GW)(YX)(CT)(QJ)(KZ)(HS)

which can be obtained from the added up alphabet at rod position 18 by the substitution

T	[illegible]	V	K	[illegible]	B	C	E	Y	U	F	H	X	Z	[illegible]	N	J	G	O	P	A	Q	I	R	L	D
H	L	D	T	W	V	K	[illegible]	B	C	E	Y	U	F	H	X	Z	M	N	J	G	O	P	A	Q	T

DECLASSIFIED
Authority NND 363016

The saga

Suppose that one was left alone with an enigma for half an hour, the lid being locked down and the Umkehrwelz not movable, what data would it be best to take down, and how would one use the data afterwards in order to find out the connections of the machine ? Can one in this way find out all about the connections ? This problem is unfortunately one which one cannot often apply, but it helps to illustrate other more practical methods.

It is best to occupy most of one's half hour in taking down complete alphabets. At least nine of these are necessary, as follows from this argument. ~~In principle it would be possible to find the connections by writing down all possible sets of connections and noting out those which are not consistent with the data~~ If the solution is completely determined by the data the number of possible different data must be at least equal to the number of possible different solutions. Now the number of possible different diagonals is 26!, the number of ways in which one can wire up a wheel is also 26!, and the number of ways in which one can wire an Umkehrwelz is approximately $(26!)^{\frac{1}{2}}$, so that the number of possible solutions is about $(26!)^{9/2}$. The number of possible variations of an alphabet is about $(26!)^{\frac{1}{2}}$, so that the number of possible variations of nine alphabets is about $(26!)^{9/2}$ which is the number of solutions.

The practical minimum amount of data is surprisingly close to this theoretical minimum. It is possible to find the connections with 9 properly chosen alphabets and 10 other constatations properly chosen. However in order to shorten the work I shall take an example where we are given 11 alphabets and 10 constatations.

DECLASSIFIED
Authority NND 363016

Note for page

AAA	AAC	ABA	ABC	CAA	CAD										
AAB	AAD	ABB	ACA	BAA								ADA	CAC		
~~XXXXXXXX~~											ACB	DAA			BAD
AL	AD	AI	AM	AK	AE	AW	AN	AS	AQ	AZ		SO	UQ	MJ	HX	MA
BS	BC	BY	BS	BO	BS	BV	BP	BO	BV	BN		ZJ	LB	IL	VS	EU
CE	EK	CT	CH	CF	CR	CZ	CE	CP	CH	CO						
DH	FV	DI	DR	DE	DQ	DX	DW	DJ	DU	DF						
FM	GZ	EV	EO	GQ	FL	EJ	FG	EU	EP	EI						
GR	HN	FN	FQ	HW	GV	FO	HL	FQ	FM	GL						
IK	IT	GX	GP	IX	HK	GU	IZ	GV	GM	HX						
JN	JY	HU	IJ	JP	IN	HI	JO	HY	IZ	JR						
OZ	LU	JO	KX	LS	JP	KR	KQ	IL	JO	KP						
PV	OQ	KZ	LT	MY	MO	LZ	NU	KT	KU	MY						
QW	PS	LW	UZ	NR	UY	MT	RS	MX	RW	QV						
TY	RX	PQ	VY	TZ	WZ	NS	TX	NR	ST	ST						
UX	MW	RS	NW	UV	TX	PY	VY	WZ	XY	UW						

There will be a substitution which transforms AAA into AAB, for finding such a substitution ABA into ABB and ACA into ACB. Following the method explained in the last paragraph we form the boxes AAA AAB AAC ABA, ABB and also ABC which will be needed later

AAA	AAB	AAC					
ABA	ABB	ABC		ACA	ACB	CAA	CAC
[illegible]	[illegible]	AI		AM	SO	A S	HX
SB	[illegible]	HU		BP	[illegible]	BO	VS
[illegible]	MW	GX		CE		CP	
TY	[illegible]	DN		DW		DJ	
MP	VP	TC		FG		EU	
[illegible]	LU	ZK		[illegible]		FQ	
[illegible]	[illegible]	RS		IZ		GV	
[illegible]	[illegible]	NF		JO		HY	
GR	BC	OJ		KQ		IL	
NJ	RX	EV		NU		KT	
PV	TI	BY		RS		MX	
UX	NH	PQ		TX		NR	
IK	KE	LW		VY		WZ	

We want to rearrange the box ABB in the way that was done at the bottom of p. . The substitution which transforms ABA into ABB must also transform two constations of ACA into SO and ZJ. The only constetations from of ACA from which SO could have arisen are LH, [illegible], VY. If OS arises from either LH we should have to have a substitution which involves ZJ arising from OE in ACA, and this does not exist.

DECLASSIFIED
Authority NND 363046

~~similar observation applies to WY~~. However if we rearrange it so that XZ arises from WY we find ZJ arising from IZ. We can similarly arrange ABC to fit with them and a row with CAA and CAC, and fit CAA to fit into CAD agreeing with BAA and BAD.

Rearranged					Rearranged	
AAA	AAB	AAC	AAA	AAD	AAA	AAD
A BA	ABB	ABC	CAA	CAD	CAA	CAD
AJ	VF	GX	AL	UL	AL	TL
SB	LU	DZ	IK	AM	IK	GP
OZ	YJ	TC	TY	YV	TY	KX
TY	RS	ZX	HB	QF	HB	BC
MF	BC	RS	JN	DN	JN	OE
CE	EX	NF	NG	JI	NG	IJ
DH	TI	OJ	VP	EO	VP	HD
WQ	NH	EV	CE	CH	CE	FQ
GR	KE	BY	UX	AK	UX	VY
NJ	AD	PQ	MF	PG	MF	MA
PV	QO	LW	QW	LT	QW	ZU
UX	MW	AI	ZO	SB	ZO	WN
IK	ZO	HU	BJ	NW	BJ	BJ

We can now write down the parts of the rods which are in the columns corresponding to the window positions A, B, C, D though we do not know the correct order. They are

AVGT	YSEX	WNEU	UMAV
LFXL	MBHM	QDVZ	XWIY
JLDS	FCSA	GEBJ	IZNS
BUMB	CHNF	RKYI	KQUP
OYTN	KXFQ	RAPZ	JDQO
ZJCW	DTOC	PQLD	
TPZR	HIJH	VOWN	

The substitution which transforms the letters in the first column of these rods into those on the same rods in the second column is

(AVOYSLFCREXWN)(BUM)(ZJDTPQHI)(GK)

That which transforms the second into the third is

(VGUMAPZH)(FX)(LDJ)(YTOWIJCSKBRNE)

and that which transforms the third into the fourth

(GTNFQOCWRMBJH)(XLDSAVZK)(EUP)(YI)

These three substitutions have now to be arranged one under the other in such a way that the substitution which transforms the third into the second is the same as that which transforms the second into the first, this substitution being a slide of one on the diagonal. Clearly (FX) in the ~~third~~ second has to fit under either

(~~AA~~) or (~~BB~~) in the ~~xxxxxx~~ first; if X is under G we cannot fit the second and third together, for Y occurs in a bracket of 13 in the third, and G in a bracket of 9 in the second. If X is under Z we can fit the three together like this

(AVCYTLFCKLAOW)([illegible])([illegible])(GK)
(SHNNRYTOWIJC)([illegible])(VGUMAPCH)(XF)
(RPOCWECJUHT)(PXH)(RALCAVZ)(TY)

The diagonal is

AP\BORYFKV.HIXGJWEIJBCTCHS

~~xxx xw xxx xxxx xxt~~ Of course we do not know where the diagonal 'starts', but with a hatted diagonal like this it does not matter. We can use the diagonal to put the rods in order and to give them numbers. There is likely to be an error in our naming, because we shall not know where to start naming ~~them. This is equivalent~~ to saying that we know in what order to write the letters in the left hand column of the code strip for the wheel, but do not know where to start; or again it is equivalent to knowing the connections of the wheel except for a rotation of the ~~xxxxx~~ plate contacts relative to the spring contacts. This error is known as 'wheel twist'. It is extremely difficult to remove it. We need to have some data to know which true window positions and ~~Ringstellung~~ are involved

either the rows or the columns. The difficulty about naming the columns simply means that we do not know the Ringstellung or the absolute positions involved. If we have the columns correctly named but the rows wrongly we shall have the wheel right except that the plate contacts are rotated with respect to the spring contacts. It is very difficult to eradicate this. ~~xxx xxxxx

DECLASSIFIED
Authority NND 963016

The rest of rods is

[illegible]	z
[illegible]	h
[illegible]	i
[illegible]	x
[illegible]	e
[illegible]	j
[illegible]	w
[illegible]	c
[illegible]	l
[illegible]	u
[illegible]	d
[illegible]	m
[illegible]	t
[illegible]	o
[illegible]	n
[illegible]	s
DTOC	s
[illegible]	p
[illegible]	q
AVGT	b
[illegible]	o
[illegible]	r
[illegible]	y
UMAV	f
[illegible]	k
[illegible]	v

LFXL

and we can now transform all our data about other alphabets into the form of data about rod couplings. The ones we need first are

AA AB AC AD
ch ex yw fv
be bl eh es
ou ow bd
dt dz px
fi ey gt
gw fj ki
jn ko zo
kq ms vl
lz nu ns
mo pt um
px qv jq
rv rh fo
sy iz sr

From these we can get the upright of the middle wheel. The first step is of course to add up the alphabets. Here they are added up with % as standard

AA*AB*AC*AD*

pi qj vu hx
ol rd dg mb
nd sl yo
mc to ow
kx uk es
je ve jh
wn zy xf
vb cp im
ah em pq
tr bn tn
qk wh lr
y z fx ze
f xi bk

DECLASSIFIED
Authority NND 363016

We go box AA* with AB* and AB* with AC*, and then rearrange AB*
A C* so that as to find the substitution which transforms
AA* AB*
A B* into AC* and AC* into AB*

AA*	AB*	AB*		
AB*	A C*	AC*	rearranged	
pi	[illegible]	ir	[illegible]	[illegible]
fq	hw	[illegible]	[illegible]	pc
je	ot	xf	xf	[illegible]
vl	nh	ok	ok	[illegible]
n d	ku	uk	uk	[illegible]
rt	ve	vr	vr	[illegible]
ol	sl	lc	ls	[illegible]
sw	rd	tr	tr	[illegible]
hu	gi	tk	tk	[illegible]
[illegible]	ms	vv	vv	[illegible]
fe	zy	zf	zf	[illegible]
[illegible]	op	[illegible]	[illegible]	[illegible]
[illegible]	xf	ox	xf	[illegible]

~~The upright of the middle wheel~~ This substitution sends each letter of the upright of the middle wheel into the next on the upright; hence the upright is

lsezftrdgpjyxniqchukbmvwo

As we added up to position Z as standard this upright is the upright for position Z. We can make out part of the rod square from it, there being difficulties about where to begin as before

ZABCD

LNJHB	z
SWKOL	h
EVRUP	i
YDQW	x
MBEZ	g
TOLHC	j
RUINH	w
DXSIQ	e
GAXBV	l
PGOZD	u
JRHMK	d
YITVN	m
XCZSU	t
NHADF	o
IPMKJ	n
QTVWO	s
CZERS	a
HLYAE	p
UFPLI	q
KQUXR	b
BDGYT	o
MJFCA	r
WXNPG	y
VSQJM	f
ABWTX	k
OECGY	v

DECLASSIFIED
Authority NND 363016

We can now transform our raw data into information about couplings of the middle wheel rods. By sliding the diagonal up the side of the rod square we can get the couplings immediately into added up form

A*	B*	C*	D*	A* B*	B* C*	B* A* rearranged
rm	an	ny	kd	rm	an	wl
bt	bn	bi	ox	sl	gz	or
ee	or	ol		wj	eq	do
di	do	dr		kg	jk	vf
fo	eq	ez		zv	tx	nb
gk	fv	fn		fo	ph	iu
h y	gz	gn		di	wl	my
jw	hp	hw		un	or	an
ls	iu	xp		bt	do	gz
mx	jk	jq		xm	vf	eq
n u	lw	kt		yh	nb	jk
pq	my	mu		pq	iu	tx
vz	tx	vo		ec	my	ph

The left hand wheel upright is

rwdmqxeptznschkvbgfiyjounls

zhixgjweludmtenaspqhorvfkv

and under it has been written the diagonal. This serves to transform A or A* into the lm wheels connections. They are

yv,fn,ee,zw,ol,mu,rd,qx,pk,nd,bt,hz,al

'Adding up' methods

Some practical methods of finding the connections of the machine depend on getting a long crib, either by 'reading on depth' (see Colonel Tiltman's paper) or by pinching. In many cases we expect the diagonal to have some special value, (e.g. qwertzu because the original commercial machine had such a diagonal). In this case the amount of crib necessary is not very much. To estimate the amount of material that we have it is best to work out

(Length - 2.5) × square of average 'corrected depth'.

Call this the 'material measure'. By corrected depth we mean the actual number of constatations, so that this can never exceed 13. As regards the amount of material necessary, it will almost always be impossible to get the wheel out with less than a measure of 90, from 90 to 140 it will be a matter of chance whether it comes out or not. From 140 onwards it will always come out, but with increasing reason the material measure mounts up. With a material measure of 500 it is so easy that the trouble of adding up further material would be more than would be gained in shortening the further work. The method is essentially the same as we used for finding the middle wheel in the case of the sage. Here however we have to do with partial alphabets or even single constatations instead of complete alphabets. We cannot therefore do any boxing. After we have added the material up we take some hypothesis about the upright, e.g. that F immediately follows K and work out its consequences. If for instance we find the (added up, I shall omit to mention this in future) constatations R and F immediately following one another we can infer that T immediately follows R on the upright. This we may express in the form

$$KF - RT$$

the dash denoting logical equivalence. We follow out the consequences until we reach a confirmation or a contradiction. When there is

KF means 'F follows K on the upright'. KF^2 would mean 'K or F we have spent on

DECLASSIFIED
Authority NND 963016

DECLASSIFIED
Authority NND 363016

Plenty of [illegible] we do not usually start to work a hypothesis unless there is going to be an immediate confirmation, e.g. if TC implies RJ from two different parts of the crib. This will mean to say that the constatations $\overset{Y}{R}$ and $\overset{J}{C}$ occur ~~twice~~ consecutively twice over. Alternatively we can say that $\overset{T}{R}$ occurs twice over at a certain distance, and that $\overset{J}{C}$ also occurs twice over at the same distance. In order therefore to find these profitable hypotheses we have only to look for repetitions of constatations (half-bombes as they are rather absurdly called) . For this reason and ~~xxxxxxxx~~ also because later we will want to be able to spot occurrences of a given letter at a glance, we put our material as we add it up intothe form in Fig 14 .

Now to take a particular problem. We are given material six deep and 100 long, and we expect that the diagonal is qwertzu. Our material is

MYC..
NGJ..

RCA..
YID..

DA..
TTV..

YON..
RMI..

OFL..
V..O..

MUX..
NJ..

(I must apologise for it not making sense) . ~~xxxxxxx

DECLASSIFIED
Authority NND 963016

Fig 19

Fig 20

Fig 21

DECLASSIFIED
Authority NND 363016

However we put the material directly into the form of Fig 19 . We see numerous half-bombes and do not need to make any analysis of their lengths in order to find a profitable start. The half bombes Q and F suggest the two possible starts Q F = HH and Q HEJF (the two strokes meaning a double implication, not equality!). The consequences of the second of these are shown in Fig 20 . A contradiction is quickly reached. The consequences of QF in Fig 21 . The loop QF-ZO-MB-UJ-QF gives a second confirmation, and our hypothesis is now a virtual certainty. We now abandon the tree figure for an alphabet with consecutives written against them (Fig 22). All goes smoothly except that there is clearly an error in our data as we have a few contradictions. We sort out the good from the bad by using pairs of letters two apart on the upright. Thus JO - AF confirming JZ,ZO,AQ,QF. When we have checked them all we can write out the upright of the ....

A[illegible]FTEVKYNC[illegible]JUOD[illegible]HTINGNL

We then have to find the upright of the ... To do this we use the same process as we did with the ... We have to find the added up couplings of the middle wheel. This can actually be done without either adding up separately or writing out the rod square, simply by having two movable strips with the upright and qwertzu written out on each, and sliding these above the(added up crib)till the constitations agree with pairs of letters on the strips directly above. We then read off the coupling from the row of qwertzu letters, taking the pair of letters in column 1 for columns 1-7 of the crib column 2 for 27-33 etc. Under Fig 19 is shown the strips as set for reading off one of the added up couplings for 53-59, viz. aq. The added up couplings that we get are

1-7	27-33	53-59	79-85	105-[illegible]
go	hv	[illegible]	jn	zm
wh	[illegible]	wf	xv	ti
ef	mu	eg	tr	
ry	nk	th	fb	
tn	rn	rv	gl	
zu	te	xx	up	
ix	zy	um	oy	
os	is	io	ds	
sg	ev	sk	wb	
dm	dj	db	ci	
hw	fm	fy	gx	
je	wb	pn	xm	
kl	pl	el	km	

([illegible] heavily [illegible] obtained from related [illegible] [illegible])

DECLASSIFIED
Authority NND 963016

[illegible] the [illegible]

1-7	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	hx	[illegible]
lk	xy	[illegible]
ef	fm	[illegible]
nd	[illegible]	wj
jc	jd	np
[illegible]	bg	um
ry	ok	eg
[illegible]	[illegible]	zx
[illegible]	[illegible]	vr
[illegible]	ov	th
lx	rn	fy
hv	pl	ol
[illegible]	gk	cl

When we fit these boxes together we fall miserably, and so we have to assume that there is a double T.O. somewhere in spite of the boxes all turning out the same shape. We find that this is between the first [illegible] and the [illegible], and that the remainder can be fitted together with the upright

whnkpovrtlxlmzqgpfkmoudj

DECLASSIFIED
Authority NND 363016

I will give a second example of the 'adding up' method for a case where it is only just possible to get the problem out. The material is given in Fig 23 all ready added up. There are no 'equidistances' (half-bombs with equal distances) and so we have to make an analysis showing all the consequences of any hypothesis that one letter follows another on the upright (Fig 24). For instance from the analysis we see that ~~xxxxxxx~~ AV, HT, NF, ZA, are all consequences of HA. The pencil letters round the outside ~~xxx~~ were put in table with the making of the analysis and were used in connection with columns 30, 33 of the material. Of course some of the consequences will be false owing to turnover, but as we are dealing only with distances of 1 we can hope to neglect this without harm. We now pick out ~~xxxx~~ squares with a large number of entries in them and follow out the further consequences of them, making trees as before, and hoping to find confirmations. When we get contradictions we leave the tree for the present but have to remember the T.C. possibility (Figs 28-30). When we get stuck we can sometimes continue using consequences which are of the form that two letters are at distance 2 on the upright. For this purpose an analysis of positions at which letters occur is useful (Fig 24). ~~xx~~ In particular we need this at Fig 30. Now VW and WY imply VY^2 and PR and RS imply PS^2 and these imply one another from columns 19, 21. We also get GL^2 which starts off another train of consequences involving another confirmation (Fig 31). Eventually we get stuck with the bits of ~~xxxx~~ upright

VWY
N.Q PRS
UHJK
FGIL.O
B.E

We might try putting in KA as a hypothesis, ~~xxxxxxxx~~ afterwards try KB etc. (KA appears at first to give confirmations, but these are bogus. The only reliable rule about confirmations is to ~~see if one can leave~~ my identity a constatation out and then see if it can be inferred from the hypothesis). We might also try

DECLASSIFIED
Authority NND 363016

putting in as many more constellations as possible which are consequences of those we have found out available information about the upright, and then start off afresh with some new distance on the upright, say 5. But there is a quicker road to success. Note the constellation J in 1 and I^{G} in 17. Since we have J following H and I following G on the upright it seems highly probable that we have HG^{16} and JI^{19}. If this is so we have this as part of the upright

FGIL..G....GHJE

Hence GH^{G} which implies IE^{G} giving us this as upright

FGILNOGPEGHJE

From this we get many confirmations and are able to fill in the whole of the upright (except which goes in the one remaining place), [illegible] that the T.G. which actually occurs between 24 and 25 has not troubled us at all.

DECLASSIFIED
Authority NND 963016

Clicks at twenty-six-difference

This is a method for finding the connections when we do not know the diagonal. It is very similar to the ~~xxxxxx~~ beginning of the game, in principle. It depends on making hypotheses ~~xxxx~~ about pairs of letters being on the same rod, and drawing conclusions ~~xof the xxxxxxxx~~ to the effect that other pairs of letters are on the same rod. Suppose for example that in our crib were the following constatations

5	6	31	32	57	58	83	84
A	E	F	E	T	U	P	U
F	G	T	R	P	R	A	G

We might make the hypothesis that on the rod which has A in column 5 there is G in column 6. We could then infer that there was another rod with F and E in columns 5,6, and likewise rods TR, PU and this confirms our hypothesis that there was a rod AG. Proceeding in this way we can with sufficient material find sufficiently much of some of the rods to be able to find the diagonal by the same method. The amount of material needed is very great. We count a measure similar to the one for 'adding up' viz

(length-39)$\times$square of average corrected depth

I believe it is practically impossible to solve any problem with this measure less than 2000. It ~~xxxxxxxxxxxx~~ should be possible for 3000 but might sometimes involve a great deal of labour. With the example given here the measure is 4400.

When the material is sufficient we avoid taking hypotheses at random, and choose ones which we can see ~~xxxxxxxxxx~~ without very much analysis, to lead to an confirmation. This would be the case for example with these constatations

5	6	31	32
R	E	R	E
V	D	V	D

Either the hypothesis that R follows E or that D follows it on a rod would be immediately confirmed. In the absence of other information the probability that one or other of these

DECLASSIFIED
Authority NND 363016

hypothesis is correct in about 79%. Our first job therefore is to look for such configurations of letters. All that we have to do is to analyse the material constatations which have exactly the same right hand wheel position, and ring round any repetitions. We then write out the ringed constatations on a separate sheet (Fig 14). With the first occurrence of each constatation we give a number showing how far on the other occurrence is. This ~~sheet~~ plan also shows us where the T.O. is likely to be. It should be mentioned that in the case of this material there were two turnovers known to be 13 apart. The principle of spotting the turnover is this . Consider for example the constatations HK at h,II and b,X and JK at i,II and i,X. The first pair of these constatations shows that there must have been a ~~couplix~~ pair in common between the coupling at b,II and b,X . Likewise there must be one in common between those at i,II and i,X . It is therefore fairly likely that there is no turnover between h,II and ~~kpk~~ i,II, as if there had been it would have been quite likely that after the T.O. there would no longer have been a pair in common in the couplings. The evidence from a single such instance is rather slight, but with as much material as we have in our present problem we can ~~ix~~ it ~~fairly occurredly~~ with no doubt at all, as occurring between n z and a and between m and n.

It is worth while writing down all the favourable hypotheses under the pairs of columns of the rod square involved (Fig 35). We have done this only for the cert a to m, and find that in five cases there are two favourable hypotheses viz. col. b with e col. b with h, col. d with j , col. e with i, and col g with j. We hope that in some of these cases the favourable hypotheses will imply one another, making them both virtual y certain. ~~AGAIN X for the case of d with j they contradict one another~~. The consequences of these hypotheses are shown in Figs 36 - 40 . The notation is this. An expression like OF under the head 'd onto j' means that the rod with O in col. d has F in col. j, and the strokes joining these mean that one can be deduced from the other. In the case of g onto j the two hypotheses are essentially the same and we have an immediate

DECLASSIFIED
Authority NND 963016

confirmation. With b onto h we find that both of the first alternatives of the one hypothesis con radict both alternatives of the other. With d onto j we manage to connect the two hypotheses together and with e onto i we fail to connect but one of the hypotheses confirms itself. The information we have obtained about the rods from this is expressed in the Fig 4a. In order to avoid bogus confirmations in what follows it is as well whenever we make a deduction to cross out one of the constations used in the deduction. Up to this point the crossing out has been done with red strokes slanting up to the right. (Green vertical strokes were used to eliminate repetitions of a constation, red vertical strokes to remove contradicted constatations.) . From now on for a time we will use similarly slanting green strokes.

Up to now we have simply been trying to 'get a start' , and so long as we could get some fairly considerable bits of the rods square fixed we did not very much care what parts they were. But now we have got a fully adequate start, and we should consider a plan of campaign. In general what we want is most of the letters of the rods in columns p, $p+q$, $p+r$, $p+q+r$, t, $t+u$, $t+r$, $t+u+r$, of which any number may coincide, provided q, r, u are none of them 0. If we then find the permutation which transforms col. p into col. $p+q$ expressed in cycles as on p 18 or p 26, and similarly for col. $p+r$ and col. $p+q+r$. A slide of r on the diagonal will transform these into one another. We get further information about a slide of r on the diagonal by finding the substitutions that transform col. t into col. $t+u$, and col. $t+r$ into col. $t+u+r$. Between the two sets of information we should have enough to reconstruct the diagonal (unless $r=13$ and as long as the bits of rods are not too incomplete

DECLASSIFIED
Authority NND 363016

In the present case we can take the columns c,d,f,g,j,k; giving them the numbers 5,4,6,7,10,11 instead of the letters this corresponds to p^{+3}, q^{+3}, r^{+6}, s^{+4}, t^{+1}. In order to get these columns we look on Fig 35 for suitable hypotheses to work in order to add in the extra columns. These hypotheses enable us to write in extra letters in the Fig 4(a) and we continue to write in letters in this figure until we reach a confirmation ~~xxxx or~~ or a contradiction. Until we reach a confirmation it is as well to differentiate the letters that are certain from the rest. The hypotheses that we actually used were : ~~xxxx~~ c into g IQ=SE: g into k XE=ND. After a considerable amount of work our ~~trial~~ rods look like Fig 4b. The lines crossed out are ones that have been amalgamated with others. We now think we can start to look for the diagonal, and therefore make up the permutations transforming c into f, d into g, f into j and g into k. The notation is that of p 19, except that we are mostly unable to complete the brackets, and leave dots.

c into f

...DCY.FVJZTAXHIN...SGOPR...KE...LUB...M...W...

d into g.

...KWCM...ANSY...GLIJ...TUQ...DKBXOR...FIZV...H...

f into j

...QTK...UHJNGR...BSZN...FWA...CXIM...YD...E...L...V...

g into k

...IND... (XX) ...KF...TYHZ...MABLJMURG...PA...C...S...O...V...

We have now to write the c into f permutation over the ~~f~~ d into g permutation, and the f into j over the g into k in such a way that ~~the~~ a given letter in ~~xix~~ 'c into f and f into j stands over the same letter in 'd into g and 'g into k. To get a start on this observe the configuration of the ringed letters. This suggests that we arrange the permutations in this way

DCY.FVJZTAXHIN
DKBXOR
{YD}
{XE}

DECLASSIFIED
Authority NND 363016

This is further confirmed many times, and so we the permutations arranged like this

(DCY[illegible]FVJ[illegible]TAXHEN) MSGOPR
(EBXORANSYGLIJD) KWCMTU[illegible]

(YD) [illegible]OTK UHMNGHCX[illegible]PFA
(XE) OTYHL [illegible]DJ[illegible]BLJWURG

giving us the partial diagonal slide of 1

...BC[illegible]...[illegible]NJ IHK...L[illegible]Y[illegible]OQRF...WMGAV...UP...

Z must be followed either [illegible] E,L,W,or U . If it is followed by U we get

LUB
FPZV

and the diagonal slide as

(BC[illegible]UPLXYTO[illegible]F[illegible]NJ IH[illegible]WMGAV)

If Z is followed by L we have the bits

MSGOPR KE LUB W
KWCMTUQ H FPZV

to fit together, which we find [illegible] can only be done like this

(KEMSGOPR) (BWUL) (KEWLUBMSGOPR)
(HKWCMTUQ) (FPZV) or like this (HFPZVKWCMTUQ)

giving the diagonal slides

(KDNJ IHK)(...)

(UP)...

both of which are impossible. If Z is followed by W we have the bits

MSGOPR KE W LUB
KWCMTUQ,H FPZV

which fit together only as

(KEMSGOPR) (LUBW)
(HKWCMTUQ) (VFPZ)

and as before the K configuration makes this impossible. We cannot have Z followed by E because of the impossibility of fitting KE onto H FPZV. The diagonal is therefore

BC[illegible]UPLXYTO[illegible]RFKDNJ IHKWMGAV

DECLASSIFIED
Authority NND 963016

After the previous examples that have been given it is hardly necessary to explain how to get the uprights of the various wheels after this point. The upright of the right hand wheel would be obtained by rearranging our bits of rod, and the middle wheel by the method described on p. 28 . With luck we might find other messages on the same day with different L.H.W. positions and so find the L.H.W. upright. In the case that the Umkehrwalz is movable this may be rather tricky [redacted]), but in such a case there are or probably no Stecker, and we should be able to solve other days by single wheel processes, with the known wheels in the R.H.W. position, and hope for the unknown wheels to occur in the L.H.W. position.

In the example given above the diagonal is actually ABCD... with Stecker. We might have had a hatted fundamental diagonal with Stecker, and of course in such a case we could not have said what the fundamental diagonal was. We should then have had to proceed to try to solve other days keys by spider methods, without diagonal board, and assuming temporarily some arbitrary diagonal fundamental diagonal, and non reciprocal steckering. With two or three such keys we should be able to find the actual fundamental diagonal by comparison of the steckered diagonal.

Finding new wheels, Stecker knock-out

So far we have been dealing with the problem of getting out the connections of an entirely new machine, or one for which we know no more than the diagonal. There is another problem, that of finding the connections of some newly introduced wheels, the old wheels, or at any rate some of them, remaining as well: this includes the case of a change of Umkehrwalz.

The most hopeful case for getting out the new wheels is when ~~it~~ one of the known wheels occurs in the R.H.W. position. If the machine has no Stecker there is no difficulty. We solve some messages by using wheel processes. This will be slightly more difficult than when we know the connections of the middle wheel, as we shall have to guess what is said in ~~its~~ three or four different turnovers. However ~~in fixed that is~~ when the R.H.W. rod start has been found from a guess in one turnover it does not take any time to test a not probable throughout the message (the rods on which the various letters of the message occur can be written down once for all, and the not probable punched out and run over the inverse oblong). For simplicity let us suppose that we have read the message right through. We then have the couplings in several ~~turns~~ consecutive positions of the middle wheel, and can apply the method of p 28, 29 to find its upright.

In the case that the machine has Stecker we need rather more data, and very much more patience. The sort of data that one needs is a crib of length about 70, or else one of length ~~18~~ 28 and depth 2. The trouble about cribs without any depth is that one uses up ~~the~~ a great many of the contactations ~~after~~ between each turnover in determining the coupling.

An example is shown of ~~this~~ a crib of length 18 and depth 2. This is to be regarded as one of ~~length 26 which has been cut down~~ greater length which has been cut down to allow for turnover. The text of the crib is shown at the top of Fig 42. ~~There are~~ ~~[illegible]~~ We are taking the worst case of 13 Stecker. There are several half-bombes in the crib, and we decide to work with TW. We have to make ~~[illegible]~~ 17576 different hypotheses, (app) corresponding to the 26 possible different places on the R.H.W.

DECLASSIFIED
Authority NND 963016

DECLASSIFIED
Authority NND 363016

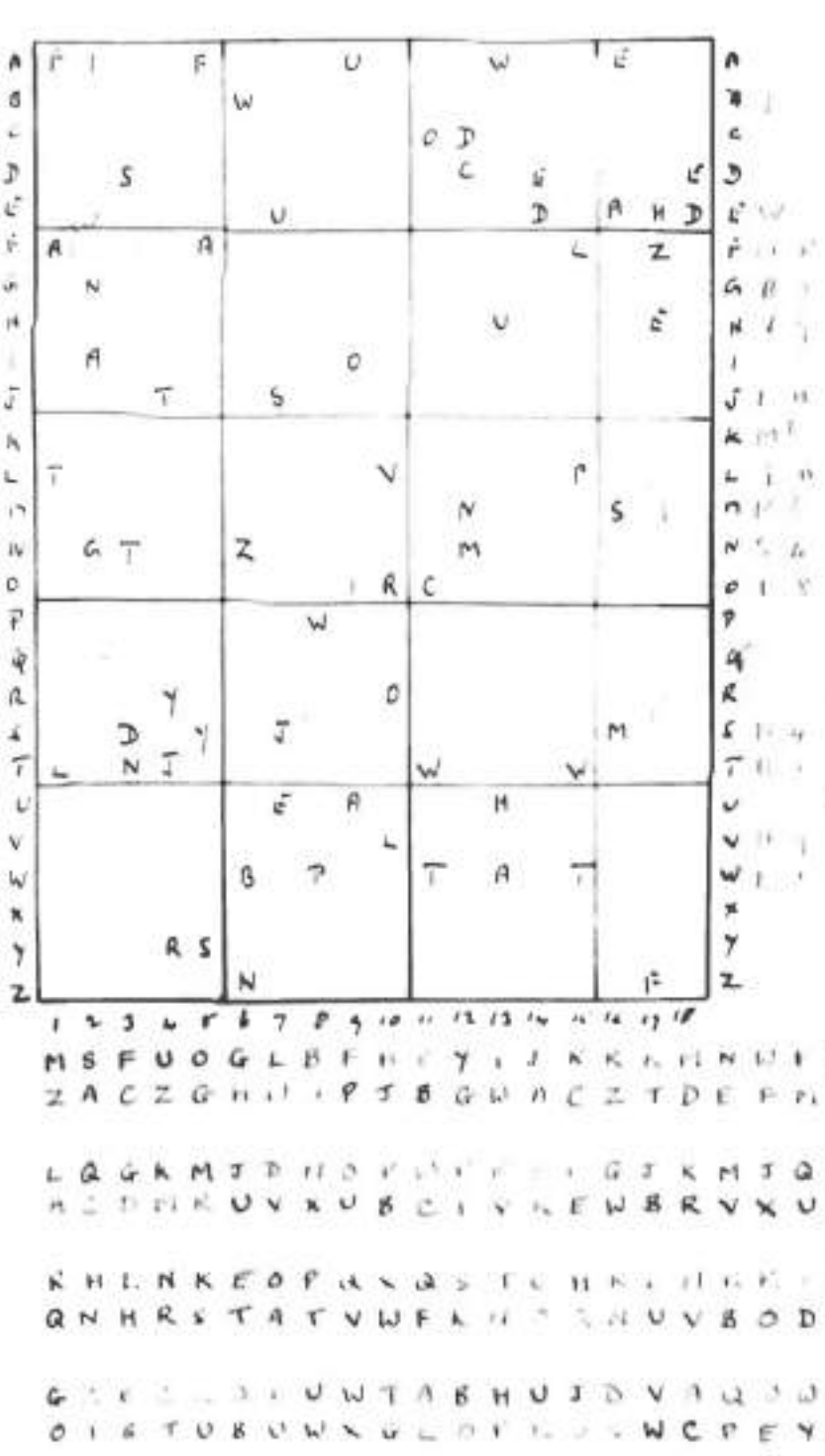


Fig 62. Investigating a correct hypothesis in a Stickers knock.-out.

DECLASSIFIED
Authority NND 363016

And the possible different 'Steckerwerte' of T and W. Any assumption as to the Steckerwerte of T and W implies two rod pairings, and when we have set these rods up we can look round and see if there are any other Stecker which are consequences of the rod pairings and the Stecker we have already. Any new Stecker we find may allow us to set up more pairs of rods. So we go on until either no new consequences can be drawn (this may be rather frequently the case), or there is a contradiction. If there is confirmation and afterwards we can draw no further consequences it may be worth while bringing in extra hypotheses.

In the actual working it seems best to set the crib out as in Fig 41, so that the occurrences of any letter can be spotted at once. We write the Stecker values of the letters in pencil on the right, possibly on a separate sheet which slips underneath. In order to avoid bogus ~~contradictions~~ finds we cover up the constatations with shirt buttons as they are used. Fig 41 shows the working for the correct hypothesis W/E,T/B. The 'covered' letters are shown ringed. In order to show how the working was done the steps have been numbered, the number being put against the constatation used and also against the Stecker values or rod pairing which resulted. The work as shown is not quite complete. It is possible to go further and get the Stecker values of all letters except D,X. There are six or more confirmations.

There are a number of other possibilities besides working from a half-bombe. It depends largely on the number of Stecker expected which will be the most profitable. When the number of Stecker is low (say 6) it is probably best to try half-bombes as unsteckered and to look for clicks which have all four letters unsteckered.

It seems unlikely that this method will ever be applied, partly because of the difficulty of obtaining the right kind of data. However ~~the~~ much the same method could be applied to find a new Umkehrwalz with data of the kind that arises with the air enigma. ~~Therefore~~ one may find the Ringstellung by Herivelismus, and also have a certain number of constations at known window positions arising from CILLI's

The whe l order may also be known fro CILLIs more or less accurately. ~~If~~ no make up rods giving, not the effect of going through the W.H.W. butthrough all three wheels, and with the columns not corresponding tothe all possible positions, but to the positions where there are known nonstatetions, and use them instead of the ordinary rods: there is no difficulty about T.O.

DECLASSIFIED
Authority NND 363016

DECLASSIFIED
Authority NND 363016

Identification of wheels

When one has found the connections of a wheel one naturally wants to verify that it is not one of the wheels used in some other known machine. A convenient way of doing this is to find the class of substitutions which transforms one column of the rod square into the next (see p [illegible]). Thus the class of the wheel found on p 26 was 13,8,4,2. ~~In the example of an Umkehrwalz~~ This 'class' is independent of what point of the ~~next~~ rod square we take to be the top left hand corner, and so is an absolute characteristic of the wheel. It even remains the same if the wheel is used in a machine with a different diagonal. In the case of an Umkehrwalz we can form the class of the substitution consisting of going through the U.K.W. and then sliding one position backwards on the diagonal. A list of characteristics for the known machines is given below

K enigma

I. 19,7

II. 14,12

III. 1[illegible],8,5,3

U.K.W. 1[illegible],9,1,1

Service machine

I. 1[illegible],6,4,[illegible]

II. 1[illegible],10

III. 7,7,6,6

IV. 11,11,2,[illegible]

V. [illegible]

VI. [illegible]4,2 two short 9,[illegible],6,3

VII. 12,5,[illegible],4

VIII. [illegible]4,2 [illegible] [illegible],4

[illegible]

B. 1[illegible],7,[illegible],1

C. 1[illegible],[illegible],2,[illegible]

Railway machine

I. 24,2 two short 1[illegible],5,2,1

II. 1[illegible],[illegible],4,[illegible]

III. 14,[illegible],3,1

U.K.W. 24,2

Commercial

I. 18,8

II. 1[illegible],7

III. 1[illegible],9,4,1

[illegible] 22,[illegible],1,1

DECLASSIFIED
Authority NND 363016

Chapter IV. Single-wheel processes. (Unstecker and Lauber)

We now suppose that we know the connections 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 words used, especially at the beginnings and ends of the messages. Suppose then that we think that a message starting FCSJWHGYLBHPVX becomes when deciphered DANZIGVON... We shall have to take several independent hypotheses as to which wheel is in the U.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 seperate hypotheses as to what rod position the message starts in. ~~When we are trying out the hypothesis that the pre-start is at rod position 26~~. We write the message out in guage with the rods, and when trying out the hypothesis that the pre-start is at 26 on the rods we block out the rods starting with F and D and lay them with D under the D of the message and crib as in fig 43. We find on the rods at position 4 Z W which implies that the Z of DANZIG should have been enciphered as 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 F we find that it also gives us V. This is now on a 'clock', and when we set up the pair giving T we get also 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 there was no T.O. In this way we get DANZIGVON.ANN H.N suggesting the decode DANZIGVONSANDHEIM... with a T.O. between the ~~second H and the E of~~ H and the E of

DECLASSIFIED
Authority NND 963016

[illegible] . Consequently before the in order to decode some of the [illegible] we should be unable [illegible] either to [illegible] the three couplings after the turnover to read a little more. This is shown in fig 4b . It is not possible to fill in the intermediate letters [illegible] to find some other method. One is to try decoding after the T.O. with various assumptions about the which wheel is in the middle position, and what rod position the T.O. 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 fact known to occur after the T.O. In fact we have the seven couplings ku,en,fq,vn,ev,td,vh is before the T.O. and the three two on, in after it ~~and possibly also bw.~~ We could test these 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 set out the rods. It is sufficient 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 one after the T.O. For example there are the bits of rod

1F
ZA
VO

and therefore if the message starts in rod position 1 for the middle wheel the coupling uv must have occurred before the T.O. In order that [illegible] 1, we can exclude this condition, colour for the middle wheel is impossible. Thus the middle wheel rods can be used in this way to exclude 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 conditions for the middle wheel is rod 11, and we have for couplings after the T.O. [illegible]uv,uv,kt,kh,ws,sm,el,or [illegible] and the rest of the message from the first to the second T.O. reads

[illegible]
[illegible]

Fig 66. Strip of Purple stress-code for FRISTRMAX
DANZIGVON

Authority NND 968016

Fig 66. Strip of Purple cross-code for [illegible]

DECLASSIFIED
Authority NND 968010

DECLASSIFIED
Authority NND 363016

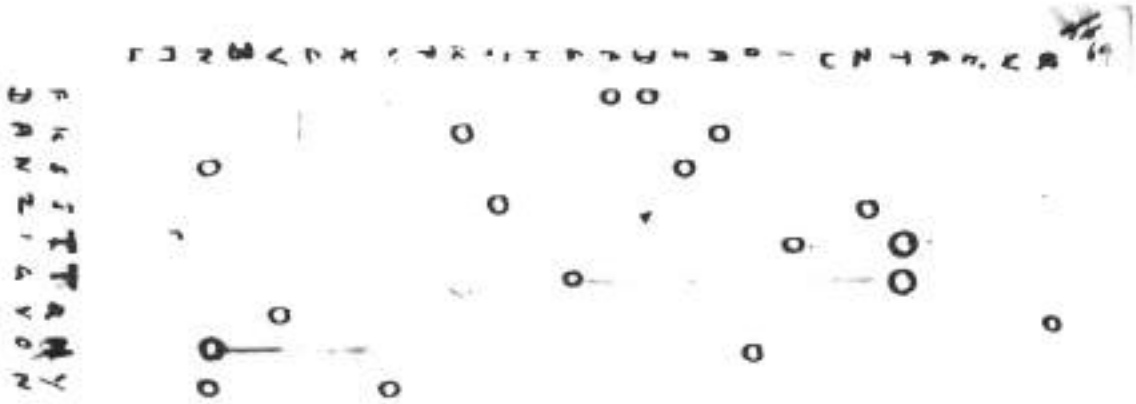


Fig 47. Perpendicular mark for Danzig with

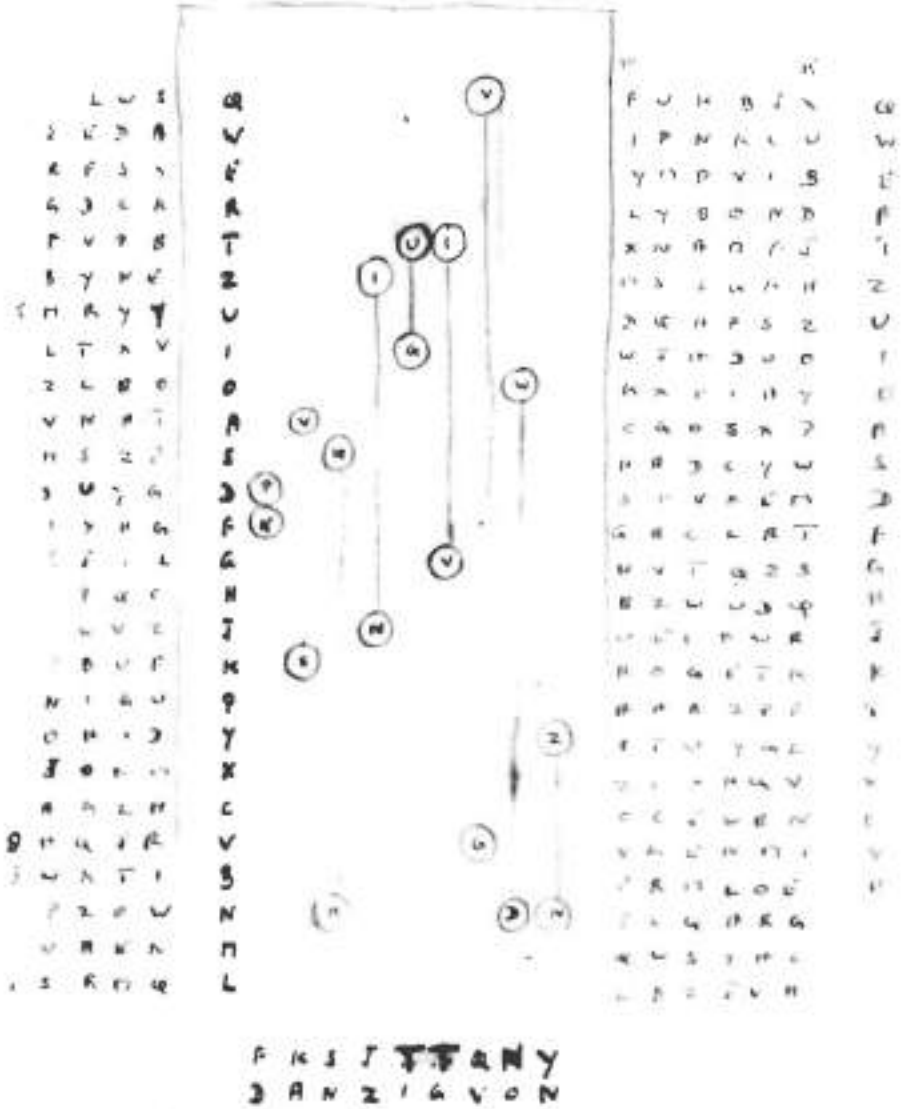


Fig 48. Mark in position - Taking pre-sheet 26

DECLASSIFIED
Authority NND 363016

[illegible] fill this in to read, for the hole message up to this point [illegible]. The other couplings [illegible], rf, jr, [illegible] can now be read off the filled-in letters, and [illegible] altogether we now have the couplings of the [illegible] rods qo, er, ab, sx, wc, jm, pw, fi, yu, zl, hn. We can decode as described in Chap 11; 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.. and U.K.. 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.

The inverse rods

Instead of picking out the [illegible] 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 constrtations, thus when testing pre-start 26

[illegible]
[illegible]
[illegible]
wjsonm[illegible]

The contradiction which is found before by setting up the pair ow n p[illegible] shows itself in the form of two contradictory couplings ok, oq. In the case of pre-start 4 we have

[illegible]
[illegible]
upt[illegible]
kedwfnkf[illegible]

and our confirmations (ellcks) [illegible] titions of the couplings uk, qf. If we actually did this we should lose time in comparison [illegible] the original [illegible], but we actually get [illegible] the difference [illegible] method.

We have the lines of the lower [illegible] (p 10) written out on rows [illegible] width, called 'lowers rods'. We

DECLASSIFIED
Authority NND 363016

Set up the ~~rats~~ inverse rods named after the letters in the crib, and lay them down in pairs, stag crib them backwards. This is best seen in Fig 46 . The various columns in this set-up show up 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 ~~ANALAR~~ 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 ~~beginning~~ end, and in rather small letters. In order to work a particular crib we take some paper in place with the inverse oblong and write the diagonal down the side of it, and ~~numbers 1,2,3,.. along the top. We also number our crib, or they~~ write the crib along the bottom. Then for each letter of the crib (either code or decode) we punch a hole ~~direct~~ 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 showing through the two holes in a column give 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.

DECLASSIFIED
Authority NND 963016

Charts.

When we want to try the same decode for ~~xxxx~~ 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

PERCOMMANDANTE charts.

This is the perfect form of chart for use when the position of the crib in the message is known. The chart ~~xxxx

DECLASSIFIED
Authority NND 963016

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

	A	B	C . .	W . . .
x^1x^1				B 19
x^2x^2				
x^3x^3				

all entries apart from the one corresponding to the click shown in Fig 44 having been omitted. The letters 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 guage 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 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 seperate 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 44 would be represented on sheet I in line W by the entry B 19^{B} in green. The chart is usually used one sheet at a time;

DECLASSIFIED
Authority NND 963016

the message is written out with plenty of room for entries below it. Whilst using sheet 1 xxxlook for each letter of the message we 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 xxxxxxxxxxxxxxxxxxxx enter the rod start on the message under the letter which corresponds tothe first xxxxxxxx letter of the crib. We know where this is because the entry on the chart gives the crib position. When we get xxx the same number twice in a column we try out the corresponding rod position and position in the message.

A possible improvement of the key out which might combine the advantages of the PERCOMANDANTE and BRUESSEL type charts would be to take a fairly wide columnfor each click distance, all the columns being th e same width, xxxxxxxxxx instead of having seperate 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. xxxxxxxxxxxxxxxxxxx

DECLASSIFIED
Authority NND 363016

Making of charts

Although there is so much room for variation in the form which a chart can take the manner in which they are made is fairly stereotyped. Th ere 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 th e 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.

Wh en catalogueing cross clicks we make 26 pictures like Fig 45 , by writing the crib diagonally and filling up a square with rods, and finally copying the left lower half intothe right upper h alf symmetrically across the diagonal. The different pictures

~~A I W A Q K N P P N~~
~~K Q T B~~

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 n umber in the 'index' position. The click distance (i.e. the shee t, with BRUESSEL type) is determined by how far th e 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 butthe columns. Some of the

~~inventaingthxxdirectxclicks~~

squares do not correspond to possible entries, as they could only arise from rods paired with th emselves. These ~~xxx~~ squares h ve been crossed out in Fig 5D .

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

X [illegible] [illegible] [illegible] K [illegible] [illegible] K L X A crib

D G G K W C U E L A B rod

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

DECLASSIFIED
Authority NND 363016

all with the same click distance, rod start and crib positions. In cataloguing these either in a PERCOMMANDANTE or a 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 26 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.

~~Two The correct form of chart for X-chart for X-chart and ordinary chart.~~ 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

DECLASSIFIED
Authority NND 363016

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 from the rod position 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 57 . This will measure 26 x 26 and only one of them will be needed. It will simply consist of a rod-square rearranged with the X's down the diagonal. When making the entries for a particular value of rod position of the first constitution 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.

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

DECLASSIFIED
Authority NND 963016

DECLASSIFIED
Authority NND 363016

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 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 on 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 toth e left. In our DANZIGVON example we could have used the backward consecutives as soon as we had found the couplings ku,ep,fx,qn,sy,td,vh,lw before the T.O. and sw,os.le after it. We should have laid rulers against the lines o,s of the backward consecutive square, and read off the consequences before the T.O. of having on 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 os. 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.

DECLASSIFIED
Authority NND 363016

III Green

16.

R Z Q O X F M C P W H B I E Q N T L G A U W Q D J S
C J R L B P F W Z Q X V V M A K H S I P T Q N Y K G

U U A C G L V Y E J D O R W M Z Q H B I E N F K D T
G O W R R U P S B Y J L F O Z Q M V E N D I T L C A

I S V H Q B X R K F A T E L U W J D O R M Q P F Z I
W M O V P H A I T D U C K G O R Y B P S F F J Q X Z

D B J W N C T P G S Z R Q I E K F A T L H Y G U O O
H D Y G W N C J G L R M P X X B I Q F O Z J E M V K

N K E M V Z Y H D U T W O R P G S Z Q J X H I A A F
T Q N I C K G O U R B Z X J F I E P V K A D D H L Y

P R L B U X J F I Z E A T Y H D U W K C J O S S G M
J G S P F Q B X H A M E N K Y Y V U L D I T H W N C

L A B Y J S O Z F I P Q H A T X N Y D G G K W C U E
B P U S Z M Q Q R H I X J F B A Z E N V Y L C O T W

S N X K D A U G O B Y J B Z C M X F H H P E V I R Q
F X H E M V K D Q T L Y C C N O W G A U K R L B P J

M C P F S I H A N X K D U V L C G J J Y R B O T W D
Q V K Z A T N L L E G U Y H D V O T W B C P M X I R

V Y G D O J S M C P F I B Q V H K K X T N A Z E F L
A E T T I Y D N X K Q G A U W L B R M J O Z Q Y S H

X H F A K D L V Y G O N W B J P P C Z M S U R G Q B
E L C J T O R B M M W F Z P G S C I R Q V X K N Y U

K T Q N Y G E U W C B L S R J D O Y Z W M X P H V
O F I Q E E Z K A V P H M D I T L N C W B S U R M X

Z W M X H R I E V N N Q D T K F A X U E L C Y B P
Y I D U L W W T J O C K G N S U R M B X Q V A Z E K

Railway Carriage Wheel III.

Page 5 in Output of U.K.W. & L.H.W. for
construction of Wheel catalogue.

DECLASSIFIED
Authority NND 363016

Chapter V. Coupling catalogues

When we have found the rod position of the L.H.W. and a few couplings for a mes sage it is possibleto find the postions of th other wheels from a suitable catalogue.

Short catalogue

One method is to try independently all the possible positions for the middle wheel. We shall want to know the middle wheel couplings which are consequences of these various assumptions. This can be done by setting up inverse rods for the middle wheel. The rods are paired off according to the M.H.W. couplings, i.e. M.W. output, ~~xxxxxxxxxxxx~~.This has been done for the the couplings ku,fx,ep which arose in the DANZIGVON crib in Fig 5B, assuming the red wheel in the middle. The pairs in each column of this set up give possible M.W. couplings. We have ~~xxix~~ now to find out whether these couplings are possible. Our procedure is rather different according as the U.K.W. does or does not rotate. In the case that the U.K.W. does not rotate it will be sufficient to have a (the rows and columns lettered preferably with the diagonal alphabet) Foss sheet ~~xxxx~~ in which, in the RW square ~~xxxx~~ are entered the position s of the left hand wheel at which the ~~xxxxxxxx~~ RW is one of the pairs in the L.H.W. output alphabet. This is known as the 'short catalogue' for this wheel. To use it in connection with the DANZIGVON crib we should take each column of Fig 5B in turn and look up the pairs in it on the short catalogue and see if all the squares had a number in common. If we found such a case the number in the square would give the L.H.W. rod position, and the column of ~~xxx~~ Fig 5B would give the M.W. position. Actually the U.K.W. rotates for our example so that we should have no success.

In the case that the U.K.W. rotates, we need essentially the same short catalogue, but we arrange it slightly differently. In stead of the lines of the catalogue corresponding to fixed output letters they correspond to fixed distances on the diagonal, between the output letters. This can be seen from Figs 6B,6C which illustrate such a catalogue. The pairings are written above the ~~xxxxxxxxxxxxxxxxxxxxxxxx~~ ~~they occur~~ figures giving the positions ~~in~~

DECLASSIFIED
Authority NND 963016

of the L.H.W. in which these pairings occur, the U.K.W. understood to be in the zero position . Either form of short catalogue may be made by setting up the L.H.W. rods paired according to the U.K.W. as in Fig 5W, and analysing the resulting pairs.

To understand the use of the short catalogue when the U.K.W. rotates we must remember that if the U.K.W. and L.H.W. are rotated in step the effect is a slide along the diagonal of the resulting pairs. If we are given actual pairs for which the U.K.W. was not in the zero position we can slide the pairs along the diagonal until we have pairs which would have occurred with the U.K.W. in the zero position. This will show up on the catalogue because there will be a number in common in the squares under these pairs. For instance in the case ofthe DANZIGVON crib we found the middle wheel to be red in position 11. This gives the middle wheel couplings pn,ve,hm,uy as consequences of the R.H.W. couplings qn,uk,fx,ep . These can be read off from Fig 5G, although of course we should only set up the M.W. inverse rods in a case where we did not know the M.W. position. If we slide pr,hn,ev,uy ten places forward along the diagonalwe get wg,mi,zf,ke, and in each of the squares wg, mi,zf, ke on the green (L.H.W.) short catalogue we find the number 4, i.e. these pairs occur at U.K.W. 0 L.H.W. 4: consequently qn,... occur at U.K.W. 10,L.H.W.14. The mechanical process would actually be to take pr on the small sheet of the catalogue and lay it against ve on the large sheet. This automatically results in wg and mi being together and all other pairs of pairs resulting from sliding pr,ev along the diagonal. We look in the pairs of squaresto see if there are numbers in common. When we find such a case we have to look in a third square resulting from sliding hm. It is as well therefore to have rulers in gauge with the catalogue to measure off the distances. Having found the right amount of slide forward on the diagonal, i.e. to the right in the catalogue we calculate the positions of the wheels from the formulae

DECLASSIFIED
Authority NND 363016

7

...OAZWGSYHDCPENKTITLBFRKUJEQOM G
...AZKXKDOMJEYWHFLVTGLBTQNURHAZ F

...LVZUEMSIJDOPHLCKWTWBXAQGRFL N
...ZSALOVXVEMCURDITGSVKPNQWYIZB

...CJPEXUBZYKMLVPRQOTWSIYGAMCNCJ
...MCPQNORLSGSZFYHBFLOUHJZIXKMC

...QJPCKGBXTLVUAUWMHZYOPTESDIQ
...KGRCINUXPLQBYTWAZEDOXHSVMLKG

Page 66. Setting of cipher rules for M.W. [illegible] 57 into "[illegible]" column 6 "

DECLASSIFIED
Authority NND 363016

U.K.W. position = slide forward on diagonal

L.H.W. position = number in square + slide

The Turing sheets

The short catalogue should work very well when the Umkehrwalz rotates, and there is no information connecting the position of the U.K.W. with the positions of the other wheels. In the case of a fixed U.K.W. we can often make use of an analysis of M.H.W. couplings.

The lay out of the catalogues is largely determined by the special method by which they are made, but it seems to be reasonably convenient in use. The catalogue is divided into sheets numbered 1 to 13. Each of these sheets consists of a 26x26 square with margin at top and left hand side, preferably on 1/3" gauge. ~~The numbers on the sheets give the distance along the diagonal between the two letters for the margin on the left hand side of each sheet; example 12, will be found on a pair of letters in each line. The entries are numbered 1 to 26.~~ One such sheet is shown in Fig 56 partly constructed. The letters and numbers in ink are the only ones concerned when the sheets are being used, the others being part of the construction, and left on to help in tracing errors. The entries 10,18,21 in the square in column 15 and the row with KV in the margin mean that the coupling KV occurs when the M.W. is in position 15 and L.H.W. in any of the positions 10,18,21. In order to find the positions at which two couplings can occur we have only to find the corresponding lines of the catalogue against one another and compare the numbers in the adjacent squares. It is fairly easy to find the right sheet because the number of the sheet gives the distance along the diagonal of the two letters of the pair, e.g. K and V are at distance 5 along the diagonal (KIYXCV) and KV occurs on sheet 5.

DECLASSIFIED
Authority NND 36 5016

Construction of the Turing sheets

The construction of the catalogue depends on making almost simultaneously all the entries corresponding to cases in which the current flows through the same two wires of the M.W. In the partially constructed sheet 5 in Fig 5b some of the diagonals have been filled in fully, and each of these corresponds to a pair of wires of the M.W. As the M.W. rotates the rod points at the right hand ends of the wires move steadily backwards along 'the diagonal'. We see also that as we move along the filled in diagonal the rod position steadily increases, and the letters in the pairings move slide backwards along 'the diagonal'. Meanwhile the left hand ends of the wires are steadily rotating, so that the middle wheel couplings are sliding along 'the diagonal'. The entries in the squares are the positions of the L.H.W. where these M.W. couplings can occur, and the slide along the diagonal amounts to a diagonal movement along the short catalogue. Take for instance the fff filled in diagonal on Fig 5b nearest to the central diagonal. The second entry on this diagonal is 2,5,16,26 which is the entry at HL in Fig 5l : next along the diagonal in Fig 5b is the entry 10 which occurs at GM in Fig 5l , and so on , the diagonal in Fig 5l being repeated backwards in Fig 5b .

This phenomenon may also be explained with reference to the rod square, instead of the wheels: this is really more practical, as we have to make the catalogue up from the rod square. A possible method for making up the catalogue would have been this. In each square on the sheets we write in, in pencil, the M.W. couplings which would be needed to produce the part of the beginning of the line M.W. ouput at the beginning of the M.W. position given by the column in which the square occurs. To do this we should have to write down in each line the inverse rods named after the letters at the beginning of the line. This has been done in part of Fig 5b (top .H corner). We should then have the square filled with one inverse (. .) square, with top and bottom reversed, and another such reversed square somewhat displaced upwards. The entries in the link could be obtained by

DECLASSIFIED
Authority NND 363016

repalacing each pair of pencil letters by the corresponding entry on Fig 51, i.e. by the position of the L.H.W. at which that pair of letters occurs as L.H.W. output. Now the whole of the pencil square can be obtained from its top line simply by filling in along diagonals. Translated into terms of the green ink entries this means to say that we only need to be given the positions at which we start copying from the short catalogue.

Actually we copy out the diagonals of the short catalogue onto staircase shaped strips (known as 'Christmas decorations' or 'hand frills') in reversed order, with the position in the short catalogue written above each square. These hand frills are numbered by the (constant) distance apart on the diagonal of the pairs of letters on them; e.g. in the hand frill shown in position for copying in Fig 56 I and F are at distance 5 on qwertzu and so are D and K. Instead of actually filling in the whole square with pairs of pencil letters we take the entries which might have been made in the top line, and write them in the top margin, and also put the entries which might have gone in the left hand column into the left hand margin. In order to find what hand frill to use for a particular diagonal the distances apart along qwertzu of the letters along the top are calculated. This should be done quite independently, to give a check on incorrectly copied letters (see 'Mystic numbers').

The reason for having the imaginary pod squares implied in the construction inverted is in order that the writing of diagonals may be from left to right and downwards, which is considered easier than from right to left and downwards.

DECLASSIFIED
Authority NND 36 5016

Solving a short crib

The chief application of the Turing sheets is to the solution of cribs from a length of 2 to 6 letters, when the U.K.W. does not rotate. We set up the inverse rods as usual, but find that by no means all the incorrect positions are eliminated by coupling contradictions. We therefore look to see whether there is any position in which the couplings can occur. Take for example the crib ANK, with and wheel order I III II (red, green, purple), U.K.W. pos. O cipher ARC. We set up the inverse rods as in Fig 57, and for each column of the resulting set up compare the lines of the catalogue named after the pairs in the column. For each pair we shall want to find quickly the right sheet on which to look, and this means subtracting the pairs on the diagonal (i.e. finding their distance apart on qwertzu). To do this we can either have a table of differences or else use 'mystic number rods'

'Mystic numbers'

Fig 58 shows a table of 'mystic numbers' for the red wheel. The meaning of the table is this. Take the 8th line for example. It could be made by taking inverse rod Q and inverse rod O, O being eight places on along qwertzu from Q. We lay the two rods together and find the differences of the resulting pairs: e.g. the fifth entry in line 8 is 6, and the fifth letter of the red inverse rod Q is Y, the fifth letter of inverse rod O is F, and Y and F are 6 apart on qwertzu(FGHJKLY). If then we had a set up of inverse rods including the pair QO we could use the series of numbers of line 8 of the mystic numbers to tell us on which sheets the various pairs should be looked up. However we can also use line 8 of this table on many other occasions. Suppose for example that the pair ES of inverse rods is up. The series of sheets on which we have to look is again given by line 8, but we have to start in the third column under E instead of at the beginning under Q. Quite a convenient arrangement is to have the lines of the table written out on rods in groups with the inverse rods and of double length. (This was once done for the service machine wheel III. Three lines of the table were put onto three sides of Mr Knox's blank wooden inverse rods, and the fourth side occupied with the letters of the diagonal, in that case ABCD... It was

DECLASSIFIED
Authority NND 363016

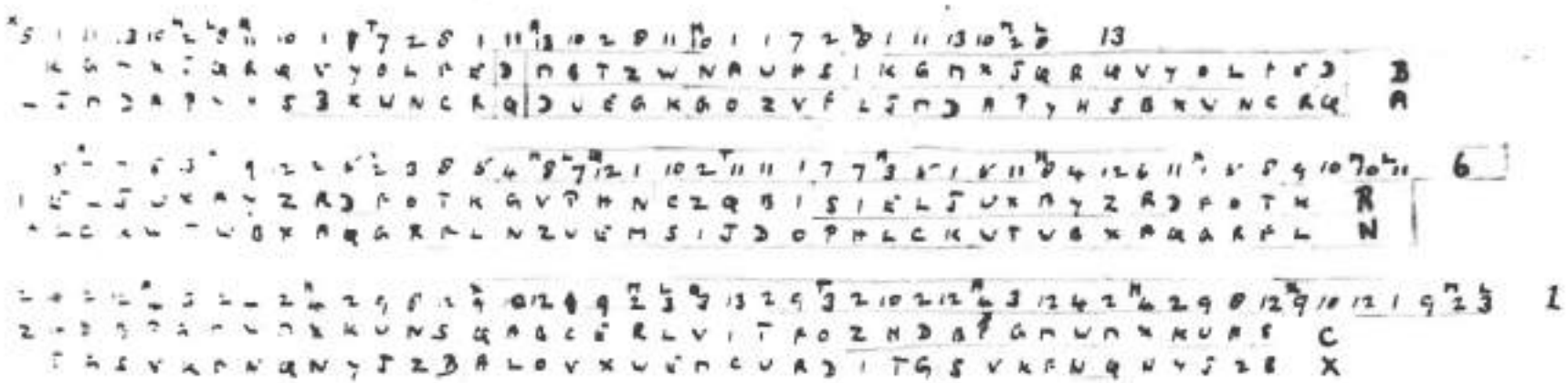


Fig 57. Set of 8 cross-rods for BRC ANX, and regular no. rods for finishing repeat check.

DECLASSIFIED
Authority NND 363016

	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
1	3	13	2	9	3	2	10	2	12	4	3	12	4	2	4	2	9	8	12	9	10	12	1	9	2	3
2	10	11	7	6	5	8	8	1	8	7	9	10	2	6	6	11	9	6	5	1	2	13	8	11	1	6
3	8	6	4	4	8	6	6	6	5	5	13	12	2	8	11	7	5	3	11	11	3	4	10	8	4	7
4	9	9	2	12	3	8	10	3	9	9	11	10	4	9	3	5	12	7	3	12	6	2	7	5	9	5
5	12	11	12	12	11	12	13	11	5	7	7	8	13	1	9	12	2	5	2	3	8	8	4	8	7	12
6	12	1	10	2	11	11	1	7	7	3	5	1	5	11	8	4	12	6	11	1	5	8	9	10	10	11
7	4	3	4	6	8	3	3	9	11	1	4	9	7	6	8	10	11	3	13	4	2	5	11	1	13	9
8	6	9	8	9	6	1	1	13	13	8	12	5	10	10	6	9	6	5	10	7	11	3	2	4	11	7
9	6	5	11	3	2	1	3	11	4	10	2	4	6	4	5	8	4	2	7	6	13	12	5	6	5	9
10	2	2	1	7	4	5	5	2	4	2	7	6	8	3	12	6	7	1	6	4	4	9	7	4	7	3
11	1	12	5	5	8	7	12	6	10	11	3	6	7	12	10	9	10	12	8	13	7	7	3	2	5	1
12	11	8	3	1	10	10	4	8	1	1	9	7	10	12	13	12	3	10	1	10	9	9	1	12	1	3
13	11	10	1	1	7	2	8	1	11	13	10	2	8	11	10	1	1	7	2	8	1	11	13	10	2	8

I

Red.

Fig 5-8. Nyabi numbers for Railway Wheel I

DECLASSIFIED
Authority NND 363016

Jeffreys sheets

In cases where the wheel order is unknown it is useful to have the positions and wheel orders where a coupling occurs all catalogued together. In order to make comparison of couplings feasible one puts the catalogue into the form of punched sheets, which can be laid one on top of another. These are known as Jeffreys sheets.

The actual form of the Jeffreys sheets catalogue is this. There are 325 sheets labelled AB,AC,...AZ,BC,...,BZ,...,...,...,YZ. Each sheet measures 26"x20$^4/_5$" plus margins of about three inches. They are divided into columns an inch wide, and lines $^4/_5$" deep. The whole is further subdivided into squares $^1/_5$" x $^1/_5$". The $^4/_5$" x 1" rectangles correspond to the different possible rod positions of the L.H. and M.W. The subdivisions of the rectangles correspond to the twenty possible wheel orders for L.H.W. and M.W. with the five first wheels of the service machine.

Jeffreys-Turing sheets

There is a possibility of speeding up the work with short cribs where the U.K.W. rotates by making the Turing sheets in punched form. Suppose we expand every square of the Turing sheets into a rectangle 7/5"x4/5" divided into 28 small squares, numbered 1 to 26 with two unused, and for each entry on the Turing sheet punch a hole in the corresponding small square. Then the effect of laying two of the sheets on top of one another, in such a way say that the lines VM and CR coincided would be to give us the positions in which the two couplings VM and CR occur when the U.K.W. is in the zero position; we also get the positions in which the couplings slid along qwertzu occur: but these after making a correction for the amount of slide are just the positions at which VM and CR occur including all possible rotations of the U.K.W. One would presumably normally place three sheets on top of one another, and there would have to be four different layings(because one could not have the sheets in cylindrical form). For this reason it would be better to have the sheets in double depth,but this would probably be out of the question.

[illegible] found a useful compromise by having two copies of the Turing sheets; one of which [illegible] by photography. [illegible] D.T.

DECLASSIFIED
Authority NND 963016

not a success as the rods were incorrectly copied). For the crib

BRC
ANX th ese mystic number rods are shown in position over the inverse rods in Fig 67. Every fifth letter from the top of the mystic number table is also shown.

Another use for the mystic number table is in the making of the Turing sheets. The line of pencil numbers along the top of any sheet is the lin e of mystic numbers with th e sheet number as its line number, and starting at column L. Gap. Page 68, 69

The mystic numbers can of course be made by actual subtraction from the inverse rods. However it is actually easier to do the calculation in terms of the letters of an upright. It turns out that one can manage with one upright, which one subtracts from itself, staggered various amounts. One can transfo m the letters into numbers to simplify the subtraction. I shall not give the details of this.

KDNS cat logues

In this chapter and the last we have not exhausted all the possible methods of dealing with the Unsteckered enigma, and enigma with known Stecker. When the Umkehrwalz does not rotate we can catalogue the result of encoding a short word such as KDNS at every pos ible position. The details of this are explained in Chapter

DECLASSIFIED
Authority NND 963016

Chapter VI. The steckered enigma, Bombe and Spider.

When one has a steckered enigma to deal with one's problems naturally divide themselves into what is to be done to find the Stecker, and what is to be done afterwards. Unless the indicating system is very well designed there will be no problem at all when the Stecker have been found, and even with a good indicating system we shall be able to apply ~~straightforward~~ the methods of the last two chapters to the individual messages. The obvious example of a good indicating system is the German Naval enigma cipher, which is dealt with in Chapter VII. This chapter is devoted to methods of finding the Stecker. Naturally enough we never find the Stecker without at the same time finding much other information.

Cribs.

The most obvious kind of data for finding the keys is a 'crib', i.e. a message of which a part of the decode is known. We shall mostly assume that our data is a crib, although actually it may be a number of constatations arising form anoth er source, e.g. an number of CILLIs or a Naval Banberismus.

FORTYWEEPYYWEEPY methods.

It is sometimes possible to find the keys by pencil and paper methods when the number of Stecker is not very great, e.g. 5 to 6. One would have to hope that several of the constatations of the crib were 'unsteckered'. The best chance would be if the same pair of letters occurred twice in the crib (a 'half-bombe'). In this case, assuming 6 or 7 Stecker there would be a 25% chance of both constatations being unsteckered. The positions at which these constations occurred could be found by means of the Turing sheets(if th ere were three wheels) or the Jeffreys sheets. The positions at which this occurred could be separately tested. Anoth er possibility is to set up th e inverse rods for the crib and to look for clicks. There is quite a good chance of any apparent click being a real click arising from because all four letters involved are unsteckered. The position on the right hand

wheel is given by the column of the inverse rod set-up, and we can find all possible positions where the click coupling occurs from the Turing sheets or the Jeffreys sheets. In some cases there will be other constatations which are made up from letters supposed to be unsteckered because they occur in the click, and these will further reduce the number of places to be tested.

These methods have both of them given successful results, but they are not practicable for cases where there are many Stecker, or even where there are few Stecker and many wheelorders.

DECLASSIFIED
Authority NND 363016

A mechanical method. The Bombs.

Now let us turn to the case where there is a large number of Stecker so many that any attempt to make use of the ~~xxxxxxxx~~ unsteckered letters is not likely to succeed. To fix our ideas let us take a particular crib.

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

24	25
I	V
Q	T

Presumably the method of solution will depend on taking hypotheses about parts of the keys and drawing what conclusions one can, hoping to get either a confirmation or a contradiction. The parts of the keys involved are the ~~xxxxxxxxxxxxxxxx~~ wheel order, the rod start of the crib, whether there are any turnovers in the crib and if so where, and the Stecker. As regards the wheel order one is almost bound to consider all of these separately. If the crib were of very great length one might make no assumption about what wheels were in the L.H.W. position and M.W. position, and apply the method we have called a 'Stecker knockout' (an attempt of this kind was made with the 'Feindseligkeiten' crib in Nov. '39), ~~xxxxx~~ or one might sometimes make assumptions about the L.H.W. and M.W. but none, until a late stage about the R.H.W. In this case we have to work entirely with constatations where the R.H.W. has the same position. This method was used for the crib from the ~~xxxxx~~ Schluesselgettel of the Vorpostenboot, with success; however I shall assume that all

DECLASSIFIED
Authority NND 363016

wheel orders are being treated separately. As regards the turnover one will normally take several different hypotheses, e.g.

1) turnover between positions 1 and 5
2) " " " 5 and 10
3) " " " 10 and 15
4) " " " 15 and 20
5) " " " 20 and 25

With the first of these hypotheses one would have to leave out the constatations in positions 2 to 4 out, and similarly in all the other hypotheses four constatations would hve to be omitted. One could of course manage without leaving out any constatations at all if one took 25 different hypotheses, and there will always be a problem as to what constatations can best be dispended with. In what follows I shall assume we are working the T.O. hypotheses numbered 5) above. We have not yet made sufficiently many hypotheses to be able to draw any immediate conclusions, and must therefore either assume something about the Stecker or about the rod start. If we were to assume something about the Stecker our best chance would be to assumethe Stecker values of A and E, or of E and I, as we should then have the two constatations corrected for Stecker, with only two Stecker assumptions. With Turing sheets one could find all possible places where these constations occurred, of which we should, on the average, find about 28.1. As there would be 686 hypotheses of this kind to be worked we should gain very little in comparison with separate examination of all rod starts. If there had not been any half-bombes in the crib we should have fared even worse. We therefore work all possible hypotheses as to the rod start, and to simplify this we try to find characteristics of the crib which are independent of the Stecker. Such characteristics can be seen most easily if the crib is put in to the form of a picture

DECLASSIFIED
Authority NND 363016

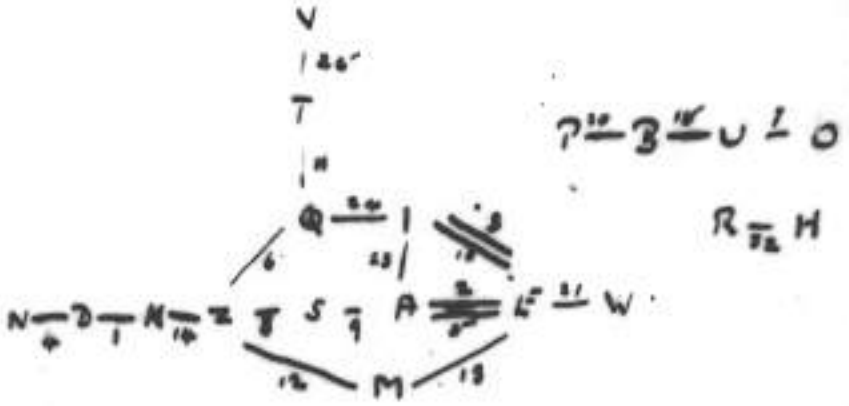


Fig 59. Picture from KOTHE ZUSAETZE

Note. Calculation is only omitted to allow for turnover.

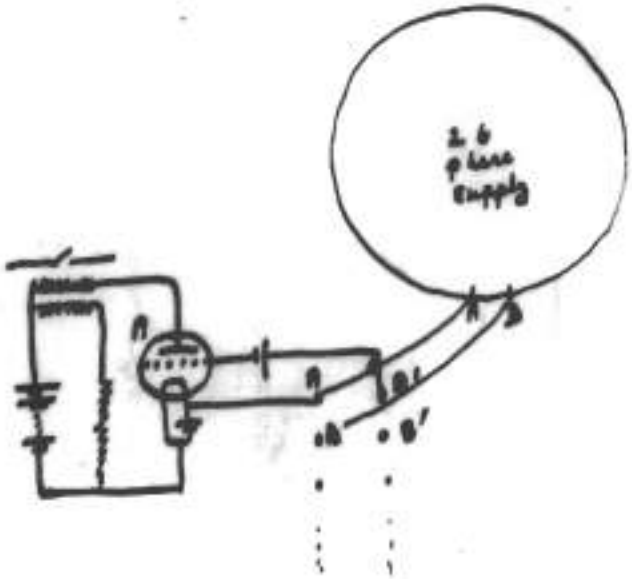
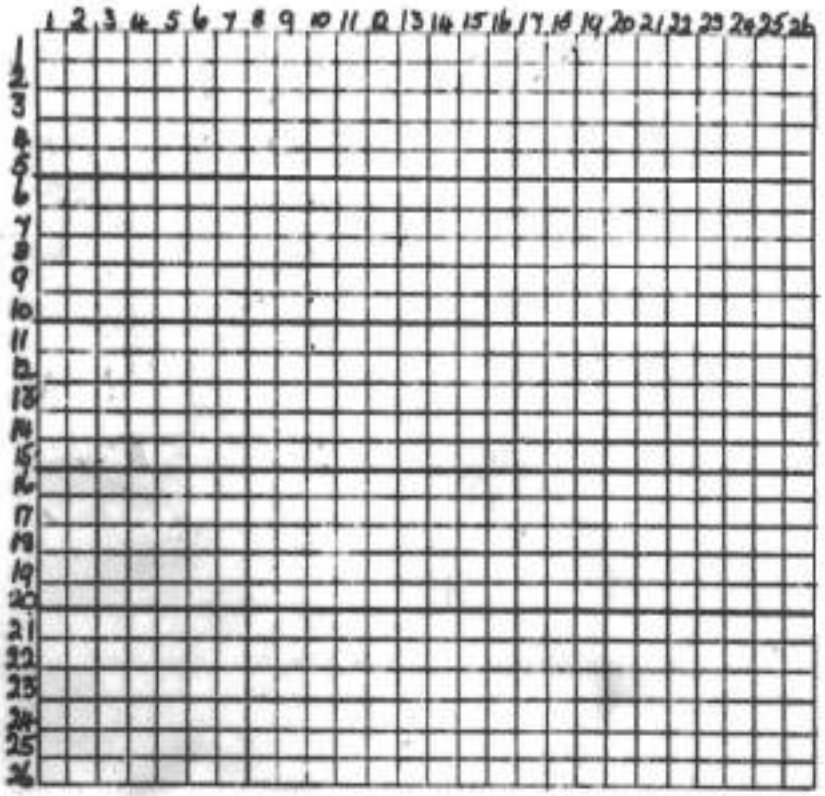


Fig 60. Circuit for Pye simultaneous scanning.



DECLASSIFIED
Authority NND 963016

001

DECLASSIFIED
Authority NND 363016

like Fig 57. From this picture we see that one characteristic which is independent of the Steecker is that there must be a letter which enciphered at either position 2 or position 5 of the crib gives the same result. This may also be expressed by saying that there must be a letter ~~xxxxx~~ such that, if it is enciphered at position 2, and the result reenciphered at position 5 the final result will be the original letter. Another such condition is that ~~xxxxxxxxxxxxxxx~~ the same letter ~~xxx~~ enciphered successively at the positions 3,10 must lead back to the original letter. ~~Two~~ Three other conditions of this kind are that the successive encipherments at positions 2,23,3 or at 2,9,8,6,24,3 or at 13,12,8,9,5 starting from the same letter as before must lead back to it. There are other such series. e.g. 13,12,6,24,3 but these do not give conditions independent of the others. ~~xxxxxxxxxxxxxx

DECLASSIFIED
Authority NND 363016

this condition will be quite sufficient to reduce the number of possible positions to a number which can be tested by hand methods. It is actually possible to make use of some of the other conditions mechanically also; this will be explained later.

In order to apply the multiple encipherment condition one naturally wants to be able to perform the multiple encipherments in one operation. To do this we make a new kind of machine which we call a 'Letchworth enigma'. There are two rows of contacts in a Letchworth enigma each labelled A to Z and called the input and output rows: there are also moveable wheels. For each position of an ordinary enigma there is a corresponding position of the Letchworth enigma, and if the result of enciphering F at this position is R, then F on the input row of the Letchworth enigma is connected to R on the output row, and of course R on the input row to F on the output row. Such a 'Letchworth enigma' can be made like an ordinary enigma, but with all the wiring of the moveable wheels in duplicate, one set of wires being used for the journey towards the Umkehrwalz, and the others for the return journey. The Umkehrwalz has two sets of contacts, one in contact with the inward-journey wiring of the L.H.W. and one in contact with the outward-journey wiring. The Umkehrwalz wiring is from the one set of contacts across to the other. In the actual design used there were some other differences; the wheels did not actually come into contact with one another, but each came into contact with a 'commutator' bearing 104 fixed contacts. These contacts would be connected by fixed wiring to contacts of other commutators. These contacts of the commutators can be regarded as physical counterparts of the 'rod points' and 'output points' for the wheels.

DECLASSIFIED
Authority NND 363016

If one has two of these 'Letchworth enigmas' one can connect the output points of the one to the input points of the other and then the connections through the two enigmas between the two sets of contacts left over will give the effect of successive encipherments at the positions occupied by the two enigmas. Naturally this can be extended to the case of longer series of enigmas, the output of each being connected to the input of the next.

Now let us return to our crib and see how we could use these Letchworth enigmas. For each of our 'chains' we could set up a series of enigmas. We should in fact use 18 enigmas which we will name as follows

A1,A2	with the respective positions	2,5
B1,B2		3,10
C1,C2,C3		2,23,3
D1,D2,D3,D4,D5,D6		2,9,5,6,24,3
E1,E2,E3,E4,E5,		13,12,8,9,5

By 'position 8' we here mean 'the position at which the constatation numbered 8 in the crib, is, under the hypothesis we are testing, supposed to be enciphered'. The enigmas are connected up in this way: output of A1 to input of A2: output of B1 to input of B2: output of C1 to input of C2, output of C2 to input of C3: etc. This gives us five 'chains of enigmas' which we may call A,B,C,D,E, and there must be some letter, which enciphered with each chain gives itself. We could easily arrange to have all five chains controlled by one keyboard, and to have five lampboards shewing the results of the five multiple encipherments of the letter on the depressed key. After one hypothesis as to the rod start had been tested one would go on to the next, and this would usually involve simply moving the R.H. of each enigma forward one place. When 26 positions of the R.H. have been tested the M.H. must in turn make a move forward too. This movement of the wheels in an enigma can be very easily done mechanically, the right hand wheels all being driven continuously from one shaft, and the motion of the other wheels being controlled by a carry mechanism.

It now only remains to find a mechanical method of registering whether the multiple encipherment condition is fulfilled. This can be done most simply if we are willing to test each Steckar value of the central letter throughout all rod starts before trying the next Steckar value. ~~In this case we have an electric current always entering with a value other~~ Suppose we are investigating the case where the Steckar value of the central letter is K. We let a current enter all of the chains of enigmas at their K input points, and at the K output points of the chains we put relays. The 'on' points of the five relays are put in series with a battery (say), and ~~a current with~~ to another relay. A current flows through this last relay if and only if a current flows through all the other five relays, i.e. if the five multiple encipherments applied to K all give K. When this happens the effect is, essentially, to stop the machine, and such an occurrence is known at Letchworth as a 'straight'. An alternative possibility is to have a quickly rotating 'scanner' which, during a revolution, would first connect the input points A of the chains to the current supply, and the output points A to the relays, and then would connect the input and output points B to the supply and relays. In a revolution of this scanner the output and input points A to Z would all have their turn, and the right hand wheels would then move on. This last possible solution was called 'serial scanning' and led to all the possible forms of registration being known as different kinds of 'scanning'. The simple possibility that we first mentioned was called 'single line scanning'. Naturally there was much research into possible alternatives to these two kinds of scanning, which would not enable all 26 possible Steckar values of the central letter to be tested simultaneously without any parts of the machine moving. Any device to do this was described as 'simultaneous scanning'.

DECLASSIFIED
Authority NND 363016

DECLASSIFIED
Authority NND 363016

The solution which was eventually found for this problem was more along mathematical than along electrical engineering lines, and would really not have been a solution of the problem as it was put to the electricians, to whom we gave, as we thought, just the essentials of the problem. It turned out in the end that we had given them rather less than the essentials, and they therefore cannot be blamed for not having found the best solution. They did find a solution of the problem as it was put to them, which would probably have worked if they had had a few more months experimenting. As it was the mathematical solution was found before they had finished.

Pye simultaneous scanning

The problem as given to the electricians was this. There are 52 contacts labelled A,...Z, A',...,Z'. At any moment each one of A,...,Z is connected to one and only one of A',...,Z': the connections are changing all the time very quickly. For each letter of the alphabet there is a relay, and we want to arrange that the relay for the letter R will only close if contact R is connected to contact R'.

The solution

The latest solution proposed for this problem depended on having current at 26 equidistant phases corresponding to the 26 different letters. There is also a thyratron valve* for each letter. The filaments of the thyratrons are given potentials corresponding to their letters, and the grids are connected to the corresponding points A',...,Z'. The points A,...,Z are also

---

*A thyratron valve has the property that no current flows in the anode circuit until the grid potential becomes more negative than a certain critical amount, after which the current continues to flow, regardless of the grid potential, until the anode potential is switched off.

DECLASSIFIED
Authority NND 363016

given potentials with the phase of the letter concerned. The result is that the difference of potential of the filament and of thyratron A the grid oscillates with an amplitude of at least [illegible], E being the amplitude of the original supply 26 phase, unless A and A' are connected through the chain, in which case the potentials remain the same or differ only by whatever grid bias has been put into the grid circuit. The thyratrons are so adjusted that an oscillation of amplitude [illegible] will bring the potential of the grid to the critical value and the valve will 'fire'. The valve is coupled with a relay which only trips if the thyratron fails to fire. This relay is actually a 'differential relay', with two sets of windings, one carrying a constant current and the other carrying the current from the anode circuit of the thyratron. Fig 60 shows a possible form of circuit. It is probably not the exact form of circuit used in the Pye experiments, but is given to illustrate the theoretical possibility.

The Spider

We can look at the Bombe in a slightly different way as a machine for making deductions about Stecker when the rod start is assumed. Suppose we were to put lamp-boards in between the enigmas of the chains, and label the lamp-boards with the appropriate letters off figure . For example in chain C the lampboard between C1 and C2 would be labelled A. If we were using the machine with a key-board could be labelled with the 'central letter'. Now when we depress a letter of the key-board we can read off from the lamp- boards some of the Stecker consequences of the hypothesis that the depressed letter is steckered to the central letter; for one such consequence could be read off each lampboard, namely that the letter lighting is steckered to the name of the lamp-board.

When we look at the Bombe in this way we see that it would be natural to modify it so as to make this idea fit even better. We have not so far allowed for lengthy chains of deductions; the possible deductions stop as soon as one comes back to the central letter. There is however no reason why, when from one hypothesis about the Stecker value of central letter we have deduced that the central letter must have another Stecker value, we should not go on and draw further conclusions from this second Stecker value. At first sight this seems quite useless, but, as all the deductions are reversible, it is actually very useful, for all the conclusions that can be drawn will then be false, and those that remain will stand out clearly as possible correct hypotheses. In order that all these deductions may be made mechanically we shall have to connect the 26 contacts at the end of each chain to the common beginning of all the chains. With this arrangement we can think of each ~~xxxxxxx~~ output or input point of an enigma as representing a possible Stecker, and ~~xxx~~ if two of these points are connected together through the enigmas then the corresponding Stecker imply one another. At this point we might see how it all works out in the case of the crib given above. This crib was actually enciphered with ~~xxxxxx

DECLASSIFIED
Authority NND 963016

In Fig 4 at the top are the chains, with the positions and the letters of the chain. In each column are written some of the letters in which can be inferred to be Steckers values of the letters at the heads of their columns from the hypothesis that X is a Stecker value of the central letter E. By no means all possible inferences of this kind are made in the figure, but among those that are made are all possible Stecker values for E except the right one, L. If we had taken a rod start that was wrong we should almost certainly have found that all of the Stecker values of E could be deduced from any one of them, and this will hold for any crib with two or more chains. Remembering now that with our Bombe one Stecker is deducible from another if the corresponding points on the lamp boards are connected through the enigmas, a correct rod start can only be one for which not all the input points of the chains are connected together; the positions at which this happens are almost exactly those at which a Bombe with simultaneous scanning would have stopped.

This is roughly the idea of the 'spider'. It has been described in this section as a way of getting simultaneous scanning on the Bombe, and has been made to look as much like the Bombe as possible. In the next section another description of the spider is given.

The spider. A second description. Actual form.

In our original description of the Bombe we thought of it as a method of looking for characteristics of a crib which are independent of Stecker, but in the last section we thought of it more as a machine for making Stecker deductions. This last way of looking at it has obviously great possibilities, and so we will start afresh with this idea.

In the last section various points of the circuit were regarded as having certain Stecker corresponding to them. We are now going to carry this idea further and

DECLASSIFIED
Authority NND 963016

have a metal point for each possible Stecker. These we can imagine arranged in a rectangle. Each point has a name such as Pv: here the capital letters refer to 'outside' points and the small letters to 'inside letters'; an outside letter is the name of a key or bulb, and so can be a letter of a crib, while an inside letter is the name of a contact of the Eintrittswalz, so that all ~~information~~ constatations obtained ~~from an~~ ~~instrument~~ the enigma without Stecker give information about inside letters rather than outside. Our statements will usually be put in rather illogical form; statements like 'Jis an outside letter' will usually mean 'Jis' occurring in so and so as the name of a key rather than of a contact of the 'Eintrittswalz'. The rectangle is called the 'diagonal board' and the rows are named after the outside letters, the columns after the inside letters. Now let us take any constatation of ~~our~~ crib e.g. Q I at 24. For the position we are supposed to be testing we will have an enigma set up at the right position for encoding this constatation, but of course without any Stecker. Let us suppose it set up for the correct position, then one of the pairs in the alphabet in position 24 is OC: Consequently ~~if~~ ~~it~~ Qo then Io (i.e. if outside letter Q is associated with inside o then outside I is associated with inside o). Now if we connect the input of the (Letchworth) enigma to the corresponding points of the diagonal board on line Q and the ouput to line I then since the 'o' input point is connected to the 'o' output point we shall have Qo on the diagonal board connected to Io through the Letchworth enigma. ~~So any deduction that can be made about Stecker are permitted in connection with contacts of the diagonal board; if the~~ We can of course put in a Letchworth enigma for every constatation of the crib, and then we shall have all the possible deductions that can be made about the association of inside and outside letters parelleled in the connections between the points of the diagonal board. We can also bring in the reciprocal ~~m~~ property of the Stecker by connecting together diagonally oppositepoints of the diagonal board, e.g. connecting Pv to Vp. One can also bring in other conditions about the

DECLASSIFIED
Authority NND 363016

Steckar, e.g. ifone knows that the letters which were unsteckered on one day are invariably steckered on the next then, having found the keys for one days traffic one could when looking for the keys for the next day, connect together all points of the diagonal board which correspond to non-steckers which had occurred on the previous day. This would of course not entirely eliminate the inadmissible solutions, but would enormously reduce their number, the only solutions which would not be eliminated being those which were inadmissible on every count.

One difference between this arrangement and the Bombe, or the spider as we described it in the last section is that we need only one enigma for each constatation.

Our machine is still not complete, as we have not put in any mechanism for distinguishing correct from incorrect positions. In the case of a crib giving a picture like Fig 6 where most of the letters are connected together into one 'web' it is sufficient to let current into the diagonal board at some point on some line named after a letter on the main web, e.g. at the E point inthe case of the crib we have been considering. In this case the only possible positions will be ones in which the current fails to reach all the other points of the E line of the diagonal board. We can detect whether this happens by connecting the points ofthe E line through differential relays to the other pole of our current supply, and putting the 'on' points of the relays in parallel with one another and in series with the stop mech. Normally current will flow through all the differential relays, andthey will not move. When one reaches a position which might be correct the current fails to reach one of these relays, and the current permanently flowing in the other coil of the relay causes it to close, and bring the stopping mechanism into play. Mostly what will happen is that there will be just one relay which closes, and this will be one connected to a point of the diagonal board which corresponds to a Stecker which is possibly correct; more accurately, if this Stecker is not correct the positions is not correct. Another possibility is

DECLASSIFIED
Authority NND 363016

that all relays close except the one connected to the point at which the current enters the diagonal board, and this point ~~[illegible]~~ in the en corresponds to the only possible Stecker. In cases where the~~m~~ data is rather scanty, and the stops therefore very frequent, other things may happen. e.g we might find four relays closing simultaneously, all of them connected together through the enigmas andthe cross connections of the diagonal board, and therefore none of them corresponding to possible Stecker.

~~[illegible]~~

In order for it to be possible to make the necessary connections between the enigmas,the diagonal board and the relays there has to be a good deal of additional gear. The input and output rows of the enigmas are brought to rows of 26 contacts called 'female jacks'. The rows of the diagonal board are also brought to female jacks. The 26 relays and the current supply are also brought to a jack. A ny two female jacks can be connected with 'plaited jacks' consisting of 26 wires plaited together and ending in male jacks which can be plugged into the female jacks. In order to make it possible to connect ~~the~~ three or more rows of contacts together one is also provided with ~~an~~ 'commons' consisting of four ~~row~~ female jacks with corresponding points connected together. There is also a device for connecting together the ~~input~~ output jack of one enigma ~~with~~ and the input of the next, both being connected to another female jack, which can be used for connecting them ~~anywhere~~ to anywhere else one wishes.

On the first spider made there were 30 enigmas, and three diagonal boards and 'inputs'i.e. sets of relays and stepping devices. There were also 15 sets of commons.

DECLASSIFIED
Authority NND 363016

Figs 63, 64 show the connections of enigmas and diagonal board in a particular case. The case of a six-letter alphabet has been taken to reduce the size of the figure.

The actual origin of the spider was not an attempt to find simultaneous scanning for the Bombe, but to make use of the reciprocal character of the Stecker. This occurred at a time when it was clear that very much shorter cribs would have to be worked than could be managed on the Bombe. Welchman then discovered that by using a diagonal board one could get the complete set of consequences of a hypothesis. The ideal machine that Welchmang was aiming at was to reject any position in which a certain fixed-for-the-time Stecker hypothesis led to any direct contradiction: by a direct contradiction I do not mean to include any contradictions which can only be obtained by considering all Stecker values of some letter independently and showing each one inconsistent with the original hypothesis. Actually the spider does more than this in one way and less in another. It is not restricted to dealing with one Stecker hypothesis at a time, and it does not find all direct contradictions.

Naturally enough Welchman and Keen set to work to find some way of adapting the spider so as to detect all direct contradictions. The result of this research is described in the next section. Before we can leave the spider however we should see what sort of contradictions it will detect, and about how many stops one will get with given data.

First of all let us simplify the problem and consider only normal stops, i.e. positions at which by altering the point at which the current enters the diagonal board one can make 26 relays close. The current will then be

DECLASSIFIED
Authority NND 363016

entering at a correct Stecker if the position is correct. Let us further simplify the problem by supposing that there is only one 'web', i.e. that the 'picture' formed from the part of the crib that is being used forms one connected piece, e.g. with the crib on p we should have one web if we omit the constatations $\overset{P}{B}$, $\overset{B}{U}$,$\overset{U}{O}$,$\overset{R}{H}$. ~~Clearly a sufficient condition for a stop is that the 'multiple encipherment' conditions should hold. Supposing that the number of independent chains or 'closures' is c then the number of positions where the multiple encipherment conditions hold will be about 26^{4-c}~~ Some of the constatations of the web could still be omitted without any of the letters becoming disconnected form the rest. Let us choose some set of such constatations, ~~which cannot be omitted without breaking~~ in such a way that we cannot omit any more constatations without the web breaking up. When the constatations are omitted there will of course be no 'chains' or 'closures'. This set of constatations may be called the 'chain-closing constatations', and the others will be called the 'web-forming constatations'. At any position we may imagine that the web-forming constatations are brought into play first, and only if the position is possible for these are the chain-closing constatations used. Now the Stecker value of the input letter and the web-forming constatations will completely determine the Stecker values of the letters occurring in the web. When the chain closing constatations are brought in ~~the~~ it will already be completely determined what are the corresponding 'unsteckered' constatations, so that if there are c chain-closing constatations the final number of stops will be a proportion 26^{-c} of the stops which occur if they are omitted. Our problem reduces therefore to the case in which there are no closures. It is, however, also fairly clear that the number of stops will

DECLASSIFIED
Authority NND 363016

not be appreciably affected by the ~~xxxxxxxx~~ branch arrangement of the web, but only by the number of letters occurring in it. These facts enable us to make a table for the calculation of the number of steps in any case where there is only one web. The method of construction of the table is very tedious and uninteresting. ~~xxxx~~ The table is reproduced below

No. of letters on web	H-M factor
2	0.92
3	0.79
4	0.62
5	0.44
6	0.29
7	0.17
8	0.087
9	0.041
10	0.016
11	0.0060
12	0.0018
13	0.0004
14	0.000095
15	0.000016
16	0.0000023

$$\text{No. of answers} = 26^{4-c} \times \text{H-M factor}$$

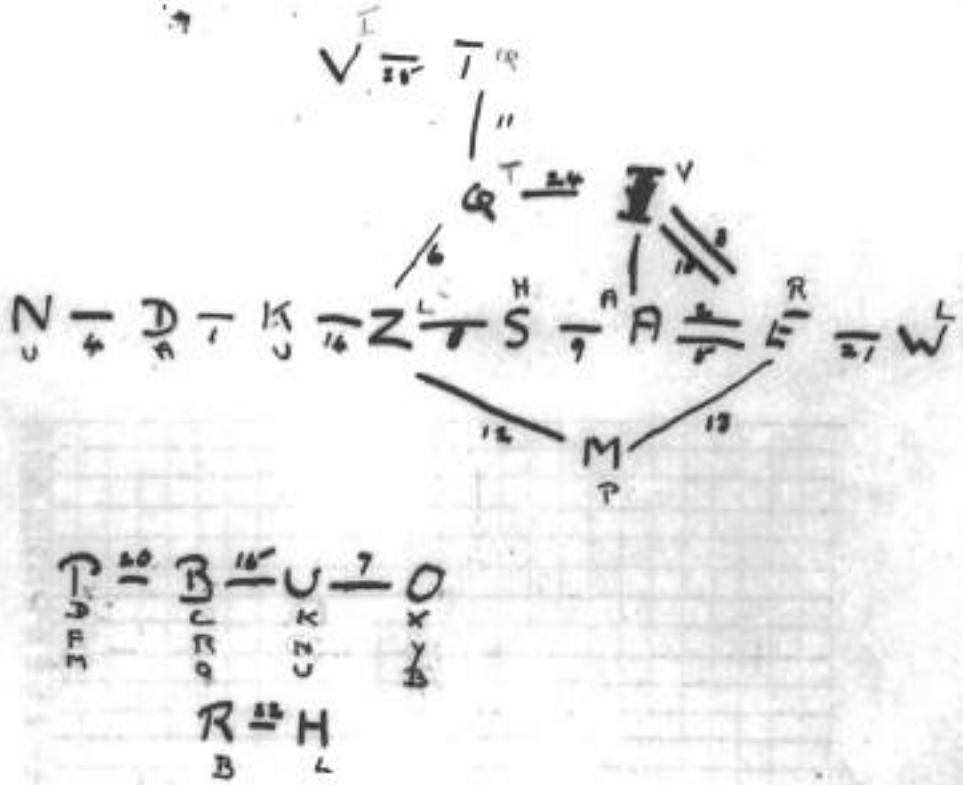
c is number of closures

A similar table has also been made to allow for two webs, with up to five letters on the second. To the case of three webs ~~Beyond this~~ it is not worth while and hardly possible to go. One can get a sufficiently good estimate in such cases by using common-sense inequalities, ~~xxxxxxx

DECLASSIFIED
Authority NND 363016

To see what kind of contradictions are detected by the machine we can take the picture, Fig 64 and on it write against each letter any Stecker values of that letter which can be deduced from the Stecker hypothesis which is read off the spider when it stops. This has been done in Fig 65 for a case where the input was on letter E of the diagonal board, and the relay R closed when the machine stopped; if the position of the stop were correct at all the correct Stecker would be given by the points of the diagonal board which were connected to Er, and they will also be the direct consequences of the Stecker hypothesis E/R. As we are assuming that R was the only relay to close this relay cannot have been connected to any of the others, or it would have behaved similarly. We cannot therefore deduce any other Stecker value for E than R, and this explains why on the 'main web' in Fig 65 there is only one pencil letter against each ink letter. Wherever any pencil letter is the same as an ink letter we are able to write down another pencil letter corresponding to the reciprocal Stecker or to the diagonal connections of the board. In one or two cases we find that the letter we might write down is there already. In others the new letter is written against a letter of one of the minor webs; in such a case we clearly have a contradiction, but as it does not result in a second set of pencil letters on the main web the machine is not prevented from stopping. There are other contradictions; e.g. we have Z/L, W/L, but as L does not occur in the crib this has no effect.

DECLASSIFIED
Authority NND 363016



Relevant parts of alphabets

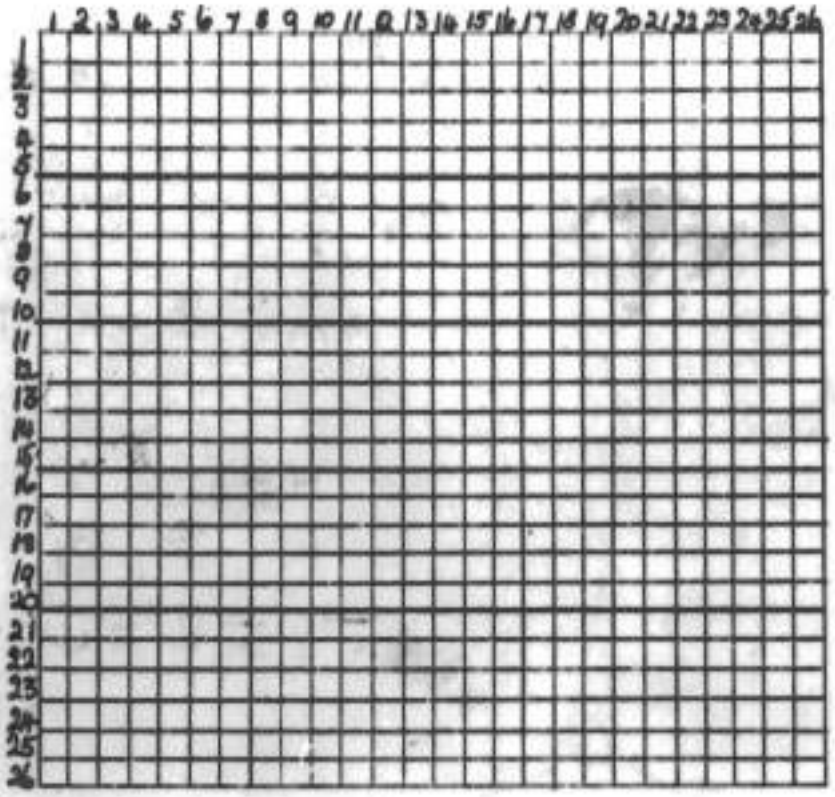
1	2	3	4	5	6	7	8	9
AU	AR	AV	AD	AR	AL	KA NY US	AH	AN

10	11	12	13	14	15	16	17	18
AV	QT	LP	MF	AU	CM AN OU			

19	20	21	22	23	24	25	26
DA AR MD	AL	GL	AV	VT	QI		

Fig 65. Illustrating the kind of position in which the Spider will stop. Here the input letter may be supposed to be E and the relay which closes R. The shaken values of the letters, which are consequences of the hypothesis E/R are written against the letters. There are unhandicaps such as R/A, W/A: P/D, P/F, P/M which are not experienced by the spider.

DECLASSIFIED
Authority NND 363016



DECLASSIFIED
Authority NND 363016

The machine gun

When using the spider there is a great deal of work in taking down data about stops from the machine and in testing these out afterwards, making it hardly feasible to run cribs which give more than 5 stops per wheel order. As the complete data about the direct consequences of any Stecker hypothesis at any position are already contained in the connections of the points of the diagonal board it seems that it should be possible to make the machine do the testing itself. It would not be necessary to improve on the stopping arrangement of the spider itself, as one could use the spider as already described, and have an arrangement by which, whenever it stopped a further mechanism is brought in to play, which looks more closely into the Stecker. Such a mechanism will be described as a machine gun, regardless of what its construction may be.

With almost any crib the proportion of spider stops that would be passed by a machine gun as possible would be higher than the ratio of spider stops to total possible hypotheses. Consequently the amount of time that can economically be allowed to the machine gun for examining a position is vastly greater than can be allowed to the spider. We might for instance run a crib which gives 100 spider stops per wheel order, and the time for running, apart from time spent during stops might be 25 minutes. If the machine gun were allowed 5 seconds per position, as compared with the spiders 1/10 second only 8 minutes would be added to the time for the run.

When the spider stops, normally the points of the diagonal board which are energised are those corresponding to supposedly false Stecker. Naturally it would be easier for the machine gun if the points energised corresponded to supposedly correct Stecker. It is therefore necessary to have some arrangement by which immediately after the spider stops the point of entry of the current is altered to the point to which the relay which closed was connected, or is left unaltered in the case that 25 relays closed. Mr Keen has invented some device for doing this, depending entirely on relay wiring. I do not know the details at present, but it might be something like this: let us suppose that the [illegible] of the diagonal [illegible] of the machine [illegible], but apparently the effect is that the machine does not stop at all except in cases in which either just one relay closes or 25 relays close. In the case that 25 relays close the current is allowed to continue to enter at the same point, but if just one relay closes the point of entry is changed over to this relay. This method has the possible disadvantage that a certain number of possible solutions may be missed through not being of normal type. This will only be serious in cases where the frequency of spider stops is very high indeed, e.g. 20%, and some other method, such as 'Ringstellung cut-out' is being used for further reducing the stops. An alternative method is to have some kind of a 'scanner' which will look for relays which are not connected to any others. Which method is to be used is not yet decided.*

At the next stage in the process we have to see whether there are any contradictions in the Stecker; in order to reduce the number of relays involved this is done in stages. In the first stage we see whether or not there are two different Stecker values for A, in the second whether there are two different values for B, and so on. To do this testing we have 26 relays

* Not has been decided to use scanner.

DECLASSIFIED
Authority NND 363016

which are wired up in such a way that we can distinguish whether or not two or more of them are energised. When we are testing the Stecker values of A we have the 26 contacts of the A line of the diagonal board connected to the corresponding relays in this set. What is principally lacking is some device for connecting the rows of the diagonal board successively to the set of relays. This fortunately was found in post-office standard equipment; the clicking noise that this gadget makes when in operation gives the whole apparatus its name. If we find no contradictions in the Steckers of any letter the whole position is passed as good. The machine is designed to print the position and the Stecker in such a case. Here again I do not know the exact method used, but the following simple arrangement seems to give much the same effect, although perhaps it could not be made to work quite fast enough. The Stecker are given by typing one letter in a column headed by the other. When any letter is being tested for Stecker contradictions the relays corresponding to the Stecker values of the letter close. We can arrange that these relays operate corresponding keys of the typewriter, but that in the case that there is a contradiction this is prevented and some special symbol typed instead shewing that the whole is wrong. When no relay closes nothing is typed. The carriage of the typewriter is not operated by the keys but only by the space bar, and this is moved whenever there is a change of the letter whose Stecker are being examined.

DECLASSIFIED
Authority NND 963016

Authority NND 363046

Additional gadgets

Besides the spider and machine-gun a number of other improvements ~~xxxxxxxxxx~~ of the Bombe are now being planned. We have already mentioned that it is possible to use additional data about Stecker by connecting up points of the diagonal board. It is planned to make this more straightforward by leading the points of the diagonal board to 325 points of a plug board; the plug board also has a great many points all connected together, and any Stecker which one believes to be false one simply connects to this set.

Another gadget is designed to deal with ~~xxxxxxxxxxxxxxxxxx~~ ~~xxx~~ cases such as that in which there are two 'webs' with six and no chains letters on each. A ~~xx~~ little experiment will show that in the great majority of cases with such data, when the solution is found, the Stecker value of a letter on either web will imply the whole set of Steckers for the letters of both webs: in ~~xx~~ the current terminology, "In the right place we can nearly always get from one web onto the other". If however we try to run such data on the spider, even with the machine gun attachment, there will be an enormous number of stops, and the vast majority of these will be cases in which " we have not got onto the second web". If we are prepared to reject these possibilities without testing them we shall not very greatly decrease the probability of our finding the right solution, but very greatly reduce the amount of testing to be done. If in addition the spider can be persuaded not to stop in these positions, the spider time saved will be enormous. Some arrangement of this ~~xxx~~ kind is being made but I will not attempt to describe how it works.

~~In connection with some special problems~~

With some of the ciphers there ~~may be~~ is information about the Ringstellung (Derivelismus) which makes certain stopping

DECLASSIFIED
Authority NND 363016

places wrong in virtue of their position, and not of the alphabets produced at those positions. There is an arrangement, known as a 'Ringstellung cut-out" which will prevent the machine from stopping in such ~~m~~ positions. The design of such a cut -out clearly presents no difficulties of principle.

There are also plans for "majority vote" gadgets which will enable one to make use of data which is not very reliable. A hypothesis will only be regarded as rejected if it contradicts three(say) of the unreliable pieces of data. This method may be applied to the case of unreliable data about Stecker.

DECLASSIFIED
Authority NND 363016

Chapter VII. The German Naval Enigma Cipher

Historical

In the period from about 1931 to April 30, 1937 the Naval cipher ~~xxxxxx~~ used much the same indicating system as the other German service enigma ciphers, viz. the 'boxing' method recommended by the firm that sold the 'commercial' enigma. With this ~~xx~~ system as well as the set up ofthe machine consisting of wheel order, Ringstellung, and Stecker, there was a window position fixed for the day, and known as the 'Grundstellung'. When it was desired to encipher a message one first chose three letters at random from a list of about 1700 trigrams, e.g. ~~ZLE~~ ~~xxxxxxx~~. One then set the machine to the Grundstellung and enciphered ~~ZLEZLE~~. The resulting six letters were put at the beginning of the message, and the remainder of the message consisted of the result of enciphering the plaintext with pre-start window position ZLE. (This differs from the other boxing indicating systems in that ~~xxx~~ most of these allow the trigramme such as ZLE to be chosen at random instead of from ~~xxxx~~ a restricted list.

The weakness of this indicating system is that a great deal of information is given away about the 'Grundstellung'. If there were no Stecker, and a known diagonal the traffic amounted to 100 messages per diem it would be possible to find the connections of the machine, and if there were Stecker but the connections of the machine were known it would be possible to find the keys every day ~~with~~ from the same amount of traffic. ~~xxxxxx

DECLASSIFIED
Authority NND 363016

In the two indicators UJOOBL and UAHODH the repetition of the first letters is followed by a repetition of the fourth letters. That this must always happen is clear from the fact that the fourth letter arises from the first by enciphering at the position directly after the Grundstellung and re-enciphering three places further on. This phenomenon enables us to tell very quickly with any cipher whether the Boxing form of indication is being used. From the indicators we can find the effects of the three repeated encipherments. In Fig 66 we have entered in one of the columns against each letter the effect of enciphering it first at the position immediately after the Grundstellung and then at the position four places after the Grundstellung: thus we have the entry J against A, with five dots. This means that A enciphered at the first and fourth positions gives J, and that this information has been given us from six indicators, which are actually ALAJMB,AYIJPI,AFLJVI, AFTJNA,AVRJKX,AUKJJJ. The other two columns give us the results of the encipherments at the second and then the fifth position, and at the third and then the sixth. We get for the results of these double encipherments

G_4G_1

...NZQAJSKP...TGLZV...(DSHUGVKXBRGKY)

G_5G_2

(PWUJBQCLAFVKY)(GHDWSAIXETGAZ)

G_6G_3

(V)(I)(JFNRKPWSHOLX)...DUQEZGTAJYMC...

G_4G_1 here means the encipherment with the first alphabet and then with the fourth, the reversal of the natural order being in agreement with mathematical tradition. There can be no doubt as to how the substitution G_6G_3 is to be completed, but at first sight it might appear that there are two possibilities for G_4G_1. However if we remember what we found out in the section 'Alphabets and boxes' we see that it must be possible to pair off the cycles of G_4G_1 into ones of equal length.

DECLASSIFIED
Authority NND 363016

There are various things which could be done now. Of course one might put the whole data onto the spider, but at the time that this system was in force no such machine had been thought of. Another method, which was that principally used by the Poles is to have a permanent catalogue of the box shapes for G_4G_1, G_5G_2, G_6G_3 for every Grundstellung, assuming that there is not a T.O. between the first and last of the six alphabets. ~~Each of the box shapes or numbers~~ If we give some standard order to the box shapes, we can also put the possible series of three box shapes into an order, and can enter against each set of three box shapes the Grundstellungen for which this set is realised. To use this catalogue with our problem we should work out the box shapes viz. G_4G_1 is 26, G_5G_2 is 26, G_6G_3 is 24,2. The box shapes ~~actually have the number~~ 26 actually has the nuber 1 and 24,2 the number 2: they are the two commonest shapes as can be seen from the table p 14a. We then look up 1.1.2 in our catalogue, and find about 150 entries against it for each wheelorder. Each of these will have to be tested out in some way or other. The most satisfactory method seems to be this. We form the permutation $G_6G_3G_5G_2$. It is

(PNOMSRQDJYWHIBKEAUFV)(CXZL)(G)(T)

so that this permutation is of the class 20,4,1,1. For each possible Grundstellung it is possible to calculate the corresponding class for the unsteckered alphabets. This can fortunately be done mechanically by means of a form of 'cyclometer'. It would be as well to enter against each position the class of this permutation, and this might have have been done at the time of construction of the catalogue. In the case in question the right Grundstellung is found to the position 1,1,26 with wheel order I,II,III (service machine, Uhr Kreuzl A). The corresponding boxes are

DECLASSIFIED
Authority NND 363016

DT PL CZ
MS RN TQ
HL UO XU
UP JL JD
CK BE FO
AI QX RM
RJ OD NY
XV TK XB
BQ MI PV
RS FW WL
OR AS ID
YW KH HZ
ZZ XE RS

We ~~extrapolyx~~ must have V/A or V/S. If V/A we can identify the cycle (OHIWSADXRETGHZ) of the G_5G_2 with stecker, with the half compartment of the second box in this way

(OHIWSADXRETGHZ)
(CHSWIVDXXLGHZ)

i.e. we ~~xxxxx~~ have to assume the stecker O/C,I/S,A/V,T/L,R/H, and that HTW,D,X,E,G,Z are unsteckered. This large number of unsteckered letters is a strong confirmation, and the repetition of the Stecker I/S is further confirmation. When we fit the rest of the boxes together we find that these five are all the Stecker.

There are other methods that can be applied, depending onthe number of Stecker being small. The number of Stecker used in the Naval was 6 from 1931 to Nov. 1938 and possibly later. We might for instance have assumed that A and S were both unsteckered and therefore assumed that the constetation $\overset{A}{S}$ occurred in both the alphabets $G_5$and G_6 . With the Turing sheets we could find the possible positions for this, andthen use a cyclometer to test ~~thxx~~ the box shapes in those positions. This is naturally only worth while if we have no box-shape catalogue. Another possibility is to 'equate' the boxes, i.e. to find out from the permutations G_4G_1 etc what the original ~~xxxxxx~~alphabets $G_1$and G_4 were. In our case there are actually 13 different possibilities for G_1, 13 for G_4 and 18 for G_3. There are two things we can do to distinguish between the correct and the incorrect possibilities. We can use known statistics about the list of admissible message settings, choosing that combination of alphabets that gives the ~~xxxx~~ greatest number of ~~xxxxxx~~ ~~settings that have xx occurred xxx.~~

DECLASSIFIED
Authority NND 363016

repetitions between the message settings for the day in question and message settings of previously solved days. We might also do a 'Benburismus' i.e. we might make use of the fact that if two messages are written out with letters that were enciphered at the same position written in the same column, then the number of repetitions of letters in a column will be the same as if the messages had not been enciphered, and therefore will be on average greater than if the messages had been otherwise placed. Actually this effect was very small for the Naval traffic in 1937 and earlier. The repetition frequency was 1/20, as compared with 1/16.5 for the 1940 Naval traffic and the Air traffic, and 1/12 for plain language German, and 1/26 for incorrectly placed enciphered messages (the repetition frequency is the ratio of the number of identical pairs in the columns to the total number of pairs in columns, identical or not). With so low a repetition frequency it is extremely difficult to equate the boxes unless the traffic is rather heavy. This method however applies quite well with the Air traffic up to Sept 14 1938, but there are better methods of equating. Once the boxes have been equated by one means or another we shall have many more cases of half-bombes which we can assume to have been unsteckered. This method will nearly always get the result, if the equating can be done.

After we have found the rod position of the Grundstellung and the Stecker it only remains to find the Ringstellung. Usually this would be known already, as, at this period, the wheel order and Ringstellung were only changed about once a fortnight. However if these have just been changed it is necessary to read one message. This could always be done, as a great many messages were sent in two or more parts. In such cases the call signs and signatures of the parts were essentially the same, and the sent parts after the first began by saying that they were continuations, giving the time group of the last part of the message as a reference. The method of giving numbers at that time was to use

DECLASSIFIED
Authority NND 363016

the top row of the keyboard and P thus

QWERTZUIOP
1234567890

The number was put between Y's to show that it was a number, and the whole repeated as a check. The continuation of a message whose time group was 2330 would begin FORTYWEEPTYWEEPY . We could then find the position where this message started by single wheel processes, and as we already know the window position of the start, we can calculate the Ringstellung.

On the 1st May 1937 a new indicating system was introduced. The first two groups (four letters each) of the message were repeated at the end. This clearly showed that these two groups formed the indicator. The repetition also showed that no check could be expected within the first two groups themselves. This was discouraging, as the essential weakness of the boxing method was that the something was enciphered twice with the machine. With the new method of indicating, whatever it is, the best one can hope is that either it will enable us to set the messages, or that from some information about the setting of the messages obtained elsewhere we may be able to deduce something about the machine setting. However the first thing to be done was to find out how the indicators worked, and it was necessary therefore to try and read some messages with which the new system was being used. To do this one can use the FORTYWEEPY messages, and apply one of the methods described at the beginning of the last chapter. In this way the Poles found the keys for the 8th of May 1937, and as they found that the wheel order and the turnovers were the same as for the end of April they rightly assumed that the wheel order and Ringstellung had remained the same during the end of April and the beginning of May. This made it a simple for them to

Authority NND 963016

find the keys for other days at the beginning of May and they actually found the Stecker for the 2nd, 3rd, 4th, 5th and 8th, and read about 100 messages. The indicators and window positions of four (selected) messages for the 5th were

Indicator	Window start
KFJX EWTW	P C V
SYLG EWUF	B Z V
JMHO UVQG	M E M
JMFE FEVC	MYY K

The repetition of the EW combined with the repetition of V suggests that the fifth and sixth letters describe the third letter of the window position, and similarly one is ledto believe that the first two letters ofthe indicator represent the first letter of the window position, and that the third and fourth represent the second. Presumably this effect is somehow produced by means of a table of bigramme equivalents ofletters, but it cannot be done simply by replacing the letters of the window position with one of their bigramme equivalents, and then putting in a dummy bigramme, for in this case the window position corresponding to JMFE FEVC would have to be say MYY instead of MYK. Probably some encipherment is involved somewhere. The two most natural alternatives are , i) The letters of the window position are replaced by some bigramme equivalents and then the whole enciphered at some 'Grundstellung', or ii) The window position is enciphered at the Grundstellung, and the resulting letters replaced by bigramme equivalents. The second of these alternatives was made far more probable by the following indicators occurring on the 2nd May

EXDP IVJO	V C P
XXXX JXJY	V U E
RGXX JLWA	N U M

With this second alternative we can deduce from the

DECLASSIFIED
Authority NND 363016

first two indicators that the bigrammes XX and XX have the same value, and this is confirmed from the second and third, where XX and XX occur in the second position instead ofth e first.

It so happened that the change of indicating system had not been very well made, and a certain torpedo boat, withthe call sign AFA: had not been provided with the bigramme tables. This boat sent a message in another cipher explaining this on the 1st May, and it was arranged that traffic with AFA: was to take place according tothe old system until May 4, when the bigramme tables would be supplied. Sufficient traffic passed on May 2,3 to and from AFA: for the Grundstellung used to be found, the Stecker having already been found from the FORTYWKEPY messages. It was natural to assume that the Grundstellung used by AFA: was the Grundstellung to be used with the correct method of indication, and as soon as we noticed the two indicators mentioned above we tried this out and found it to be th e case.

There actually turned out to be some more complications. There were two Grundstellungen at least instead of one. One of them was called the Allgemeine and the other the Offiziere Grundstellung. This made it extremely difficult to find eithter Grundstellung. The Poles pointed out another possiblity, viz that th e trigrammes were still probably not chosen at random. They suggested that probably the window positions enciphered at the Grundstellung, rather than the window positions th emselves were taken off the restricted list.

In Nov. 1939 a prisoner told us that the German Navy had now given up writing numbers with Y...YY...Y and that the digits of th e numbers were spelt out in full. When we heard this we examined the messa es toward th e end of 1937 which were expected to be continuations and wrote th e expected beginnings under them. The proportoin of 'crashes' i.e. of letters apparently left unaltered by encipherment, then shows how nearly correct our guesses were. Assuming that the change

DECLASSIFIED
Authority NND 363016

mentioned by the prisoner had already taken place we found that about 70% of these cribs must have been right. Further 'crash analyses' were made for other periods up to Aug 1939, all with fairly favourable results. At the same time there had been some changes in the machine, known toh ave taken place because of the corresponding changes in the machine used by the army and air whose traffic had been read. In the summer of 1937 the Umkehrwalze had been changed from A to B, and in Dec 1938 two new wheels ~~x~~ IV and V had been introduced. ~~xxxxxxxxxxxxxxxxxxxx~~ After the beginning of the war (Sept 1939) the FORTYWEEPT messages were no longer traceable, because there were no more call signs. However there had been some traffic at various times during ~~manoeuvres~~ manoeuvres and crises since the occupation of Austria, ~~There~~ ~~xxxxxxxxxxxxxxxxxxx

'pinched' from a German boat, enabling us set the keys for April 22-27 1940. At the same time we pinched a book of instructions telling us the precise form of the indicating system.

To encipher a message the operator chooses two trigrammes out of a book. The first of these trigrammes is called the 'Schluesselkenngruppe'. The choice of this is partly determined by the nature of the message: e.g. all 'dummy' messages have the Schluessel kenngruppe taken from one part of the book and genuine messages have them taken from elsewhere; we do not know very much about these. The second trigramme is called the Verfahrenkenngruppe. Suppose the Schluesselkenngruppe is CIV and the Verfahren kenngruppe is TOD then the operator chooses two dummy letters, Q and X say, and writes this down

Q C I V
T O D X

From the Verfahren kenngruppe is obtained the window position for the start of the message, by enciphering at the Grundstellung. From the eight letters above one also obtains the indicator for the message, by substitution from a table which gives bigramme for bigramme. The substitution is done by replacing the vertical pairs above with bigrammes, e.g. in this case, if the substitute for QT were DA, and CH were CO, PO for ID, and CN for VX then the indicator for the message is DATH POCN. Apart from the Schluessel kenngruppe feature this is the method we had inferred was being used. This extra feature accounts for the bigrammes in the indicators being almost perfectly hatted. Also the fact that it is never the message setting itself which is chosen at random by the operator eliminates any remaining hope that one might use 'operator's psychology' to help in finding out the alphabets. From our point of view of course the Schluessel kenngruppen which at any rate did not exist, and the 'bigramme lists' to use remain Form sheets with on a letter entered in each square, and not two. There is however the restriction that there must be exactly 26 occurrences of each letter.

*

*This has gone out of date

DECLASSIFIED
Authority NND 363016

Methods of reading the individual messages

With the system of indication that has been used since May 1937 we are not able to read all the messages as soon as we have read one. A few may be read by single wheel processes, starting from a short crib, but we cannot hope to read the whole traffic in this way. Also, when we have found the Grundstellung ~~xxxxxxxxxxxxxx~~, and if there is plenty of traffic, we may be able to make use of ~~xxxx~~ some bigrammes which occurred in messages already read. These methods are not enough by themselves. In the 1937 traffic there was no 'not probable', and we had planned a method for finding the right starting position, making use of the fact that the correct decode would probably have more letters E in it than any of the others. It was intended to have a long punched paper roll, the punching shewing the effect of enciphering E in the various positions. This paper was to move under a series of about 500 brushes whose position was determined by the letters of the enciphered message. The number of brushes which poked through the holes at any moment was the number of letters E in the decode of the message, the window position ~~xfxthe~~ being determined by the position of the roll. All positions giving more than a certain number of letters E were to be recorded and these positions independently tested. This machine was called 'the rack'.

It was never necessary to make a rack because when the 1938 messages were read it was found that the ~~xx~~ word KINS occurred veryfrequently. We therefore made a catalogue of the encoded values of KINS at every possible starting position, and arranged the encoded values in alphabetical order. The unanalysed catalogue was made by enciphering first E at every possible position, then I, N and S. This was done with the automatic typewriting machines. The values of I were stuck below the values of E with a stagger; the values of N and S were underneath the same again, with suitable stagger. The result was that the effect of enciphering KINS appeared in vertical columns.

DECLASSIFIED
Authority NND 363016

This unanalysed catalogue was known to the girls as 'corsets'. In analysing the catalogue we took 25 sheets named A to Z, with X omitted: each sheet had 25 lines, named A to Z with X omitted. Supposing on sheet 13 and line 4 of the corsets we found LVOM as a value of EDNS we would enter OM 13.4 on line V of sheet L. In a later form of the catalogue we also made 'existence sheets'. In the existence sheets we would enter M in line V and column O of sheet L. To use the catalogue we first analysed the tetragrammes in the messages according totheir first letters. One would then take the A existence sheet and go through all the messages marking the tetragrammes which occurred on the existence sheet, and marking against them the entry (e.g. 13.4) from the catalogue. Afterwards one would have to go back to the corsets, and search in the right line for the tetragramme, and work out its position: this was done with a cardboard strip and known as 'masking'. Having found the position one would have to set up the machine, decipher the tetragramme, verifying that it gave EDNS and then continue to decipher and see if one continuedto get sense.

This process has since been greatly improved. Instead of making the corsets off the 'X-machines' we have a machine called the 'test-plate' or 'baby' which typed out the results of enciphering EDNS in all positions in a much more convenient form. Also we no longer analyse the groups by hand, but have them punched on cards, together with their position, which are then sorted into alphabetical order, and listed. A further improvement is that the test-plate is now made to punch the cards directly.

Roughly, our programme when the wheel order, Ringstellung, and Stecker for a day have been found, is as follows. We make an EDNS catalogue, and use it to get out pairs of messages in which the second indicator bigramme of one is the same as the third indicator bigramme of the other. If we have four such cases we have sufficient data about the Grundstellung to be able to find it by means of the Bombe, provided that we have