HW 25/3

CCR 1
102(1)

TOP SECRET
ULTRA

65/4/7A

I. A description of the mach ine.

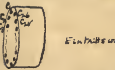
We begin by describing the 'unsteckered enigma'. The machine consists of a box with 26 keys labelled with the letters of the alphabet and 26 bulbs which shine through stencils on which letters are marked. It also contains wheels whose function will be described later on. When a key is depressed the wheels 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 underst nd 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 whe els.
- The mechanism for turning the wheels and for describing the positions of the wheels.

The circuit of the machine without the wheels.

Fig 1

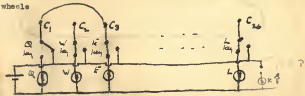


The machine contains a cylinder called the Eintrittswalz (E.W) on which are 26 contacts $C_1, \ldots, C_{26}$. The effect of the wheels is to connect these contacts up in pairs, the actual pairings of course depending on the positions of the wheels. On the other side the contacts $C_1, C_2, \ldots, C_{26}$ are connected each to one of the keys. For the moment we will suppose that the order is ~~qwertzuioasdfghjk~~ 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 th e diagonal, for reasons which will appear in Chap

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

The diagram shews the connections when the key Q is depressed and supposin g 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

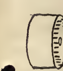
If two contacts C, C' of the Eintrittswalz are connected throughthe wheels th en the result of enciphering the letter associated with C is the letter associated with C'.

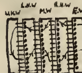
Notice that if P is the result of enciphering G, then G is the result of enciphering P at the same place, also that the result of enciphering G can never be G.

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

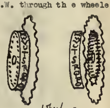
<u>Connections through the wheels.</u>

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 h as 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 positions when in the machine) Each spring contect ie connected to one end only one plete contect. On the wheele ere ringe or tyres oerrying elphebete , end rotetable with respect to the rest of the wheel; more ebout this under 'turnovers'. When the mechine is being used three of the wheele ere put in between the U.K.W. emd the E.W. in some presoribed order . The wey that the current might flow from tha E.W. through th e wheele end back ie ehewn below


Umkehrwalz Fig 3



Connections through wheels Fig 5


Wheel Fig 4

<u>Tuernovers, Ringstellung, Window poeition , rod position.</u>

From the point of view of the legitimete deoipherer, the poeition of th e wheele is described by the lettere on the tyres ~~of the wheels~~ which shew through the three (or 4 if the U.K.W. rotetee) windowe in tha oaeing of the mechine. Thie sequence of lette we celllthe 'window poeition'. When e key ie depreesed tha window position ohengee, but doee not ohange further ~~as~~ when the key ie ellowed to riee. We will sey that the position ohengee into tha 'following' position. The poeition which followe e given one depende only on tha order of tha wheele end on the original window position. This ie beceuse the mechenism for ohanging the poeitions ie cerried on the tyree .

The turning mechanism cohsiete of

Three palle opereted by th e keye, one lying juet to the right of th e right hand wheel, one between the R.H.W end M.W. end one between the M.W. end th e L.H.W.

26 cetches fixed on ~~the right~~ eech wheel on the right .

One (or ~~in the case of~~ poeeibly more, here we will elways eseume it is only one)cetch on eech tyre~~s~~ on the left.

The effect of the right hend pell is to move the ~~right the~~ R.H.W. forward one piece every time a key ie depreesed. The middle pell normally comes into contact with the smooth surface of the tyre of the R.H.W., ~~prexxxxing~~ which prevents it from ~~maxingx~~ 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 ie in the R.H. position then th e 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 ~~xxx~~ turnover E-F, ~~XX~~ R.H.W. T.O. Q →R

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

Fig 6

The effect of enciphering a letter depends only on the wheel order (Walzenlage) and the position (i.e. amount rotated) of the wheel proper (i.e. not the tyre). To describe this position we could imagine that there was a set of letters attached to the business part of each wheel, and that these letters could ~~xxxx~~,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 th e expression 'rod position' will be seen in Chap). The position of the tyre relative to th e business part is fixed by means of a clip on the business part which can drop into holes near the letters. When the clip ~~ix~~sin the hole near the letter C we eay thet the Ringstellung is C for thet wheel. It is oleer that some equetion of the form

Window position = Rod position + Ringstellung + e oonstent must hold(it being understood thet A,B,C,... ere regardad aa interohangeabls with 1,2,3,...). ~~[illegible]~~ Mormelly ~~[illegible]~~ one errenges thet this oonstent ia zaro (see also)

The ateokered enigme.

In some enigmes the esaooiation of the oon teots of the Eintrittewalz withthe keys and bulba oan be veried. Thsre are 26 pairs of sookets lebelled with the letters of the alphabet one of saoh pair leading to a oontaot of the Eintrittswelz end the other to one of the keys. Normally the two sookets are oonneoted together by a hidden spring, if however e'Steoker' is plugged into two paira of sookets, W end R sey, thsse springs ere foroed eway end nsw oonneotione ere made through the Steoker, ths W key being oonneoted to the oontaot whioh would otherwise be oonnsoted to th e R key , end vioe-veraa. Thet W end R are oonneoted by auch a plug is expressed in the form 'W/R' or 'R/W' . Th e effeot of the Steoker on the enoipherment is quite simple. If et e osrtain position of the wheels A enoiphered givea N, (ebbreviated to AN) then et the seme position with Steoker A/V,N/O, end perhaps othere, we heve VO; if inatead we heve the Steoker A/V but none involving N , we should heve VN (or ee we sometimes aey the 'oonstetation' VN). Thus if e possibls enoipherment without eny Steoker were

~~[illegible]~~ DIESERBE[redacted]
~~[illegible]~~ KYMVKEYO

then e possible enoipherment starting from the seme positions of th s wheels(or es we say, from the seme plece) ~~[illegible]~~ with the Steoker D/S, R/N, B/K, V/Y would be

SIEDENKE
BVMYBEVO

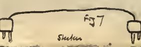
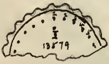


Fig 7

Each short plug is connected to a long one

Conventions for electricians

For the purpose of desribing the wiring of wheels to electricians one works from s'spot' on the right hend (spring contsct besring) side of the wheel, or if there is no spot, from the contact which is uppermostwhen any writing on the face is horizentsl



Upper half of wheel.

Fig 8

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

Spring contscts	1	2	3	4	5	6	7	8	...
Fixed contadts	6	3	16	14	...				

Fig 9

From the poin t of view of the cryptogreph er the most naturel wey of naming th e contacts is rsther diffsrent. One would put the Ringstellung to zsro, then put zero (Z) in the window, and neme any contact on the right of the R.H.W. ~~by~~ sfter the letter associated with ths contsct of the E.W. which it touches, there being sssumed to be no Stecker. To connect these two notstions it would be necessary to taks into considerstion the relstive positions of the Zontsct C_{26} of the E.W. snd the windows, snd also the positions of the clip snd spot on the wheel. Here ie s rule of thumb for obtaining electricians dsta from the cryptographic dats, illustrated by Railwey Wheel I.

Write down th e first upright of the inverse square for the whee unsteckered snd above it the ddagonal. Use the top two lines to'trsnspose'the

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

Fig 10

third lins into numbers. Then rub out the second end third lines.

This rule is not ~~xx~~ absolutely relieblw because of possible variations of designs of wheels end machinee.

The comic strips.

For demonstretion purposes it is best to replece the machine by e paper model. We replsce each wheel by a ~~paperxxstripxxofxx~~ strip of squsred paper 52 squares by 5 equares. The squares in the right hand column of the strip represent the spring contects of tha wheel in neturel order (to make th e squeres of the strip egree with the contects of the wheel one must wrap th e strip round the wheel with th e writing on the strip inwards). The squeree on the left represent the plete contects. In the right hend column is written the diagonal twice over, these being tha 'cryptogrephers names' of the contects es expleined in the lest section; in the left hand column letters ere elso written, end in such e way that squares conteining the same letter ~~xxx~~ represent contects which are connected together. Down th e centre column may be written the numbers 1,...,26,1,..., 26. These numbers ssrve to describe the poeition of the wheel, either the rod position or the window position eccording to how they ere used. The Umkehrwalz is represented by e strip three squaree wide, conteining in one column the diegonel repeated(thie is not entirely essentiel) in another the numbers 1,...,26 repeatsxd, The third column represents the contects;end equeres representing contacts which ere connected contein the seme number (which does nor exceed 13). The machine itsel is represented by e eheet of peper with slots to hold the 'wheels'. In a column on tha right is written the unsteckered diegonal ~~twice~~ ~~xxxx~~ to represent the Eintrittswalz. It ie convenient to repeat ~~thexxxx~~ this elphebet between each peir of wheels. The square bearing tha letter Q between the R.H.W. and the M.W. will bw called R.H.W.'rod point Q' or M.W.'output point Q'. Between the wheels we also write 1,...,26 repeated. These ~~xerxxxtoxdescribe~~ ~~thexRing~~ ere ueed for describing the position of the wheel when tha Ringstellu ng ie given. To underetend how this can be done we need only notice that the same effect es e moveble type

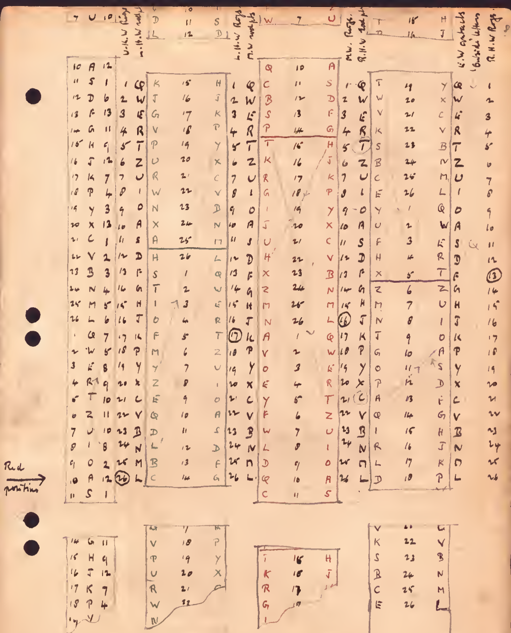


Fig 11

Set up of Railway Comic Strips for the wheel order III I II with Ringstellung 26 17 16 13 and window position 10 5 26 5. As the turnover line is just below the Ringstellung circle for R.H.W the next window position will be 10 5 1 6. In the position shewn the result of encyphering Y is P: the path of the current is traced out. In the column 'Outside letters' we shew the effect of the stecker Q/S.

could be obteined by having windows end pawls which could be roteted roung the wheels in etep. To use thie Ringstellung device on the comic strips we make pencil marke egeinst the numbere on th e fixed eheet end reed off the window positions on the strips opposite these marks. We elso make permanent linee on the etrips to shew where the turnove occurs. When these linee pass the Ringstellung marke e turnover occurs.

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

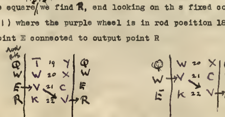
The rule of thumb for the making of comic strips is to teke the last upright of the rod square for the left hand columns of the etrips.

I t may appear rether strange that the letters written on the fixed ehEeet between th e etrips ehould be in the order of the diagonel, rather then eay ABCD... ; the point of writing the letters in this order is that wherever a etrip is put into the machine there wi ie the eeme errangement of letters on either side of it. If this were not eo it would be necessary to heve one 'rod square' for the wheel when in the R.H. position end enoth r for the other positione.

Chapter II. Elementary uses of rods.

Th e rod square and inverse rod square

It is convenient to have a table giving immediately the effect of a wheel in any position. We can make this out in the form of a square measuring 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 14A we find R, and looking on th e fixed comic stripe (Fig 11) where the purple wheel is in rod position 18 we find the rod point E connected to output point R



Rod pos 18 Fig 12 Rod pos 19

This square is known as the 'rod square' for the wheel; its rows are known as 'rods' and its columns as 'uprights'.

We can make out a rather similar square in which the rows are named after the output letters and the letters in the squares are th e 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 xxxx backwards name. That this must happen is obviousfrom the fact that if one proceeds steadily roun d the E.W. as the wheel moves forward one will always be in contact with the same point of the R.H.W. and therefore connected to the same point on the left hand side of the R.H.W. This point is moving steadily round and therefore the rod points describing its position move backward along th e diagonal.

Encoding & decoding on the rods

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

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

	V Y R P S	D M T K W			q
	M A V T N	T C W Z K	O		o
	Z X F G Q	U Y R J M	P M		e
	J W C A E	K G M F Z	U		v
	E V S R P	H L G U I	C		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 E			x
	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 E	H		m
	O F N J G	M A V H R			j
	H J E O C	Z P Q X Q			t
	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		r
	W O M Z A	C F S V U			f
	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 V S R S	Q I D B H	F N O C G	L V A U P	Z M L R Y T	h
N V U P R	B D T Y J	Q H I O V	W G M S X	R X A K C Z	n

First R.H.W rods up

2nd R.H.W rods up

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

Fig 13

```
12 13 14 15 16 17 18 19 20 21 22 23 24 25 26                  12.
M A U G E J C V L . . . .                         s
W V R C S K D U P A . . .                         n

N G X H A C F O W V . . .                         q
V K D B H S R N K . . .                           e

E U P A I M V J N . .                             p
L P G U Q X T W O . .                             z

Z R F Y G O X D I Q . .                           l
D E L X W Y O H A . .                             v

R Q C E X A J S Z K O . . .                       b
I Y S O L B K M J Z                               y

O J T P B N W F T E X . . .                       f
A R B I T D Q G Y X . .                           o

H C J S V G A E B . .                             w
K Z Y N M E G Z R . .                             g

F S W M Y Q P I G O R . .                         c
G M K F Z L Y R Q . .                             t

S I H R K V B Q D R W . .                         d
J O E V U R S L F P Y .                           i

T N O Z F W H X C M A . .                         a
P F N J D 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
```

Deciphering of message 10   First set-up of R.H.W rods.

```
14 15 16 17 18 | 19
    Q  S  Z  V |
    D  E  U  T |
```

Fig 14

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
O	M	T	L	C	Z	N	X	F	U	L	S	I	H	R	K	V	B	Q	D	R	W	Y	J	A	P	d
T	B	C	D	O	E	S	W	P	N	Y	G	M	K	F	Z	L	Y	R	Q	I	B	A	H	J	X	b
R	G	S	T	F	R	X	L	C	J	Q	Y	H	I	W	C	Z	E	A	M	D	K	P	V	U	M	u
S	E	M	P	D	T	J	F	X	O	V	Q	W	Z	K	O	U	N	C	H	B	G	R	A	T	L	k
E	N	O	Q	B	J	A	E	G	S	P	U	X	M	L	R	H	U	T	V	Y	F	C	D	W	I	h
A	C	P	M	G	Q	Z	U	S	V	G	D	E	L	X	W	Y	O	H	A	T	J	I	R	B	K	v
K	I	N	R	M	X	T	B	Y	D	Z	M	A	U	G	E	J	C	V	L	S	E	Q	P	H	O	s
U	W	B	I	L	V	H	O	W	F	A	K	Z	Y	N	M	E	G	Z	R	C	P	D	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	r
H	I	Z	G	T	C	Q	V	K	W	X	J	O	E	V	U	R	S	L	F	P	Y	B	I	L	N	i
P	T	A	S	H	L	P	J	U	R	N	Z	B	F	Y	G	O	X	D	I	Q	C	G	M	V	E	l
D	F	K	W	X	P	O	Z	L	I	M	H	C	J	S	V	G	A	E	B	J	Q	N	T	X	U	w
M	A	W	N	K	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	H	K	H	Z	E	B	T	V	D	P	F	I	Y	S	U	L	X	F	N	C	m
N	V	F	A	R	D	E	Y	M	X	H	L	P	G	U	Q	X	T	W	O	N	S	J	K	C	Z	z
F	U	H	Z	V	W	B	P	E	C	K	A	R	B	I	T	D	Q	G	Y	X	N	O	Q	M	J	o
X	Q	J	E	I	O	F	N	J	G	T	W	V	R	C	S	K	D	U	P	A	Z	M	Y	D	B	n
C	H	I	Y	J	B	D	M	R	T	O	X	D	A	Q	N	P	L	K	U	F	I	E	G	Z	W	x
J	O	X	K	N	F	L	T	Z	A	C	F	S	W	M	Y	Q	P	I	G	O	R	H	U	E	V	c
V	Y	L	H	W	U	I	D	B	H	F	R	Q	C	E	X	A	J	S	Z	K	O	T	N	P	S	b
R	L	Y	F	Z	K	G	C	A	B	W	E	V	P	A	I	M	V	J	N	H	T	S	Z	Q	D	p
G	P	E	C	Y	A	V	Q	O	L	J	V	K	D	B	H	S	R	N	K	W	M	Z	C	I	R	e
Q	X	G	U	T	H	V	S	N	E	R	I	Y	S	O	L	B	K	M	J	Z	D	U	W	F	T	y
I	J	U	B	E	N	Y	R	V	P	S	T	N	O	Z	F	W	H	X	C	M	A	W	L	K	G	a
L	Z	Q	V	U	M	C	G	I	Q	D	O	J	T	P	B	N	W	F	T	E	X	K	S	Y	A	f
Z	S	D	J	Q	Y	K	I	T	M	U	N	G	X	H	A	C	F	O	W	V	H	L	B	R	Y	q

Second set up of P.H.W rods.

First set up. K

										B	S	C	18	19	20	21	22	23	24	25	26
F	K	S	J	I	T	Q	N	Y	L	Q	S	Z	V	I	D	Y	M	P	N	E	X
D	A	K	I					U	F	A	N	N	H	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	I	N	E	N	A	L	A			

Third setup.

Pag 15

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

QSZVI DMFPN EXACM RWWXU JYUTY 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 ~~window position~~ machine should be set to the window position 10 5 26 1 and the deciphering then begun. We first work out the turnovers in terms of rod positions. Wheel II has window T.O. E-F i.e. 5-6, and since the Ringstellung for this wheel is 13 the rod T.O. is 18-19. The middle wheel window T.O. is ~~MN~~ 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 ~~the rod position of the R.H.W.~~ over the letters of the message the rod positions of the R.H.W. at which they are to be enciphered, remembering that the ~~position~~ window position at which the first letter is enciphered is not th e 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 M.W. set to this position)They are qo, ev, ba, kg, sx, wo, mj, td, ~~px~~ pr, fi, yu, zl, ~~bx~~ hw. From these we wish to obtain th e connections between the right hand wheel rod points for all relevant positions of the M.W. If we set up the rod rods

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

Fig 16

message with rod position + T.O.s

according to tha pairs qo, ev,... (see Fig 13). In any column of the resulting ~~column~~ 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 ~~t~~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 conatations when the U.K.W., L.H.W., and M.W. have the positions 10 14 10 and the R.H.W.has the positions given at the head of the dolumn. We can therefore use ~~it for~~ 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 (FIGS 15)

Chapter III, Mathods for finding the oonnections of a maohine.

Alphabete and boxes

For eny position of the wheels of e maohine tha lettere of the ~~alp~~ alphebet oan ba put into 13 pairs so th-t th e reeult of enoiphering one member of a pair is the other member. These peirs are usually written one under the other and oelled 'the alphabat' at tha position in queetion. Thus tha alphabet for the wheel order Graan Red Purple and rod position 10 14 11 17 is

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

Tha ordar in which thasa are written ia immaterial.

When we heve two alphabete to deal with it is aometimes helpful to desoribe both alphabets eimultanaously in the form of a'box'. Take for instanoe th e two alphabete

κ	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 e box from thesa wa ohoose a letter et random, say T, and ~~look for it in~~ write it down with ita partner in the first alphabet, Y, following it, thus TY; we than look for Y in the eaoond alph abet and find it in YK; we write the K diagonally downwarde to th e left from Y, thus TY
K ; now we look for K in

```
the first and finding it in KU write   TY . From this we get to
                                       KU
TY  and  TY , but now if we were to continue the process we should
KU       KU
V        VM

get TY
    KU
    VM
    TY
    KU
    VM
    TY
     .
     .
```

We therefore draw a line, select a new letter, R say, 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' (αβ 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 form the same alphabets can always be transformed into one another by a combination of the processes

i) Reerrenging the order of the compertments

ii) Moving e number of lines from the top of tha compertment to the bottom, the order of tha lines remeining tha same

iii) Rotating e compertment through 180° ebout ite centre, end then roteting eech letter of it through 180° ebout its centre .

At first eight it would seem possible that in meking e box one might reach a etete of affeirs like this

```
AB
CD
E.
```

and thet EA occurs in the first elphabet, end one would not than know whet to do. This is not ectuelly possible es EA in th e first elphabet would contredict AB, For the seme reeson it is not possible to heve E coupled with eny othar letter which ehs alreedy occured.

If we think of the columns in a compertment of e box we see thet the effect of going down the left hand column of e compartment, or up the right hend column gives tha result of enciphering e letter with the first elph ebet end then enciphering the result with the second. Consequently if instead of being given the alphebets we have the result of this double enciphearment we shall almost have the box. We shall not know how much to slide the opposite sidee of a compartment relative to one enother, end in the case of compartments of equel size we shell not know how to pair off tha sides.

The effect of enciphering first with α then with β I shell call 'the permutetion $\beta\alpha$ ', likewise the effeet of enciphering with α than β then γ will be celled $\gamma\beta\alpha$. For these permutations there ie a notetion similer to the boxes. However this kind of 'generel box' does not enable one to recover the original elphabets. It is elso more oonvenient to write them horizentelly (the seme epplies to ordinery boxes, but the tradition there is firmly established). As en exemple of the notation

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

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 th e compartments of this box will be the same as in the original box: in fact the 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 D G Y T N B H F I K O L U E M S R Q C J A V X W P
```

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

α'	β'		$\alpha'\beta'$
AL	AJ	and the box	CW
PI	EU		KJ
TQ	IV		AL
BZ	~~[illegible]~~ HF -LC		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	[illegible]		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(ssy), and then a substitution with the required property will be the one which transforms letters in corresponding positions into one another.

The sizes of th e compartments in a box, and the lengths of the brackets (cycles) are important, as they remain the same if all th e letters involved are subjected to the same substitution,(which might be a Steckering). If we write down the lengths of the cycles of a substitution 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, eith er by the lengths of the compartments or by the numbers of letters in them. 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%
	66.8

The phenomena involved

Before trying to explain the actual methods used in finding the connections of a machine it will be well to shew 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 ~~XREAXFKAX~~ REA FKA WMA and also at REB FKB WMB then there is ~~a~~ at any rate one substitution which will transform the alphabet REA into REB, FKA into FKB etc. The substitution is that which transforms the letters of the column of the rod square corresponding to position A into the letters on the same rod square 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 th e 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	NP	QD	PG	UL	FU	UL	FU
HG	JM	NL	EU	ZF	HB	NK	EZ	KN	ZE
CD	AG	GC	MA	RN	VE	HG	JM	RT	VX
YV	KL	ZR	HV	VJ	LN	CD	AG	WI	ID
FS	BY	IO	DC	OC	CA	MQ	SP	PB	TW
RT	VX	PA	TQ	KL	ZU	JZ	NH	YV	KL
QM	PS	BW	WI	GS	MY	RT	VX	JZ	NH
WI	ID	TV	XL	BY	WK	VY	LK	FS	BY
BP	WT	SY	YK	IP	DT	SF	YB	GH	MJ
AO	QC	MD	SG	HM	JS	WI	ID	MQ	SP
JZ	NH	EF	RB	AU	QF	OA	CQ	DC	GA
NK	EZ	UX	FO	XE	OR	PB	TW	OA	CQ

The substitution which will transform REA into REB, FKA into FKB, WMA into WMB, the box $\begin{matrix}\text{REA}\\ \text{FKA}\end{matrix}$ into $\begin{matrix}\text{REB}\\ \text{FKB}\end{matrix}$ and $\begin{matrix}\text{REA}\\ \text{WMA}\end{matrix}$ into $\begin{matrix}\text{REB}\\ \text{WMB}\end{matrix}$ 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 B M J D N Z U S 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~~ a 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~~ or the boxes made from them, in such an order .

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

REA	REB	FKA	FKB	WMA	WMB
AO	AG	AP	AM	AU	AC
BP	BY	BW	BR	BY	BH
CD	CQ	CG	CD	CO	DT
EX	DI	DM	EU	DQ	EV
FS	EZ	EF	FO	EX	FQ
GH	FU	HK	GS	FZ	GP
IW	HN	IO	HV	GS	[illegible]
JZ	JM	JQ	IW	HM	IX
KN	KL	LN	JZ	IP	JS
LU	OR	RZ	KY	JV	KW
MQ	PS	SY	LX	KL	LN
RT	TW	TV	NP	NR	MY
VY	VX	UX	QT	TW	OR

REA FKA	REB FKB	REA WMA	REB WMB
AO	AG	AO	AG
IW	SP	CD	PS
BP	NH	QM	JM
CD	VX	HG	YB
MQ	LK	SF	HN
JZ	YB	ZJ	LK
RT	RO	VY	WT
VY	FU	BP	DI
SF	EZ	IW	XV
EX	JM	TR	EZ
UL	CQ	NK	UF
NK	TW	LU	QC
HG	ID	EX	OR

and th en make from th e boxes on the right. From the right hand pair of boxes we se that E must become either O or R in the substitu tion, and we can try both hypotheses out ~~in~~ by arranging the first two ~~alphabets~~ boxes correspondingly. If the first box is left as it is, the correspon ding rearrangements of the second are

	..	..	
	..	..	
D	HN	AG	
MQ	PS	SP	NH
GA→	MJ	VX	
	ZE	LK	
	UF	YB	
	OR	RO	
	BY	FU	
	KL	EZ	
	XV	JM	

The first of these rearrangements is impossible. It implies for instance that in the substitution C becomes H and M becomes P but ~~whereas~~ in the third box C and M occur on opposite sides of a compartment while in the fourth ~~they~~ H and P 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 ~~FKB~~ REB 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 REA FKA . The only possibility is th at BH arises from FZ, and we can check th e result with the AG.

& complete

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

1	34	6
Z	DJ	Y
D	KW	P
G	EC	A
Y	VX	I
T	CD	E
N	FA	D
B	ST	R
H	ZG	O
F	HZ	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	GU	H
C	IY	B
J	XK	F
A	PM	Q
V	LH	U
X	JE	O
W	RO	G
P	AS	L

It is

(ZDKNFH)(GEOTCIUBSMWRYVLQ)(JX)(AP)

and the substitution which transforms the ~~third~~ 4th column into the ~~fourth~~ 6th is

(JYBNSLZWPTRXIVMQ)(CADEOG)(HU)(FK)

These two substitutions are of the same 'shape8, and if we write them like this

(YVLQGEOTCIUBSMWR)(NFHZDK)(PA)(JX)
(JYBNSLZWPTRXIVMQ)(CADEOG)(HU)(FK)

each letter in the lower line is below the letter which is three places further on along the (QWERTZU) 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~~ back along the diagonal and then move the ~~whole~~ result three places to the right and three upwards we get the fourth and sixth columns.

A rather similar phenomenon is useful when we know the diagonal of the machine. In such a case we can make a correction to our constatations transforming them into connections between the contacts on the right of theR.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 withtwo 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 (CD)(FR)(TV)(XO)(JK)(WQ)(AG)(PY)(BZ)(HM)(IL)(EN)(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

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

to the ordinary alphabet. It is

(FR)(TV)(BG)(DQ)(IO)(XY)(WZ)(AS)(HN)(UK)(LP)(CJ)(ME)

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. 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 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)(OT)(QJ)(KZ)(HS)(

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

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

The sage

Suppose that one was left alone with an enigma for half an hour, the lid being locked down and the Umkehrwalz 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 crossing out the ones 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 th e number of possible different ~~sx~~ solutions. Now the n umber of possible different diagonals is ~~approx~~ 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 Umkehrwalz 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 th e 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~~ly~~ 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.

Date for sage

✓AAA	AAB	✓AAC	AAD	✓ABA	ABB	✓ABC	ACA	✓CAA	BAA	✓CAD
AL	AD	AI	AM	AK	AE	AW	AM	AS	AQ	AZ
BS	BG	BY	BS	BO	BS	BV	BP	BO	BV	BN
CE	EK	CT	CH	CF	CR	CZ	CE	CP	CH	CO
DH	FV	DM	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	LQ	NU	KT	KN	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

✓ACB	ADA	DAA	CAC	BAD
SO	UQ	MJ	HX	MA
ZJ	LB	IL	VS	EU

BR
TZ

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

AAA ABA	AAB ABB	AAO ABC
AL	AD	AI
SB	QO	HU
OZ	MW	GX
TY	ZG	DM
MF	VF	TC
CE	LU	ZK
DH	YJ	RS
WQ	PS	NF
GR	BC	OJ
NJ	RX	EV
PV	TI	BY
UX	NH	PQ
IK	KE	LW

ACA	ACB
AM	SO
BP	ZJ
CE	
DW	
FG	
HL	
IZ	
JO	
KQ	
NU	
RS	
TX	
VY	

CAA	CAC
A S	HX
BO	VS
CP	
DJ	
EU	
FQ	
GV	
HY	
IL	
KT	
MX	
NR	
WZ	

AAB
We want to rearrange the box ABB in the way that was done at
A AA
the bottom of p. .The substitution which transforms ABA
AAB
into ABB must also transform two constations of ACA into SO and ZJ. The only constatations ~~frm~~ of ACA from which SO could have arisen are LH, ~~OE~~, 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.

~~A similar objection applies to WS~~. However if we rearrange it so that OS arises from VY we find ZJ arising from IZ. We can similarly arrange $\overset{\text{AAC}}{\text{ABC}}$ to fit with them and agree with CAA and CAC, and fit $\overset{\text{A AA}}{\text{CAA}}$ to fit onto $\overset{\text{AAD}}{\text{CAD}}$ agreeing with BAA and BAD.

Rearranged AAA A BA	 AAB ABB	 AAC ABC
AL	VF	GX
SB	LU	DM
OZ	PJ	TC
TY	RS	ZK
MF	BC	RS
CE	EX	NF
DH	TI	OJ
WQ	NH	EV
GR	KE	BY
NJ	AD	PQ
PV	QO	LW
UX	MW	AI
IK	ZG	HU

AAA CAA	AAD CAD
AL	UZ
IK	AM
TY	YV
HD	QF
JN	DR
RG	TI
VP	EO
CE	CH
UX	XK
MF	PG
QW	LT
ZO	SB
BS	NW

Rearranged AAA CAA	 AAD CAD
AL	TL
IK	GP
TY	KX
HD	HC
JN	OE
RG	IJ
VP	RD
CE	FQ
UX	VY
MF	MA
QW	ZU
ZO	WN
BS	BS

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   YSKX   WNEU   UMAV
LFXL   MBRM   QHVZ   XWIY
SLDS   FCSA   GKBJ   IZHG
BUMB   CRNF   REYI   KGUP
OYTN   EXFQ   NAPE   JDQO
ZJCW   DTOC   PQLD
TPZK   HIJH   VOWR
```

The substitution which transforms the letters in the first column
o
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)(LDQ)(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 th e second is the same as that which transforms the second into the first, this substitution being a slide of one on the diagonal. Clearly ~~YI~~ (FX) in the ~~third~~ second has to fit under either

(~~FK~~ GK) or (~~XF~~ KG) in the first; if F is under G we cannot fit the second and third together, for F occurs in a bracket of 13 in the third, and G in a bracket of 8 in the second. If F is under K we can fit the three together like this

```
(AVOYSLFCREXWN)(BUM)(ZJDTPQHI)(GK)
(SKBRNEYTOWIJC)(QLD)(VGUMAPZH)(XF)
(NFQOCWRMBJHGT)(PEU)(KXLDSAVZ)(IY)
```

The diagonal is

APQBORYFKVZHIXGJWELUDMTCNS

Of course we do not know where tha 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 names. 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 comic 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 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 in 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.

It can only be done if we have a great deal of information about actual window positions and Ringstellung, e.g. if there is a Herivelismus or if the letters of the Ringstellung are restricted to be alldifferent and notwo consecutive in the alphabet except Z and A.

Our set of rods is

IZHG	z
HIJH	h
XWIY	i
EXFQ	x
GKBJ	g
VOWR	j
REYI	w
LXFL	e
KGUP	l
JDQO	u
MBRM	d
OYTN	m
FCSA	t
NAPE	o
PQLD	n
BUMB	s
DTOC	e
CRNF	p
YSKX	q
AVGT	b
ZJCW	o
WNEU	r
SLDS	y
UMAV	f
TPZK	k
QHVZ	v

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
ah	ax	yw	fv
be	bl	ch	es
cu	cw	bd	
dt	dg	px	
fi	ey	gt	
gw	fj	ki	
jn	ko	zo	
kq	ms	vl	
lz	nu	ns	
mo	pt	um	
px	gv	jq	
rv	rh	fc	
sy	iz	ar	

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 Z as standard

AA*AB*AC*AD*

pi	qj	vu	hx
ol	rd	dg	mb
nd	sl	yc	
mc	to	cw	
kx	uk	es	
je	ve	jh	
ws	zy	xf	
vb	op	im	
uh	am	pq	
tr	bn	tn	
qg	wh	lr	
y z	fx	ze	
af	gi	bk	

We now box AA* with AB* end AB* with AC*, end then re-rrenge
AB*
A C* so ~~that~~ es to find the eubetitution which transforms
AA* AB*
A B* into AC* and AC* into AD*

AA* AB*	AB* A C*	AB* AC* reerrenged		
pi	qj	[illegible]	[illegible]	jq
gq	hw	[illegible]	cmx	pc
je	ot	[illegible]	[illegible]	yz
vb	nb	[illegible]	[illegible]	em
n d	ku	[illegible]	[illegible]	ig
rt	ve	[illegible]	[illegible]	dr
ol	sl	[illegible]	[illegible]	ls
sw	rd	[illegible]	[illegible]	ev
hu	gi	[illegible]	[illegible]	uk
kx	ma	[illegible]	[illegible]	ha
fa	zy	[illegible]	[illegible]	to
mc	op	[illegible]	[illegible]	wh
yz	xf	[illegible]	[illegible]	cr

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

[illegible] leezftrdgpjyxniqohukbmwvao

As we edded up to poeition Z es stendard thie upright is the upright for position Z. We can make out pert of the rod equare from it, there being difficultiee ebout where to begin ee before

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

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

				A*	B*	B*	
A*	B*	C*	D*	B*	C*	~~A~~* C	rearranged
ra	es	ay	kd	ra	es	wl	?
bt	bn	bdi	ox	sl	gz	or	
ce	cr	cl		wj	eq	do	
di	do	dr		kg	jk	vf	
fo	eq	ez		zv	tx	nb	
gk	fv	fn		fo	ph	iu	
h y	gz	gs		di	wl	my	
jw	hp	hw		un	or	es	
le	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		<u>ec</u>	<u>my</u>	<u>ph</u>	

Ths left hand wheal upright is

rwdmqxeptznsohkvbgfiyjouel

zhixgjwaludmtcnsapqboryfkv

and under it has baen written the diagonal. This serves to transform A or A* into the Umkehrwalz connections. They are

yv,fs,oe,zw,oi,mu,rj,qx,pk,nd,ht,bg,el ?

'Adding up' method

Most prectical methods of finding the connections of the machine depend on getting a long crib, either by 'reeding 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 hed such s diegonsl). In this case th e 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)x square of average 'corrected depth'

Csll~~ing~~this the 'material measure'. By corrected depth we mean the actual number of constatations, so that this can never exceed 13. As regerds 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 esses the material measure mounts up. With a material measure of 300 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 es-entially the same as we used for finding the middle wheel in the case of the saga. 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 $\frac{K}{F}$ snd $\frac{T}{R}$ 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

Here KF means 'F follows K on the upright'. KF² would mean 'K & F are two apart on the upright' plenty of material we do not usually start to work a hypotheeis unlass there is going to be an immediate oonfirmation, e.g. if TC impliaa RJ from two different parts of the crib. This will mean to say that the conetatations $\overset{T}{R}$ and $\overset{J}{C}$ occur coneeoutivaly twioe over. Alternatively we can say thet $\overset{T}{R}$ occure twice over at a certain distanoe, and that $\overset{J}{C}$ also uoccurs twioe over at the same distance. In order therefore to find these profitable hypotheses we have only to look for repatitions of constatations (half-bombas as they are rather absurdly called) . For this reason and also because later we will want to be able to epot oocurrenoes of a given letter at a glance, we put our materi l as we add it up intothe form in Fig 19 .

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

```
MYC..
NGJ..

RCA..
YID..

DAS..
TTV..

YON..
RMI..

OFL..
VQO..

MUX..
NJQ ..
```

(I muet apologise for it not making senea) .

We dacide to try out tha hypothesde that there is no T.O. in the first eaven columne, and therafore we add up the columns 1-7,27-33,53-59, getting

```
LGN..
MJY..

TBF..
XAH..

FBG..
ZUM..
...
```

	1	2	3	4	5	6	7
A	B	B				H	I
B	A	A	R			Y	E
C		J		N			
D		U	E	Q			
E		H	D			I	B
F	Z		H	H			Y
G			M				K
H		E	F	F	W	A	
I						E	A
J		C					
K					M		G
L	M						
M	L		G		K		
N			Y	C	Q		
O		P				X	
P		O			T		
Q		S	S	D	N		
R			B	U			
S		Q	Q				
T	X				P		
U		D		R			
V							
W					H		
X	T					O	
Y			N			B	F
Z	F						

	27	28	29	30	31	32	33
A	V	U		D	K	B	O
B			P	O		A	P
C		Y		J		R	
D		H		A			Z
E							
F			Y	Z			N
G	J	P			Y		
H		D					
I				M	N	P	
J	G			C			
K					A	T	
L					M	Z	
M			Z	I	L		
N			U		I		F
O				B			A
P		G	B			I	B
Q	X				X		
R						C	
S	O						
T			X			K	
U		A	N			V	
V	A					U	X
W							
X	Q		T		Q		V
Y		C	F		G		
Z			M	F		L	D

	53	54	55	56	57	58	59
A				I			
B	P			J	P		
C		X					
D						L	
E					X		O
F		T	O		J	G	U
G		V			V	F	
H			V				
I		U		A		X	Q
J	A			B	F	U	
K				T			
L	O			Y		D	
M	U		U			V	R
N							
O	L	P	F				E
P	B	O			B		W
Q		Z	X	U			I
R							M
S			Z		Z		
T		F		K		Y	
U	M	I	M	Q		J	F
V		G	H	X	G	M	
W	Y						T
X		C	Q	V	E	I	
Y	W			L		T	
Z		Q	S		S		

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

Fig 19

m l q w e r t z
W L A Q F P E V

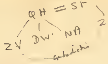
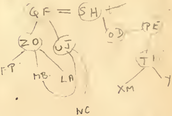


Fig 20



NC

(Rings mean that all [illegible]

Fig 21

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

Fig 22
L

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 $\overset{Q}{S}$ and $\overset{F}{H}$ suggest the two possible starts Q F = SH and Q H=SF (the two strokes meaning a double implication, not equality;). The consequences of the second of these are shewn 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 writtem 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^2- AF^2 confirming JZ,ZO,AQ,QF. When we have checked them all we can write out the upright of the R.H.W.

AQFPEVKYNCUJZODXMBSHTIRGWL

We then have to find the upright of the M.W. To do this we use the same process as we did with the saga. 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 moveable strips with the upright and qwertzu written out on each, and sliding these above the added up crib till the constatations 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 shewn 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	105-111
qp	hx	qs	jn	zm
wb	qs	wj	xv	ti
ef	wu	eg	tr	
ry	ek	th	fh	
tn	rn	rv	ql	
zu	to	zx	up	
ix	zy	um	oy	
os	ia	io	da	
ag	ov	sk	wb	
dm	dj	db	oi	
hv	fm	fy	gz	
jo	gb	pn	em	
kl	pl	ol	ka	

(some of these being supposed obtained from material not yet given)

Boxing these together we get

1-7	27-33	53-59
27-33	53-59	79-85
qp	hx	qa
lk	zy	ks
ef	fm	db
md	uw	wj
jo	jd	np
tn	bg	um
ry	ek	eg
zu	sq	zx
wb	ei	vr
ga	ov	th
ix	rn	ry
hv	pl	oi
os	ot	cl

When we fit these boxes together we fail 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 and second alphabets, and that the remainder can be fitted together with the upright wbnhcovrtixlyazqgpfkmseudj

I will ive a aaoond example of tha 'adding up' method for a oese where it is only just poasible to gat tha problam out. The material ia given in Fig 23 all ready added up. Thare are no 'equidiatanoea' (half-bombas with aqual diatances) and eo we hava to make an analyais ehewing all tha oonsequenoae of any hypothaeie that ona latter follows another on the uprigh t(Fig 32). Fob instanoe from the analyaia we see that ~~AXXxHTT~~ AV,HT,NF,ZA, are all oonsequenoas of IM. Tha panoil letters round the outside ~~xxx~~ wera put in to help with the making of tha analysis and were uaed in oonnaotion with oolumn s 32,33 of tha material. Of oourse some of the oonsaquanoas will be falsa owin g to turnover, but as wa e a dealing only with distanoes of 1 we oan hope to neglaot this without h arm. Wa now piok out ~~larg~~ squares with a large number of antriaa in tham and follow out th a further oonsaquanoea of them, making treas ae before, and hoping to find oonfirmations. Wham we get oontradiotions we leave the trea for the present but hava to remember the T.O. possibility . Figs 25-30 Whan we gat atuok we oan aometimea oontinue using oon sequanoes whioh are of th e form th at two lettera are at distanoe 2 on tha upright. For this purposa an analysia of positiona at whioh latters ooour ia usaful (FIg 24). ~~xt~~ In partioular we naed for thia at Fig 30 . Now VW and WY imply VY^2 and PR and RS imply PS^2 and these imply on e another from oolumna 19,21. Wa aleo gat GL^2 whioh starts off another train of ooneequenoes involving another oonfirmation (Fig 31). Evantually we get atuok with the bita of ~~xxx~~ upright

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

Wa might try putting in KA as a hypothesis, ~~Thixxxxx~~ aftarwards try KB ato.(KA appears at firat to giva oonfirmations, but thase are bogus. Th e only reliabla rula about oonfirmatione is to ~~see if one can leave~~ by leaving a oonst tation out and than see if it oan be infarred from the hypothesie). Wa might also try putting in as many new constatations as possible which are consequences of those we have and our available information about the upright, and then start off afresh with some new distance on the upright, say 5. But there is a quigker road to success. Note the constation $\overset{H}{J}$ in 1 and $\overset{G}{I}$ 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^{16} . If this is so we have this as part of the upright

FGIL.O....UHJK

Hence $OH^{\underline{6}}$ which implies PK^{6} giving us this as upright

FGILNOQPRSUHJK

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

```
1     4 5 6 7 8 9 10 11 12 13 14 15    17 18 19 20 21 22 23 24 25 26 27 28    31 32 33
T W G J C N I U J X C S L S K K B N V G W I T S U Q I U J A U L J
R I D E Q I Z W F S N Z E Y H T H U P K R J R R G U D D V T F M I

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

Fig 23

A	5 8 24 30
B	2 11 17
C	5 11 24
D	3 16 28
E	3 4, 13 15,
F	7 9 25 31
G	3 11. 14. 15 17 20 26
H	1 10 15 16 17 20 26
I	2. 6 7 18 17 22 26 27 32 33
J	1 4 5 9 22 28 29 33
K	15 16 19 20 23 29 30
L	13 18 23 25 32
M	6 7 8 27 32
N	6 11 14 18
O	9 27
P	4 9 15 19 23
Q	5 26 31 33
R	1 21 23 24 28
S	3 10 12 16 21 22 24 29 31
T	1 12 14 16 27 30
U	2 8 19 25 26 28 31 33
V	4 6 19 29
W	2 8 21 30
X	10
Y	10 14 20 21 22 32
Z	7 12

Fig 24

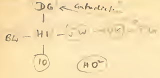


Fig 25

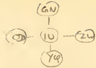


Fig 26

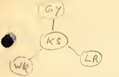


Fig 27

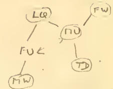


Fig 28 MF² — FJ²

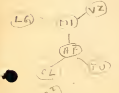


Fig 29

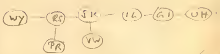


Fig 30

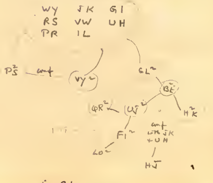


Fig 31

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
13																										
14																										
15																										
16																										
17																										
18																										
19																										
20																										
21																										
22																										
23																										
24																										
25																										
26																										

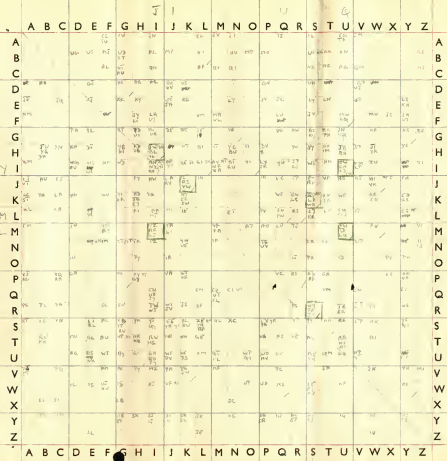


Fig 32
Consequences of hypotheses as to successive letters in upright.

Clicks at twenty-six-distance

This is a method for finding the connections when we do not know the diagonal. It is very similar to the beginning of the easy, in principle. It depends on making hypotheses about pairs of letters being on the same rod, and drawing conclusions 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 migh t make th e 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 Fand 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 easy method. The amount of material needed is very great. We adopt a measure similar to the one for 'adding up' viz

(length-39) x square of average corrected depth

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

When th e material is sufficient we avoid taking h ypotheses at random, and choose ones wh ich we can see 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 E follows R 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 hypotheses is correct is 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 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 shewing how far on the other occurrence is. This plan also shews 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 HE at b,II and b,X and JE at j,II and j,X. The first pair of these constatations shows that there must have been a pair in common between the coupling at b,II and b,X . Likewise there must be one in common between those at j,II and j,X . It is therefore fairly likely that there is no turnover between b,II and j,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 fix it ~~fairly accurately~~ with no doubt at all, as occurring between 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 part 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 virtually certain. The consequences of these hypotheses are shewn 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 confirmation. With b onto h we find that both of the first alternatives of the one hypothesis contradict both alternatives of the other. With d onto j we manage to connect the two ~~par~~ hypotheses together and with e onto i we fail to connect but ~~the~~ one of the hypotheses confirms itself. The information we have obtained about the rods from this is expressed in the Fig41a. In order to avoid bogus confirmations in what follows it is as well whenever we make a deduction to cross out ~~th~~ one of the constatations 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 constatation, 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 to have 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 rod are not too incomplet

In the present cese we cen teke the columns c,d,f,g,j,k; giving them the numbere 3,4,6,7,10,11 instead of the lettere thie correeponds to p+3 , q+3 , t+6 , u+4 , r+1 . In order to get these columnes we look on Fig 35 for suitable hypotheeee to work in order to edd in the extre columne. These hypotheeee enable us to write in extre lettere in the Fig 41a and we continue to write in lettere in tnie figure until we reech e congirmetion or e contrediction. Until we reech e confirmetion it is es well to differentiete the letters thet are certain from the reet. The hypotheeesthet we ectually used were : c into g IQ=SE; g into k XE=ND. After a coneiderable emount of work our rode look like Fig 41b. The linee crossed out ere onee thet heve been amalgemeted with othere. We now think we cen etert to look for the diagonel, end therefore make up the permutatione treneforming c into f, d into g , f into j end g into k. The notation ie that of p 19 , except thet we ere mostly unable to complete the breckets, and leeve dots.

c into f

...DCYQFVJZTAXHIN...SGDPR...KE...LUB...M...W...

d into g

...KWCM...ANSY...GLIJ...TUQ...DEBXOR...FPZV...H...

f into j

...QOTK...UHJNGR...BSZW...PFA...CXIM...YD...E...L...V...

g into k

...IND... (EX) ...KF...TYHZ...MQBLJWURG...PA...C...S...O...V...

We heve nowto write the c into f permutation over the d into g permutetion, end the f into j over the g into k in such e wey that a given letter in 'c into f and, in f into j' stande over the seme letter in 'd into g' end 'g into k'. To get e etert on thie obaerve the configuration of the ringed letters. Thie suggeete thet we errenge the permutationa in thia wey

```
 DCYQFVJZTAXHIN
DEBXOR
 (YD)
 (XE)
```

Thie ia further oonfirmad many timee, and we get the permutetions errangad like thie

```
(DCYQFVJZTAXHIN)     MSGOPR
(EBXORANSYGLIJD)    KWCMTUQ

(YD)  QOTK   UHJNGRCXIMPFA
(XE)  OTYHZ    INDMQBLJWURG
```

giving us the partial diagonal slide of 1

...BCSZ...EDNJIHK...LXYTOQRF...WMGAV...UP...

Z must ba followed aither by ~~either~~ E,L,W,or U . If it ia followed by U we get

```
     LUB
    FPZV
```

and tha diagonal alide as

(BCSZUPLXYTOQRFEDNJIHKWMGAV)

If Z is followed by L we have tha bite

```
 MSGOPR   KE     LUB  W
KWCMTUQ   H    FPZV
```

to fit together, whioh wa find ~~impossible, quite apart from the initial~~, oan only be done like this

```
(KEMSGOPR) (BWUL)                  (KEWLUBMSGOPR)
(HKWCMTUQ) (FPZV)  or like thia (HFPZVKWCMTUQ)
```

giving tha diagonal elidee

(EDNJIHK)(...)

(UP)...

both of whioh are impoesibla. If Z ia followed by W we have the bits

```
 MSGOPR KE    W   LUB
KWCMTUQ,H   FPZV
```

which fit together only as

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

end as before the $\overset{E}{K}$ configuretion makea this impoasible. We oannot hava Z followed by E because of the impossibility of fitting $\overset{KE}{H}$ onto

```
      with K over Z
           |
      FPZV |
```

. The diagonal is therefore

BCSZUPLXYTOQRFEDNJIHKWMGAV

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 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 M.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 as 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.

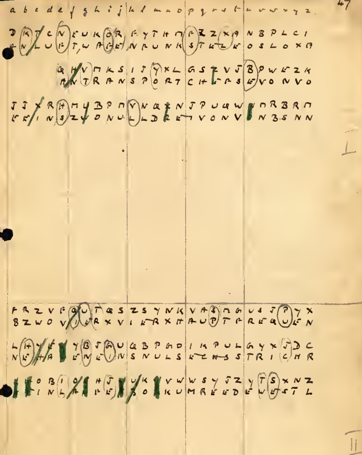

a b c d e f g h i j k l m n o p q r s t u v w x y z
D K T C N E U K O R E Y T H M E Z Z X A N B P L C I
A N L U E T W A E E N E U N K S T K L K O S L O X A
Q H V M K S I J Y X L G S Z V J B P W E Z K
A N T R A N S P O R T C H E A S E V O N V O
J J X R H M Y B P M V N Q X N J P U Q W W M R B R M
E E I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

Fig 33. Material for 'Circles at 26 distance'.

Letters across top give relation with right hand wheel position, and the pieces fit together in order of Roman numerals. Green vertical strokes eliminate merely confirmatory substitutions. Red ones eliminate contradictory ones. Meaning of slanting strokes explained in text.

This Fig continued on seven further sheets

```
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

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

Y S   O V   Z D   L H   J   J D     N A H H F   G J E P B B
O M   I N   S E   N S   B   E N     T O E J S   O L A J E I

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

III

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

                                  ~~W Z X D U A G E S K J~~
                                    W Z X D U A G C S V X J
                                    A N T R A N S P O R T C

O   Q C Y   M X V D I   A Q W P H     L L G C   X   C   W W
N   S E H   S N U L N   U L L V R     E S D R   E   D   E M

Q   I   Q     I Y   Y   Q M J           N   X   Q Q   E M
T   U   D     E I   E   F A H           S   E     H   L T

  C B G Y Q     A X     B T   N E   S O E S     I K   O I H
  M N O-O O     R O     I H   I M   V V V M     O-O   W A R
```

IV

Prog 33 cont.

```
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 P U S Z | U J X Z O | Y A L E W | U V R V L | Y X Z E K G
K L L E A | B S E T Z | E N X H A | P E N B E | Z I R K S W

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

                                      T P H I | B W Q B C O
                                      U U U J | A G E R A N

W X ▮ I V | V E G G J | Q V ▮ L I | O ▮ ▮ ▮ ▮ | S R V O W J
N U ▮ N U | L E T R K | A R ▮ M E | Y ▮ ▮ ▮ ▮ | N Z I N E I      V

R O I J ▮ | H X ▮ ▮ M | V U Z ▮ L | K N ▮ ▮ ▮ | ▮ O W Z T E
V I K W ▮ | I T ▮ ▮ N | U L S ▮ C | H S ▮ ▮ ▮ | ▮ U L U M R


D I W ▮ X | N Y P R I | N G S Y V | T X R V S | G D N A J K
E L L Y B | L E I B T | Z U M V E | R K W H R | M I T P L U

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

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

R Q Z B ▮ | C A ▮ ▮ E | D R T Q A | V Y C E O | V ▮ T G R J
N S V I ▮ | R V ▮ ▮ R | L T R S O | N S T W I | E ▮ N Z W O      VI

▮ R ▮ ▮ N | J R ▮ ▮ Q | ▮ ▮ O B G | ▮ N P ▮ ▮ | ▮ S Y Q U W
▮ X ▮ ▮ S | I S ▮ ▮ B | ▮ ▮ Y M I | ▮ U S ▮ ▮ | ▮ R G R A D
```

Fig 33 cnt

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

L G K L V L Y V X W N K M Π
G Z E G E N B E S E T Z T

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

A N Z S P W T Y K G N Z K N B N Π O K D Y C Π F
X S T A N D O R T M L D E N U N D A F F X T X N

VII

~~O L A F N O H V I O E K Q C Y B C A H H C L L C O N~~
~~F O S K I T O G R U P E~~

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

Q Π
W X

Q I4 T Π D Y P B R G Y Z Z Z V J X A V Z
Y Z I S U L N U L V I R Π Π B B B Y R E

Fo 33 ml.

```
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

X T S O N  P Q Z X Y  H N S K
  E L N S     C H S    U L

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

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

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

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

VIII

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

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

X C R S  Q Y J B O  G S C C U  A G X
N G E H  N D A N T  W O R T N
```

```
~~A I E A Y D E V G D H U W S L O H J W W T U H L S E~~
~~W O V I E R X V~~
~~S Z W O V I~~
W A I L A  Y N E V G  A U W S  L O H J W  T U H L
B I S Z W  O Y I E  X I E R  X E N S  U E N F

G R N M  H  D C L W D  A L B I  A Y T O
L N U L  T  T Q M Y S  C H T X  I R B I
      U L
```

IX

Rq 33

```
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

L D T Y Z   L S T N B L S K M P   N I E V T V H Y K
Y N N A R   I K W E A E N Z A H   R E I C H E R K R

J M G W N P Y W J J G U X W I R C J W G Y F Y Y B
O R D N P R D W E S T   I N S Y W O L K   N C I R
```

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

X

```
Y H P N X Y X Z O O Y D R S F F T T   N N G I N U D
S E I   S   U L N U L N U L M K   E       Z S C H
                            N U L M   T E R

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

Q V K B G N M   L U   A Z H B       F   O Y F B   Q K
  O P F E V O   V O   B D U U       I   F U N K   P
```

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

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

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

D   D T T S E W L H J Q Z X   U G K N
N B E T R E I B E N Y   E B   L

    A D T D F C C       U D E J   O T Z C W     N C
    C E E A U F A       N T I K   C H A L T     S E
```

XI

Fig 33 wr

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.

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

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

~~E B K H P L S E A A E B N U E S M B V H Z J J V V 1~~
~~T E N P A T R O N E N L U C I Y Y D R E I Y S E C H~~

XII

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

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

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

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

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

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

XIII

Pg 23 wd

~~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~~

~~K V K Q D N Y H E K R H H N D Z A J B N A V H B D F~~

~~Z I N N A R V I K A U S G F S C H A L T C T~~

```
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

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

D P G Y C   Y D H T Y
H T Z W H   S N X K L

X   J R Q D T   J U   Z T Z   Y P F T L A   D D H
N   F U E R R   N N   I J S   A C B E R     E N L

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

IV

```
V C N P B B S Z U L Z U C A I Q B N V P P N H G X F
H I E R H E R B E S T I N N T E S G E R A E T I N H

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

K J O J   P P   W X K U K   I     G G I Q Y V H V
N E R N E   N S   L L   I   S     S Z W O N U L L
```

XIV

Fg 33 wk

	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
I	KN GA 8 7 HS 9	TV OF RE 7 5 5	VL YO 4 5 14		PS XL 11 14	BE 14
II	HE IL 8 8	IQ EU AT GI 4 11 8 11 BN EJ 4 8			PS 4	TW ES CJ 9 5 9 PU 10
III		DE LN ER 3 2 8		KS 3	PH LU 12 4	KJ BT NX AF HN 8 11 5 3 8 BI 3
IV	BN 3	XN NO 4 8 EI 1 7	DE 4	AW 1	NS KI 1 6	EK EW 1 1 NO 1
V	HJ EK 7 9	HO LN 2	RV DK 2 2	EH AW 8 EI 6	FU UV NR KL 5,10 3 5 10 HK NS KT 3 10	LN EK EW LT 2 6 RZ NO 8
VI	FX NO NS 8 2 2 KV 2	IQ DE FO PZ 2 BN ER RS 8	OY	AK 9 QS	EY PS 6	BI AF DK 6
VII	BL EK 2 1 DN	IN NY HO IR 4 2 3 DL 6	BL RV DK 4		LU HN 5	ES LN
VIII	NX KT IS NO NS 7 4 1 KV AQ EK LS 4	EQ PZ 1 GR TV 1 NX	UW DE		HK EV	NX
IX	CU JU IS NO 1 6 1 GL KN HS	KQ EI TW GR NY 6 1		NU 3	KW 5	HN 3
X	CU KH NO IL	UY AT TW IR 4 EJ	RU 3 KW		FU NR KI 5	CU SZ 2 5
XI	OH 1	IN PR HO KI	BL	KI		KJ TW LJ LT HN HN
XII	HJ ET LS HO 1	AN 1	AE 3	NU	CR AY HN 1 FS	DK CU PU HN
XIII	LS	NU PR DL GI AN 2 EU	RU	EH UW 1	AY 1,2 CR	RZ
XIV	FX NO EK	UY RS	KW	UW	AY KW	AT AR HL 1 1
XV	CU JU NX	NU KI	AE LV	AK	AY KT AK EL FU FH NR	BE AR HL SZ

Fig 34

	A	B	C	D	E	F	G	H	I	J	K	L	M
A					LV NO		GL NY		CV IW		NX LV		
B				KT LS	KW HS	HB IL	NY RS	HE RT	IV VE EI ES				
C							IS KR	BN IPO		IS GR			
D					HOKV NS					HOKV FE LS AN			
E							QA RV	IL RT	IL NO ES TW	NS IZ	QA VL		
F							IU BN				IN WX RL		UY EW
G									EV GI	RL EA LR CD	YN IE		BR
H									RT EI			HO RX	HO DH
I										DI RC			OF YO
J													RC YO
K													
L													RV DK
M													
N													
O													
P													
Q													
R													
S													
T													
U													
V													
W													
X													
Y													
Z													
	A	B	C	D	E	F	G	H	I	J	K	L	M

F735

d into j

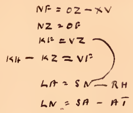


Fig 36

d into j

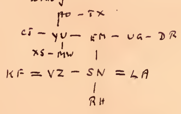


Fig 37

e into i

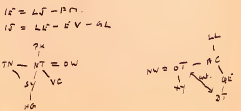


Fig 38

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
13																										
14																										
15																										
16																										
17																										
18																										
19																										
20																										
21																										
22																										
23																										
24																										
25																										
26																										

b into h

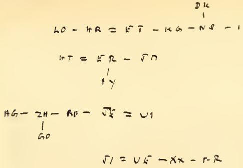


Fig 39

q into j

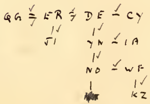


Fig 40

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
13																										
14																										
15																										
16																										
17																										
18																										
19																										
20																										
21																										
22																										
23																										
24																										
25																										
26																										

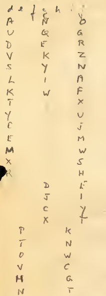
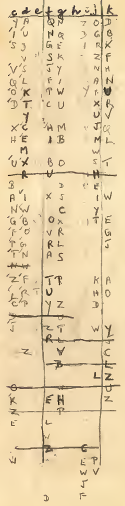


Fig 41(a)

c onto g   1Q = SE

g onto k   XE = ND



Fg ~~42~~ 41(b)

Finding new wheels. Stecker knock-out

So fer we heve been deeling with the problem of getting out the connectione of en entirely new mechine, or one for which we know no more then the diegonel. There is enother problem, thet of finding the connectione of some newly introduced wheels, the old wheels, or et eny rate some of them, remeining ee well: this includee the cese of e chenge of Umkehrwalz.

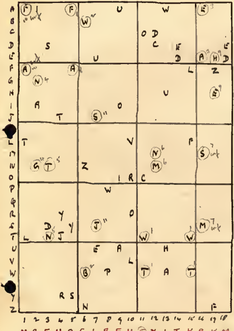
The most hopeful cese for getting out the new wheels ie when one of the known wheels occurs in the R.H.W. poeition. If the mechine hee no Stecker there is no difficulty. We solve some messeges by singda wheel proceesee. Thie will be slightly more difficult than when we know the connectione of the middle wheel, es we shall heve to guess what is seid in three or four different turnovers. However when the R.H.W. rod etert hes been found from e guess in one turnover it doee not teke eny time to teet e mot probable throughout the meesege(the rods on which the verious letters of the meseege occur cen be written down once for ell, end the mot probeble punched out end run over the inveree oblong). For eimplicity let us euppose thet we heve reed the messeges right through. We then heve the couplings in eeverel ~~three~~ consecutive poeitions of the middle wheel, end cen epply the method of p 28, 29 to find its upright.

In the cese that the mechine hes Stecker we need rather more dete, end very much more petience. The sort of dete that one needs is e crib of length ebout 70, or elee one of length 26 end depth 2. The trouble ebout cribs without eny depth is thet one uses up ~~the~~ e greet many of the constetetions ~~after~~ between eech turnover in determining the coupling.

An exemple is shewn of e crib of length 18 end depth 2. This is to be regerded es one of greeter length which hes been cut down to ellow for turnover. The text of the crib ie chown et the top of Fig 42 . We ere teking the worst cese of 13 Stecker. There ere severel helf-bombes in the crib, end we decide to work with TW. We heve to meke 17576 different hypotheses, (epp) correeponding to the 26 poesible different plecee on the R.H.W.

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

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



A	G	2	✓
B	T		✓
C			
D			
E	W		✓
F	O	8	
G	A	3	
H	V	9	
I			
J	L	11	
K	M	6	
L	J	11	
M	K	6	
N	S	4	
O	F	8	
P			
Q			
R			
S	N	4	
T	B	1	← ✓
U			
V	H	9	
W	E	1	← ✓
X			
Y			
Z			

M S F U O G L B F H E Y I J K R K M N W B E F H E L o
Z A C Z G H N A P J B G W A C Z T D E F M F H I R W j 1

L Q G K M J D N O P W P R S B G J K M J Q R X K Z T t
A C D M R U V X U B C I V K E W B R V X U O Y Z A H e 1

R H L N K E O P Q X Q S T C H K L N K R S Y L A U M u
Q N H R S T A T V W F K N O Q N U V B O D X P U K O x 2

G Z B C L Q T U W T A B H U J D V A Q U W T N X Y Z d 5
O I B T U B U W X G L O P R O V W C P E Y Q V L P R y

Fig 42. Investigating a correct hypothesis in a Stecker knock-out.

and the poesible diffdrent 'Stecker values' of T and W. Any assumption as to the Stecker values of T ehd W implies two rod pairin ge, and when we have set these rods up we can look round and see if there are any other Stecker which are conseequences 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 42 , 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 con~~tradict~~firmatione we cover up the constatations with shirt buttons as they are used. Fig 42 shews the working for the correct hypothesis W/E,T/B. The 'covered' letters are shewn ringed. In order to shew how the working was done the steps havebeen numbered, the number being put against the constatation used and also against the Stecker values or rod pairing which resulted. The work as shewn is not quite complete. It is possible to go further and get the Stecker valuesof 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, much the same method could be applied to find a new Umkehrwalz with data of the kind that arises with the air enigma. ~~There~~ One may find the Ringstellung by Herivelismus, and also have a certain number of constatations at known window positions arising from CILLI s

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

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 substitution which transforms one column of the rod square into the next (see p 19a). Thus the class of the wheel found on p 26 was 13,8,3,2. This 'class' is independent of what point of the ~~wheel~~ 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 throughthe 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) machine

I. 19,7

II. 14,12

III. 10,8,5,3

U.K.W. 15,9,1,1

Service machine

I. 13,6,4,3

II.16,10

III. 7,7,6,6

IV. 11,11,2,2

V. 9,9,6,2

VI. 24,2 two apart 9,8,6,3

VII. 12,5,5,4

VIII. 24,2 two apart 22,4

U.K.W. A. 9,8,4,2,2,1

B. 10,7,8,1

C. 13,8,2,2

?

3

Railway machine

I.24,2 two apart 18,5,2,1

II. 12,8,4,2

III. 14,8,3,1

U.K.W. 24,2

Commercial

I. 18,8

II. 19,7

III. 12,9,4,1

U.K.W. 22,2,1,1

Chäptsr IV. Single-wheel processes. (Unstsckered Enigma)

We now euppose that we know the connections of the machine, and that thsre are no Stecker. This practically preeuppoess that we have elreedy reed some of the treffic, end therefore that we know something of the probable words ~~being~~ ussd, especially at the beginninge end ends of the messegss. Suppoee then that we think that a message st$\overset{t}{\text{a}}$ring FKSJRNQMYLBBP$\overset{KY}{\text{S}}$KX becomee when dsciphered DANZIGVON... Weshall have to teke several independent hypotheees ae to which wheel ie in the R.H.W. position, unlese other meesages for the dey have already been solved. Let us suppose that the purple wheel ie on the right. We shall then heve to make 26 seperete hypotheees ee to what rod position the ~~m~~ meesege sterts in. ~~Then we are trying out the hypothesis that the pre-start is at rod position 26~~ . Ws write the message out in guage with the rods, and when trying out the hypothesie that ths pre-stert is at 26 on the rode we pick out the rode eterting with F end D end ley them with $\overset{F}{\text{D}}$ undsr the $\overset{F}{\text{D}}$ of the message end crib ee in Fig 43. We find on the rods at position 4 $\overset{Z}{\text{W}}$ which impliee th et ths Z of DANZIG should have been enciphsrsd as W instead of J, or else that there was a turnover bstween the D ahd the Z . As we do not think this latter alternative very likely we go on to the hypothesis thet the pre-stert was at 1, end this also gives us a contradiction or else e T.O. So we go on until we try pre-start et 4. When we set up the peir of rods that gives $\overset{E}{\text{D}}$ we find that it also gives us $\overset{O}{\text{V}}$, This is known as a 'click', and when we sat up the pair giving $\overset{T}{\text{I}}$ we get also $\overset{N}{\text{O}}$. This, ~~makes~~ together with the fact that there are no contradictions, makes it practically certein that we have found the right rod stert. We cen then decipher a few more letters of the messege, assuming th ere was no T.O. In thie way we get DANZIGVON.ANN$\overset{H.N}{\text{..}}$ suggssting the decode DANZIGVONMANNHEIM... with a T.O. ~~somewhere~~ between the ~~second N and the E of~~ H and the E of

MANNHEIM . ~~Consequently before the~~ In order to decode more of the message we ~~shall have to~~ can ~~either~~ try using the three couplings after the turnover to read a little more. This is shewn in Fig 45 . It is not possible to fill in the intermediate letters and we have to find some oth er 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 M.W. is in. We shall not actually need to do the decoding for each such position, as a very large proportion of the possibilities is immediately eliminated by th e FIM ~~xxxxxxx~~ known to occur after the T.O. In fact we have the seven couplings ku,ap,fq,xn,ay,td,vh 15 before the T.O. and ~~the~~ ~~threex~~ ~~two~~ sw, oa, ie after it ~~and possibly also bw~~. We ~~xxxxxx~~ could treat these couplings with respect to the middle wheel in the same way as we treated the original crib with respect to the right h and wheel. However it is not really necessary to get out th e rods. It is easiest to work with th e rod square and for each possible position of the middle wheel look and see what coupling before the T.O. is a consequence of oa after the T.O. For example there are the bits of red rod

```
12
MA
VO
```

and therefore if the message starts in rod position 1 for the middle wheel the coupling mv must hve occurred before the T.O. in order that oa may occur after it. Consequently this position & colour for the middle wheel is impossible. That the middle wheel rods can be used in this way amounts to nothing more than that they can be used in decoding in the way described on p. 14,15. In this way we find that the only possible position~~s~~ for the middle wheel ie ~~(if red)~~ ~~xxxxxred 2xxxd~~ ~~xxdx~~ ~~xxxxxx2xxxd~~ red 11, and we have for couplings after the T.O. yg,uv,kt,kh,ws,om,al,oa ~~2xxxxx1&xxfr,jw,ik,ix,xg,dx,xx~~ and the part of the message from th e first to the second T.O. reads

```
VKXUZH RBZOQVFTKVLDKSNRDBS
EIM.GAN.A.MEETOTER.IT...E.
```

We cen fill this in to reed, forthe whole message up to thispoint ~~Danzigxvonxmannheimxx~~ DANZIGVONMANNHEIMXGANZARMEETOTERBITTEBEFEHL. The other couplings ~~mx,~~ rf,jz,qi cen now be reed off the filled in letters, end ~~thisxgivesxxxx~~ eltogether we now heve the couplings of the M.W. rods qo,er,eb,sx,md,jm,pf,fi,yu,zl,hn. We cen decode ee described in Chap II; the two remeining middle wheel couplings will soon be found.

We might of course use either the middle wheel couplings or the right hand wheel couplings to find the position of the L.H.W. end U.K.W. end we could then do the decoding on e mechine insteed 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 ~~xxx~~ first parts of the process.

The inverse rods

Insteed of picking out the R.H.W. rods end leying them egeinst the cribes in Figs 43,44 we might write down the ~~xxxxxxxx~~ rod couplinge which ere consequences of each of the constetetions,thus wheh testing pre-start 26

```
FKSJTTQNY
DANZIGVON
omuqikids
wjeonmyyy
```

The contrediction which we found before by setting up the pair ow now shows itself in the form of two contredictory couplings ow,oq. In the cese of pre-start 4 we heve

```
FKSJTTQNY
DANZIGVON
uptlqxuky
kedwfnkie
```

end our confirmations (clicks) show up es repetitions of the couplings uk,qf. If we ectually did this we should lose time in comperison with the original process, but we cen ectually get ell the couplings in the different positions by e more mechenicel method.

We heve the lines of the inverse squere (p 10) written out on rods in double length, celled 'inverse rods'. We

~~#4~~ 5

```
          10     15       20        25 30 1       5        10       15        20        30  for [illegible] starts
               10         15         20           25 26        5         10         15         20         25
...C N K D G | B C R L T | A M Q F I | X H J M Y | E | D W Z P U | C N K D G | B C R L T | A M Q F I | X H J M Y | E    F
...Z X B J S | F V K E M | R O N L D | U Y G H N | P | W I Q T K | Z X B J S | F V X E M | R O N L D | U Y G H N | P    D

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

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

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

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

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

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

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

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

Fig 4. Strip of Purple crossword   F K S J R M Q X Y
                                      D A N Z I G V O N

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

Fig 43. Tasting pre-start 26

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

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

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

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

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

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

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

Fig 44.
Pre-start 4

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

Fig 45. Consequences of EIM after T.O.

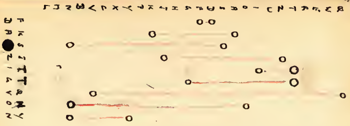


Fig 47. Preparation of mask for Danzig rods

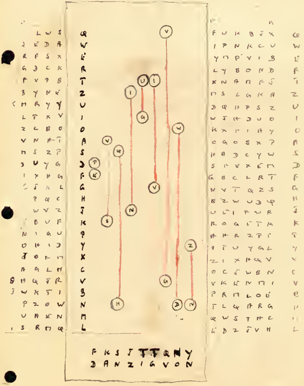


Fig 48. Mask in position. Taking pin-shot 26

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

Masks

There is another ~~xxxxxx~~ 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 gauge with the inverse oblong and write the diagonal down the side of it, and ~~numbers 1,2,... along the top. We also number~~ ~~xxxxxx~~ 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 shewing 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.

Charts.

When we want to try the sama dedode for xxxx e great many different meseages, end perhapa for many different places in tha eame messags it may be worth while to maks special statietios for that orib. Ws can make etstistioa of the positions in which there will b s 'clicks'. Thsre is quite e problem es to ths form in which the statistics ought to bs presented. I will dssoribe two forms which have sotually been used; namsd aftar tha prinoipal cribs for which they were made. Fiest howaver I must axplain

PEROOMMANDANTE charts_.

~~This is the perfect form of chart for use when the position of the crib in the message is known. The chart xxxxxxxxxxxxxxxxxxx xxxxx has ssverel major division s according tothe different~~

tha tsrminology I shall use. Let us taks for sxampla ths orib XBRUESSELXX fitted onto a part of the messegs AEIRCMTWBZJ. There is a click as shewn below

```
19 20 21 22 23 24 24 26  1  2  3   rod positions
 A  E  I  R  C  M  T  W  B  Z  J  message
 X  B  R  U  E  S  S  E  L  X  X  crib

 N  V  Y  L  C  O  T  W  B  P  U  rod
 D  G  G  K  W  C  U  E  L  A  B  rod
```

Fig 49

As the constatations of ths olick are oonsecutive I shall say thet ths 'click distance'ie I. W is oallad the 'first cipher letter' and B the second cipher lettsr, E ths first and L the second 'crib lstters! As tha firat lattsr of the crib comes at rod position 19 we xxxx eay that tha 'rod start' is 19. As the first crib lettar E is the aighth lattar of the crib we say that tha crib position of ths click is 8.

PERCOMMANDANTE type charts.

Thie is the parfact form of ohart for usa when the position of the crib in the maesage is known sxactly. Ths chart has severel major divieions according to ths different possibla first crib letters. Each of these major divisions is further divided into linea laballed with the second crib lstters, and columns laballad with the first cipher lsttars. In the xxxxxxx reaulting small rectangles are written the secon d cipher letter and the rod start. Thus th e eighth ma j or division of a PERCOMMANDANTE type chart made out for XBRUESSELXX would look like this

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

all entries apart from the one corresponding to the click shown in Fig 49 having been omitted. The ~~letters~~ numbers written above and tothe righ t of the letters in the n ames of the rows distinguish between different occurrences of the same letter in the crib. By writing the message downwardin guage with the lines of th e chart it is very easy to see the possible clicks. We note down th e rod starts, and, if we find one of th em repeated try it out by th e method described at the beginning of the chapter.

BRUESSEL type charts.

These have the advantage over the PERCOMMANDANTE type charts th at one can investigate all possible positions of the crib in the message without doin g them all in dependently, but it h as some counterbalancing disadvantages. In the form in which they were made for the Railway traffic all three colours were put togeth er and there were separate sheets for the different click distances. I now think that it might be better to separate the colours and to have three or four click distances on a sheet. In any case the sheets are further divided into lines accordin g to the different first cipher letters and the entries in the lines consis t of the secon d cipher letter, the rod start and the crib position of the click. Thus the click shewn in Fig 49 would be represented on sheet I in line W by the entry B 19^8 in green.The chart is usually used one sheet at a time;

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

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

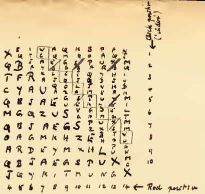

Click position ('window')
1
2
3
4
5
6
7
8
9
10
4 5 6 7 8 9 10 11 12 13 14 ← Rod position

Fig ~~49~~ 50. Making a chart. Cross clicks with rod start 4.

Making of charts

Although thara 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 are are two kinds of click to be catalogued, caled'direct'and 'cross'. Direct clicks arethose in which both lettars of tha crib occur on th e same rod. Both clicks in Fig 44 are direct clicks. Cross clicks have one of the crib lettera on one rod and the other on the other.

Wh_en cataloguing cross clicks we make 26 pictures like Fig 50 , by writing the crib diagonally and filling up a square with rods, and finally copying the laft lowar half intotha right upper h alf symmetrically across the diagonal. Tha different pictures ~~S I W A Q K B P P N~~ ~~E Q T G~~ correspond to different rod starts. Each square above the diagonal gives us an entry for tha chart. Tha lower latter ia the first cipher letter,and the upper ie tha 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 sheet, with BRUESSEL type) is determinad by how far th_e square is from the central diagonal; in.tha figure tha squarea corrasponding to click distance III ara ringed in pancil. With a PERCOMMANDANTE type chart we should not use the diagonals but the columna. Some of the ~~[illegible]~~ aquares do not correspond to possible entries, aa thay could only ariae from rods paired with th emselvea. These squares have been crossed out in Fig 50 .

For cataloguing direct clicks we haveto find all cases in which a pair of latters on a rod can fit with a pair of lattera of the crib, e.g.

X	B	R	U	E	S	S	E	L	X	X	crib
D G	G	K	W	U	U	E	L	A	B		rod

Each such case will giva us 25 diffarent entrias in the ch art, all with the same click distance, rod start and crib positionx. In cataloguing these either in a PERCOMMANDANTE or a BRUESSEL chart it is sufficient if we put the second cipher letters all in simi;ar positions and only once enterthe remainin g 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 22 genuine clicks between X's per T.O. : there will also be an average of about 0.5 ~~xxxx~~ apparent clicks arising from letters which are not X, giving altogeth er 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 kn ow where the T.O. is these figures have to be modified. In the righ t place we have 3.7 clicks per length of 26, and in th e wrong place 2.0.

~~Thxx There are two forms of X-charts, one favoured by Kendrick and one by Turing~~. With X-charts there are less variables involved then with ordinary charts, as th ere is no question as to wh ere the crib should be set against the message. The variables involved therefore are the first and second ~~[illegible]~~ cipher letters, the click distance, and the rod position ofthe 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 ~~the first cipher~~ there are 26 lines named after the first cipher letters and 26 columns corresponding to the possible click distances. The second cipher letter an d 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 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 th e implied rod start of the message by subtracting the position in th e message of th e 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 th e position in the message of the first cipher letter. The rod start with the greatest number of entries against it is presumed to be th e right one. To read the message after we have found th e R.H.W. rod start we can try setting up th e rods giving the clicks and see if this results in any further iden tifications, 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 makin g an X-chart we can make a set-up like Fig 50 . 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 th e diagonal. When making th e entries for a particular value of rod position of the first constatation of theclick (i.e. th e entries wh ere a particular number is written in the square) we copy in pencil 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 inany column then can be seen by looking at the top. Having made these entries we rub out the lines at the top and replace them with oth ers.

In Kendrick's type of X@chart the names of the lines give the first of the oipher lettere/ The oolumns give the position seoond oipher letter end of the other oipher letter, end the entry in the square is the position of th e first oipher letter. This form of ohart ie pertioulerly useful when we heve e hunoh about the rod st^rt.

Consecutive tables.

In the second part of the process, where we are finding the position of the middle wheel we osn speed up the work by the use of consecutive tebles. These sre of two kinds, forward end backward, snd look very like rod equares. The letter in column 18, sey and row R of the forward consecutive square is th e letter which occurs in column 19 of the rod with R in column 18. The letter in column 18 snd row R of the backward consecutive square is th at which occurs in column 17 on the same rod. Like rod squares end inverse squares these consecutive squasres 'have a disgonslIi.e. osn be ~~prepared by~~ filled in from e single upright by writing 'the diegonsl' disgonally downwards toth e left. In our DANZIGVON example we could h sve used the backward consecutives es soon es e we hed found the couplings ku,ep,fx,qn,ey,td,vh,lw before the T.O. snd sw,oe,le sfter it. We should heve laid rulers sgeinst the lines o,s of the beckward consecutive square, end reed off the consequences before the T.O. of havin g oe efter it, in the verious possible positione of th e middle wheel, end would heve looked to see whether th ese consquences were consistent with our deta. We eh ould then heve repeated with ws ~~[illegible]~~ looking only et the positione consistent with oa. The forward conseoutives cen be used wh en the plsce has been found for reeding off the couplings sfter the T.O. (elthough this is only s small edvantsge), or in e ceee where we heve eterted from the end of the message end worksd backward s.

Chapter V. Coupling cetelogues

When we heve found the rod position of the R.H.W. end e few couplings for e meesege it is possibleto find the poetions of th other wheels from e euiteble cetelogue.

Short cetelogue

On e method ie to try independently ellthe possible poeitions for the middle wheel. We shell want to know th e middle wheel couplinge which are consequences of these various eesumptione. This cen be done by eetting up inverse rods for the middle wheel. The rods ere paired off sccording to the R.H.W. couplinge, i.e. M.W. output, ~~xxxtxxFigxxxxx~~.This hee been done for the the couplings ku,fx,ep which erose in the DANZIGVON crib in Fig 56, assuming the red wheel in the middle. The pairs in each column of this set up give possible M.W. couplinge. We have ~~xxxx~~ now to find out whether these couplings are poesible. Our procedure is rather diff-erent eccording ee the U.K.W. does or doee not rotate. In the oese that the U.K.W. does not rotete it will be sufficient to heve e Fose sheet ~~xitk~~ (the rows end columns lettered preferably with the diagonel alphabet) in which, in the RW square ~~thxxx~~ ere entered the poeition s of the left hend wheel et which the ~~xxxpling~~ RW is one of the pairs in the L.H.W. output alphabet Fig 61. This ie known ss the 'short catalogue' for thie wheel. To use it in connection with th e DANZIGVON crib we should teke eech column of Fig 56 in turn end look up the peirs in it on the short cetelogueand see if all the squares had e number in common. If we found such e oese th e number in the square would give the L.H.W. rod position, and the column of ~~xtx~~ Fig 56 would give the M.W. position. Actually the U.K.W. rotetee for our example so thet we should have no success.

In th e cese thet th e U.K.W. rotates we need essentielly the same short cetelogue, but we arrenge it elightly differently. In steed of th e lines of the catalogue corresponding to fixed output letters they correspond to fixed distecee (or quantity) on the diegonal, between the output lettere. This may be seen from Figs 62, 63 which illustrete euch e cetelogue. The pairinge ere written ebove the ~~positionsxinxwhichxxtheyxoccur~~ figures giving the positions ~~of~~

84.

Green III

	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	✓
	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		10. 22.				8. 16 26	14.	3.	7 9.	16.18			11 24			26	2.12.	5.13	25	6.		19.		4.	1.17. 20.	21.	Q
W	1 22		26	6. 16		12.13 20.	18	1.27. 25.	11. 14	3.9.	24.			4.		19.				17.	8.23	15.	21.	5.			W
E		26		22	8.	7.				12.	17.	21.		6.23			4.13.		2.5.18.	1.10. 16 20		24.	9.25	3.16.	11. 14		E
R		6. 16	20.			3. 9.11.	10.	8.15.		17.	20	26	9.15.	2. 5.		14.	18 23	24. 26.			1. 2.4.				12.	7.	R
T			8.				21. 25.	6.	22.	26	11.	4.	2. 14.20 22.	3.	17.	16.18.	5.9.			24.	7.12.		10.15.	1.13. 14.			T
Z	8. 16 22	12.13 20	7.	3. 9.11.				26.		10 29			4.		21.	2.5. 24.	6.	9.18.	1.	25. 26.	14.			17.	15.		Z
U	14.	18.		10.	8. 25.				2 15.	11.		9.12.	5.16	1.	20		7.8.		13.	4.22. 23.		17.	3.19. 26		24	6.	U
I	3	1.2. 25.7.		8.15.	6	26.			5.			23	17.	12.16 19	9. 10.	21.				16.	18.	11.13.	24	20 22.	4.		I
O	7.9.	11. 14			22.		2.15.	5				6		17.	8		26	19.		13	24	3 25.		10.18 21.	16 33.	4.12. 20.	O
A	15.18.	3.9.	12	17.	26.	10 32	11.				5.		14		19. 24	4.		2.20.	23.	7.16. 3.		16.	13.			8. 26	A
S		24.	17. 19	20	11.					5.		7.14	1.26.	9.26	23		15.	16.	4.9.		13.	12. 21			2.6. 22	3.10. 18	S
D			21.	26.	4.		9.12.	23.	6		7.14		10	8.13	1.22	11.			16.24		20. 25		2.18	19.	3.5.	15. 17.	D
F	11.24			9.13.	2.19. 20 23.	4.	5.16	17.		14	1.25	10.		19 22				6.15	26.	8.	3.			12.	17. 21.		F
G		4.	6.23	2.5.	3.		1.	10.16 19.	17.		9.26	8.13	18 22			15.	11.		7.21			20.		24. 26	10.	14.	G
H					17.	21.	20.	9.10.	8.	9 24.	23	1.22				13.			15.	3.11.		4.14 18	6.12.	7.	25.	2.6. 16.26	H
J	26	19.		14.	16.18.	2.5. 24.		21.		4.		11.		15	13		20 26	1.8. 23	26.10 12.17. 24.			9.	7.				J
K	2.12.		4.13	18 33	5.9.	6	7.8.		1.26		15.			11.		20 26		3.10. 21.	14.				17.			19.22. 24.	K
P	5.18			24. 25.		9.18.			19	2.20.	16.		6.15.			1.8. 23.	3.10 21.			12.	17.	7	4.11. 22.4.	26.			P
Y	25.		2.5. 18			1.	13.			22.	4.8	16 24	26	7.21.	15.	26.10 12.17. 33.	4.				19.		20.		9.	11.	Y
X	6.	17.	1.10. 15.20		24.	26.	4.22.14. 23		13.	7.16 21.			9.		3.11			12.			9.	26	5.	2.	18.19		X
C		8.23		1.4. 21.	7.10.	14.		18	24.		13.	20 35.	3.					17.	19.	9		5. 13.16 35.		6.11. 15.	26		C
V	19.	15.	24.				17.	11.13.	3. 35.	1.6.	12. 21.			20.	4.14 18.	9.		7.		26.	5.6. 16.16 22.		8			23.	V
B		21.	9.25		10.15.		3.19. 26.	24.		13.		2.18.		~~6.10~~	6.12	7.	16.17.	4.11. 14.22	20	5		8		23		1.	B
N	4.	5.	3.16.		1.13. 14.	17.		23 33.	21 10.18			19.	12.	24 35.	7.			26.		2	6.11 16.		23.		8	9.	N
M	1.17. 20.		11.14.	4.12		15	24.	4.	16 23.		2.6. 22.	3.5.	7.21.	10.	25.				9.	18.19.	26.			8		13	M
L	21			7.			6.		4.12. 30.	8.35.	15.3. 10	15.17.		14.	2.5. 16.26		19.22 21.		11.			23.	1.	9	13		L
	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	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L	

Fig 57, Short catalogue.

Railway III

Fig 52. Short catalogue for use with rotating

[illegible] · Rotor III

1	A	QW	WE	ER	RT	TZ	ZU	UI	IO	OA	AS	SD	DF	FG	GH	HJ	JK	KP	PY	YX	XC	CV	VB	BN	NM	ML	LQ
	B	10,22	26	22		·			5		5	7	10	18,22	·	3	20,22	3,10,21			7	2,5,10,16,22	8	23	8	13	21
2	C	QE	WR	ET	RZ	TU	ZI	UO	IA	OS	AD	SF	DG	FH	GJ	HK	JP	KY	PX	YC	XV	CB	VN	BM	NL	MQ	LW
	D	·	6,16	9	3,19,11	21,25	26	2,15				1,25	8,13	·	15		1,8,23	14	12	19	26	·	·	·	9	1,17,20	·
3	E	QR	WT	EZ	RU	TI	ZO	UA	IS	OD	AF	SG	DH	FJ	GK	HP	JY	KX	PC	YV	XB	CN	VM	BL	NQ	MW	LE
	F		·	7	10	6	·	11	·	6	14	9,26	1,22	·	11	·	3,6,10,12,17,22	·	17	·	5	6,11,15	·	1	4		·
4	G	QT	WZ	EU	RI	TO	ZA	US	ID	OF	AG	SH	DJ	FK	GP	HY	JX	KC	PV	YB	XN	CM	VL	BQ	NW	ME	LR
	H	·	12,13,20		8,15	22	10,22		23	·	·	23	11	·	·	15	·	·	7	20	2	26	23		5	11,14	7
5	I	QZ	WU	EI	RO	TA	ZS	UD	IF	OG	AH	SJ	DK	FP	GY	HX	JC	KV	PB	YN	XM	CL	VQ	BW	NE	MR	LT
	J	8,16,23	18	·		26	·	7,12	17	17	19,24		·	6,15	7,21	3,11	·	·	4,11,14,22	·	18,19	·	19	21	3,16	12	·
6	K	QU	WI	EO	RA	TS	ZD	UF	IG	OH	AJ	SK	DP	FY	GX	HC	JV	KB	PN	YM	XL	CQ	VW	BE	NR	MT	LZ
	L	14	1,17		17	11		5,16	12,16,19	8	4	15	·	26	·	·	9	16,17	26	9		·	15	9,25	·		·
7	M	QI	WO	EA	RS	TD	ZF	UG	IH	OJ	AK	SP	DY	FX	GC	HV	JB	KN	PM	YL	XQ	CW	VE	BR	NT	MZ	LU
	N	3	11,14	12	20	4	4	1	9,10	·		16	16,24	8	·	4,14,18	7	·	·	11	6	8,23	24		4,13,14	15	6
8	O	QO	WA	ES	RD	TF	ZG	UH	IJ	OK	AP	SY	DX	FC	GV	HB	JN	KM	PL	YQ	XW	CE	VR	BT	NZ	MU	LI
	P	7,9	3,9	17,19	26	2,19,20,23		20	21	1,26	2,20	4,8	·	3	20	6,12			·	25	17	·	·	10,15	17	24	
9	Q	QA	WS	ED	RF	TG	ZH	UJ	IK	OP	AY	SX	DC	FV	GB	HN	JM	KL	PQ	YW	XE	CR	VT	BZ	NU	MI	LO
	R	15,18	24	21	9,13	3	21			19	23	·	20,25	·	·	7		19,22,24	5,13		1,10,15,20	1,4,21	·	·	·	4	4,12,20
10	S	QS	WD	EF	RG	TH	ZJ	UK	IP	OY	AX	SC	DV	FB	GN	HM	JL	KQ	PW	YE	XR	CT	VZ	BU	NI	MO	LA
	T				2,5	17	2,5,24	7,8	·	·	7,16,21	13	·	·	24,25	25		2,12	·	18		7,12	·	3,19,26	22	16,23	8,25
11	U	QD	WF	EG	RH	TJ	ZK	UP	IY	OX	AC	SV	DB	FN	GM	HL	JQ	KW	PE	YR	XT	CZ	VU	BI	NO	MA	LS
	V			6,23		16,18	6		·	13		12,21	2,18	12	10	2,5,16,26	26	·	·		24	14	17	24	10,15,21		3,10,18
12	W	QF	WG	EH	RJ	TK	ZP	UY	IX	OC	AV	SB	DN	FM	GL	HQ	JW	KE	PR	YT	XZ	CU	VI	BO	NA	MS	LD
	X	11,24	2	·	14	5,9	9,18	13	14	24	1,6	·	19	7,21	14		19	4,13	24,25	·	25	·	11,13	·	·	2,6,22	15,17
13	Y	QG	WH	EJ	RK	TP	ZY	UX	IC	OV	AB	SN	DM	FL	GQ	HW	JE	KR	PT	YZ	XU	CI	VO	BA	NS	MD	LF
	Z	·			18	4,22	18	16	3		13		3,5					18,23		1	4,22,23	18	3,25	13		3,5	·

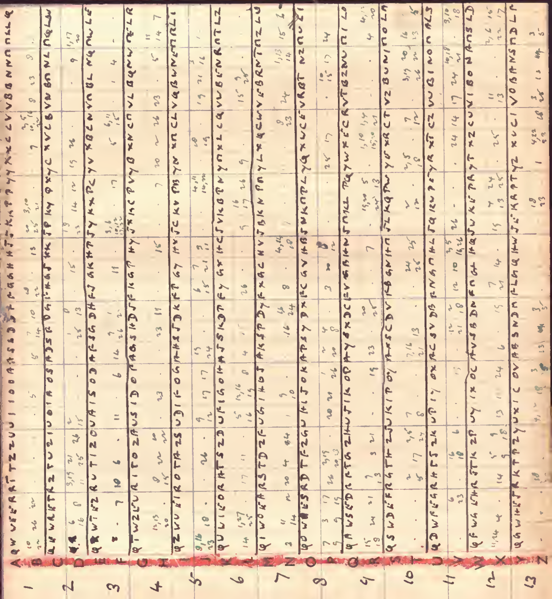


Fig 53. Small sheet of short catalogue for rotating backwardly.

III Green.

```
                                     17 18 19 20 21 22 23 24 25 26
R X 2 O X F M C P W H S I E Q N T L G A U W B D J S   a
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   k

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

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

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

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

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   y
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   g

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

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

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   d
A E T T I Y D N X K Q G A U W L B R M 7 O Z Q Y S H   l

  H F A K D L Y Y G O N W B J P P C Z M S U R G Q B   f
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   x

K T Q N Y G E U W C B B L S R J D O Y Z W M X P H Y   p
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   n   N

Z W M X H R I E V N N Q D T K F A X U E L C Y B B P   y
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 N   B
```

Railway Couplings Wheel III

Fig 54. Output of U.K.W + L.H.W. for Combination of that catalogue.

Combination

of th e L.H.W. in which these pairings occur, the U.K.W. being 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 54, and analysing the resulting pairs.

To understand the use of the sh ort 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 th e squares under these pairs. For instance in th e case ofthe DANZIGVON crib we found the middle wheel to be red in position 10. This gives the middle wheel couplings pn,ve,hn,uy as consequences of the R.H.W. couplings qn,uk,fx,ep . These can be read off from Fig 56, 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. Th e 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~~ zf 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 hn. It is as well therefore to have rulers in gauge with the catalogue to measure off the distances. Having found the righ t amount of slide forward on the diagonal, i.e. to th e right in the catalogue we calculate the positions of the wheels from the formulae

```
                5         10         15         20         25
. . . O|A|Z W G S Y|H D C P E|N X T I T|L B F R K|U J E Q O|M    Q
. . . A|Z|K X K D O|M J E Y W|H F C V P|G L B T Q|N U R H A|Z    F

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

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

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

Fig ~~65~~ 58. Setup of reverse rods for M.W in connection with DANZIGVON into 'Greek' column G 11.

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

L.H.W. poeition = number in square + elide

The Turing aheets

The ehort catalogue should work very well when the Umkehrwalz rotatee, and there ie no information connecting the poetiion of the U.K.W. with the positione of the other wheels,. In the caee of e fixed U.K.W. we can often make use of an analyeie of R.H.W. couplinge.

The ley out of th e cetaloguee is largely determined by the speciel method by which they ere made, but it seems to be reeeonably convenient in use. The catalogue ie divided into sheets numbered 1 to 13. Eech of these eheate coneiets of e 26x26 equare with margin at top end left hend side, preferably on 1/3" geuge. , One suoh sheet ie ehown in Fig 56 pertly construoted. The letters and numbere in ink era the omly ones oonoerned when the eheets are being used, the others being part of th e conatructioh, and left on to help in trecing errors. The entries 10,18,21 in the aquare in column 15 an d the row with KV in the margin mean that the coupling KV occure when the M.W. ie in poeition 15 end L.H.W. in eny of the positions 10,18,21. In order to find the poeitione et which two couplinge cen occur we have only to find the oorreeponding linee of the catelogue ageinst one another and compare the numbers in the edjecent equaree. It ie feirly eaey to find the right sheet b ecause the number of the eheet gives the distence along the diegonal of the two letters of the pair, e.g. K and V are at dietance 5 along the diagonal (KPYXCV)and KV aocurs on sheet 5.

Construction of the Turing sheete

The construction of tha catalogue dependa on making almost simultanaously all the antrias corresponding to ~~pairs for~~ oases in which the ourrent flowe through tha eama two wiree of the M.W. In th e partially constructed sheet 5 in Fig 56 eome of the diegonels have baen fillad in fully, and each of thase oorraspondsto a pair of wires of the M.W. As the M.W. rotates the rod points at the right hand ands of th a wires mova steadily backwarde along 'the diagonal'. Wa eee ~~that this~~ also that as we move slong the fillad in diagonal the rod position steadily increases, end the lettare in the peirings move elida beckwarde along'the'diagonal'. Meanwhile tha left hand ends of the wiras are eteadily rotating, so that the middle whael couplinge are eliding along 'the diagonsl'. The entries in tha squares are the positione of the L.H.W. where these M.W. couplinge cen occur, end t tha slide along the diagonal amounts to a diagonal movament along the short catalogua. Take for instance the ~~fff~~ fillad in diagonal on Fig 56 nearest to th e central diagonal. The second entry onthis diegonal is 2,5,16,26 which is tha entry et HL in Fig 51 : next along tha diegonal in Fig 56 is the antry 10 whioh occurs at GM in Fig 51 , and so on , tha diagonal in Fig 51 baing repeated backwards in Fig 56.

This phenomenon may also ba axplainad with refarence to the rod equara, instead of the wheals: thie is really more practical, ee we heva to make the catalogue up from the rod square. A possible method for making up tha catalogue would have been this. In each square on th e sheets we write in, in pencil, tha M.W. couplings which would be needed to produce tha pair at the beginning of the line as M.W. ouput ~~required~~ et the M.W. position given by the heading of the column in which th e square ooours. To do this we should heve to write down in each line the inversa rods named after the lattere at the beginning of the line. This has been done in a part of Fig 56 (ton R.H cornar). We ehould then have the square fillad with one inverse (M.W.) equara, with top and bottom revarsed, an d another such raversed square somewhat displaced upwards. Tha entries in green ink oould be obtained by rapalacing each pair of pencil lattars by the corresponding entry on Fig 51, i.e. by th a position of tha L.H.W. at which that pair of lattars occurs as L.H.W. output. Now the whole of the pencil square can be obtained from its top lina simply by filling in along diagonals. Translated into tarms of the green ink entries this means to say that wa only naad to ba given tha positions at which ~~the~~ to start copying from the short catalogua.

Actually we copy out the diagonals of th a short catalugue onto staircase shapad atripa (known as 'Christmas decorationa' or 'hand frilla') in revarsad order, with the position in th e short catalogue writtan above each aquare. These hand frilla are numbered by the (conatant) distance apart on 'the diagonal' of the paire of letters on tham; e.g. in the hand frill no 5 shown in position for copying in ~~M~~ Fig 56 I and F are at distance ~~12~~5 on qwertzu and so are D and K. Instead of actually filling in the whola square with pairs of penoil lettera wa take the antries which migh t hava been made in the top line, an d write them in tha top margin, and alao ~~make~~ put the antrias which might hawa gone in the left hand oolumn into tha left hand margin. In order to find what hand frill to use for a particular diagonal the diatancas apart along qwertzu of tha lettera along the top are calculated. This should ba dona quite indapandantly, to give a check on incorractly oopied letters (aee 'Mystic numbers').

Tha reason for having the imaginary rod squares implied in tha construction inverted ie in ordar that tha writing of diagonala may be from left to right and downwards, which ia considered easiar than from right to left and downwards.

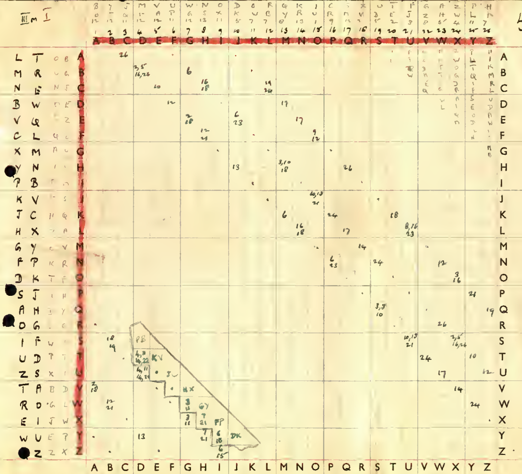


Fig 56. Construction of Turing charts. Part of hand table with wall shown in position for copying.

Solving e short crib

The ch ief epplicetion of the Turing sheets is to the solution of cribsfrom e length of 2 to 6 lettere when th e U.K.W.does no rotate. We set up tha inverse rods es usuel, but find thet by no meene ell th e incorrect poeitions ere eliminated by coupling contredictions. We therefore look to see whether there is eny position in which th e couplings cen occur. Teke for exemple th e crib ANX, with end wheel order I III II (red,green, purple), U.K.W. pos. 0 cipher ~~NUI~~ ARC. We set up th e inverse rods es in Fig 57 , en d for eech column of the reeulting eet up compere the lines of the cetelogue nemed efter th e peirs in the column. For eech peir we shall wnt to find quickly the right sheet on which to look, end this meens subtrecting the peirs on the diegonal (i.e. finding their distence epert on qwertzu). To do this we cen either have e table of differences or else uee 'myetic number rods'

'Mystic numbere'

Fig 58 shows e teble of 'myetic numbere' for the red wheel. The meening of the teble is thie. Teke the 8th line for exemple. It could be mede by teking inverse rod Q end inverse rod O, O being eight pleces on elong ~~the~~ qwertzu from Q. We ley the two rods together end find the differences of th e resulting pairs: e.g. the ~~third~~ fifth entry in line 8 ie 6, end the fifth letter of th e red inverse rod Q is Y, the fifttth letter of inverse rod O is F, and Y end F ere 6 epert on qwertzu(FGHJKPY). If then we hed e set up of inverse rods including the peir QO we could use the eeries of numbers of line 8of the mystic n umbers to tell us on which sheets the verious peirs should be looked up. However we cen elso use line 8 of this teble on meny other occesi ns. Suppose for exemple thet the peir ES of inverse rods is up. The series of eheets on which we heve to look is egein given by line 8, but we heve to stert in th e third column under E instead of et the beginnin under Q. Quite e convenien t er engemen t is to heve the lines of the teble written out on rods in geuge with th e inverse rods end of double length. (Thie wes once done for the service mechine wheel III. Three lines of th e teble were put onto three sides of Mr Knox's blenk wooden inverse rods, end the fourth side occupied with the letters of the diegoenl, in thet cese A BCD... It was

```
     X              M  L  Q           T              A              H              X              M  L
....  8  1 11 13 10  2  8 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    13
... I K G M X | J Q R Q V | Y O L F E | D | M B T Z W | N A U H S | I K G M X | J Q R Q V | Y O L F E D |  B
... L J M D A | P Y H S B | X W N C R | Q | D U E G K | G O Z V F | L J M D A | P Y H S B | X V N C R Q |  A

       A        H           X                 M  L  Q           T              A              H              X              M  L
11  5  7  7  8 13  1  9 12  2  5  2  3  8  5  4  8  7 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    6
I E L J | U X A Y Z | R D F O T K | G V P H N | C Z Q B I | S I E L J | U X A Y Z | R D F O T | K |  R
H L C K | W T W B X | A Q G R F L | N Z V E M | S I J D O | P H L C K | W T W B X | A Q G R F | L |  N

             A           H                    X              M  L  Q                 T                    A           H                    X                    M  L
 2 10  2 12  4  3 12  4  2  4  2  9  8 12  9 10 12  1  9  2  3  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    1
Z H D | B P G M W | M X K U N S | Q A B C E | R L V I T | F O Z H D | B P G M W | M X K U N | S |  C
I T G | S V K F N | Q N Y J Z B | A L O V X | W E M C U | R D I T G | S V K F N | Q N Y J Z | B |  X
```

Fig 57. Set up of converse rods for $\frac{\text{BRC}}{\text{ANX}}$, and mystic no. rods for finding right sheets.

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

Fig 58. Mighi numbers for Railway wheel I

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 ~~xxx~~ 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. Compare Figs 68, 66

The mystic numbers can of course be made by actual subtraction from the inverse rods. However it is actually easier to ~~subtract the~~ ~~subtraction~~ 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 ~~the transform~~ transform the letters into numbers ~~xxx~~ to simplify the subtraction. Ishall not give the details of this.

EINS catalogues

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 EINS at every possible position. The details of this are explained in Chapter

Jsffreys sh sets

In ceses whers the wheel order is unknown it is ussful to have the positions and wheel orders where a coupling occurs all catalogued togethsr. In order to make comparison of couplings fsasibls one puts ths catalogue into the form of punched shsets, which can be laid ons on too of another. Thsse are known as Jeffreys shsets.

T hs actual form of ths Jeffreys she ts catalogue is this. There ars 325 shests labslled AB,AC,...AZ,BC,...,BZ,...,...,...,YZ. Each sh sst measurss 26"x20^{4}/5" plus margins of about three inches. They are divided into columns an inch wids, and linss ^{4}/5" desp. The whole is furthsr subdivided into squarss ^{1}/5" x ^{1}/5". Ths ^{4}/5"x 1" rsctanglss corrsspond to ths different possible rod positions of ths L.H. and M.W. The subdivisions of ths rectanglss corrsspond to ths twsnty pos ibl whsel orders for L.H.W. and M.W. with the fivs first whsels of the ssrvice mochins.

Jsffreys-Turing shsets

Thsrs is a possibility of spseding up th s work with short cribs wh re the U.K.W. rotates by making ths Turing sheets in punchsd form. Suppose we expand svsry square of ths Turing she ts into a rectangle 7/5"x4/5" dividsd into 28 small squares, numbsred 1 to 26 with two unused, and for sach entry on the Turing sheet punch a hole in the corresponding small square. Thsn th s sffsct of laying two of th s sheets on top of ons another, in such a way say that ths linss VM and CR coincidsd would be to give us ths positions in which ths two couplings VM and CR occur whsn th e U.K.W. is in the zsro position: we also gst the positions in which the couplings slid along qwertzu occur: but thsse aftsr making a corrsction for th e amount of slids are just ths positions at which VMand CR occur including all possibls rotations of ths U.K.W. One would presumably normally place three shsets on top of ons anothsr, and thsrs would havs to bs four diffsrsnt layings(because ons could not have ths shsets in cylindrical form). For this reason it would bs bsttsr to hav the shsets in double dspth,but this would probably be out of ths question.

Mr Knox has now found a useful compromise by having two copies of Turing sheets: one of them transparent & obtained by photography. This [illegible] P.T.O.

a scheme on foot for putting the catalogue into cards.

Chapter VI. The stsokered enigma. Bombe end Spider.

When ons hse e steckered snigma to dssl with ones problems nsturally divids themselvës into whst is to bs done to find ths Stsoker, and whet is to bs dons aftsrwsrde. Unleee the indicating systsm ie vsry wsll design ed there will be no problsm at all when the Stsoker have bsen found , and even with a good indiosting systen we shall be able to epply ~~xixxixxxxxxx~~ th e methods of the lset two chspters to ths individual meesagss. The obvious exsmple of e good indiosting system is ths Germsn Nevel snigma oiphsr, whioh is dealt with in Chapter VII . This ohaptsr is dsvotsd to methods of finding the Steoker. Naturally snough we never find the Stsoker without et the sams time finding much othsr information.

Cribs.

The most obvious kind of dsts for finding the keys is a 'orib', i.s. s message of which a part of ths dsdode is known. We shall mostly assume that our dste is a orib, although sotually it may be e numbsr of oohstststions arising form anoth er souroé, e.g. a number of CILLIs or a Nsvel Banbarismue.

FORTYWEEPYYWEEPY methods.

It is sometimss possible to find the ksye by penoil snd pspsr methods when the numbsr of Stsoker is not vsry great, e.g. 5 to 8. Ons would hevs to hope that eeversl of ths oonstetatione of the orib wsre 'unstackered'. The bset ohanos would bs if tha ssme pair of letters oocurred twios in the crib (a 'half-bombe'). In this osss, essuming 6 or 7 Steoker thsrs would be e 25% ohance of both oonstatstions bsing unsteokerád. The positions at whioh thsss oonstetations oocurred could be found by mesns of the Turing ehsets(if th sre were thres whesle) or ths Jsffreys ehsate. The poeitione at which this ooourred eould bs ssparately teeted. Anoth er possibility is to sst up th e inverse rods for the orib snd to look for oliok s. There ie quite a good ohanoe of sny epparent oliok bsing a real cliok erising ~~from~~ bsosuse sll four lettsrs involved ere unstsokersd. The position on the right hend wheel is given by the column of the inveree rod aet-up, and we can findalll poesible poeitions where the click coupling occurs from the Turing sheets or the Jeffreys shete. In some oesee there will be other constetations which are made up from lettere supposed to be unsteckered because they occur in th e click, and these will further reduce the number of placea to be tested.

These methods h ave both of them given auc essful resulta, but they ere not practiceble for casea wh ere there are many Stecker, or even where there are few Stecker and many whe lordera.

A mechanicel method. The Bombe.

Now let us turn to the case where there ie a large number of Steck so many thet any attempt to make use of the unsteckered letters is not likely to euoceed. To fix our idees let ue teke e particuler crib.

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

Presumably th e method of eolution will depend on teking hypotheses ebout parts of the keys and drawing what concluelona one oan, hoping to get either e confirmation or a contradiction. The parte of the keys involved are the wheel order, the rod start of the crib, whether there are eny turnovers in the crib and if so where, end the Stecker. Aa regarda the wheel order one ie elmost bound to consider all of these seperetely. If the crib were of very great length one might make no essumption ebout what wh eels were in the L.H.W. position en d M.W. poeition, and apply th a method we have celled a 'Stecker knockout' (an attempt of thia kind was made with the 'Feindaeligkeiten' crib in Nov. '39), or one might sometimes make aasumptions ebout the L.H.W. and M.W. but none, until a late stege ebout the R.H.W. In this cese we have to work entirely with constetetions where the R.H.W. has the same position. Thia method was used for th e crib from the Schlueeselzettel of the Vorpostenboot, with success: however I shall assume that all wheel orders are being treated seperately. As regards ths turnover one will normally take several different hypotheses, e.g.

1) no turnovsr between positions 1 and 5
2) " " " 5 snd 10
3) " " " 10 end 15
4) " " " 15 and 20
5) " " " 20 and 25

[illegible]

With the first of these hypothesees one would have to leave out the constatations in positions 2 to 4 ~~out~~, and similarly in all the other hypothesees four constatetions 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 constatetions can best be dispended with. In what follows I shall assume we are working the T.O. hypothesis 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 a 626 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

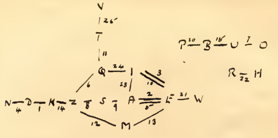


Fig 59. Picture from KEINE ZUSAETZE

cnb. Constatations 18 to 19 omitted to allow for turnover.

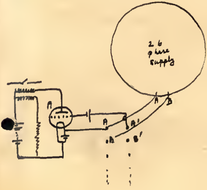
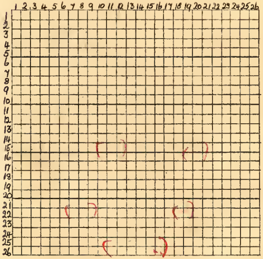


Fig 60. Circuit for Pye simultaneous scanning.


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

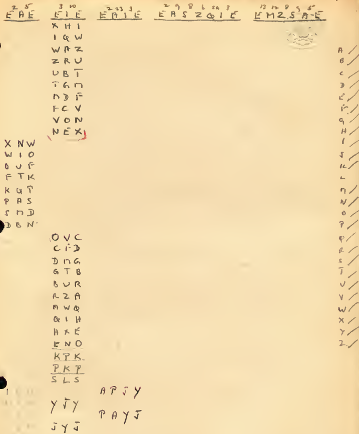


Fig 61. Stecker deductions with crib on p , with correct wheel start i.e. correct alphabets, but starting from an incorrect Stecker hypothesis E/X. All other incorrect Stecker values of E are deduced.

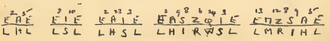


Fig 62. Stecker deduction with same alphabets as Fig 61, but from correct Stecker hypothesis E/L.

I E A $\overset{2}{E}$ $\overset{29}{A}$ I $\overset{3}{E}$

W⇐A→P
Q⇄K
T⇄F
U⇄O
I⇄W
.N→X
B⇄D
M⇄S
W→Q
I⇄H⇄L
X⇄E⇄Y
N⇐O→U
F→T
K⇄Q
P⇄A
S⇄M
D⇄B
X→N
W→I
A→Z⇄J
R⇄U
V→C⇄V
M⇄G⇄R
~~[illegible]~~
U⇐R
C⇄V=C $\overset{2}{S}$ $\overset{11}{M}$ $\overset{3}{O}$ V

3

3 3

B A Y J

A T J Y

S F L 11   L H S L

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 /

like Fig 57. From this picture we see that one characteristic which is independent of the Stecker 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 ~~which~~ 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 the same letter ~~whi~~ 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. ~~There are also other conditions of a different kind~~ The letter to which all these multiple encipherments are applied is, of course, the Stecker value of E. We shall call E the 'central letter'. Any letter can of course be chosen as 'central letter', but the choice affects the series of positions or 'chains' for the multiple encipherments. There are other conditions, as well as these that involve the multiple encipherments. For instance 'the Stecker values' of the letters in Fig must all be different. The Stecker values for E,I,M,Z,Q,S,A are the letters that arise at the various stages in the multiple encipherments and the values for W,T,V,N,D,K can be found similarly. There is also the condition that the Stecker must be self-reciprocal, and the other parts or 'webs' of Fi 57, P-B-U-O and R-H will also restrict the possibilities somewhat. Of these conditions the multiple encipherment one is obviously the easiest to apply, and with a crib as long as the one above ~~it will be quite sufficient~~

thie condition will ba quite eufficient to reduce the ~~number~~ ~~of~~ poesible poeitions to a number which can be tested by hand methode. It is ectually possible to maka use of eome of the oth er conditions mechaniceally elao; thie will be explainad later.

In order to apply the multiple encipharmant condition one natu relly wants to ba eble to parform the multiple encipharmate without Skeleton in one oparation. To do this we make e new kind of machina which we call e 'Letchworth enigma'. There are two rowa of contects in a Letchworth anigma aach laballad A to Z and called the input ~~[illegible]~~ and output rows: thare are alao moveable wheels. For each position of an ordinary enigma there is e corresponding poeition of th e Letchworth anigma, and if tha reault of encipharing F at this poeition is R, than F on the input row of the Letchworth anigma is connectad to R on the output row, end of course R on the input row to F on the output row. Such a 'Letchworth anigma' can be mada ~~[illegible]~~ like an ordinery enigma, but with all the wiring ~~in duplicate~~ of tha movable wheale in duplicate, one setof wires being used for the journey towards tha Umkehrwalz, and the othera for the return journey. The Umkahrwalz has two sete of contects, one in contact with ~~the~~ ~~[illegible]~~ contact with the inward -journey wiring of the L.H.W. and one in contect with the outward-journey wiring. The Umkahrwalz wiring ie from the one eet of contacts ecroes to the other. In tha actual design used there were some other differences; th e wheele did not eotually coma into contect with one another, but each came into contect with a 'commutator' bearing 104 fixed contecte. These contecte would be eonnacted by fixed wiring to contecte of other commutators. These contacts of the commutatora can be regarded as physical counterparts of the 'rod points' and output points' for th e wheels.

If one hes two of these 'Letchwdrth enigmas' one cen caonnect the output points of the one to the input points of h the other end th_en the connections through the two enigmes between th_e two sets of contects left over will give the effect of eucce-sive enciphermente et the positions occupied by the two enigmae. Naturelly this een be extended to the cese of longer series of enigmes,[illegible] the outout of eech being conneeted to th_e inout of the next.

Now let ue return to our orib end see how we could use these Letchworth enigmas. For eech of our 'cheins' we could set up e eeriee of enigmas. We should in fect use 18 enigmee which we will name es fbllows

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

By 'poedtion 8' we here meen 'the poeition et which the conetet-etion numbered 8 in the crib, is, under the hypothesis we are testing, eupposed to be ehoipBered'. The enigmes are connected up in thie wey: output of A1 to inout of A2: outout of B1 to input of B2: output of C1 to input of C2, output of C2 to inout of C3: etc. This gives us five'cheins of enigmes' which we may cell A,B,C,D,E, end there must be some letter, which encioh ered with eech chein gives itself. We could eesily errenge to heve ell five ch_aine controlled by one keyboerd, end to h eve five lampboerds shewin_g the resultsof the five multiple encipherments of the letter on the dpressed key. ~~If the work~~ [illegible] After one hy othesis es to the rod stert hed been tested one would go on to the next, end this would usuelly involve simply moving the ~~right~~ R.H.W. of each enigme forwerd one plece. When 26 positions of the R.H.W. heve been tested th_e M.W. must be mede to move forwerd too. This movement of the wheels in step cen be very eesily done mechenicelly, the righ t hend wheels ell being driven continuously from one sheft, end the motion of th_e other wheels being controlled by e cerry mechenism.

It now only remains to find a mechanical method of ~~determining~~ registering whether the multiple encipherment condition is fulfilled. This can be done most simply if we are willing to test each Stecker value of the central letter throughout all rod starts before trying the next Stecker value. ~~In this case we have an electric current always entering all the chains at the~~ Suppose we are investigating the case ~~of~~ where the Stecker value of the central letter~~is~~ E 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 will f~~to another relay. A current flows throughthis 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~~s~~ 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 the 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 Stecker values of the central letter to be tested ~~xx~~ simultaneously without any parts of the machine moving. Any device to do this was described as 'simultaneous scanning'.

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 latest solution proposed for this problem depended on having current at 26 equidistant phases corresponding tothe 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.

given potentiels with the phase of the letter ooncerned. The result is that the difference of potential of the filement end of thyratron A the grid oeoillates with an amplitude of at least $2\pi E/27$, 26 phase E being the amplitude of the original supply, unlese A end A'8are oonneoted through the chain, in whioh oase the potentielsremain the seme or differ only by whatever grid bias hee been put into the grid oircuit. The thyratrons are so adjusted that an oscillation of amplitude $2\pi E/27$ will bring the potential of the grid to the oritioal value and the valve will'fire'. The valve is coupled with a relay whioh only trips if the thyratron feils to fire, This relay is eotually a 'differentiel reley', with two sets of windings, one carrying a constent ourrent end the other oarrying the ourrent from the enode oircuit of the thyretron. Fig 60 shewa a possible form of oircuit. It is probably not the exact form of circuit used in the Pye experiments, but is given to illustrate the theoretioal possibility.

The Spider

We oen look at the Bombe in a slightly different way as e machine for making deduotione about Stecker when the rod stert is essumed. Suppose we were to put lamp-boerds in between the enigmas of the oheine, end lebel the lamp-boards with the appropriate letters off figure . For example in ohain C the lampboard between C1 end C2 would be labelled A. If we were ueing ~~the machine~~ one ~~with a~~ The key-board ~~this~~ could be labelled with the 'central letter'. Now when we depress a letter of the key-board we oan read off from the lamp- boards some of the Stecker oonsequenoes of the hypothesis that the depressed letter is steokered to the oentral letter; for one such consequence could be read off each lampboard, namely that the letter lighting is steokered 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 th e central letter. There is however no reason why, when from one h ypothesis 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 th e 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 c n think of each output or input point of an enigma as repr senting a possible Stecker, and if two of these points are connected together through the enigmas th en the corresponding S ecker imply one another. At this point we might see h ow it all works out in the case of the crib given above. This crib was actually enciph_ered with alph abets which , when corrected for their sSteoker, are those ~~of Fig~~ given below , the numbers over th e crib constatetions giving the columns ~~of Fig~~ headings . The alphabets below most used are 2,3,5,10,23, and these are reproduced h ere for reference

2	3	5	10	23
XN	XH	MD	TB	LV
AP	BU	JZ	IH	WC
QK	EN	CV	RU	DI
CV	PK	SA	XE	OM
TF	QI	YE	CV	XU
UO	AW	GR	JY	FT
MS	OV	PQ	DF	JP
BD	JY	NW	SL	GE
IW	DM	LH	ON	AY
JZ	RZ	BX	QW	NB
GR	SL	FU	AZ	HS
YE	GT	OI	PK	ZQ
HL	FC	KT	GM	RK

In Fig 61 at the top are the chaine, with the po itions end the lettersof the chain. In each column ~~is~~ ere written eome of the letters ~~is~~ which ~~xxxxxxx~~ can be inferred to be Stecker values of the letters et the heads of their columns from the hypotheeis that X is a Stecker value of the central letter E. By no meane all poesible 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 etart that was wrong we should almost certainly have found that ell of the Stecker values of E could be deduced from eny one of them, end this will hold for any cribs with two or more cheine. Remembereing now that with out ~~xxxxx~~ Bombe one Stecker is deducible from another if the corresponding points on the lamp boards ere connected through th a enigmas, a correct rod etart can only be one for which not all th e input points of the chains ere connected together; the poeitions at which thia happens are almoet exactly those at which ~~the~~ a Bombe with simultaneous scanning would have stopped.

~~When we were describing the Bombe~~

Thia is roughly the idea of the 'spider'. It has been deecribed in this section ae a way of getting simultaneous scanning on the Bombe, and hes been made to look as much like the Bombe es poseible. In the next section another description of the spider ie given.

The spider. A second d scription. Actual form.

In our original description of the Bombe we thoug ht of it ee e meth od of looking for characterietics of a crib which are independen t of Stecker, but in th e last eection we thoug ht of it more as a machine for making Stecker deduetion s. This last wey of lookin g at it he obviously great possibilities, and so we will start afresh with thie idea.

In th e leet section verioue points of th e circuit were regarded es ~~corresponding~~ having certain Stecker correeponding to them. ~~Here~~ We ere now going to carry thia idee further and have a metal point for each possible St cker. 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 that~~ constatations obtained from ~~an~~ ~~experiment with~~ the enigma without Stecker give information about inside letters rather than outside. Our statements will usually be put in rath ~ 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 th e '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. $\overset{Q}{I}$ 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 se up for the correct position, then one of the pairs in th e alphabet in position 24 is OC: Consequently if ~~it~~ Qo than Ic (i.e. if outside letter Q is associated with inside o then outside I is associated with inside c). 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 th e "o" input point is connected to the "o" output point we shall have Qo on the diagonal board connected to Ic through the Letchworth enigma. ~~Ex every deduction that can be made about the Stecker are paralleled in connections between points of the diagonal board. If we then~~ 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 th e association of inside and outside letters paralleled in the connections between th e points of th e diagonal board. We can also bring in the reciprocal ~~ex~~ property of the Stecker by connecting together diagonally opposite points of the diagonal board, e.g. connecting Pv to Vp. One can also bring in other conditions about the

Stecker, e.g. ifone knows that the letters which were ~~xtmxkarmdx~~ ~~xxxxxxxxxy~~ unsteckered on one day are invariebly steckered on the next th en, having ~~xxixxd~~ found the keye for one days traffic one could when looking for the keye for the next day, connect together all points of th e diagonal board which correspond to non-steckers wh ich had occu rred on the previous day. This would of course not entirely eliminate the inadmissible solutions, but would enormously reduse their number, the only solutions which would not be eliminated being those which were inadmissible on every ~~xxxxy~~ count.

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

Our mach ine is still not complete, as we have not put in any mechanism for distinguishing correct from incorrect positions. In th e case of a crib giving a picture like Fig 59 where most of the letters are connected together into one 'web'it is sufficient to let current into the diagonal board ~~xx~~ at some point on some line ~~xith~~ named after a letter on the main web,e.g. at the Ee 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 th_e other points of the E line of the diagonal board. We can detect whether this h_appens by connecting the points ofthe E line through differential relays to the oth er pole of our current supply, and putting the'on'points of the relays in ~~series~~ parrallel with one another and in series with the stop mec. 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 ~~i~~ one of th_ese relays, and the current permenently flowing in the other ~~wiring~~ coil of the relay causes it to close, and bring the stopp ing mechanism into play. ~~This will mostly happen with~~ 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 position~~s~~ is not correct. Anoth_er possibility is that all relays close except the one connected to the point at which the current enters the diagonal board, and this point then corresponds to the only possible Stecker. In cases where the 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 to possible Stecker.

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. Any 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 three or more rows of contacts together one is also provided with 'commons' consisting of four female jacks with corresponding points connected together. There is also a device for connecting together the ~~input~~ output jack of one enigma ~~wit~~ and the input of the next, both being connected to another female jack, which can be used for connecting them 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 stopping devices. There were also 15 sets of commons.

Figs 63 , 64 shew 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 ~~[illegible]~~ an attempt to find simultaneous scanning for th e Bombe, but ~~[illegible]~~ to make use of the reciprocal character of the Stecker. This oc urred at a time when it wa clear that very much shorter cribs would have to be worked than could be managed on the Bombe. Welchman then discovered that ~~[illegible]~~ by us ng a diagonal board one could get the complete set of consequences of a hypothesis . The ideal machine that Welchman was ~~[illegible]~~ 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 shewing each one ~~[illegible]~~ 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 di rect contradictions.

~~[illegible]~~.

Naturally enough ~~[illegible]~~ WelchmanA and Keen set to work to find some way of adapting the spider so as to detect all direct contradiction s. The result of this research is described in the next section. Before we can leave the spider however we should ~~[illegible]~~ 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 th e problem and consider only ~~[illegible]~~ normal stops, i.e. positions at which b y altering th e point, at which the current enters the diagonal board to another pt on the same line one can make 25 relays close & there is only one such pt. The current will th en be

	5out, D	5out, E	5out, F	5out A	5out, B	5out, C
Input jack	Fa	Fb	Fc	Fd	Fe	Ff
	5in, A	5in, B	5in, C	5in, D	5in, E	5in, F
Engine 5						
	5out, A	5out, B	5out, C	5out, D	5out, E	5out, F
Output jack	Ca	Cb	Ce	Cd	Ce	Cf
	5in, D	5in, E	5in, F	5in, A	5in, B	5in, C

	1out, F	1out, D	1out, E	1out, B	1out, C	1out, A	
	Fa	Fb	Fc	Fd	Fe	Ff	
Input jack	1in A	1in, B	1in, C	1in, D	1in, E	1in, F	(arising from substitution $\frac{F}{A}$)
Engine 1							
	1out, A	1out, B	1out, C	1out, D	1out, E	1out, F	
Output jack	Aa	Ab	Ac	Ad	Ae	Af	
	1in, F	1in, D	1in, E	1in, B	1in, C	1in, A	

	2out, B	2out, A	2out, D	2out, C	2out, F	2out, E	
	Aa	Ab	Ac	Ad	Ae	Af	
Input jack	2in, A	2in B	2in C	2in D	2in, E	2 in F	
Engine 2							(arising from $\frac{A}{C}$)
Output jack.	2out A	2out B	2out C	2out D	2out E	2out F	
	Ca	Cb	Cc	Cd	Ce	Cf	
	2in, B	2in, A	2in D	2in C	2in F	2in E	

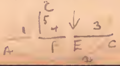
	3out, F	3out D	3out, E	3out B	3out, C	3out, A	
	Ca	Cb	Cc	Cd	Ce	Cf	
Input jack	3in A	3in B	3in C	3in D	3in E	3in F	
Engine 3							(arising from $\frac{C}{E}$)
Output jack	3out A	3out, B	3out, C	3out, D	3out E	3out, F	
	Ea	Eb	Ec	Ed	Ee	Ef	
	3in, F	3in, D	3in, E	3in, B	3in, C	3in A	

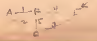
	4out, C	4out, E	4out, A	4out, F	4out, B	4out, D	
	Ea	Eb	Ec	Ed	Ee	Ef	
Input jack	4in A	4in B	4in C	4in D	4in E	4in F	(arising from $\frac{E}{F}$)
Engine 4							
Output jack	4out A	4out B	4out C	4out. D	4out, E	4out, F	
	F.a	Fb	Fc	Fd	Fe	Ff	
	4in, C	4in, E	4in, A	4in, F	4in, B	4in, D	

Fig 63. Spider connections with engines for 6 letter alphabet and with

	1	2	3	4	5		1	2	3	4	5
	A	C	E	F	F	alphabets	A F	A B	A F	A C	F C
	F	A	C	E	C		B D	C D	B D	B E	B E
							E C	E F	C E	D F	D A

Names of contacts are given in purple ink, contacts to which they are connected in green. Connection of diagonal board to engines Fig 64.





Aa , 1out, A 2in, A	Ab Ba 1out, B 2in, B	Ac Ca 1out, C 2in, C	Ad Da 1out, D 2in, D	Ae Ea 1out, E 2in, E	Af Fa 1out, F 2in, F
Ba , Ab	Bb	Bc Cb	Bd Db	Be Eb	Bf Fb
Ca , Ac 2out, A 3in, A 5out, A	Cb Bc 2out, B 3in, B 5out, B	Cc C 2out, C 3in, C 5out C	Cd Dc 2out, D 3in, D 5out D	Ce Ec 2out, E 3in, E 5out, E	Cf Fc 2out, F 3in, F 5out, F
Da , Ad	Db Bd	Dc Cd	Dd	De Ed	Df Fd
Ea , Ae 3out, A 4in A Input A, current voltage	Eb Be 3out, B 4in, B Input B (voltage)	Ec Ce 3out, C 4in, C Input C	Ed De 3out, D 4in, D Input D	Ee 3out, E 4in, E Input E	Ef Fe 3out, F 4in, F Input F
Fa Af 4out, A 1in, A 5in, A	Fb Bf 4out, B 1in, B 5in, B	Fc Cf 4out, C 1in, C 5in, C	Fd Df 4out, D 1in D 5in, D	Fe Ef 4out, E 1in, E 5in, E	Ff 4out, F 1in, F 5in, F

Fig 64. Connections of diagonal board. See fig 63. 'Input' is at E. Current hypothesis E/A. The squares in this figure represent contacts. As in fig the purple letters are names and the green letters show the contacts to which they are connected.

entering et e cor ect Stacker if the position is correct. Let us further simplify the problem by supposing thmet th sre is . only one 'web', i.s. thet the 'picture' formed from ths part of th s crib that is being ussd forms one connected piece, s.g. with the crib on p   we should havs one web if ws omit the constatations $\overset{P}{B}$, $\overset{B}{U}$,$\overset{U}{O}$,$\overset{R}{H}$. ~~Clearly a sufficien t condition for a stop is th at the 'multiple encipherment' conditions should hold. Supposing th at the number of independent chains or 'closures' is c then the number of positions where th e multiple en cipherment conditions hold will be about 26^{4-c}~~. Some of th e constatations of the web could still be omitted without eny of th s letters becoming disconnected form ths rest. Let us choose soms sst of such constatations, ~~whichxxxxxxx [illegible]~~ in such a wey th at we cannot omit eny more constat tions without th s web breaking up. When the constatati ns are omitted there will of course be no 'chains' or 'closures'. This set of constatations may be called th e 'chain-closing constatation s', and th s others will be called th e 'web-forming constatations'. At any position we may imagine that th e web-forming constatations are brought into play first, and only if th e position is possible for these are th s chain-closing constatations used. Now the Stecksr value of the input letter an d th e web-forming constatations will completely determine the Stecker values of the letters occurring in the web. When the chain closing constatations arebrought in ~~the~~ it will already be completely determined what are the corresponding 'unsteckered' constatation s , so that if there are c chain-closing constatation s the final number of stops will be a proportion 26^{-c} of the stops wh ich occur if they are omitted. Our problem reduced therefore to th e case in which there are no closures. It is, I hope, also fairly clear that the number of stops will not be appreciably affected by the branch arrangement of the web, but only b_y the number of letters occurring in it. These facts enable us to make a table for the calculation of th e number of stops in any case where there is only one web. The meth_od of construction of the table is very tedious and uninteresting. The table is reproduced below

(H-M for Holler J-Martin, of British Tabulating Machine Company

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	0.00045
14	0.000095
15	0.000016
16	0.0000023

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

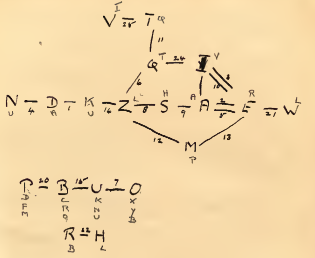
c is number of closures

A similar table h as also been made to allow for two webs, with up to five letters on the second. ~~Beyond this~~ To th e case of th_ree webs it is not worth wh ile and hardly possible to go. One/can/ get a sufficiently good estim te in such casees by using common-sense inequalities, e.g. if we denot e the H-M factor for the case of webs with m,n,and p letters by H(m,n,p) we shall have th e common sense inequalitiee

$$\frac{H(m,3,2)}{H(m,0,0)} < \frac{H(m,3,0)}{H(M,0,0)} . \frac{H(m,2,0)}{H(M,0,0)}$$

$$H(m,3,2) > H(m,4,0)$$

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 E, 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.



Relevant parts of alphabets

1	2	3	4	5	6	7	8	9
AU	AR	RV	ND	AR	GL	KX NY UB	LH	AH
10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
RV	GT	LP	ME	LU	CK RN OU			
19	**20**	**21**	**22**	**23**	**24**	**25**	**26**.	
DC FR MD	RL —	BL	AV	VT	GI			

Fig 65. Illustrating the kind of position at which the Spider will stop. Here the input letter may be supposed to be E and the relay which closed R. The Stecker values of the letters, which are consequences of the hypothesis E/R are written against the letters. There are contradictions such as Z/L, W/L: P/D, P/F, P/M which are not appreciated by the spider.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										
11																										
12																										
13																										
14																										
15																										
16																										
17																										
18																										
19																										
20																										
21																										
22																										
23																										
24																										
25																										
26																										

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 th e 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 brough t in to play, which looks more closely into th e 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 ~~machine gun~~ spider stops that would be passed by ~~the~~ a machine gun as possible would be higher than th e ~~proportion~~ ratio of ~~total~~ 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 spider's 1/10 second only 8 minutes would be added to the time for the run.

When th e epider etone, norm lly the points of the diagonal boerd which are energieed are these corresponding to supposedly false Stecker. Naturelly it would be easier for the machine gun if the points energieed ~~were~~ corresponded to supposedly correct Stecker. It ie therefore necessary to have some arrangement by which immediately after the epider stops the point of entry of th e current ie altered to th e point ~~at~~ to which the reley which closed was connedted, or is left unaltered in th e caee th et 25 relays olosed. Mr Keen has invented some device for doing thie, depending entirely on reley wiring. I do not know th e details at present, but apparently the effect ie that the mechine does not etop at all except in cases in which ~~the~~ either juet one relay closes or 25 releye close. In the case that 25 relays close the cu rrent is allowed to continue to enter at the same point, but if just one reley closes the point of entry is ch anged over to this reley. Thie method hes the possible dis dvantege that e certain number of poesible solutione mey be miesed through not being of normal type. This will only be serious in cases where the frequency of epider stops is very high indeed,e.g. 20%, end some oth er method, such as'Ringstellung out-out' ie being usedfor further reducing the etops. An alternative method is to have some kind of a'scanner' which will look for ~~letters which~~ relays which are not connected to any otherme. 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 contradictione in the Stecker; in order to reduce th e number of relays involved this ie done in stages. In the ~~fi~~ first etage we ee whether or not there are two different Stecker values for A, in the second wheth er there are two different values for B, and so on. To do this testing we have 26 relays

* Now has been decided to use scanner.

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 ofthe 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; ~~and~~ 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 ~~printing~~ typing one letter in a column headed by the other. When any letter is being tested for Stecker contradictions the relays corresponding tothe 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 is ~~written~~ typed instead shewing that the whole is wrong. When no relay closes nothing is typed. The ~~keys~~ 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 ~~changes~~.

Additional gadgets

Besidee th e spider and mechine-gun a number of other improvements of the Bombe are now being plenned. We have alrerdy mentioned thet it ie possible to use additionel dete about Steoker by connecting up points of th e diegonel boerd. It ie plenned to mcke this more streigh tformerd by leading the points of the diagonal bberd to 325 points of e plug boerd; the plug boerd elso h_as a great many points ell conneoted together, end eny Stecker which one believes to be false one simoly oonn ote to|this set.

Another gadget is designed to deel with oeees such as that in which there are two 'webe' with six end no ohains letters on eech. A little experiment will show thet in the greet majority of cases with sûch dete, when the solution is found, the Steoker value of e letter on either web will imply the whole eet of Steckers for the letters of both webs: in the ourrent terminology,"In the right plece we oan nearly always get from one web onto the other". If however we try to run suoh dete on the spider, even with the machine gun attachment, there will be en enormous number of stops, and the vast majority of these will be oases in which " we have not got onto the second web". If we are prepered to reject these possibilities without testing them we shall not very greatly decreese the probebility of our finding the right solution, but very greatly reduce th e emount of testing to be done. If in addition the epider oen be persuaded not to etop in theee positions, the spider time saved will be enormous. Some arrangement of thie kind is being made but I will not attempt to describe how it works.

With eome of the oiphers there is information ebout the Ringstellung (Herivelismue) whioh mekee certain stopping 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 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 relaible. 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.

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

	H	I	J	K	L	M
A	KSREKYB	K●SBC	KTNN	UQEE	MNWH	
B	OVWKZ	RTH	QP	UJTLXGL	NU	MNEL
C	ZP	TEL		FQSW	P	OTM
D	LJLM	LN	UTE	ELEU	NU	QKKY
E	JVXIQF(I)U	JTNXVJLO	RRYRNT	UYWN	SMFLYN	TIFWXSZ(4)
F	H	OOP	ZZO	NUZI	Y	NJWKO
G	THNS	IRVYM(I)	MRR	TX	UO	KI
H	IOOO	X	SNZ	N	TQ	JQ
I	YPMK	S	NTRRXM	SZ	QZU	UXLL
J			KSU	NY	PN	NT(7)
K	S	ST	T		OTXRL	
L	Z	NNV	S	V(V)YVX	NQUZW	WXS●(5)
M	RN		UN(U)	V		SZ
N	WW	PYOQT	SUOZ	Z	SQ	SU●
O	RS	X	ZTUX	TUQ		YYW●
P	S		U	RS		U
Q		XR	VW	ST		
R	TYTSX			VUW	SVTV	YTUX(Ø)
S	V		VUWY			Z
T		ZY~~Y~~W(W)		YZ		U
U	W		W	V		W
V			Z		S	W
W						Y
X						
Y		Z				
Z						

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

	T	U	V	W	X	Y	Z	
A	KTNZIH	BHRP	MY	EHRIF	FFLURR	ICUSB	IZN	A
B	VUR	EIISKE	STUNLT	RG	SRQR	ETRL	IM O	B
C	RNX	JWL	PJO	DGY	JHTUJ	XPUU	RJEVZ	C
D	ZQV	REN	IFYPR	IUE	KKN	HSN	WMHX	D
E	ILIXFL	YJXNVLJH	SPQM	SLQSVYUFK	NKKVM	YWWMV	RZL	E
F	GS	HKQV	NL	N	S	LO	LNJJH	F
G	RXKZ	TSNO	WORVU	YWO	ZI	WKTN	W	G
H	NTN	QVN	WT	T	TNRN	TRPLL	NRNI	H
I	JOXQ	OW	KOZKS	XVZQ	OYLV	TM	WJNO	I
J	SL		LN	QKY	PS	L	O	J
K			O	S	Y	SNYXT	OUR	K
L	SUV		T	PRNN	OTR	U	ZTTV	L
M	X	SUY	N	T	TS	XR	NORV	M
N	T	OS	W	XTXQY	OOYSTTV	TSSX	XTOS	N
O		QX	UQ	WSX	X	R		O
P	WR		V	X	UU			P
Q		S			R	S		Q
R	SV	UV	YZS	ZZ	VY	NW		R
S	W				XT		ZZ	S
T			WUW	W		XZ	U	T
U					ZV	V		U
V	W			X		Z	A	V
W	Y							W
X			Y	Y				X
Y		Z						Y
Z								Z

λ

AB A KEA FKA WMA.

CD

EF REB FKB WMB.

A□B

B C

C D

[illegible]

E F

F

G

H

I

J

K

if alphabet REA is A|D then B|E will be part of alphabet REB.

But this is not true if there is a turnover between A & B

Suppose A|D

B E [illegible]

Turing

19/5 1736/92 44

18-9

```
    5    10    15    20    25    30    35    40    45    50    55    60    65    70    75    80
NUEXEORAXNEONVTHYGLOIHTSVXTEIITLEZRRUNUODLEBHEUSAUTJHBFVEDDBESERCANEHETFCTFTSVEU

   85    90    95   100   105   110   115   120   125   130   135   140   145   150   155   160
AREONCFEEESURJLJIUGLTFNEONEEUBMIORTNIHLIISCUJBBLAXIAXZGMSBSSJNVITODSGNTEDKEDVREF
```

Chapter VII. The German Naval Enigma Cipher

Historical

In the period from about 1931 to April 30, 1937 the Naval cipher much used the same indicating system as the other German service enigma ciphers, viz. the 'boxing' method recommended by the firm that sold th e 'commercial' enigma. With this 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 trigrammes e.g. ZLE. One then set the machine to th e Grundstellung and enciphered ZLEZLE. The resulting six letterms were put at th e beginning of the message, and the remainder of the message consisted of th e result of enciphering the plaintext with pre-start window position ZLE. (This differs from the other boxing indicating systems in th at most of these allow the trigramme such as ZLE to be chosen at random instead of from a restricted list.

The weakness of this indicating system is that a great deal of information is given away about th e 'Grundstellung'. If there were no Stecker, and a known diagonal and the traffic amounted to 100 messages per diem it would be possible to find th e connections of the machine, and if there were Stecker but the connections of th e machine were known it would be possible to find the keys every day from the same amount of traffic. To explain the possibility of finding the keys let us suppose that the following were a set of indicators for on a day's traffic/

UJOOBL
VEYITM
ALAJMB
XDVBXV
QLYAMM
GRYLZM
JIPSWW
YEIFTI
BMARFB
TZNGOR
AYIJPI
UJNOBR
OQBVCY
FNXDUJ

AFIJVI
MIEHWZ
KMIPFI
NUZIJG
IIFQWN
KGAPRB
SMLKFX
RFXCVJ
LGKZRP
BANRDR
GXJLEF
EKXXYJ
TXNGER
OIKVWP

TIOGWL
LNVZUV
CZNYOR
RLFCMN
LMWZFC
MIDHWU
AUXJJJ
UWIOSI
FXRDEK
EYYXPM
ZCDWLU
EZSXOH
VZPEOW

RSICAI
APTJNA
GJWLBS
CWUYSQ
RBDCQU
IHVQIV
OOFVCN
RZHCOO
AVRJKK
GIILWI
UAMODC
SCQKLE
DLYMMM
EYVXPV

JNZSUG
UANODR
HALUDX
UOG OHT
ZFUWVQ
JSWSAS
ZDIWXI
KPBPNY
FTGD T
HEKUTP
UHWOIS

In th e two indicators UJOOBL and UANODR th e repetition of th e first letters is followed by a repetition of the fourth letters. Th at this must always happen is clear from the fact that th e fourth letter arises from the first by enciphering at the postition directly after the Grundstellung and re-enciphering three places further on. This phenomenonenables us to tell very quickly with any cipher whether the Boxing form of indication is being used. From th e indicators we can find the effects of th e 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 th e entry J against A, with ~~four~~ five dots. This means that A enciphered at the first and fourth positions gives J, and that this information h as been given us from six indicators, which are actually ALAJMB,AYIJPI,AFIJVI, APTJNA,AVRJKK,AUXJJJ. The other two columns give us the results of the encipherments at th e second and then the ~~thi~~ fifth position, and at the third and then the sixth. We get for the result s of these double encipherments

G_4G_1

...NIQAJSKP...TGLZW...(DMHUGVEXBRCYF)

G_5G_2

(PNUJBQCLMFVKY)(OHIWSADXETGRZ)

G_6G_3

(V)(I)(JFNRKPWSHOLX)...DUQEZGTABYMC...

G_4G_1 here means the encipherment with the first alphabet an d then with the fourth, the reversal of the natural order being in agreement with mathematical tradition. There can be no doubt as to h ow the substitution G_5G_2 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 'al phabets and boxes' we see that it must be possible to pair off the cycles of G_4G_1 into ones of equal length.

49
132

here are varioue things which could be done now. Of course onemight put the whole data onto the epider, but at th e time that this syetem 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 ofthe box shapes ~~which~~ for G_4G_1, G_5G_2, G_6G_3 for every Grundstellung, assuming that there ie not e T.O. between the first and last of the eix alphabets. ~~It is the box shapes are independent of the Stecker~~

or numbers

If we give some standard order to the box shapes, we can also put the poesible series of three box shapes into an order, end can enter egeinet each set of three box ehapee th e Grundstellungen for which th ie set is realieed. To use thie catalogue with our problem we ehould work out the box ehapee viz. $G4G_1$ is 26, G_5G_2 ie 26, G_6G_3 ie 24,2. The~~se~~ box shape~~s~~ ~~actually have the numbers 1~~ 26 actually hae the nuber 1 and 24,2 the number 2: they are the two commonest shapes as can be seen from the table p 19a . We then look up 1.1.2 in our catalogue, and find about 150 entriee against it for each wheelorder. Each of th ese will have to be tested out in some way or other. The moet satisfactory method seems to be this: We form th e permutation ~~$G_4G_1G_5G_2$~~ $G_6G_3G_5G_2$. It is

(PRGKMNQDJYWHISBEAUFV)(CXZL)(O)(T)

so th at thie permutation ie of the olass 20,4,1,1. For each possible rundetellun it is possible to calculate ~~this~~ the corresponding class for the unetec~~k~~ered 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 th e time of con struction of the catalogue. ~~It will~~

In the case in question the right Grundstellung is found to have th e position 1,1,26 with wheel order ~~III~~ I,II,III (service machine, Umkehrwalz A). The corresponding boxes are

DT	PZ	CL
MG	RN	TQ
HL	UG	XU
UP	JL	JD
CK	BE	FO
AI	QX	RM
EJ	OD	NY
XV	TV	KB
BQ	MI	PV
NS	FW	WL
OR	AS	IG
YW	KH	HZ
FZ	YC	AS

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

(OHIWSADXETGRZ)
(CHSWIVDXELGNZ)

i.e. we ~~xxxxx~~ have to assume the stecker O/C,I/S,A/V,T/L,R/N, and that H,W,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 res of the boxes together we find that these five are all the Stecker.

There are other methods that can be applied, dependin 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 constatation $\overset{A}{S}$ occurred in both the alphabets $G_3$and G_6 . With the Turing sheets we could find the possible positions for this, andthen use a cyclometer to test ~~xxxx~~ 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 ~~xxxx~~ alphabets $G_1$and G_4 were. In our case there are actually 13 different possibilities for G_1, 13 for G_2 and 12 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 ~~message settings that have xx occurred pre~~

repetitions between the message settings for the day in question and message settings of previously solved days. We might also do a 'Banburismus' 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 ~~letter~~ 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 ~~there~~ are better methods of equating. Once the boxes have been equated by one means or another we shall have many more cases of ~~the~~ 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 ~~next~~ parts after the first began by saying that they were continuations, giving the time group of the last part of the ~~previous~~ message as a reference. The method of giving numbers at that time was to use the top row of the key board and P thus

QWERTZUIOP
1234567890

The number was put between Y's to shew that it was a number, and the whole repeated as a check. The continuation of a message whose time group was 2330 would ~~FORTY~~ begin FORTYWEEPYYWEEPY . We could then find th e 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 th e indicator. The repetition also showed that no check could be expected within the ~~in~~ first two groups themselves. This was discouraging, as the essential weakness of the boxing method was that the same thing was enciphered twice with the machine. With the new method of indicating, whatever it is, th e best one can hope is that either it will enable us to'set'the messages, or that ~~wx~~ from some information about the setting of the messages obtained form elsewhere we may be able to deduce something about the ~~affixx~~ 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 th e wheel order and Ringstellung had remained the same during the end of April and the beginning of May. This made it easier for them to find th e keys for othe days at th s beginning of May and th ey actually found the Stecker for the 2nd, 3rd, 4th, 5th and 8th, and read about 100 messages. The in dicators an d window positions of four (selected) messages for th e 5th were

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

The repetition of the EW combined with th e repetition of V suggests that the ~~third and fourth~~ 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 th eir bigramme equ valents, 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 equiv lents 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
XXKX JXJY	V U E
RCXX JLWA	N U M

With this second alternative we can deduce from the first two indic tors that the bigrammes EX and XX have the same value, and this is confirmed from the second and third, where XX and EX 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 teke plece eccording tothe old system until May 4, when the bigramme tables would be supplied. Sufficient traffic passed on May 2,3 fmr to and from AFA: for the Grundstellung used to be found, the Stecker having alre dy been found from the FORTYWEEPY messeges. It was natural to assume that the Grundstellung used by AEA: 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 et least two Grundstellungen instead of one. One of them was called the Allgemaine and the other the Offiziere Grundstellung. This made it extremely difficult to find eithter Grundstellung. The Polee 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 prison er told us that the German Navy had now given up writing numbers with Y...YY...Y and that thxxyxxxx the digitw of th e numbera were spelt out in full. When we heard this we examined the messages toward th e end of 1937 which were expected to be continuati ns an d wrote th e expected beginxiinings under them. The proportoin of 'orsshes' i.e. of letters apparently left unaltered by encipherment, xhxx then shews how nearly correct our guesses were. Assuming that the change xxx mentioned by the prisoner had already taken place we found th at 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 chan ges in the machine, known toh ave taken place because of the corresponding changes in the machine used by the army and air whose traffic h ad been read. In the summer of 1937 the Umkherwalze had been changed from A to B, and in Dec 1938 two new whe-ls ~~ix~~ IV and V had been introduced. ~~[illegible]~~ After the beginning of the war (Sept 1939) the FORTYWEEPY messages were no longer traceable, because there were no more call signs of this kind.

Some [illegible] [illegible] Sept but The Secret War has 15 Dec December must be accepted

However there had been some traffic at various times during ~~manoeuvres~~manoeuvres and crises sinde the occupation of Austria, ~~There~~ ~~seemed to be a chance that one might be able to find some~~ ~~keys by using FORTYWEEPY~~ and there were a few days where there was both traffic with and without call signs. We hoped that we might be able to find the keys for some such days and~~xx~~ so to find the kind of thing that was said in the traffic without call signs. ~~[illegible] actually found the keys found~~ There seemed to be some doubt as to the feasibility of this plan, as ~~[illegible]~~ the call signs traffic on any day was always either the whole of the Baltic traffic or the whole of the non-Baltic traffic, and the Baltic traf ic in 1937 usedto be on a differen t key from th e rest. Following this programme we found the keys for Nov. 28 1938 and for a number of days near there. The number of Stecker w s 6. Th e wheel order and Ringstellung seemed to remain constant for about a week; at an y rate they did not change between Nov 24 and Nov29. The Stecker ~~[illegible]~~ were not hatted; the same letter was never steckered on t o consecutive days. This of course might be extremely valuable. If the traffic had been h eavier it would have enabled us to find th e keys so long as this lasted, and there were any cribs. Actually we got no furth er than this, as at this point a good deal of data was.

'pinched' fr m a German boat, enabling ue get the keys for April 22-27 1940. At the eame time we pinched a book of instru otions telling us th e precise form of the indioating syetem.

To enoipher a message the operator oh oosee two trigrammes ou t of a book. The first of these trigrammes is oalled the 'Sohluesselkenngruppe'. The ohoice of this is partly determined by the neture of th e message: e.g. all 'dummy' messa es heve th e Sohluessel ksengruppe taken from one part ofthe* book and genuine messages heve them taken fr m slsewhere; we do not kn ~~ow~~ very much ebout th eee. Th e ssoond trigramme isoalled the Verfsh~~ren~~kenngruppe . Suppoee the Schluesselkenngruppe ie CIV and the Verfahren kenngrupps is TOD then the operator ohooses two dummhy letters, Q and X say, and writes this down

```
Q O I V
T O D X
```

From the Verfehren kenngruppe is obtained the window poeition for th e start of th e message, by eh ciphering at the Grundetellung. From th e eight letters sbove, one also obtains the indioator for the messege, by substitution from e tsble whioh gives bigfemme for bigramme. Th e ~~xarxix~~ subetitution is done by replsoing the vertical pairs ebovs with bigremmes, e.g. ~~ifx~~ in this oase, if the subetitute for QT were DA, end TH for CO, PO for ID, and CN for VX then the indioetor for the mesesge is DATH POCN. Apart from the Sohlueseel kenngruppe feature thie is the method we had inferred was being used. ~~Thexthe~~ This extra feeture accounts for the bigrammes in th e indioatore being elmost perfectly h stted. Also th e foot that it is never the message eetting itself wioh ie ohosen at random by the operator sliminates eny remaining hope th at one might use 'operstor's psychology' to help in finding out th e alphabete. From our point of view of course the Sohlueseel kenngruppen migh t ss well not exist, an d th e (bigram e lists'to us remain Foes eheets with on e letter entered ~~xxxxx~~ in each square, and not two . There is however the restriction that there must be exsotly 26 oocurrences of eaoh letter.

* This has gone out of date

Methods of reading the individual messages

With th e system of indication that h as been used since May 1937 we are not able to read all the messages as soon as we have read on e. A few may be read by single wheel processes, starting from a short crib, bu t we cannot hope to read the whole traffic in this way. Also, when we have found the Grundstellung , an d if there is plenty of traffic, we may be able to make use of some bigrammes which occurred in messages already read. These methods are not enough by themselves/ In th e 1937 traffic there was no 'mot probable', and we had planned a method for finding the right starting position, making use of the fact that th e 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, th e punching shewing the effect of enciphering E in the various positions. This paper was to move under a series of about 200 brushes whose position was determined by th e letters of the enciphered message. The number of brushes which poked through the holes at any moment was th e number of letters E in th e decode of the message, the window position bein g 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 indepen dently tested. This machine was called 'th e rack'.

It was never n ecessary to make a rack because when the 1938 messages were read it was found th at the word EINS occurred veryfrequen tly. We therefore made a catalogue of th e encoded values of EINS at every possible starting position, an d 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 on lines. The values of I were stuck below the values of E with a stagger: the values of N and S were underneath th ese again, with suitable staggers. The result was that the effect of enciphering EINS appeared in vertical columns.

This unanalysed catalogue was known to th e girls as 'corsets'. In analysing the catalogue we took 25 sheets n amed A to Z, with E omitted: each sheet had 25 lines, named A to Z with I omitted. Supposing on sheet 13 and line 4 of th e corsets we found LVOM as a value of EINS 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 th e messages accoring totheir first letters. One would then take th e A existence sheet and go through all th e messages marking the tetragrammes which occurred on th e 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 'snaking'. Having foun d the position one would have to set up th e m chine, decipher the tetragramme, verifying that it gave EINS 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 encipherin g EINS in all positions in a much more convenient form. Also we n o longer analyse the groups by hand, but have together with their position them punched on cards, which are then sorted into alphabetical order, and listed. A further improvement is th at the test-plate is now made to punch the cards directly.

Roughly, our programme when the wheel order, Ringstellung, and Stecker for a day h ave been found, is as follows. We make an EINS 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 th e other. If we have four such cases we have sufficient data about th e Grundstellung to be able to find it by means of th e Bombe, provided that we have found th e double T.O. ~~Wh~~ We then continueto get messages out with the EINS catelogue; eech message gives us some ~~xx~~ values of bigrammee, which are entered on e Foes eheet. From time to time we go th rough the messegee eubstituting for the bigremmee the velues thet heve recently been found from the messegee. With messagee for which we know the values of two of the bigrammes we epply th e method known es 'twiddling' or 'bonking'. We have to decipher the firet few lettere of the meesage at ell of the 26 pleces consistent with our knowledge of the bigremmee. Thie is usually done in columns,one column at e time,eech column corresponding to a letter of the meesage. The twiddling is best don e on the Letchworth enigmae, ee they h eve no automatic T.O. Some more messegee can be eolved ~~by~~ when one bigramme ie known, preferebly thet corresponding to the L.H.W. on th e test-plate by deciphering e few lettere et every one of the 676 pleces. But this method is rather difficult to work in practice. It seems much more difficult to spot the right enewer when one has to look through eo many poseibilitiee. The right answer ie hardly ever noticed unless it is one of the obvioueones such as BIENE?WESPE,MUECKE,MOSKITO,HORNISSE,KRKR,ANAN,ADMX,GRUPPE,~~BDUUU~~ Bsee. The case where the R.H.W. bigramme is known cannot be done on th e test-plate at all. One ~~xxxxx~~ cen of couree use the X-machinee in much the eame wey as wee done with th e originel form of EINS cetelogue. Thie hes never been e succees. One can also use 'hand methods'. On e cen go through the message looking for plecee wh ere two consecutive letters occur on th e samerod. The deciphered values elso occur on the same rod, end we cen examine the rode for possible bigrammes. Combining this with th e Turing ehe te, Kendrick hee eolved quite e number of mee egee. Thie method is known ee 'clicks on the rods'.

We now have the EINS catalogue collated with the messages of the day so that the only remaining work in EINSing is the testing of each possible EINS on the machine & working out the start

Identificationof bigramme lists and efvaluation of unknown bigrammes.

The Vehfahrenkenngruppe (V.K.G. or trigramme) is as we have explained not chosen at random , but from a list of a out 11,000, and within this list the shoised are not made at ~~random~~ uniformly . This fact enables us to identify which bigramme lists are being used , for if we choose the right bigramme list and work out the V.K.G. we shall find that a comparatively large proportioj of the m have occurred bdfore, and if we choose the wrong one , a comparatively small proportion.

The more precise theory of this identificationis as follows. Let us suppose that o Nthe 26^3 diffesent trigrammes n_1 have ~~the~~ been used before once ~~xtimes~~, n_2 twise etc. Let us call a trigramme which has occurred before r times a trigramme of the r-class". We can them express our information in the form:

Of the occurrrences of trigrammes there have been n_1 in the 1-class, $2n_2$ in the 2-class, $3n_3$ in the 3-class etc:

Now take a random sample of these occurrences, forming a proportioj α of the whole, and let us imagine thet thés random sample sonsists of the last of the trigrammes which were found. There will be αn_1 in the 1 class,. $2\alpha n_2$ in the 2 class,ete. Now the ones in the 1 class would have been , when they were fpund,ones which had not occurred before, and those ~~which~~ in the 2 class ones which had occurred before once, and so on. Hence we can say that for the laest ~~trigrammes found~~ occurrences of trigrammes entered, the numberee which had occurred before not at all, once,twise,threetimes,... are in the retios of n_1 , $2n_2$, $3n_3$,...
We must expect these retios to hold also of the next few occurrrences to be entered. The process of finding new occurrences of trigrammes and lookinfgup th numbers of previous occurrences can therefore be regarded ad like having an urn containing cards, each of which bears a trigramme and a number, and making drawsfrom the urn. The mujmber of cards bearing the nukber r is th be proportional to $(r+1)n_{r+1}$. On the other hand we have to consider the process of choosing trigrammes at random. This i s to be ~~regarded as~~ compared with drawing cards from an urn containing cards in ~~different~~ known proportions.

This process worked well initially. The popular trigraphs were at the top of columns on the centre pages of the K-book, but the German instructions were to mark any trigraph as it was used, and not to re-use it. Thus the repeat rate of the new trigraphs with those known to have been used gradually dropped. The part of the K-book used for this trigraph selection contained all trigraphs, in hatted order. I J. Good in 1941 devised a quicker method, using the non-randomness of the free-choice dummy letter.

JELM 8/2/78

Each of the 26^3 trigrammes must occur equally often on cards in this urn, and must of course have with it the number of previous occurrences of this trigramme. Now imagine that we have worked out a certain number of V.K.G. using a given bigramme table, anf that we have found out how many times each of them had occurred before. This can be compzred with being givewn one of the urns, and told It is Q:1 on this being the random urn, and then drawing a certain number of cards from the urn. After the draw we have a new idea of the odds that the urn is the random urn, and we should have a correspondin modified idea of the odds that the bigramme list is the right one. Let us suppose that the trigrammes, in the order as they were ~~found~~ worked out, had the numbers r_1, r_2 ____ r_s of previous occurrences, and thatrcorrespondingly the cards drawn frok the urn bore the numbers $r_1, r_2, \ldots\ldots r_s$. The proportion of cases of draws of s cards from the urn, giving these results with the same order, is $u_{r_1}, u_{r_2}, \text{---}\ u_{r_s}$ where u_r is the proportion of r-cards in the urn. Likewise the proportionof cases where this happenswith the other urn is u'_{r_1} — — u'_{r_s} with a corresponiong meaning for u'_r. Then the odds onthe urn not being tha random one after the ~~draw~~ experiment are

$$\frac{u_{r_1}}{u'_{r_1}} \cdot \frac{u_{r_2}}{u'_{r_2}} \text{---} \frac{u_{r_s}}{u'_{r_s}} : Q$$

In other words the drawing of a card with the number x m improves the odds by a factor of $\frac{u_m}{u'_m}$, which is equal to $\frac{26^3 (m+1) r_{m+1}}{\left(\sum_{m+1} (m+1) r_{m+1}\right) r_m}$ except in the case $m = 0$ when it is $\frac{26^3 r_1}{\left(\sum_m m r_m\right)\left(26^3 - \sum_1^\infty r_m\right)}$

The same method may be applied for the identification of some unknown bigrammes By taking into account a number od days traffic all using the same bigramme table we may fing a number of indicatorms whose V.K.G. would be completely known if we knew the value of a certain bigramme. If we make the right hypothesis as to the value, we should get trigrammes agreeing with the statistics as before. In this sort of case, as tha data is liable to be very scanty, it is essential to use tha accurate theory as described above.