GENERAL REPORT ON TUNNY

With Emphasis on Statistical Methods.

TABLE OF CONTENTS

Part 5 MACHINES

GENERAL REPORT ON TUNNY

With Emphasis on Statistical Methods.

TABLE OF CONTENTS

Part 6

61 Raw Materials and Production with Plans of Tunny Links

Part 7. REFERENCE

71 Glossary and Index
72 Notation
73 Bibliography
74 Chronology

Part 8

81 Conclusions

Part 9 APPENDICES

91 5202
92 Motor Rectangles
93 Thrasher
94 QKP Research
95 Mechanical Flags

26 WHEEL-BREAKING FROM KEY

26A INTRODUCTION

Wheel-breaking from key is normally a hand process performed largely and often entirely by specially trained Testery breakers on key obtained from depth. The length of such key varies from about 100 to 400. Key obtained from a crib is usually at least 1000 in length and is broken entirely in the Newmanry, largely by mechanical methods. This chapter is concerned only with depth key except where specific reference is made to crib key. This is because

(i) The methods used on crib key are merely extreme simplifications of those used on depth key.

(ii) depth key is of far more frequent occurrence,

(iii) depth key is normally several days more current. It is in fact the quickest way of breaking the day's wheels. Frequently it enabled us to decode the traffic of the current day.

The ease with which key is broken depends on three factors: the length, the number of dots in χ_{37} and the type of limitation used. When these factors are particularly favourable the methods here described can often be simplified or short-circuited. For example, in extreme cases depth key can be treated just like crib key and broken rapidly on Colossus.

Five-to-the-inch squared paper of the kind shown in fig.26(I) is used for all hand work. The ΔK is written out in ink on a width of 62 with 9 squares intervening between each line, but for convenience we use in this report a width of 31 instead. The 5 rows beneath the ΔK are regarded as corresponding to the 5 TP impulses, and each impulse is marked off with an upright ink line on the period of the chi-length for that impulse. All subsequent work is done with pencil and eraser.

26B STARTS

The first necessity is to obtain a nucleus of $\Delta\chi$ signs of which a substantial majority are right. These are termed 'embryonic wheels' and form the basis of subsequent work.

There are three main types of start, apart from the rarely used Δ^2 method described below.

They are

(a) the 5 by 5 and 10 by 10 flags, (R₂ p. 93)

(b) the $\hat{\chi}_0$ count,

(c) the χ_5 composite flag.

(a) The 5 by 5 flag is normally used for non $\bar{X}_{\cdot}$ keys which are long enough to give a good expectation of 5 by 5 flag significance provided that the μ_{37} dottage is not very unfavourable. The method is as follows. Fig.26(I) shows the first 44 letters of a ΔK marked off in chi lengths.

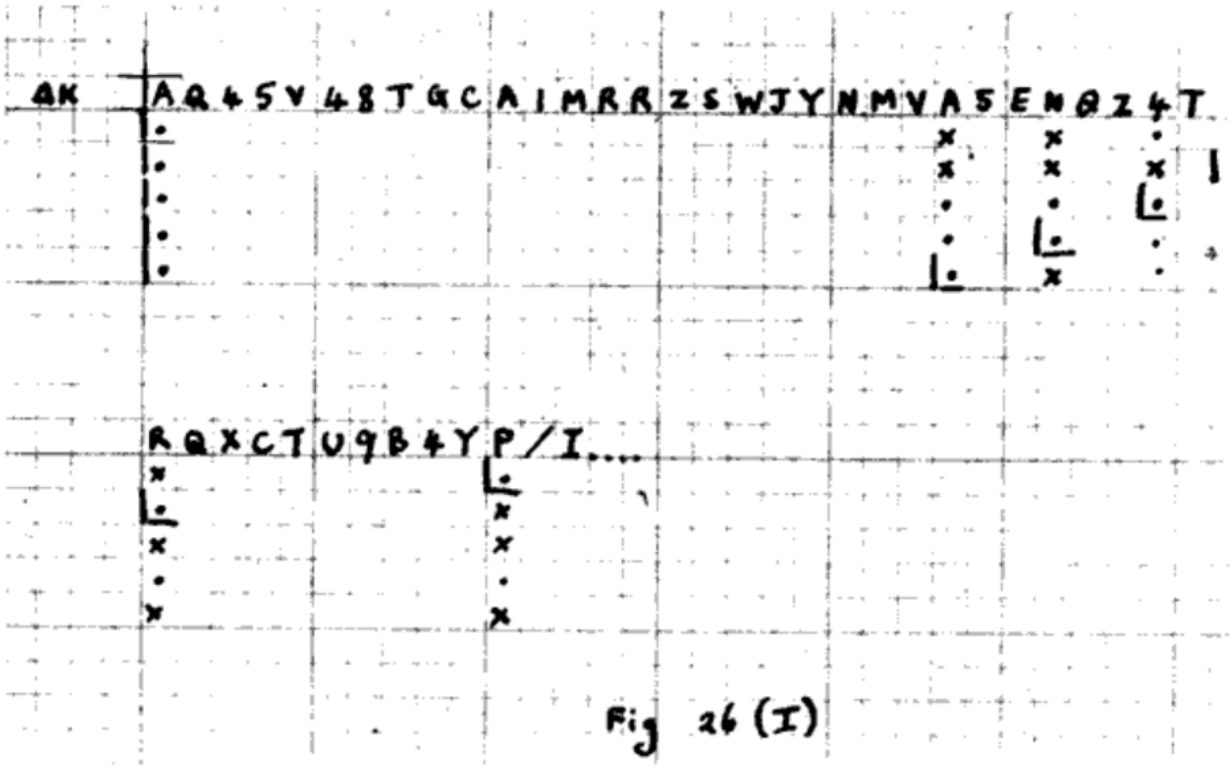


Fig 26 (I)

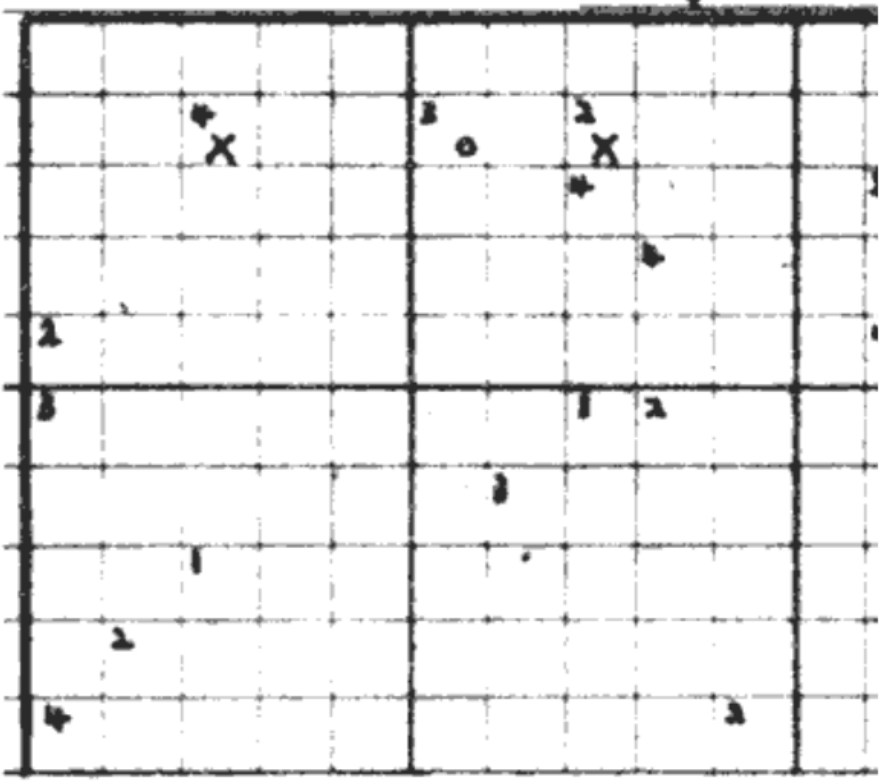
We assume, arbitrarily, that $\Delta\chi =$ these 5 $\Delta\chi$ signs in on the period of th throughout the key. Now the property P one impulse $\Delta\chi = \Delta K$ there is a probabi $\Delta\chi = \Delta K$, and conversely for $\Delta\chi \neq \Delta$ inferences indicated in fig I by signs n

These inferences are written into 5 whose widths are the lengths of the 5) number of the impulse originally assumed inference is drawn. The $\Delta\chi_5$ cage for t fig 26(II).

Fig. 26(I

fig 26(II).

Fig. 26(I



When the 5 cages have been entered v

disagreements among the signs in each col

and crosses for disagreements. For exar

entered as in fig 26(III) scores a disagr

between 3 and 4, and an agreement betweer

comparisons have been booked, we get some

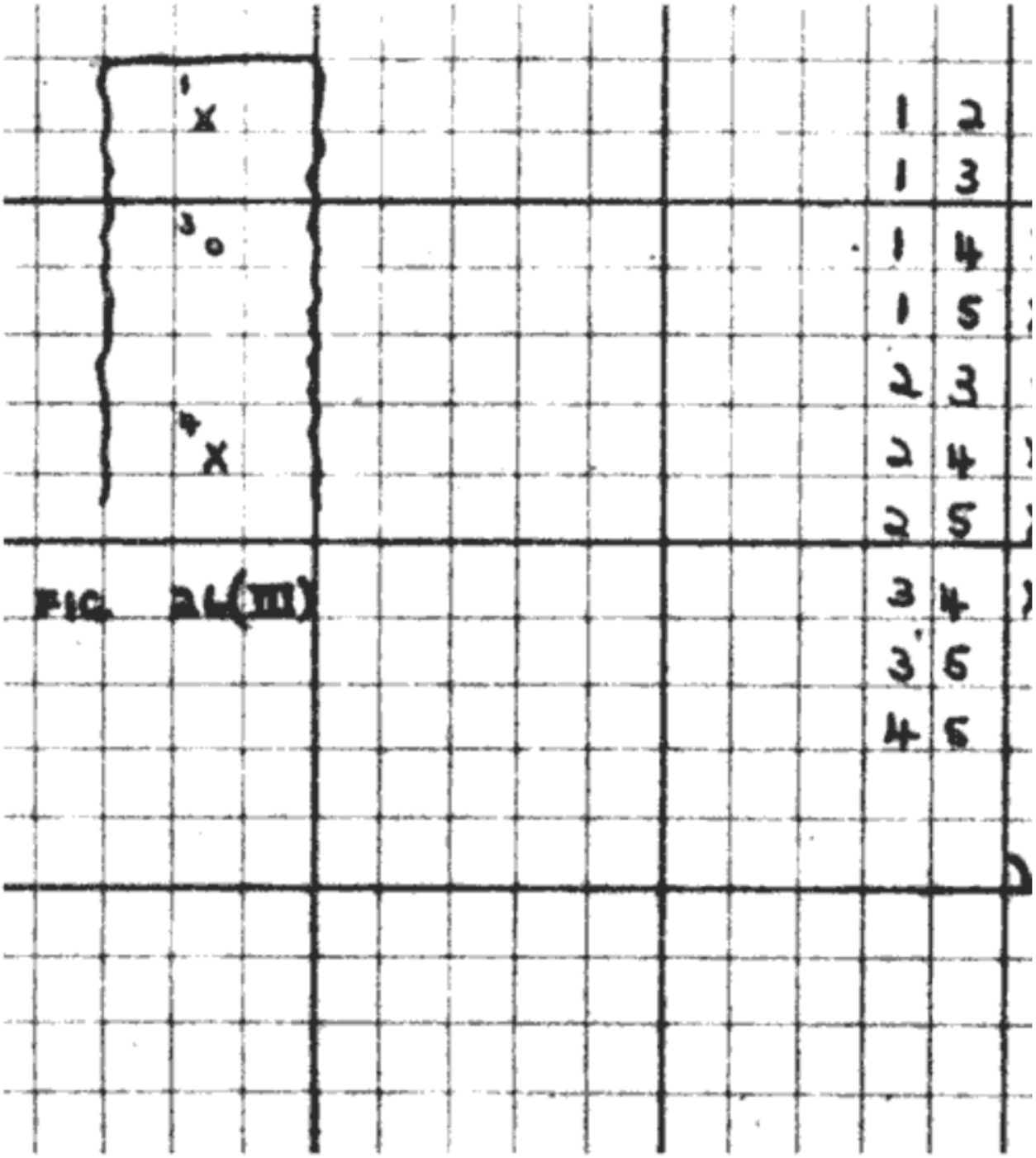
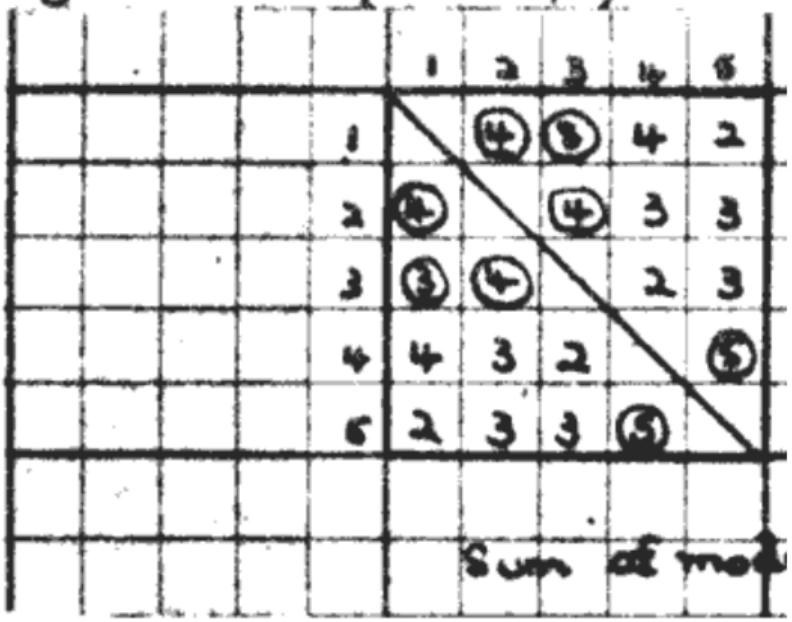


FIG. 2.4(iii)

The right hand column of numbers re
over disagreements, and these numbers ar
which is "converged" thus (see 24C)



We infer that the arbitrary assumpt
must be changed to U (or 0) to give the
comparisons. So all cage entries numbe
and the embryonic $\Delta\chi$'s obtained by su
significance test " $\frac{1}{2}\chi/\sqrt{\nu} \geq 3$", (where $\chi =$
ν = the total number of comparisons) is
start. In the example given in figs IV

To decide which of the two alternati provisionally, we add them to the first l letter. In our example the alternatives first letter of ΔK, A, give $\Delta\Psi' = 9$ and so much more likely than 9 in $\Delta\Psi'$ we acce in favour of 0 rather than U can be seen to 9 d.bs., if b = 2/3. This sort of ar additional sugnificance test for the flag letter as / or 8 we would be quite satisf letter / or 8 is so much more likely a pr alternatives.

The 10 by 10 flag is an amplification o
frequenly used when the 5 by 5 flag has j
the work for the latter flag can easily b
The first <u>two</u> letters of $\Delta\chi$, instead o
strokes, the impulses of the second lette
Then we proceed as for the 5 by 5 flag.

The inferences from $\Delta\chi_2$, 2nd place are
as distinct from those derived from $\Delta\chi_1$
R41 p47). When the comparisons between al
been booked they are entered in a square

The significance test is $\frac{1}{2}n/\sqrt{n} \geq 4$.

(b) The $\hat{\chi}_1$ count is used

(i) to establish by means of the standard significance test for short WB runs that the key is on $\bar{\chi}_1$ limitation, if this is in doubt, or if $\bar{\chi}_2$ limitation is certain, possibly to establish the correctness of the key,

(ii) to give a start for key-breaking.

The property used is

$$\Delta K_2 \xrightarrow{4} \tilde{\tilde{\chi}}_2$$

This can be derived from 22H(9), by regarding P as / throughout so that K = ΔK_2 is written out on a width of 31 and the excesses per column of dots over crosses are written as ringed and unringed numbers. The deciban value of these pips is $10\log_{10}\{(1+p)/(1-p)\}$.

Sometimes the length of key and the dottage are sufficient to give a complete $\tilde{\chi}_2$, from which χ_2 may be derived, as follows:

$\hat{\chi}_1$ is delta-ed to give $\Delta_3\bar{\chi}_1$, which is integrated and slid one to the left. This pattern is χ_2 or $\tilde{\chi}_2$, according to the correctness of the original assumption from which the integration was made. The ambiguity is immediately solved by reference back to the $\hat{\chi}_1$ wheel.

Now we add χ_1 to K_2, and by using the known $\bar{\chi}_1$ limitation we should easily be able to recognise ψ_1 and break the key as described below (26D.)

Normally, however, the $\hat{\chi}_2$ count is significant but does not yield a complete wheel. In this case we make our start as follows. The method rests on the concept that $\bar{\chi}_1$ limitation is a six-impulse key in which ΔK_6 always = . , and $\Delta\chi_6 = \Delta\psi_6' = \tilde{\tilde{\chi}}_1$. (See 22D(9).)(Rev. p. 47)

The first step is to de- this ΔK_2 with the stronger characters of $\tilde{\chi}_2$ (say scores ≥ 3). The operation performed can be expressed

$$\Delta K_{26} + \Delta\chi_{26} \text{ (since } \tilde{\chi}_2 = \Delta\chi_2 + \Delta\chi_6)$$

and the resultant signs are $\Delta\psi'_{26}$.

Thus we have a fragmentary $\Delta\psi'_{ij}$ pattern from which to make a start. A count for $\Delta\chi_5$ is done first. The properties used are

$$P(\Delta\psi'_i = \cdot \mid \Delta\psi'_{j4} = \cdot) = (1+2\beta-\beta^2)/(2+2\beta)$$

and

$$P(\Delta\psi'_i = \times \mid \Delta\psi'_{j4} = \times) = \tfrac{1}{2}(1+\beta).$$

Therefore a dot in $\Delta\Psi'_{16}$ give a factor of $\frac{1+2\beta-\beta^2}{1+\beta}$ (about 1·5 d.bs. if d = 18½) in favour of a $\Delta\Psi'_5$ dot, and therefore in favour of $\Delta\chi_5 = \Delta K_5$. A cross in $\Delta\Psi'_{16}$ gives a factor of $\frac{1+\beta}{1-\beta}$ (about 3 d.bs.) in favour of a $\Delta\Psi'_5$ cross, and therefore in favour of $\Delta\chi_5 \neq \Delta K_5$. For convenience we work in pips worth 1·5 d.bs. each, scoring 1 and 2 respectively. From this $\Delta\chi_5$ count strong characters are selected, say $\geq$ 7·5 d.bs. with which to de-chi ΔK_5. The count for $\Delta\chi_4$ makes use both of the $\Delta\Psi'_5$ characters now in the 5th impulse, and of the $\Delta\Psi'_{16}$ characters in the 2nd, while the $\Delta\chi_3$ count also uses the new characters derived from the $\Delta\chi_4$ count. The scoring for these counts is given below. (36Y(i)).

Having counted for $\Delta\chi_4$ and 3 in this way it is usual to scrap the $\Delta\Psi'_{16}$ signs in the second impulse and count for $\Delta\chi_2$, (using the signs now in impulses 3, 4 and 5), rather than first counting for $\Delta\chi_1$.

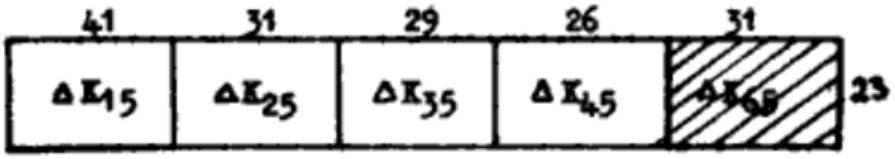
How this count is taken and all subsequent work is described below (26E)

(c) The χ_5 flag (R3 p.67) is normally used:

(i) on keys not on χ_2 limitation which are not long enough for a good chance of 5 by 5 significance,

(ii) on keys known a priori to be on χ_2 limitation but which are not long enough for χ_2 significance. The χ_2 start is then considered not to be strong enough, and the χ_5 flag is used.

Method: A type-out is made on Garbo in widths of 23, of ΔK_{15}, ΔK_{25}, ΔK_{35}, ΔK_{45}, and in the case of (ii) ΔK_{65}. These type-outs are entered diagonally into rectangles (for rectangles generally see 24) of width 23, and length 41, 31, 29, 26, and 31 respectively. The rectangles are flagged (see 24B(d)(i)) on $\Delta\chi_5$ and the flags combined by straight addition. This is of course equivalent to flagging what is called the long rectangle, shown in the diagram.



The flag is converged to give $\Delta\chi_s$ in positive and negative scores. The significance test $\frac{1}{2}\chi/\sqrt{\nu}$ is applied, where χ is the modular sum of the scores and ν is the total number of comparisons. (4, pp. 96, 97.)

The formula for finding ν is

$$\nu = .0648\,N^2 - 2N + 8 \text{ and}$$

$\nu^* = .0810\ N^2 - 2N + 10$ where ν^* is the total number of comparisons when the ΔK_{65} rectangle is included.

A simpler form of the test is

$$\frac{x}{\sigma \text{ or } \sigma^*} \geqslant 6 \text{ where}$$

$$\sigma = 2\sqrt{\nu} = .51N - 8$$
$$\text{and } \sigma^* = 2\sqrt{\nu^*} = .57N - 7$$

Each flag comparison is worth a factor of $\frac{1+\beta^2}{1-\beta^2}$. Since $10\log_{10}\frac{1+\beta^2}{1-\beta^2} \doteq 1$ for $\beta = \frac{1}{3}$ the scores for $\Delta\chi_5$ from the converged flag will be approximately in decibans.

If significant a partial $\Delta\chi_5$ obtained from these scores is taken through the 4 (or 5) rectangles (as through the long rectangle) to provide embryonic $\Delta\chi$'s for the start. The scores of the embryonics are in units of approximately 3 d.bs. as each rectangle entry is worth a factor of

$$\frac{1+\beta}{1-\beta}, \text{ and } 10\log_{10}\frac{1+\beta}{1-\beta} \doteq 3 \text{ for } \beta = \frac{1}{3}.$$

Sometimes a combined χ_4 flag is made, if the χ_5 flag fails to be significant.

The expected x^* for any converged composite flag is $2\beta^2\nu$, and the expected $\frac{x}{\sigma}^* = \beta^2\sqrt{\nu}$ (R3 p. 97) Λ. The meaning of x^* is analagous to that given in 24X(e).

Below is a table of the length, N, of ΔK required for expected $\frac{x}{\sigma} > 6$ for different dottages, d. (R3 p. 98)

d	N	d	N
14	447	22	148
15	377	23	131
16	323	24	118
17	281	25	107
18	244	26	96
19	213	27	88
20	187	28	79
21	167	29	72

For flags which include the ΔK_{65} rectangle these figures will be even smaller.

(d) Δ^2 properties.

In September 1943 (see RO, 53) it was noticed that $P(\Delta^2 \chi_i = x) > \frac{1}{2}$ and often about 2/3. Unlike $P.B(\Delta \Psi_i = x) = \beta$ the property was found to lack rigidity.

Let $P.B(\Delta^2 \chi_i = x) = \xi$

and assume $P.B(\Delta \Psi_i = x) = 0$

Then it can be shown that

$$\begin{cases} \text{P.B. } (\Delta^2 K_i = x \mid TM = . .) = 5 \\ \text{P.B. } (\Delta^2 K_i = . \mid TM = . x \text{ or } x .) = \beta 5 \\ \text{P.B. } (\Delta^2 K_i = . \mid TM = x x) \doteq 0 \end{cases}$$

So if $\Delta^2 K = 8$ we have a strong factor for TM = . . , which brings the odds in favour of TM = . . up to a little over evens for a μ_{37} dottage of 16, and even higher for higher μ_{37} dottages.

Two points arise in the selection of a possible . . in TM.

(i) If we assume TM = . . in positions 2 and 3 of K we are automatically (for χ_2 limitation) assuming x x in positions 1 and 2 of χ_2. Therefore we are assuming position 1 of $\Delta\chi_2$ = . and so it is preferable in our selection of a place in ΔK that we take one in which ΔK_2 = x . rather than . x so that we have $\Delta^2\chi_2$ = x x rather than . x

(ii) By a similar argument to that used to infer a possible . . in TM from an 8 in $\Delta^2 K$ we may infer (with even greater probability) that TM = . x or x . from a / in $\Delta^2 K$. This provides a useful check in the case where ΔK reads (say) RYY, where it greatly strengthens the evidence for TM = . . at RY.

Having chosen a double dot in TM we are already provided with 2 $\Delta\chi$ characters on each impulse, 10 characters in all. These we put through the ΔK on the chi-lengths, derive further $\Delta\chi$ assumptions from them in the normal way as in Turingery (see 43B) and collect them into cages. If the cages look good we proceed as in Turingery.

This method of using Δ^2 properties for key-breaking was never standard practice, but it occasionally yielded spectacular results, especially when the number of 8's in the $\Delta^2 K$ was significantly high, indicating a strong tendency of $\Delta^2\chi$ to cross and high μ_{87} dottage. The most outstanding success was obtained in the last few weeks of the war, when the shortest key ever to be broken, of length 97 was tackled by assuming <u>all</u> 8's in $\Delta^2 K$ to be double dots in TM, and gradually eliminating those which began to give contradictions.

For the tendency of $\Delta^2\chi$ to cross as a special case of the use of $\Delta\chi$ characteristics see R3, pp 125, 126.

26C HAND COUNTING FOR $\bar{\chi}_2 \bar{\Psi}'_1$ LIMITATION

The embryonic $\Delta\chi'$s already obtained from the 5 by 5, 10 by 10, or χ_5 flags are added to the ΔK to give fragmentary $\Delta\Psi'$, and check A is applied (see below fig. 26 XI). Except when the embryonics derive from a 5 by 5 flag, a test is immediately applied to determine 'the sign of the key', (R_{44} p. 1 i.e. whether the $\Delta\chi'$s (and therefore the $\Delta\Psi'$) are reversed or the right way round. In the case of the 5 by 5 flag start, the test is applied after 'counting once round', a phrase to be explained later.

The total number of $L_{5,0}$'s, $L_{4,0}$'s, $L_{3,0}$'s (a letter $L_{n,m}$ is defined as a letter with n dots and m crosses), and also the total number of dots and the total number of crosses in the 'spoiled columns' are counted. An 'unspoiled column' is a letter where either n = 0 or m = 0.

For each excess of $L_{5,0}$ over $L_{0,5}$ score + 2 d.bs.

$L_{4,0}$ over $L_{0,4}$ score + 1 d.b.

$L_{3,0}$ over $L_{0,3}$ score + 4 c.bs.

and for each excess of cross over dot in a spoiled column score + 4 c.bs. for the theory that the $\Delta\chi'$s are the right way round.

Significance level for the test is taken as 20 d.bs. This is generous and allows for the possibility that the embryonics may be considerably less than 80% right, 80% being the standard taken for calculating the above scoring system.

Suppose that the test is not conclusive, or that it has not been applied because the start was a 5 by 5 flag. We then do a count for $\Delta\chi_4$ first (as $\Delta\chi_5$ already has strong evidence) using only unspoiled columns.

For 1 dot or 1 cross in the other impulses score 3 d.bs. for $\Delta\Psi'_4$ being a dot or cross respectively and therefore in favour of $\Delta\chi_4 = \text{or} \neq \Delta K_4$ at the position counted.

For 2 dots or 2 crosses score 5

For 3 dots or 3 crosses score 6

For 4 dots or 4 crosses score 7. (These figures are derived from the table in Rae p. 56 by putting $q_e = .5$)

From the $\Delta\chi_4$ count we select all characters with scores > 10 d.bs. and re-de-chi ΔK_4 with the improved $\Delta\chi_4$.

We now repeat the process for the next shortest $\Delta\chi$, and so on until all 5 $\Delta\chi$'s have been counted once. We have now 'counted once round'. The test for the sign of the key is then applied again. Once significance has been achieved on this test the method of counting is changed.

Suppose that the test shows the $\Delta\chi$'s to be the right way round. Then for the next $\Delta\chi_1$ count

For 1 dot in the other impulses and no crosses, score +1 for $\Delta\psi'_1$ = dot

For 2 dots and no crosses score + 2

For 3 dots and no crosses score + 3

For 4 dots and no crosses score + 5 (R+1 p. 89)

For 1 or more crosses (and however many dots) in the other impulses score - 1. If the $\Delta\chi$'s are found to be inside out, interchange 'dot' and 'cross' throughout the above.

These figures are a crude scaling down for convenience of the decibanagsm 3,7,11,16, [illegible]. The pips are each worth approximately 3 d.bs., and the standard normally taken for accepting $\Delta\chi$ characters from the count is 5. The counting is continued until one complete $\Delta\chi$ wheel is obtained.

A useful check for key work on $\bar{\chi}_2+\bar{\psi}_1'$ key was devised shortly before the end of the war (B41 p.92). Suppose that positions n+1, n+2, n+3 of K are consecutive TM dots. Then

(i) $\chi_2+\psi_1'$ = x x x at n, n+1, n+2.

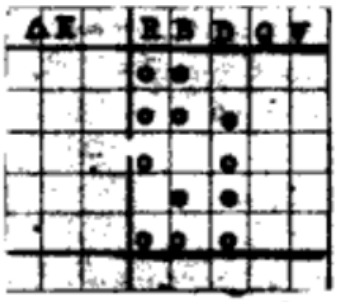
But (ii) $\Delta\psi_1'$ = . at n+1 because TM = .

Then (iii) from (i) $\Delta\chi_2$ = . at n+1.

But (iv) $\Delta\psi_2'$ = . at n+1 (as in (ii)).

Therefore (v) from (iii) and (iv) ΔK_2 = . at n+1. (The property is of course equally and more obviously true for $\bar{\chi}_2$ key.)

Hence we can only assume 3 consecutive dots in TM where ΔK_2 = . at the first of the 3 dots. So if in key-breaking we have



we know that one of these letters is not a TM dot. If we cannot decide which is the weakest and ignore all motor dot evidence derived from it we should ignore all 3 until the imposter is revealed.

To assist key-breakers on $\bar{\chi}_3\,\bar{\psi}_1'$ key a chart was made giving a standardised routine for keys started from a χ_5 flag. This chart is given in fig.26.VI.

Fig 26(88)

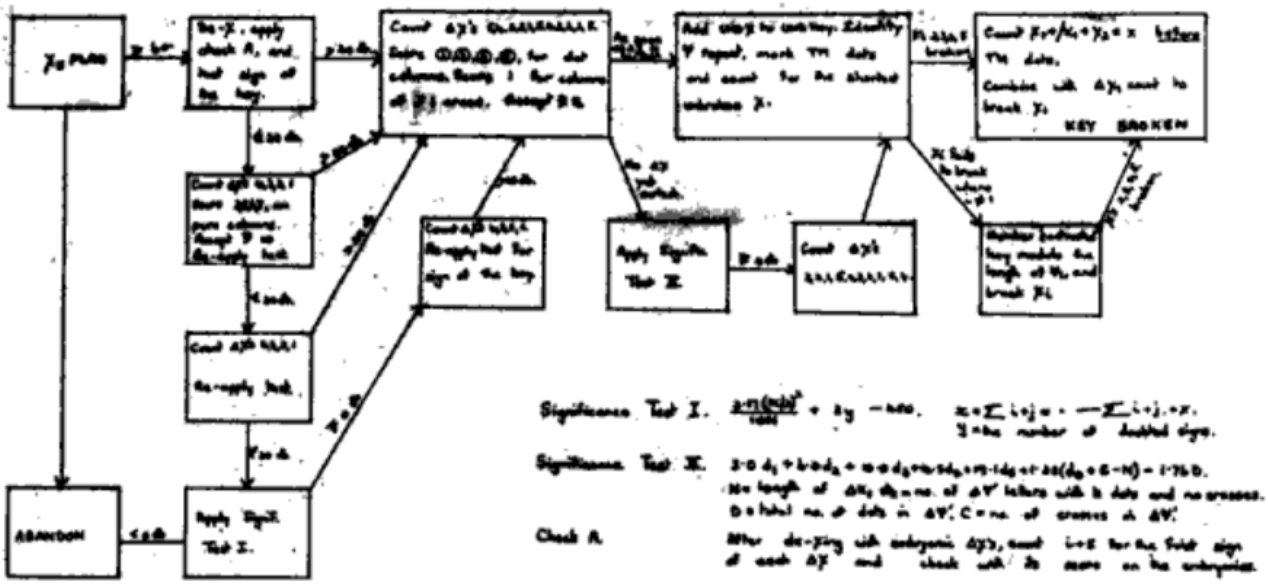


Fig 26(88) Standardized key-breaking routine for $\bar{\chi}_2$ $\bar{\psi}_1$ functions.

26D RECOGNISING THE Ψ REPEAT AND NUMBERING

As soon as a $\Delta\chi$ is obtained it is integrated, and the undifferenced χ_i is added to undifferenced K_i to give Ψ'_i. An attempt is then made to recognise the repeat of Ψ_i in its extended form. The number of groups of crosses in Ψ_i is known approximately in advance as it is a function of the number of dots in μ_{37}, and some idea of this will have been gained in working on the key. When the repeat has been recognised and the number of group of crosses established these groups are numbered, returning to 1 each time the repeat comes round. Many TM dots can now be inferred wherever a group or interval between groups is known from one appearance to be a single cross or dot but appears elsewhere extended to two or more. Other TM dots can be inferred but not located exactly (see 41D(a)). At every TM dot located $\Delta\chi = \Delta K$ and the $\Delta\chi$ values thus deduced for the shortest unknown χ are entered on the width of its wheel length.

This will normally bring out the whole $\Delta\chi$, especially if we use the TM = x positions, which each give a factor of $\frac{1+\beta}{1-\beta}$ ($\doteq$ 3 d.bs.) for $\Delta\chi_i \neq \Delta K_1$. The new $\Delta\chi$ is integrated to give a χ which is added to its K impulse to give a new Ψ'. The new Ψ' is numbered in groups as before, thus locating more TM dots. These are used with those already known to break the next shortest unknown χ, and so on.

When the TM dot evidence fails to complete a $\Delta\chi$ the method of 'numbering' is used. First the Ψ'_i already produced has to be reduced to Ψ_i. This is easy if two or more Ψ''s are already known, and nearly always possible for only one. The method is to take the shortest form in which any particular group of crosses or dots in Ψ'_i appears as representing its true size in unextended Ψ_i. The characters of Ψ_i are then numbered from 1 to the length of the Ψ wheel, and the numerical co-efficients of the Ψ_i characters are transferred to the same characters appearing in Ψ'_i.

Thus a Ψ':

[. x x x . . x . . . x . . x x . . . x . x x x x .

derived from a Ψ:

[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
[. x . . x . . x . x x . x . x x .

would be numbered

```
[1 2 2 2 3 4 5 6  7 8 9 9 10111212121314 15  1617
[. x x x . . x . . . x . . x x . . . x . x x x x .
TM [x . . x x x x (1) x x . x x x . . x x x ( 2 ) x
```

The TM deduced is also shown, with bracketed numbers representing dots whose presence but not exact location has been deduced. The process of simultaneously constructing the χ and ψ patterns of a different impulse from that of the numbered ψ' is that described in (42B(d)), with the difference that instead of taking an arbitrarily assumed sign as the start we can integrate a length of $\Delta\chi$ already made certain in the counting, and with so large a start finish the job easily and quickly.

26E HAND COUNTING ON $\bar{\chi}_2$ KEY.

We left the $\hat{\chi}_2$ start at the stage where the first count for $\Delta\chi_2$ was about to be done, after obtaining signs on $\Delta\chi'$s 5, 4 and 3. This count is taken as in counting on $\bar{\chi}_2+\bar{\psi}'_1$ key, with the same scoring.

The scores are in favour of $\Delta\chi_2$ signs, but the aim is to obtain $\Delta\chi_4(\tilde{\chi}_2)$ signs as well as $\Delta\chi_2$ signs. The process by which this is done is complex and can only be mastered by experience. The methods used depend on mathematical common sense and it is hardly necessary to describe them in detail. If a stage is reached at which a good deal of $\Delta\chi_2$ and $\Delta\chi_4$ are known, considerable use can be made of the connection between these wheels. Otherwise $\Delta\chi_4$ is treated just like a sixth impulse and the scoring system is the same as in non-χ_2 key-breaking, except that the scoring includes another term. $\wedge$ (R41 p. 67) It now reads 1, 2, 3, 5, 7 for a dot in the counted impulse, given respectively. 1, 2, 3, 4, or 5 dots and no crosses in the other impulses. (R41 p. 89)

When we start with a χ_5 flag and not a $\hat{\chi}_2$ count we start at the stage reached in the $\hat{\chi}_2$ method when partial wheels are known for all six $\Delta\chi'_3$s. The difference is that unless the compatibility or incompatibility of $\Delta\chi'_2$ and $\Delta\chi_4$ is very marked we do not know the sign of the key. This is determined by the test of 260 except that the score

for $L_{6,0}$ over $L_{0,6}$ is +3 d.b.s (R41 p 69) This test allied with the comparison $\Delta\chi_1$ and $\Delta\chi_6$ should show conclusively the sign of the key. If not we should apply a very careful check of each stage of the work.

Once the sign of the key is determined we proceed with 6-impulse counting as before. The 6th row down on the squared paper is regarded as corresponding to a 6th teleprinter impulse, and contains the known characters of $\Delta\chi_6 (-\Delta\psi'_6)$.

26F DEVIL EXORCISM (R41 p 68)

This is a powerful technique only devised two or three months before the end of the war.

It assumed that we already know the sign of the key. Now we are accustomed to regarding a sign on a $\Delta\chi$ in wheel-breaking as being either cross, dot or undetermined. But a sign can be undetermined for two different reasons, - because its scores are feeble or because they are contradictory. It has been found that, especially on low dottage keys, these two cases should be distinguished. The former is still left as a blank but the latter is entered as a ringed dot. In this way the 'devils' of the key (that is, these letters of the $\Delta\psi'$ which appear, on their known impulses, to be motor dots but in reality are not) are rendered impotent and are ultimately exorcised. For once a column of $\Delta\psi'$ gets a ringed character in it we cease to use it as motor dot evidence. Soon the false motor dots thus treated, unable to contribute to their own salvation will take a cross in one of their unknown impulses, thus resolving the contradictions, and restoring the motor dot columns which they contradicted and which have also been ear-marked as devils, to their rightful status. Devilry can also be used to indicate characters of $\Delta\chi_1$ and $\Delta\chi_6$ (on $\overline{\chi}_1$ key) which are mutually incompatible.

26G KEY WORK IN THE NEWMANRY

Apart from the χ_s flag described above in 26B (c) there are other key jobs which are done by computers.

(a) The 150 by 150 rectangle. (R_3 pp. 101, 103)

If it is specially desired to break a key, and usual methods have failed, the 150 by 150 rectangle can be made, thus:

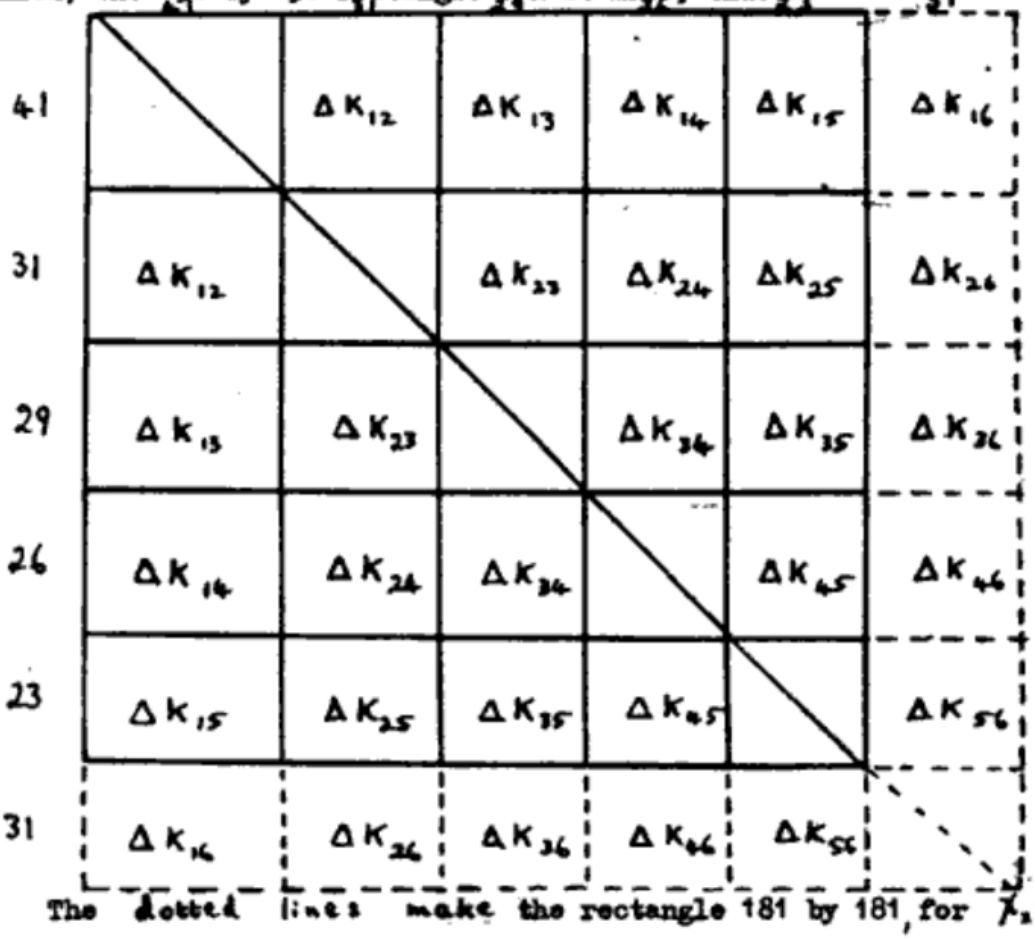


Fig. 24(XII)

The dotted lines make the rectangle 181 by 181, for λ_2 controlled key.

Care must be taken to ensure that every rectangle is entered in the positive direction of the wheels. (The square labelled ΔK_{26} merely contains the scores of the $\hat{\lambda}_2$ run written down the diagonal.) The rectangle is converged, from a λ_5 flag (or even a $\hat{\lambda}_2$ start for $\bar{\lambda}_2$ key). The pattern of length 150 (or 181), which is being taken through, should itself be modified by the new information available after it has been taken through each block.

The 150 by 150 rectangle is merely a quicker way of doing original Turingery counting (see R_{44} p. 50). Also all rectangle-convering jobs, including this and the 181 by 181 rectangle, can be done on Colossus by a series of runs of the form i + j (see 25).

An interesting identity in connection with 150 by 150 rectangle is that if we flag the 1st, 41 + 1^{th} (= 42nd), 41 + 31 + 1^{th} (= 73rd), 41 + 31 + 29 + 1^{th} (= 102nd) and 41 + 31 + 29 + 26 + 1^{th} (= 128th) rows, we perform <u>exactly</u> the same operation as the 5 by 5 flag (see above 26B(a)).

(b) With $\bar{\chi}_2$ limitation an extract from the 181 by 181 rectangle was prepared thus: (Ref. p. 65)

	41	29	26	23
31	ΔK_{21}	ΔK_{23}	ΔK_{24}	ΔK_{25}
31	ΔK_{61}	ΔK_{63}	ΔK_{64}	ΔK_{65}

Fig. 26 (VIII).

The convergence of this rectangle is begun by taking the strongest values of the $\hat{\chi}_2$ run through the top 4 rectangles, giving fragmentary $\Delta\chi$'s 1, 3, 4, and 5. These are taken right through, giving partial $\Delta\chi_2 + \Delta\chi_4$, which are both taken back again, and so on. After convergence is complete the $\Delta\chi_2$ and $\Delta\chi_4$ patterns are compared for consistency, and if their agreement is striking, as it should be, we can confidently transfer to hand-counting, or to the 181 rectangle, or to Colossus.

Colossus can do many of the operations of hand counting, but since it is unable to 'doubt' on more than one impulse at a time it is not worth trying to use any but the simplest approaches to key when using Colossus. For example to reproduce one normal $\Delta\chi_i$ count on non-$\bar{\chi}_2$ key we would have to do 17 separate Colossus runs.

Colossus is equipped with a switch for the condition "NOT 99" which effectively eliminates all gaps in the key, which are represented as series of 9's on the key tape.

The chief uses of Colossus for key-breaking are

(i) In breaking key from a crib

(ii) In doing the donkey-work of 150 by 150 or 181 by 181 convergence on sticky keys until significance and the determination of the sign of the key has been attained.

If it is progressing very quickly it may be easier to complete all χ's on Colossus, do a machine de-ch[illegible] of the key tape on Tunny, and recover the ψ's in a few minutes of hand work. But normally it is best to take it off Colossus and complete the closing and more finicky

stages by hand.

(c) Key from a crib

This normally exceeds 1000 letters in length. It is therefore so vulnerable that it can be attacked confidently from a random start and may come out in about 10 runs.

The usual random start is from a single $\Delta\chi_5$ character. The runs are of the form i+/j until the sign of the key is known. Then they are of the form i/j,k,l ... and i$\tilde{x}$/j,k,l ...

A random start such as this was not in fact generally employed. For $\bar{\chi}_2$ key a $\hat{\chi}_2$ type-out and for non-$\bar{\chi}_2$ key a converged 4+5 rectangle provided the start as well as giving a preliminary check that the key tape had been made correctly.

(d) Colossus convergence of 150 by 150 and 181 by 181 rectangles. (R3 p.108)

The series of runs below gives the Colossus formulae for converging these rectangles, assuming we start from a $\Delta\chi_5 A$ obtained from the χ_5 flag. Anything bracketed applies only to the 181 by 181 rectangle. Using $\Delta\chi_5 A$;

4+/5, 3+/5, 2+/5, (6+/5), 1+/5 giving wheels 4,3,2,(6),1A.

These 4 (or 5) wheels are checked with the embryonics provided by taking $\Delta\chi_5 A$ through the 4 (or 5) ΔK_{ij} rectangles.

Then do the following runs (using the latest versions of the wheels, of course).

5+/4, 5+/3, 5+/2, (5+/6), 5+/1.

Add the 4 (or 5) runs together to give $\Delta\chi_5 B$.

Then do

4+/3, 4+/2, (4+/6), 4+/1, 4+/5 giving $\Delta\chi_4 B$

Then do

3+/2, (3+/6), 3+/1, 3+/5, 3+/4, giving $\Delta\chi_3 B$

Then do (2+/6)*, 2+/1, 2+/5, 2+/4, 2+/3 giving $\Delta\chi_2 B$

etc. etc.

An essential of key-breaking is speed. Only in key-breaking from depth is it likely that one can decode the current day's traffic.

So the best plan is a double attack: a hit-or-miss attempt by a first-class key-breaker to rush it through in record time, and at the same time a

---

* this is done by adding $\Delta\chi_0\Lambda$ to the scores of the $\hat{\chi}_2$ run.

slow but powerful second line of defence should be in preparation in case he takes too many chances for the sake of speed and becomes bogged down. In that event he can proceed afresh from the sound start that has meanwhile been prepared by others.

The second line of defence always takes the form of a combined χ_2 flag. The 'spearhead' is normally a 5 by 5 or 10 by 10 flag for non-$\bar{\chi}_2$ key, and a $\hat{\chi}_2$ start for $\bar{\chi}_2$ key.

27 - CRIBS

27A GENERAL NOTIONS

Given a cipher and the corresponding plain language it is easy to find the (unknown) key, for

$$K = P + Z$$

From K the unknown wheels on which Z is enciphered can be broken.

The real problem is to find the correct relative positions of P and Z

In Tunny the problem is necessarily solved in two stages:

(i) log-reading predicts: this Z corresponds to some part of this P;

(ii) Z and P are added in all positions : the correct position can be identified because key has recognisable statistical properties

[27W 22 F]

The possibility of a crib depends on the retransmission of the same message (and on the previous decoding of one transmission): the statistical method demands that the retransmission shall be exact : exactitude is in practice possible only if both transmissions are sent automatically from the same plain language tape and if further the one not already decoded is sent without pauses: two hand perforations or two hand sendings of the same message always differ in punctuation and corrections. Thus only retransmissio from the same station can be used as cribs, and for this reason the organisati of the German TP system is more relevant than in other Tunny work.

When K is obtained, ordinary key-breaking methods can be applied. Because of their great length crib keys were easily broken, generally on Colossus from a random start or from a converged 4 + 5 rectangle.

For cribs of normal length, not grossly corrupt, it is unnecessary to use very powerful methods unless the dottage is too low for easy χ-setting, and in this case it is not worth while.

Crib setting can begin only after one transmission is decoded, disadvantage when the value of traffic depends on its currency.

As a matter of history, cribbing was developed when the introduction of $\overline{\chi_1} + \overline{P_5}$ limitation prevented the occurrence of depths, which had been the basis of all earlier wheel-breaking.

In this chapter section G, which describes the statistical technique, and sections W, X, Y, which explain its mathematical basis, do not assume any knowledge of sections B,C,D,E,F. Sections D,E,F,G deal with the technique of cribbing in roughly chronological order, but F will be more intelligible if G is read first.

Use of "overlaps" for <u>setting</u> messages by crib methods R2 pp 98,99; R3 pp 1,22,64.

For suggested "cribbing" with neither message decoded 22W(c) [R3 pp 62,65].

27B GERMAN TP LINKS

(a) OKH

Because, as already stated, statistical crib methods require exact letter by letter correspondence between P and Z only automatic transmissions from the same tape were cribbable.

In practice this meant messages from OKH to subordinate headquarters, sent from the same TP terminal (of which, unfortunately, OKH always had more than one). The arrangement of these terminals and of the links which they served varied considerably, especially in 1945, and finally became chaotic.

(b) Routine messages

Most cribs were provided by certain of OKH's routine messages, which had several advantages.

(i) they were rather long (3,000 - 10,000);
(ii) they were sent at about the same time each day thus aiding prediction;
(iii) they followed an elaborate formal procedure;
(iv) they sometimes had double serial numbers.

Note 1 most routines were sent by other means than Tunny.

Note 2 the procedure included the use of Roman numerals or capital letters for designating sections, bracketed letters of numerals for subsection

(c) Routines commonly used for cribbing.

Kriegsmarine Kurzlage

Daily	:	Bream, Gurnard, Cod, Whiting.
Regularly	:	Tarpon, Stickleback, Jellyfish,(irregular after Autumn
Rarely	:	Lumpsucker

Lagebericht West

Daily	:	Gurnard, Codfish, Grilse Bream (not always the same version).
Regularly	:	Jellyfish (rarely after Autumn 1944).
Occasionally	:	Mullet, Weever.

OKH Lagebericht

Daily	:	Gurnard, Codfish
Regularly	:	Bleak (erratic after Autumn 1944) Jellyfish (rarely after Autumn 1944). Weever
Occasionally	:	Grilse (erratic) Stickleback, Squid, Crooner (after mid-February 1945).

OKW Tagesmeldung

Daily	:	Jellyfish, Gurnard (not always the same version).

Daily means not a daily decode, but that log evidence suggested that the routine was sent daily by Tunny unless prevented by circumstances (movement of outstations, reorganisation at OKH). Great activity sometimes caused a routine to reappear, suggesting that it was normally sent by other means.

(d) Suitability of various links

Not all favourably grouped links were equally suitable: long QEP's with few autopauses were helpful. Gurnard and Bream were good in this respect, Grilse fair, Jellyfish and Bleak bad: on Jellyfish an OKH Lagebericht was spread over 16 hours, during which 72 QEP's were sent.

(e) Diagrams of TP links

Comparison with the diagrams of ch 61, in which the various TP terminals of OKH are distinguished, will show that the most favourable period was before November,1944; from then till February,1945 was particularly bad. The separati of Grilse (high intelligence value) was most unfortunate.

(a) Auto and Hand

In addition to automatic transmission from a punched tape, known as "auto" operators often sent minor corrections, receipts, queries, and personal items directly by operating a typewriter connected to the encoding device, a type of transmission known as "hand". The two kinds of sending were identified

on the cipher red forms submitted by Knockholt by marking each appropriate stretch as "hand" or "auto".

(b) Use of the same plain text tape on different links.

If a message was addressed to two or more different outstations the usual practice was to use a single tape for transmitting to all the addresses concern Normally the messages would be sent out on one link and, when transmission was completed, the tape would be taken to another transmitter and sent again and so on. In rare, cases, when the message was long and two transmitters were adjacent, the tape was inserted into the second transmitter before sending had been completed on the first link, with the result that we had simultaneous sending of different parts of the same plain language tape.

(c) Change of QEP

A long message was often sent in several QEP's : for 10,000 letters 3 or 4 QEP's was usual, 15 not unknown.

(d) Autopause : go-backs

There were frequently pauses in auto without any change of QEP, i.e. without breaking the continuity of key. When sending was resumed the tape was usually set back 60 - 300 letters (go-back) so that there was a break in the continuity of plain text.

(e) Go-backs and QEP changes in the decode

The effect of a go-back could generally be remedied, for it was easy to see where 60 - 300 letters were repeated. This applied to a change of QEP if both QEP's were decoded; but this was often not so.

For editing see 27E (c).

(f) Go-backs in cipher

It was impossible to tell how much plain text was repeated, so that only pause-free stretches could be used. Many otherwise favourable cribs failed because there was no sufficiently long pause-free stretch.

(g) Relative length of cipher and decode.

Because editing could restore the continuity of P through an autopause, but not that of Z, the available P was almost, though not always, longer than the Z : to simplify descriptions this is sometimes assumed without explanation.

27D CRIB PREDICTION

(a) General

Up to this point nothing has been said about how the cipher messages which contained retransmissions of plain language already at hand, or how cipher messages on two or more links expected to contain the same plain language could be identified, except to suggest that they often passed at about the same time on all links. Unfortunately this "about the same time" covered a period of several hours during which fifteen or twenty messages could be sent. Unless conditions were very favourable and we could use judgment based on an intimate knowledge of the operating practices of a link, it was not practicable to attempt an identification. Further more, the time required to try all possibilities at random was prohibitive.

(b) Receipts.

However, the Germans came to our aid with some most useful practices, the most important of which was the requirement that each message be receipted by the receiving party when transmission was completed. The usual method of doing this was to send the last two digits of the internal serial number together with the time at which the message was cleared at the receiving station. The set operator himself was not usually authorised to receipt and sent it only when a supervisor had examined the message and was satisfied with its reception. Generally this was done within a few minutes of the end of a transmission although there were exceptions frequent enough to make such an assumption in a particular case a bit unreliable. At times, too, a whole block of messages was receipted for at one time, not necessarily in the exact order of transmission. The most important feature of these receipts was the fact that they were sent, for the most part, in clear language and were recorded by Knockholt operators on log sheets together with all other plain language chat between German operators.

(c) Sixta and the identification of receipts.

The Sixta Non-Morse section had the task of reading the log sheets of the activity of each fish link and extracting from them any information of cryptographic or intercept value. In the cribs world we were mainly interested in their ability to predict or identify a retransmission. In order to give us this information the log readers listed each single serial receipt, together with the time of receipting, numerically according to the last two digits of the

serial receipted. It was possible to record this information for about six links on a single page, making it a simple matter to see quickly whether or not the same serial was receipted on more than one link. However, when the same serial was found to be receipted by two or more links, it was not possible say very definitely that the same message was involved in all cases. Since most links passed considerably more than one hundred messages daily, the number of serial coincidences for messages not at all the same, was quite substantial. Nevertheless if the same serial was receipted by several links at about the same time of day, the probability that the messages were identical was quite good. And, indeed, if we had prior knowledge that the links involved received a routine report at about this time daily, it was highly probable that the receipt clicks had identified this routine. In addition to the time element other factors were used to determine the likelihood of retransmission. For example, the logs could often tell us whether or not the messages in question had the same priority signal or if they were approximately of the same length. Sometimes, too, if the operators were quite chatty, they would make queries referring to proforma headings. Thus if one saw references to "8)" or "unter Room III,A)" on tow links and identical receipts for the traffic in question, the likelihood of a retransmission was very great.

(d) Double serial receipts.

Although most receipts were of the single serial type, double serial receipts were fairly frequent. If, for example, the internal serial number was 7867/7890, the receipt was usually given as 67/90 and a receipt click of this kind almost certainly meant a retransmission.

(e) Retransmission Slips.

From a consideration of the points just mentioned and any other information revealed by the log sheets, Sixta submitted to the cribs section daily predictions of likely retransmissions.

(f) Use of decodes : Testery Cribs watch.

Experience soon proved, however, that not all receipts were intercepted, mainly because of poor intercept conditions. In addition, some receipts were encoded and hence not available to the log readers. For these reasons it was very important that all decoded traffic be examined from a cribs point of view to ensure that no retransmission possibilities were missed. The decodes provided full information about the messages which could be used in conjunction

with log evidence to spot retransmission. To effect this examination of decodes a Testery cribs watch was organised. It began making a study of messages with multiple addresses late in June, 1944 and by the middle of July began submitting "crib forms" to Sixta for all messages likely to pass on links other than those on which they were decoded. These crib forms contained all the information about a message likely to be of use to Sixta in attempting to identify it on other links. Most successful retransmission slips were based on these crib forms since it was far easier to identify on another links message whose serial number and other characteristics were known than to predict from log evidence alone.

27E PREPARATION OF DECODE AND CIPHER

(a) Retransmission slips

Work on a crib job usually began with the receipt of a "Sixta Non-Morse Retransmission Slip". These slips were entered, according to the Sixta serial number, in a log headed "List of Slips" and then

(i) worked on immediately if the plain language was already available; or

(ii) if one of the keys of the links involved had been broken, the slip was called active since there was a reasonable prospect that the plain language would soon be available; or

(iii) if none of the keys involved had been broken the slip was called dormant.

Priority in setting and decoding was requested for the messages in question on active slips. If a significant rectangle was obtained on one of the links concerned with a dormant slip, the appropriate messages were ordered from Knockholt for priority treatment when the key was broken.

(b) Ordering of Cipher tapes.

Whenever the plain language for a slip became available, or when the cipher message containing it had set well enough to ensure it becoming available, the first job of the cribs man or cribs registrar was to examine the cipher QEP's of the retransmission candidates submitted by Sixta from the point of view of length and order all likely messages from Knockholt under Procedure D.

During the period when $\overline{X}_2+\overline{P}_5$ (or $\overline{X}_2$) was the most common limitation used and when Knockholt was not overtaxed with slip reading, all D procedure messages were perforated completely and Red Forms submitted for our examination. In February, 1945, a new instruction was issued to Knockholt in the interest of

saving time and labour. We informed Knockholt of the minimum pausefree auto passage we considered useful and requested a perforation and Red Form for all passages as long or longer than this minimum. In all cases the longest possib stretch of cipher was perforated. The usual minimum for a $\overline{\chi}_2 + \Psi_1'$ link was 1000 letters and for a $\overline{\chi}_2$ link, 600 letters. In some cases the cipher in question was a rectangling message already available.

(c) Editing Decodes

Since several messages were often contained in a single QEP, the one pertaining to the slip in question had to be identified by its serial numbers or other characteristics in case the preamble was missing. Next it was necessary to decide whether or not to use the address as part of the crib. Since October, 1944 this has not been a problem because no example was ever decoded after that date in which the body of the message was identical on two links but with different addresses. A message occasionally passed on a link not included in the address but, in these cases, the new addressee was designated in an explanatory message preceding the transmission or more informally in hand chat between the operators. Before October, however, the Testery Cribs identified several routines having identical plain language for the body of the message but differing in the address.

Go-backs were eliminated by pencilling out the repeated letters, taking great care to ensure exact continuity. Occasionally this was difficult or even impossible due to extreme corruption caused by poor conditions or to a broken tape. In the latter cases the German operator was forced to remove the tape and reset it beyond the point of break. The letters missed were then filled in by hand so that continuity was missed because of invariably different punctuation.

The problem of correcting corrupt plain language arose only when intercept was bad. The occasional wrong letter in a good decode could not affect results much but corruptions of up to twenty-five percent of the text could obscure correct settings. Fortunately bad reception by Knockholt was usually accompanied by bad reception on the part of the Germans, giving rise to numerous repeats. With the help of the Testery Cribs Section we could do a fairly good job of piecing together the original plain language.

(d) Perforation of Plain Language

A tape of the edited plain language was perforated by Testery decoders, if

available, or in Tunny. These tapes were then printed out in widths of 60 and checked letter for letter, against the decode. Corrections were indicated on tape and printout and the two corrected copies made in insert machines.

(e) Checking Decode against Red Form

To ensure letter for letter correspondence between the Testery copy of the decode and the plain language tape used by the Germans for transmitting, Cribs registrars checked each line of the decode against the cipher Red Form. When discrepancies were found, partial decodes of the parts in question were done by the decoders. Failure to check arose from several causes. The decoding machi sometimes printed an extra "8"; carbon copies occasionally had a letter missing at the beginning or end of a line; the decoding operators were known to omit a part of the message when taking up after a breakdown.

(f) Cipher Passages

Two copies of each stretch of cipher to be used were made from a copy of the complete cipher tape and numbered appropriately as ZI, ZII etc. These pause-free passages were selected with regard to length, degree of corruption and posit in the message. This last point involved an attempt to fit roughly the position of various cipher stretches with the corresponding plain language. A happy choice of the first cipher passage to try saved a great deal of tape making and running time.

27F TAPE MAKING

(a) General

This section will be more intelligible if the following section, 27G, is read first.

Tapemaking was always done on Miles and the processes for different varieties of tape are very similar. Except for $\overline{X}_2 \overline{P}_2$ limitation P* is made from P exactly as Z* is made from Z.

(b) Δ_{598} tapes

Each letter of Z* involves (see 27G (b)) not merely one letter of Z but also the letters 943, 713, 667, 598, forward, so that five Z tapes must be placed in five transmitters of Miles, staggered 943, 713, 667, 598 :

In Transmitter	T 1	a Z tape	starting	with the	1st letter
	T 2	"	"	"	943+1th "
	T3	"	"	"	713 +1th "
	T 4	"	"	"	667 +1th "
	T 5	"	"	"	598 +1th "

The output Z^* is to have in its first impulse $\Delta_{43} Z_{45}$ i.e. Z_5(present) + Z_1 (present) + Z_5(943 forward) + Z_1 (943 forward)

Accordingly $T1_5 + T1_1 + T2_5 + T2_1$ is plugged into the 1st impulse.

Similarly $T1_5 + T1_2 + T3_5 + T3_2$ " 2nd "

$T1_5 + T1_3 + T4_5 + T4_3$ " 3rd "

$T1_5 + T1_4 + T5_5 + T5_4$ " 4th "

This can easily be plugged on any existing Miles.

(c) Running on to the end.

The tape in T2 (staggered 943) will reach the end 943-598 = 345 places before that in T5 (staggered 598). It is preferable to wait till T5 is exhausted, in case it is afterwards decided to run on fewer impulses, or include the extra evidence in the letter count.

(d) Δ_μ : $\bar{x}_a$ limitation

The operation is almost identical, but tapes are staggered (e.g.) 93, 124, 279, 341, and Z^* consists of:

1st impulse : $T1_2 + T2_2$

2nd impulse : $T1_2 + T3_2$

3rd impulse : $T1_2 + T4_2$

4th impulse : $T1_2 + T5_2$

(e) Δ_{2i} : $\overline{\chi}_2 + \overline{\overline{P}}_5$ limitation

Z^* as for $\overline{\chi}_2$ limitation.

P^* consists of $\Delta_{2i}(\Delta P_1 + \overline{\overline{P}}_6)$. For two P^* impulses this can be made on Miles A in one operation. For more impulses an auxiliary tape, $\Delta P_1 + \overline{\overline{P}}_6$ in all impulses is made, using three P tapes : present, 1 forward, 2 back.

(f) Tapes for Old Robinson

The only difference was a x.x.. pattern in the fifth impulse, used as a control [27 G (1)] . On Miles A a x.x. tape in the 6th transmitter could provide this. If only 3 impulses of Z^* were wanted, only four transmitters were used for differencing, and on any Miles a 5th transmitter could provide x

If however a Z^* (or P^*) tapes was to be made on a Miles other than

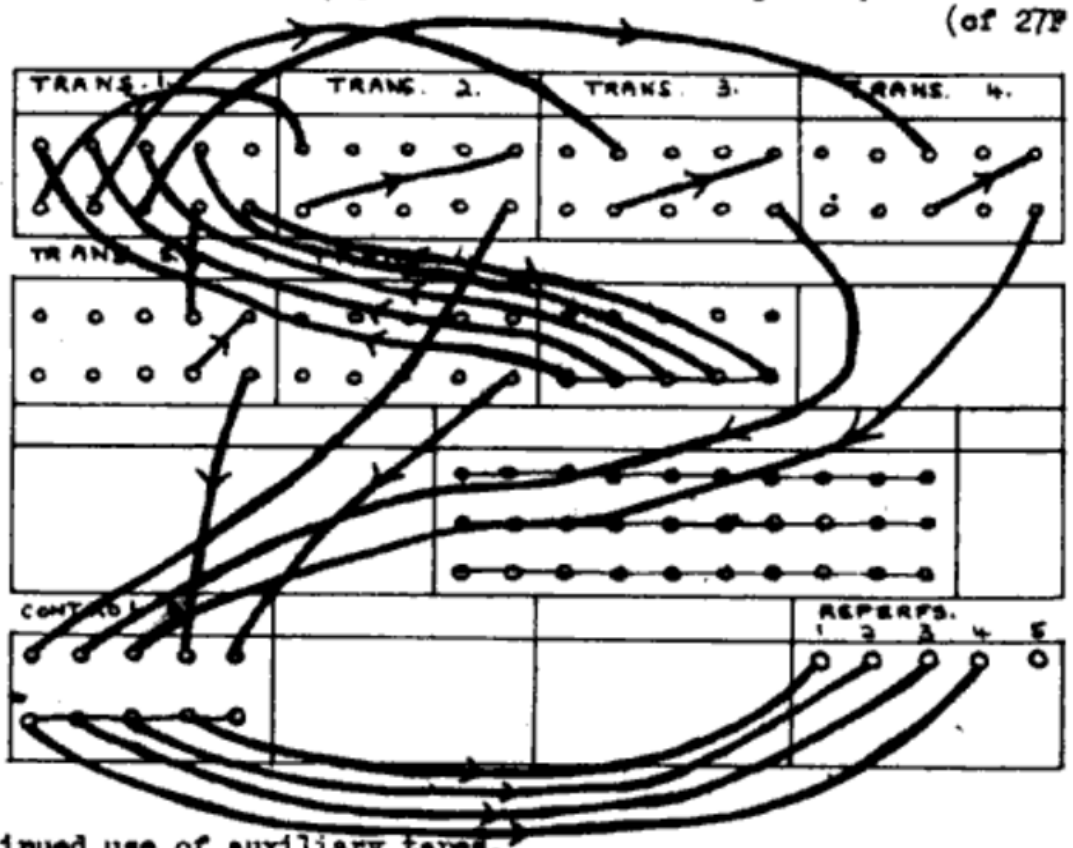
Miles A, four copies of an auxiliary tape ZQ were made, whose impulses were

Z_{15}, Z_{25} , Z_{35} , Z_{45} , x.x. pattern.

These were used in the obvious way to produce $\mathfrak{X}^*$.

For $\overline{X}_2$ limitation ZQ had Z_2 in four impulses, x.x. in the 5th.

For $\overline{X}_2 + \overline{P}_5$ limitation (ZQ had Z_2 in four impulses, x.x. in the 5th.
(PQ had $\Delta P_3 + \overline{P}_4$ in four impulses, x.x. in the 5th.
(of 27P (e))



(g) Continued use of auxiliary tapes.

The use of PQ, ZQ was continued to avoid disturbing an established routine, and because an undependable Miles was better able to cope with the individually simpler operations.

(h) Number of tapes needed.

4 P^* tapes, 2 Z^* running tapes, 2 Z^* checking tapes.

(i) Checking

The first 15 letters of every tape made were checked by hand. Tape sheets were used to record progress.

27 G STATISTICAL TECHNIQUE : RUNNING ON ROBINSON

Note: Throughout this chapter it is assumed (cf 27C (g)) that Z is shorter than P : if not Z, Z^* should be interchanged with P, P^*. [illegible] For proofs and references see 22 N.

(a) Basic Formulae

If Z is the encipherment of part of P, then in the correct position

$$Z + P = K$$

Z and P are added in all positions and their sum examined for resemblance to key. Key is characterized by

$$\Delta_{cyc}\, \Delta K_{a.s} \longrightarrow \cdot$$

where $\Delta_{598}U$ means (present U) + (U_{598} forward) with the analogous results for other pairs of impulses.

Further, for $\overline{X}_2$ limitation, if 31 ρ is any multiple of 31,

$$\Delta_{31\rho}\ \Delta K_2 \longrightarrow \cdot\ ;$$

for $\overline{X}_2 + \overline{\overline{P}}_5$ limitation

$$\Delta_{31\rho}\ (\Delta K_2 + \overline{\overline{P}}_5) \longrightarrow \cdot\ .$$

For the use of $\Delta_2 K$ characteristics see 22F (R2 p 80, R3 pp 13, 15, 76).

(b) Δ_{598} method: running for strokes in ΔK^*

The runs used are based on

$$\Delta_{943}(\Delta P_{15} + \Delta Z_{15}) \longrightarrow \cdot\ ,$$

$$\Delta_{713}(\Delta P_{25} + \Delta Z_{25}) \longrightarrow \cdot\ ,$$

$$\Delta_{667}(\Delta P_{35} + \Delta Z_{35}) \longrightarrow \cdot\ ,$$

$$\Delta_{598}(\Delta P_{45} + \Delta Z_{45}) \longrightarrow \cdot\ .$$

The last of these, for example, could be done on Robinson, by adding a $\Delta_{598} P_{45}$ tape and a $\Delta_{598} Z_{45}$ tape in all possible relative positions, in each of which $\Delta_{598}\Delta P_{45} + \Delta_{598}\Delta Z_{45} = \cdot$ is counted.

For greater power the number of places where all four runs simultaneously give a dot can be counted. This is achieved by a tape Z^* whose first four impulses carry $\Delta_{943} Z_{15}$, $\Delta_{713} Z_{25}$, $\Delta_{667} Z_{35}$, $\Delta_{598} Z_{45}$, respectively, and a tape P^* similarly derived from P. The run is then

$$\Delta Z^* + \Delta P^* = /$$

(c) Optimum number of impulses.

Differencing reduces the length of text, the reductions for Δ_{943}, Δ_{713}, Δ_{667}, Δ_{598} being of course 943, 713, 667, 598. Since the length of Z^* is the length of its shortest impulse, it may be preferable to use fewer than 4 impulses, generally 2 or 3 (see table in para.(e)).

(d) Scoring the letter count.

The runs for /'s are convenient, but waste the evidence of dots not forming a /.

Accordingly, when the run is completed, at each of the settings which gives a good score for /'s, the total number of dots in all (2, 3 or 4 impulses is counted, actually by means of a letter count, the score for any letter being the number of dots it contains. In one instance this set the crib correctly, though the score for /'s was 3.4 and only the fourth highest.

It is possible to count dots in impulses not used in the run for /'s and at places thrown away by reducing the length of K* to that of its shortest impulse.

(e) Table of formulae

Number of impulses used.	N = text length of Z* (n being text length of Z)	Running for /'s Random average	Running for /'s σ	Approx. value of σ commonly used	Minimum text for which this number of impulses is preferable.	Scoring the 1.. Average	Scoring the 1.. σ
1	n - 598	N/2	$\frac{1}{2}\sqrt{N}$			N/2	$\frac{1}{2}\sqrt{N}$
2	n - 667	N/4	$\frac{1}{2}\sqrt{3N}$		750	N	$\frac{1}{2}\sqrt{2N}$
3	n - 713	N/8	$\frac{1}{2}\sqrt{7N}$	$\sqrt{N/8}$	940	3N/2	$\frac{1}{2}\sqrt{3N}$
4	n - 943	N/16	$\frac{1}{2}\sqrt{15N}$	$\sqrt{N/16}$	4,000	2N	$\sqrt{N}$

Note: The sigma-age needed for "certainty" depends on the number of positions tried. As the number of impulses used increases, the evidence of a given sigma-age decreases (see 27X (e)).

(f) Running on Robinson

The tape of Z* is one longer than the tape of P*, so that at each revolution Z* steps one forward relative to P* . Start and stop are taken from Z* (until Z* begins to run off the end of P*.R2 p 99; R3 p 68) A set total of 2σ allows the random scores to act as a crude check that Robinson is not grossly faulty.

When the run is finished (or stopped if a very good score appears) the Z* tape is replaced by a Z* checking tape, of the same length as P*, which is set in all positions giving good scores, and a letter count made. To set the tapes the letter of P* which corresponds to the first letter of Z is marked with the aid of a hand-counter.

The score for /'s is spanned to detect slides or corruption.

(g) Very long decodes

If P^* is very long, not only must Z^* be tried at many settings, but each revolution takes a long time. P^* may be cut into overlapping sections; if machines are available these may be run simultaneously; log reading may predict which is the best section to try first. Alternatively the P^* tape may be made one shorter than a multiple of the Z^* tape, so that two or more settings are examined for each revolution of P^*.

(h) Running for dots

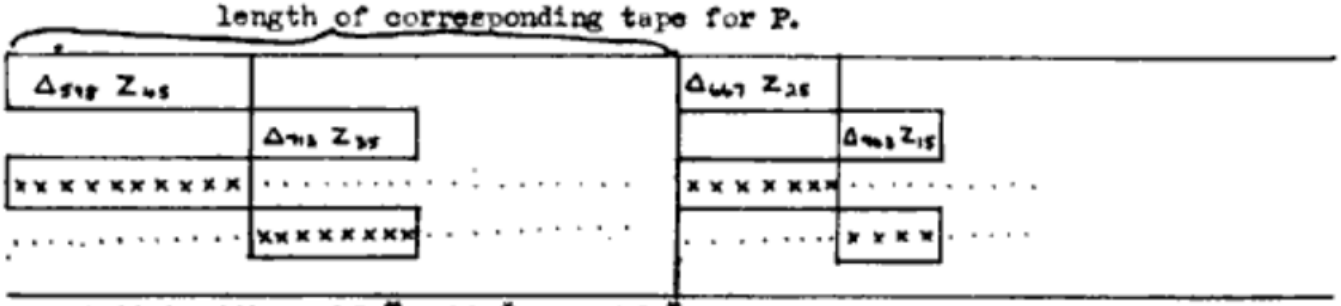
This means counting the total number of dots in $\Delta_{\%3}\Delta K_{15}$, $\Delta_{\%3}\Delta K_{25}$

etc. i.e. obtaining the "score on the letter count" (27 G (d)) in the actual run. It was not used operationally because

(i) the possible pitfalls in tape-making were so numerous that standardisation was necessary.

(ii) running for /'s, and counting dots at <u>all</u> good settings, is equally effective.

It can be done by putting $\Delta_{\text{---}} Z_{15}$, $\Delta_{\text{---}} Z_{25}$, $\Delta_{\text{---}} Z_{36}$, $\Delta_{\text{---}} Z_{45}$, end-to-end in the same impulse, and likewise for P; but this demands a roughly four-fold increase of tape length. A two-fold increase will suffice if "either-or" is used on Robinson.



Tapes could be of normal length if Robinson could count "A or B or C or D".

<u>(i) Running on Old Robinsons.</u>

This was complicated because the minimum text length was 2000, there was no spanning and long strings of dots or crosses were technically forbidden. (52 (b) (iv)).

The text of Z^* and P^* was made up to 2000 with RY's except in the 5th impulse, which was used as a control. On each tape the 5th impulse had a x.x. pattern throughout, but in the shorter text (usually Z^*) there was a phase reversal at the end of the text.

The tapes differed in length by 2, so that the stepping was two at a time : odd and even settings were run separately.

<u>Odd settings</u> P_5^* x . x . . x . x . x . x . x
Z_5^* x . x . x . x | x . x . x .
End of text

For genuine text $P_5 + Z_5 = \cdot$

Setting = 2 x reading + 1
(Reading = number of revolutio

Even Settings P_5^* x . x . x . x . x . x . x . x For genuine text $P_5^* + Z_5^* = x$
Z_5^* . x . x . x . x | x . x . x . x Setting = 2 x reading
End of text.

If only three impulses of K^* were wanted, the 1st and 5th were used for control, no separation into odd and even runs being needed.

Z_1^* . x . x . x . x . x . x
Z_5^* . x . x . x | x . x . x .
End of text.

(j) Checking on Old Robinsons

Old Robinson had no device to show whether the tapes had in fact been set correctly, and it was necessary to depend on the accuracy of hand counting. It was desirable to make many trials, even a re-run, before abandoning a high score which failed to check.

(k) Δ_{31} ($\bar{X}_3$ limitation) Running for strokes.

The technique is almost identical with that of the Δ_{sw} method, being based on $\Delta_{31}(\Delta P_2 + \Delta Z_2) \longrightarrow$.

The impulses of P^* are $\Delta_{3\times31} P_2$, $\Delta_{4\times31} P_2$, $\Delta_{9\times31} P_2$, $\Delta_{11\times31} P_2$.

(There are many references, most of them applicable to $\bar{X}_3 + \frac{R}{s}$ limitation, in the Research Logs: R2 pp 70,71,73,75,102,105; R3 pp 2,12,24,26. Somewhat different methods R2 pp 65,66,68,73.)

(l) Δ_{31} : Scoring the letter count.

This is quite different, e.g. $\begin{matrix} x \\ x \\ \cdot \\ \cdot \end{matrix}$ scores 2+ 1 + 1 = 4, because the two crosses imply a dot in $\Delta_{\text{[illegible]}} = \Delta_{31}$, and the two dots imply a dot in $\Delta_{\text{[illegible]}} = \Delta_{62}$ (R2 p 70). For one or two impulses this is absolutely equivalent to counting strokes.

(m) Δ_{31} : Table of formulae

Number of impulses used	Intervals chosen for differencing 31 times	N, text length of Z^* (n = text of Z)	These are as in 27 G (e) Average	±	Least text (n) which makes this number of impulses preferable for counting /'s	Scoring the letter coun: Score for a letter having so many dots 0 1 2 3 4	Average	±
1	1	n -31	N/2	$\frac{1}{2}\sqrt{N}$		0 1	N/2	$\frac{1}{2}\sqrt{}$
2	1,3	n -93	N/4	$\frac{1}{4}\sqrt{3N}$	210	1 1 3	N	$\frac{1}{4}\sqrt{3}$
3	1,4,6	n -186	N/8	$\frac{1}{8}\sqrt{7N}$	approx 6000	3 2 3 6	3N	$\frac{1}{8}\sqrt{}$
4	3,4,9,11	n -341	N/16	$\frac{1}{16}\sqrt{15N}$		6 4 4 6 10	5N	$\frac{1}{16}\sqrt{}$

As the number of impluses increases, the evidence of a given sigma-age diminishes.

It is rarely advisable to use 3 or 4 impulses for counting /'s, but it is useful to have more impulses on the tapes in order to score the letter counts.

(n) Δ_{31} : $\bar{X}_3 + \bar{\bar{P}}_5$ limitation

$$\Delta_{31}\,e(\,\Delta P_2 + \bar{\bar{P}}_5\,) + \quad \Delta_{31}\,e(\,\Delta Z_2) \longrightarrow \cdot$$

The P^* tape carries $\Delta_{31}e(\,\Delta P_2 + \bar{\bar{P}}_5)$, and P_2^* is not differenced on Robinson.

(o) Δ_{31}: ideal method

This means to count the dots in $\Delta_{\mu\rho}\Delta K_3$ for all values of ρ simultaneously (27 Y (b)). It is considerably more powerful than running for strokes (27 Y (g)). It might occasionally have been worth while.

Since so powerful a method would be needed only for very short texts, the method of 27 G (h) would be practicable (cf R2 p 102). Numerous alternatives were suggested. A form of "staircasing" in which all the impulses of "Z^{α}" are simply ΔZ_3 staggered at multiples of 31 is given in R3 p 2 (Δ_{31} ρ is effected by adding them: more than one run is needed). Other suggestions R2 p 105, R3 p 24.

The 5202 photographic machine (ch 91) could be used advantageously, by putting a transparent spot in the $2\rho-1^{st}$, $2\rho^{th}$ levels of $\Delta_{31\rho}\Delta Z_3 = \cdot, \times$ respectively; and similarly for ρ. A single place adj K^{th} can contribute several coincidences between transparent spots, an advantage of 5202 not exploited by the method of 27 D.

27H HISTORY OF CRIB ORGANISATION

Work on cribs was shared between

(i) Sixta Non-Morse Section (Log reading).

(ii) Testery Cribs Watch (Decode reading).

(iii) Newmanry Cribs (Statistical machine setting).

Crib prediction was so unlike other work on Tunny and involved so much liaison with Sixta and the Cribs Watch that during most of its existence the Cribs Section was the responsibility of a single cryptographer with special qualifications for such work.

The (Wren) Cribs Registrars (one on each watch) dealt competently with all standardised operations: ordering, editing, checking decode and cipher, making and checking tapes. The amount of checking needed was large even by Newmanry standards.

Men in charge

Early 1944	Newmanry DO (as one of many duties	during this period methods were gradually standardised.
Aug. 1944	Cryptographer on each shift (by rota)	
Sep. 1944	Permanent Cribs man and Mr.Y.	
Nov. 1944	Permanent Cribs man	
Apr. 1945	Section reorganized as "Robinson Section" (2 men) to facilitate experimental work on Robinsons.	

Some Statistics

Retransmission slips produced by Sixta	: 893
" " worked on by Newmanry Cribs	: 250
Days broken	: 72

Early references R2 pp 64,79).

27W BASIC CRIB FORMULA

The problem is that if recognising key.

$$\begin{aligned} &\Delta_{ij}\ K_{ij} \\ &= \Delta_{ij}(\Psi'_{ij} + \chi_{ij}) \\ &= \Delta_{ij}\ \Psi'_{ij} \end{aligned} \qquad \text{W1}$$

where Δ_{ij} denotes differencing at any common multiple of the lengths of $\chi_i\ \chi_j$.

Therefore since $P(\Delta\Psi_{ij} = \cdot) = \frac{1+\beta}{2}$

$$P(\Delta_{ij}\ K_{ij} = \cdot) = \frac{1+\beta^2}{2} \qquad \text{W2}$$

Putting $j = 6$ or by elementary methods

$$P\{\Delta_i(\Delta K_i + \text{lim}) = \cdot\} = \frac{1+\beta^2}{2}$$

For $\overline{\chi}_2 + \overline{P}_5$ limitation $P\{\Delta_{31\rho}(\Delta K_2 + \overline{\chi}_2 + \overline{P}_5) = \cdot\} = \frac{1+\beta^2}{2}$ (31 ρ is any multiple of 31)

i.e. $$P\{\Delta_{31\rho}(\Delta K_2 + \overline{P}_5) = \cdot\} = \frac{1+\beta^2}{2} \qquad \text{W3}$$

Similarly for $\overline{\chi}_2$ limitation $$P\{\Delta_{31\rho}\Delta K_2 = \cdot\} = \frac{1+\beta^2}{2} \qquad \text{W4}$$

U^* is used to denote a stream of letters whose impulses are all of the form $\Delta_{ij}\ U_{ij}$, so that W1 may be written

$$K_{ij}^* = \Psi'^*_{ij} \qquad \text{W5}$$

K, K^* often mean P + Z, P^* + Z^* which should not strictly be called K, K^* except when P and Z are correctly set. [Δ_{31} R2 p 70 $\Delta_{5\psi\psi}$; $\Delta_{5\psi\psi}$ R2 p 90]

$\Delta_{5\psi\psi}, \Delta_{31}$ are treated separately, because each has some simplifying circumstance: in $\Delta_{5\psi\psi}$ differencing at multiples of $5\psi\psi$ etc. is not needed; in Δ_{31} only the second impulse is involved.

(a) Ideal method (counting dots).

The theoretically simplest method is to count the total number of dots in the four streams $\Delta_{943}\,\Delta K_{15}$, $\Delta_{713}\,\Delta K_{25}$, $\Delta_{447}\,\Delta K_{35}$, $\Delta_{598}\,\Delta K_{45}$,(27G(h)).

The number, ν , of characters to be considered, is the positive terms of $(n-598)+(n-447)+(n-713)+(n-943)$

i.e. $n-598$, $2(n-633)$, $3(n-659)$ or $4(n-785)$ X1

As usual, average $=\frac{\nu}{2}$, $\sigma = \frac{1}{2}\sqrt{\nu}$, expected sigma-age $=\beta^2\sqrt{\nu}$ X2,X3,X4.

(b) Practical method (counting strokes)

In practice (cf 27G (b)) only those places where all these four streams have a dot are counted, i.e. the number of strokes in ΔK^*, the four impulses of K^* being $\Delta_{943}K_{15}$, $\Delta_{713}K_{25}$, $\Delta_{447}K_{35}$, $\Delta_{598}K_{45}$.

The effective text length N is

$$n-598,\ n-667,\ n-713,\ \text{or}\ n-963. \qquad X5$$

according to the number, m, of impulses used.

$$\text{Average} = \frac{N}{2^m}, \quad \sigma = \sqrt{\tfrac{1}{2^m}\left(1-\tfrac{1}{2^m}\right)N} \qquad X6, X7.$$

(c) Effect of non-normal distribution

As m increases the evidence of a given sigma-age decreases because the binomial distribution ceases to approximate to a normal distribution, and approaches, though not very closely, the Poisson distribution for rare occurrences. [22(1); R3 pp 24,26.]

In practice this demands no further calculation for g od scores are checked by counting the dots in ΔK^*.

(d) Expected frequency of each letter in ΔK^*

The frequency of strokes in $\Delta K^* \equiv \Delta\Psi'^*$ is greater than for a distribution, otherwise random, in which each character tends to a dot with probability $\frac{1+\beta^2}{2}$, because all the impulses of a letter in $\Delta\Psi'^*$ depend in part on the same letter of $\Delta\Psi'$. For this same letter there are three cases vix.

	TMx $\Delta\Psi_s x$	TMx $\Delta\Psi_s \cdot$	TM .
Probability of each case	ab	$a(1-b)$	$1-a$
" that $\Delta\Psi'_{us} = .$	b	$1-b$	1
" " $\Delta\Psi'_{us} = x$	$1-b$	b	0
" " $\Delta\Psi'_{us}$, sqs forward $= .$	b	b	b
" " " " $= x$	$1-b$	$1-b$	$1-b$
" " $\Delta_{sqs}\Delta\Psi'_{us} = .$	$b^2+(1-b)^2$	$2b(1-b)$	b
" " $\Delta_{sqs}\Delta\Psi'_{us} = x$	$2b(1-b)$	$b^2+(1-b)^2$	$1-b$

Whence the probability that a letter of ΔK^* has r dots and s crosses is $p =$

$$ab\{b^2+(a-b)^2\}^r\{2b(1-b)\}^s + a(1-b)\{2b(1-b)\}^r\{b^2+(1-b)^2\}^s + (1-a)b^r(1-b)^s$$

$$= \frac{1}{2^{r+s+1}}\left[(\alpha+\beta)^r(\alpha-\beta)^s + \frac{1-\beta}{1+\beta}(1-\beta^2)^r(1+\beta)^s + 2\beta(1+\beta)^{r-1}(1-\beta)^s\right] \quad X\ 8$$

(e) Expected decibanages

These can be calculated by "$\sum n \log n$" (22Y3). Since the frequencies are given, this is not optimistic. For counting strokes it reduces to

$$N\left[p \log 2^m p + (1-p) \log \frac{1-p}{1-\frac{1}{2^m}}\right] \quad X\ 9$$

The corresponding results for counting dots are included in the table, and show that these runs are appreciably stronger. The text for +40 decibans when counting dots assumes the ideal method of para. (a)

m (number of impulses)	Decibans per letter of Z^* counting strokes or dots, for a motor dottage: 20 strokes	20 dots	24 strokes	24 dots	28 strokes	28 dots	n−N (loss of text length due to differencing κ^*	n−N Ideal met
1	.041	.041	.116	.116	.31	.31	598	598
2	.073	.088	.214	.23	.59	.61	667	633
3	.087	.132	.28	.35	.80	.92	713	656
4	.091	.176	.31	.46	.93	1.22	943	730
Gross text for 40 decibans, and number of impulses used	1170 (3)	1020 (4)	855 (2or3)	770 (3)	730 (1)	700 (2)		

If the whole ΔK^* letter count were scored even more evidence could be obtained than from counting dots.

27Y Δ_{31} THEORY

(a) Preliminary

ΔK_2 is differenced at various intervals which are multiples of 31. In forming these differences a character of ΔK_2 is added only to characters of ΔK_2 against the same character of χ_2, and it is convenient to think of the text as consisting of 31 sets of $\frac{n}{31} = k$ letters.

(b) Ideal method

The obvious method, which wastes no evidence is to compare each of the k letters with each of the other, thus obtaining $\nu = 31 \frac{k(k-1)}{2}$ comparisons for counting $\Delta\Delta\rho\Delta K_2 = .$, but these are clearly not all independent.

It is easy to prove (as in the analagous problem of $2\Delta X(d)$ that the bulge of the score equals the bulge of the square of the half-pippages in the $\hat{\chi}_2$ run on the same key, i.e. the method is equivalent to using the χ^2 test. [R2. p 102: other references in 27G (o)].

For the standard deviation and expected score see paras. (f) (g) where this method is treated as the limiting case of methods used in practice.

(c) Practical method (counting strokes)

In practice 27G (k) the differencing is done only at $m(1, 2, 3 \text{ or } 4)$ intervals, each constituting one impulse of ΔK^{**} (not quite the same as for Δ_{sqq} etc.) Strokes in ΔK^{**} are counted.

The evidence of these strokes is not entirely independent, but if the intervals are well chosen, (cf para (h)) the formulae X6,X7 above, can be used.

(d) Effects of non-normal distribution.

Exactly as in 27I (c), the sigma-ages may be misleading, and it is

preferable to use the formula for expected decibanages

$$N\left\{\left(\frac{1+\beta^2}{2}\right)^m \log_3(1+\beta^2)^m + \left(1-\left(\frac{1+\beta^2}{2}\right)^m\right)\log_3\left[1-\left(\frac{1+\beta^2}{2}\right)^m\right]\right\} \quad Y11$$

(e) Scoring the letter count

To get more evidence from the ΔK^* letter count, consider all the comparisons made at each letter, and count those which give a dash. The number of comparisons is not merely m (as in Δ_{5+9} method) but [e.g. 276(1)]

$$m + \frac{m(m-1)}{2} = \frac{m(m+1)}{2}$$

and a letter with r dots and s crosses scores

$$r + \frac{r(r-1)}{2} + \frac{s(s-1)}{2}$$

e.g. when differencing at intervals 1x31, 4x31, 6x31, denoting each of the k letters against a particular character of χ_2 by its number, the first letter of Z^* involves explicitly the comparisons, 12, 15, 17 and implicitly 57, 72, 25.

Treating the comparisons as independent,

$V = N\frac{m(m+1)}{2}$ Average $= N\frac{m(m+1)}{2}$, $\sigma = \frac{1}{2}\sqrt{N\frac{m(m+1)}{2}}$ Y3, Y4, Y5

Expected decibanage $= 2{\cdot}17\,\beta^4 N\frac{m(m+1)}{2}$ Y6

It is shown rigorously in R3 p 70 (and a mathematically identical result is proved in 26X (a), that for a single letter the equations Y3, Y4. Y5 are in fact correct, but this particular argument does not apply to the whole text, unless $N \leq 31$ when there is only one letter of K^* against each character of χ_2.

(f) Ideal method as a limiting case.

The case $m = k-1$, and therefore $N = 31$ is the ideal method of para. (b). There is only one letter of K^* opposite each character of χ_2 so that Y3, Y4. Y5 are exact.

$V = 31\frac{k(k-1)}{2}$ Average $= 31\frac{k(k-1)}{2}$, $\sigma = \frac{1}{2}\sqrt{31\frac{k(k-1)}{2}}$ Y7, Y8, Y9

Expected decibanage $= 2{\cdot}17\,\beta^4\,31\frac{k(k-1)}{2}$ Y10

(g) Expected decibanages

m (number of impulses)	Expected decibans per letter of K* for motor dottages						$n-N$ (loss of text due to differenc
	20		24		28		
	/'s	letter count	/'s	letter count	/'s	letter count	
1	.041	.041	.116	.116	.31	.31	31
2	.058	.123	.174	.348	.49	.93	93
3	.059	.246	.189	.796	.57	1.86	186
4	.054	.41	.176	1.16	.58	3.1	341
Minimum text for 40 decibans and number of impulses used	780 (2)	350 (3)	320 (2)	210 (2)	160 (1)	140 (2)	
Ditto, ideal method	265		165		105		

(h) Choice of intervals for differencing.

Although the comparisons of para. (e) cannot be made independent, it is possible to avoid including the same comparison twice viz by making

(i) the intervals
(ii) twice the intervals
(iii) the sum of any two intervals

all different numbers.

Convenient sets of intervals which satisfy the conditions are (after removal of the common factor 31)

1 ;
1, 3 ;
1, 4, 6 ;
3, 4, 9, 11 .

28 - LANGUAGE METHODS

28A DEPTHS

(a) Definition

Two messages are said to be in depth if they are enciphered on the same key. A cross depth is a depth in which the legs are sent by different ends of the link.

(b) Importance of depths.

In the Tunny era, depths were of enormous importance in obtaining wheel patterns - it was some time before any technique independent of depth was discovered - but, owing to the nature of the indicating system, they were extremely rare.

The introduction of QSN (later QEP) numbers (November 1,1942) obliged us to concentrate all out attentions on depths whose number increased enormously as a result of the increase in the number of links and the indiscriminate use by the enemy of the cipher. (For example, a gadget was installed on the German machine enabling the operator to return the wheels to their original settings - a glorious depth-producing device.)

Statistical analysis enabled the problem of setting the wheels on single messages to be tackled again, but depths were still invaluable for obtaining wheel patterns.

The advent of the P_5 component of the limitation dealt a knockout blow to depths but its subsequent disappearance enabled us once again to employ depth-breaking methods and in the closing months of the war, depths proved of enormous value in obtaining wheel patterns with a currency which no other technique could achieve.

(c) Evidence

The existence of depths was deduced from the sequence of QEP numbers preceding intercepted messages. There was a possibility of a depth when the same number occurred twice within a short space of time, or when no QEP number was sent and the previous and following numbers were consecutive e.g. as in the sequence (i) 34 (ii) QEP not sent (iii) 35.

Originally depths only occurred between messages from the same end of the same link, but later some links used a QEP system in which both ends jointly used the same consecutive sequence of QEP numbers, After this, depths between messages from different ends of the same link (cross-depths) occurred.

In many cases it was not obvious which pair of messages were in depth, and in many cases alleged depths were in fact follow-ons. However every possible depth was teleprinted from Knockholt and investigated. There were two categories:

(i) depths which might give enough key for wheelbreaking purposes. The minimum for this in 1945 was 100 letters.

(ii) depths which might give enough key to set on known wheels. The minimum for this in 1945 was 15 letters.

(d) Treatment of Depths

From the fundamental equation of the machine

$$P = Z + K$$

we see that $P_a + P_b = Z_a + Z_b + K_a + K_b = Z_a + Z_b$ if $K_a = K_b$

Since by definition, $K_a = K_b$ for a depth, it follows that the difference of the ciphers is the difference of the clears. The conditions that $K_a = K_b$

for all places of the key are

identical wheel patterns
identical original settings
identical limitations.

It follows from (iii) that the introduction of autoclave destroys depths and that two messages enciphered on $\overline{\chi}_2$ and $\overline{\chi}_2\,\Psi_1$ lims respectively will also not be in depth.

Treatment of depths may be divided up into two subsections (i) depth scoring and (ii) depth anagramming.

(1) Depth Scoring

Since the frequency distribution of P is non-random, it follows that the Z_a+Z_b of the two messages in depth, differs considerably from a random set of letters, since the frequency P_e of a letter e in P_a+P_b is given by

$$P_e = \sum_x P_x P_{e+x}$$

It therefore follows that each letter in Z_a+Z_b contributes a factor towards (or against) the theory that the two messages are in depth. [A scoring table was devised to exploit this property (R41, pp.56,57.) (See 22W]. It is equally true that trigrams or bigrams in Z_a+Z_b make their contribution to the theory and scoring tables could be devised to make use of their contribution. Two points, however, should be borne in mind. First, language properties are very heterogenous and depths may therefore not appear obvious from a scoring table (in particular, depths on links using 'doubles' may usually be recognised purely by a count of /'s in the difference or 'clicks'.) Second the danger of slides is a very real one and their occurrence naturally make depth scoring more problematical.

(2) Depth Anagramming

Having ascertained that the depth is worth working on, the next stage is reached in which an attempt is made to divide up Z_a+Z_b into its respective P_a and P_b. The original technique of dragging (described in earlier screeds on this subject) has now been completely superseded by 'faffing' or 'fiddling', a process open only to the most experienced and capable breakers. The process consists - insofar as it is susceptible to logical exposition - of recognising common differences (e.g. F3, Y3, 58, KO, VLJ) and assuming the clear equivalents EN +N9, (DE + 9D), CH+5M, 89+95, CH+EN, SCH+5MB, then trying to extend these rudimentary breaks. It will be readily appreciated that only after considerable experience and practice, can sufficient of these 'equivalents' be memorised to enable one to employ the method. In anagramming a depth, the following aids should be borne in mind

(i) use of autopauses, which would suggest an identical clear repeat or go-back
(ii) short hand transmissions in the middle of an auto message,
(iii) stereotyped nature of message beginnings.
(iv) The common appearance of standardised forms of punctuation and the tendency of stops, when acting as abbreviation marks, to occur in clusters.
(v) the possibility of a single letter or bigram being repeated several times, particularly before an autopause.

It will be noted that these aids are, as would be expected, fundamentally the same as those employed in de-chi breaking.

(e) Determination of key

Suppose $Z_a + Z_b$ are in depth and suppose that the clears are P_a and P_b (so that $Z_a + Z_b = P_a + P_b$) Without further evidence, it is not possible to say whether $K = Z_a + P_a = Z_b + P_b$ or $K = Z_a + P_b = Z_b + P_a$. I will discuss here what methods are employed to relate the clears to their respective ciphers, omitting only those methods which virtually form part of key-breaking.

They are
(i) The existence of one or more extra messages in depth;
(ii) relating cipher pauses to clear pauses;
(iii) distinguishing between hand and auto language;
(iv) Sixta preferences based on their clear expectations;
(v) distinguishing between language characteristics at either end of a cross depth.

In addition, continuity enables one to keep on the right track, but it is often difficult even for the most experienced depth breakers to associate the clears correctly.

(g) Proteus

At the time of writing, Proteus has not yet been completed, but a brief description of its functions may be of interest. Proteus is a machine designed to take a crib through a depth difference and test the resulting letters against a dictionary of common clear-formations. For fuller account see

(h) Setting of depths on known wheels.

See Chapter 43C (b) and (d).

28B Ψ SETTING FROM DE-χ

(a) Introduction

When the χ's are set on Colossus, frequently either the motor patterns for the day are not yet known, or else Colossus time is too short to permit the mechanical setting the the motors and Ψ's. So the χ's are added to the Z at their correct settings to give de-χ (D). Thus D = Z + χ = P + Ψ'. The de- χ tape is then printed on a width of 31 and sent over to Major Tester's section, where skilled breakers attempt to set the Ψ's by non-statistical methods. This chapter is intended to give an outline of these methods.

The first de- χ was broken by Tutte, (44C) the second by Tutte and Major Tester's Section combined and the third by Mr. Newman's Section (RO p.95). This last gives the date when it became a routine to send de- χ's to Major Tester's section for Ψ -setting by hand, in place of the de- χ's on impulses 1,2,4 and 5 with the motor which was previously thought necessary for success (see 43 (1)(d)).

(b) The Problem

The breaker is given a single stream of letters which he must resolve into the two components P and Ψ'. The partial Ψ patterns obtained from stretches of de- χ which he thus resolves, must then be found on the known Ψ wheels.

(c) Prior Knowledge

To obtain such 'breaks' in the D four types of prior knowledge are used:

(i) P Characteristics
(ii) Ψ' characteristics.
(iii) Type of limitation used by the Germans.
(iv) The 32 L.C.

(i) Knowledge of P characteristics is gained from a wide range of decodes on various links. Stock forms of message beginnings and endings, call signs, priority and secrecy signs, addresses, common syllables, words and phrases of military German, - all of these are invaluable, but it is the peculiar nature of Tunny punctuation that the breaker makes most use of. A full stop may be expressed in various forms, e.g. ++M889, +M98, ++M989 +M89 etc. Tunny language showed an ever-increasing use of abbreviations, each normally followed by a stop. These abbreviations tended to occur in common sequences, producing clusters of stops. Hand transmission is marked on the de- X and here use is made of knowledge of the common phraseology of operator's remarks.

(ii) The basis of de- χ breaking is the property $\Delta\Psi' \rightarrow /$ with probability $\doteq 1-a$. Wherever $\Delta\Psi' = /$, $\Delta D = \Delta P$. The breaker therefore reads through the de-χ mentally differencing as he reads, looking for common ΔP combinations which will show through proportion $\doteq 1-a$ of the time. He also uses the property $\Delta\Psi; \rightarrow x$. Thus having recognised a ΔP combination he writes it, in its undifferenced form, beneath the relevant letters of de- χ, adds it to give Ψ', and then continues the combination backwards and/or forwards using his knowledge of P. The new Ψ' letters thus produced are examined by the two criteria given above, to judge the validity of the break. Clearly the higher the μ, dottage the stronger are these two properties and the easier it is to make and extend breaks. The breaker's knowledge of the reverse Δ of the common P combinations also helps him in making breaks.

(iii) All breaks must satisfy the conditions of the limitation known to have been used. Since the de-χ is printed on a width of 31, the breaker writes in χ_2 (or $\bar{\chi}_2$ if the lim. is $\bar{\chi}_2$ only) which is present in every type of limitatio above the top line of the de-χ and it is then correct for every line.

(iv) The de-χ is accompanied by its 32 L.C., with a comment from the D.O. on its reliability and a note on whether the limitation is $\bar{\chi}_2$ or not. If it is on $\bar{\chi}_2$, a 32 L.C. against $\bar{\chi}_2$ crosses is given. Chapter 22 G,H. gives an idea of how useful the 32 L.C. is to the breaker, in revealing the type of language and punctuation used in the de-χ.

(d) Breaking the de-χ.

It is impossible fully to describe the subtleties of exploitation used by the expert breaker with his great familiarity with plain language and its Δ forms and his faculty of instantaneous teleprint addition. We can only describe the commonest and most obvious methods of obtaining a break.

In favourable circumstances a single break may be obtained sufficient to set all the Ψ's or enough of them to be used as evidence to set the remainder. Here is an example of a line of de-χ on $\bar{\chi}_2$ limitation with $\bar{\chi}_2$ written along the top. In it the breaker sees two likely stops which he writes in, with the Ψ' which they produce.

```
χ̄2   .XXX...X..XXX.X..XX..XXX.XXX
D    /WM5EEPN/MORFORDPSTAE5OAGIWU
P                 5M89   5M89
Ψ'                APPD   GUUU
```

The Ψ' extensions all work on the limitation and the $\Delta\Psi'$ features are good. The Ψ letter D cannot be carried forward nor the G backward. But extensions are legitimate at 8TA in the de-χ. The Δ of 8T is K which is the Δ of DI, suggesting the common abbreviation DIV, which would also give 'good Ψ changes' ($\Delta\Psi$ crosses). Assuming DIV to be correct we look before the first stop for an abbreviation likely to precede DIV, such as 9PZ, 9GREN, 9JAEG, or 9INF. The ORF under $\bar{\chi}_2$ crosses immediately suggests 9PZ, and the likelihood that the number of the division has been given in figure shift suggests an 8 before the 9PZ, which gives an 8 in $\Delta\Psi$. The common word IST is strongly suggested at the end of the break, so we now have

χ_3 .xxx...x..xxx.x..xx..xxx.xxx
D /WM5EEPN/MORFORDF8TAE5OAGIWU
P 89PZ5M89DIV5M89IST9
ψ' AMMAPPDPPXGUUUMAAA

The next stage is to write out ψ in impulses

x.x.x.x.x.x
x.xx.x.xx.x
.x.x.xx.xx.
.x..x.xx.x.
.x.x.xxx.x.
AMAPDPXGUMA

The patterns are then tested against the known ψ wheels. It is found at the patterns obtained for the 1st,2nd,3rd, and 5th impulses are unique

on their respective wheels, so the patterns can be written out on either side of the break. On Ψ_4 the pattern obtained occurs twice only, so it is possible to write in what is common to both positions.

```
..x.x.x.x.x.x.x xx..x
.x.x..x.xx.x.xx.x..x.
x.x..x.x.x.xx.xx.x...
    .x.x..x.xx.x.xx.
.x.x.x.x.x.xxx.x..x.x
9LSGEMAMAPDPXGUMAFO4Z
NGFL                B
```

or

Using the new material the break can clearly be extended to the left by choosing the Ψ alternatives and extensions to give sense, until Ψ_4 is also set uniquely and the de- χ broken. In this case the first stretch should read

```
.xxx...x..x
/WM5EEPN/MO
9DIV95QTM89
9GGS5GEMMAM     etc.
```

In this example the motor dottage is high and the problem easy. But frequently two short breaks are obtained and nothing can be assumed for the intervening gap, as in the following example (limitation is ignored for simplicity)

```
D     ZZDQQNSWQTOAJ3QN
P     55M889     55M889
Ψ'    RRY333     AOQQ33
```

The Ψ is then written out on all reasonable assumptions of the number of Ψ's in the gap, and enough impulses of Ψ should be identifiable on one of the assumptions to guess the intervening P (in this case 'GREEN'). This will either set the Ψ's or reduce the number of positions still possible to obtain further evidence, or in the worst case merely provide language evidence from which to guess further P.

With difficult de- χ's, the two breaks may be at a considerable difference apart (RO p.89). Suppose each gives 5 Ψ letters. The possible positions for all wheels for each break are listed and the distance apart estimated, thus

```
7,12,15          15,22,30     Actual distance = 558
37,42            15,19,32     Approx. unextended Ψ distance
5,19,27,31,50    45           = 550 x known value of a = 400.
4,38             17,30,42
27,50            20,34,50
```

It is calculated that if the distance is taken as 397, both breaks fit all wheels, and the Ψ's are set at

12	22
37	15
5	45
4	30
50	34

To do the somewhat laborious calculation involved, a 'compatibility chart' was calculated and work was begun on an attachment to Dragon, named Salamander which would solve such problems automatically. But the end of the war prevented the machine from being completed and tested operationally.

(e) Autopauses

These signify either that the operator has inserted a new message tape or that he has pulled back the tape and sent the last stretch again. In the first case the autopause is followed by a message head with its vulnerable stock beginning. In the second case the same P occurs both before and after the pause; this is called a 'go-back'.

(f) Go-backs

The average length of a go-back is between 40 and 100 letters. A go-back can be located in two ways.

(i) by making a break on one side of the pause and then looking for the same P on the other side.

(ii) by comparing the two stretches of ΔD.

In the case of (i), once located the two indentical breaks can be extended by playing them off against each other. For obstinate de- χ's procedure (ii) is used. A complete and detailed scoring system for go-backs for all motor dottages is given in 'Report on Tunny (Major Tester's Section)' VIII, Appendix to parts A and B.

But frequently a go-back can be found by (ii) by inspection.

Let the stretches of de- χ before and after the pause, which contain the same P be D_a and D_b. Then $\Delta D_a + \Delta D_b = \Delta \Psi'_a + \Delta \Psi'_b + \Delta P + \Delta P = \Delta \Psi'_a + \Delta \Psi'_b$ The most striking feature of the sum of two $\Delta \Psi'$ streams is the proportion of /'s which is

$$(1-a)^2 + a\,(b^2 + \overline{1-b}^{\,2})^5$$

and the next most prominent feature is the proportion of 8's, which is

$$2(1-a)(ab^5) + a\left\{2b(1-b)\right\}^5 .$$

These two factors may be sufficient to locate the go-back, by sliding ΔD_a against ΔD_b and looking for 'clicks' and 'anti-clicks'. An additional check is provided by the limitation. /'s are only strong evidence where $\lim_a = \lim_b$. Even with compound limitation the two lims can be compared. As $P_a = P_b$ the P_5 element of the limitation is identical. Also $\overline{\Psi'_a} + \overline{\Psi'_b} = \overline{D_{1a}} + \overline{D_{1b}} + \overline{P_{1a}} + \overline{P_{1b}}$, $= \overline{D_{1a}} + \overline{D_{1b}}$ as $\overline{P_a} = \overline{P_b}$. So the first impulse of D can be used supposing Ψ'_1 limitation is present.

A machine, 'Aquarius', was constructed to locate go-backs mechanically, but too late for ~~current~~ operational use.

Go-backs are also used when located by (ii) for resetting a wrongly set impulse of D. Resetting a wrongly set χ by means of a go-back and also by means of a break, is described in 'Report on Tunny (Major Tester's Section) VIII 6 and 7.

(g) Overlaps

It is quite common for the beginning of a transmission to be a repeat of the P at the end of the preceding transmission.

The extent of overlapping varies considerably. The ΔP of the broken de- χ is slid against the ΔD at the start or end of the unbroken de- χ for 'clicks'. The Dragon machine is particularly suitable for exploiting overlaps.

(h) Rodding

A rod is a stick of cardboard at the head of which is written any of the 32 letters, and below in column, the letters resulting from the addition of that letter to each of the 32 letters in order. If it is desired to rod QXR4CMC of a de- χ, ten rods headed by these letters are set up adjacent to each other and each level of the rods is inspected for fragments of P. Wherever there are repeats in Ψ the P will appear on a level of the rods (RO, p.5

(j) Operational Success

The following figures (in transmissions) give a picture of the quantity of the work handled and the proportion of success gained. The figures are for April, 1945.

de- χ's	Broken
806	707

De- χ's marked 'all certain'	Of these broken	Of those broken incorrectly marked 'all certain'.
728	680	21

356 transmissions were also set on all wheels mechanically.

(k) Dragon

Dragon is a machine for the mechanical breaking of de- χ's by means of short cribs. For an account of how it works see (55A) (also see Report on Tunny (Maj. Tester's section) VIII).

28C ψ-BREAKING FROM DE- χ

(a) Introduction

When the χ's have been broken from cipher, the breaker must find sufficient P in the de- χ to give the entire new ψ patterns. This is clearly a much more difficult task than ψ setting, for a very much longer break of correct P must be made. In fact at first it was thought impossible except by using both legs of a depth set on the χ's. This was in fact how the first set of ψ's to be broken from a de- χ were obtained, on Bream of January 1944. But the February Bream ψ's were broken from a single de- χ and it was never necessary again to use a depth. As depths are rather infrequent and as from Summer of 1944 wheel patterns changed daily, this regular succes in breaking ψ's from single de- χ's was of vital importance. Between August 1944 and May 1945 failures to obtain ψ patterns numbered less than 10 as against about 365 successes, and in some of the failures the χ's were not certain. Moreover, several sets of ψ's were obtained from de- χ's made with incorrect χ's which had to be corrected during the process.

(b) Method

See Figs. I and II.

The process of ψ-breaking begins with the making of a break in the de- χ. Normally, this break should yield 17 or more letters of ψ key. The ψ-key obtained, with extensions removed is then written out in impulse form, as in Fig.II. The fragments of ψ are then "projected" forward, at their respective wheel lengths. Thus ψ_1 is re-written out at a distance of 43, ψ_2 beneath it at a distance of 47, and so on. These patterns found in Break A can now be used.

(i) for finding another break where the "projected" Ψ is expected to occur. The position is calculated as follows. In the unextended Ψ , the distance from the last Ψ letter of the original break A to the first nearly complete letter of the projected Ψ is 36. The original break will have provided an approximate indication of the motor dottage and therefore of the proportion of repeats in Ψ′. In this example the first nearly complete letter (M) of the projected Ψ is found in break B at a distance of 56 from the end of break A, showing a Ψ′ to Ψ ratio of 56/36 or very roughly 3/2.

or (ii) for identifying a break already found, about two lines ahead in the de-χ . Thus after obtaining break A, the stop giving the Ψ′-stream MMAOOO might have been discovered and the Ψ identified on the "projected" Ψ at places 54,55,56.

From the correlation of these two breaks we get much useful information. First our breaks confirm one another. Secondly they give further indication of t dottage of χ37 (by defining how many Ψ's are used in a given length between break A and break B). Thirdly, if we want to project our Ψ-stream forward, once more, or backward, we shall know with fair accuracy, where to look for such Ψ-letters or partial Ψ - letters as we get by such projections, i.e. where these letters should give clear, and most important, the new break will give us additional signs on our partial Ψ-wheels, which can in their turn be played

FIG I. 26C Page 262

DE-X CLEAR Ψ'

```
                                                                  X Z S L 3 Q Q S
                                                                  R T 9 W P P P 9
                                                                  Q E E E V E E E
```

DE-X CLEAR Ψ'

```
H 4 X I E Z I F 4 4 + K K H R G H H 9 T 8 + F K P E W E E -
V 8 8 9 A N 9 H + + M 8 8 9 G R + + M 8 8 9 S U E D 9 + +
R X 4 4 4 X 4 B B B U T T T T T K K O K / 8 3 3 Q 3 Y G G
```

[BREAK A]

DE-X CLEAR Ψ'

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

DE-X CLEAR Ψ'

```
- - - - - - - + I V 4 8 U O O / F + + / F A Z N U U 8 U U P
          9 B E T R 9 + + M C 8 8 9 D O R T + + M 8 8 9
          8 8 8 L Y A A A M A 9 9 9 9 + + M M M A O O O
```

[BREAK B]

FIG II

UNEXTENDED Ψ OBTAINED FROM BREAKS.

```
X X . X . . X . X . XX . X . X . X . X . X . X .
X . X . X X . X . X . X . X . X . X . X . X . . X
X . X . X . X . X . . X . X . X . X . X . X . X .
. . X . . XX . X . X . . XX X . XX . X . X
X . X . . . X . X . X . X . X . . X . X . XX
Q E V E I R X 4 X 4 B U T K O K / 8 3 Q 3 Y G
X . X . X . .
X . X . X . X . . X
. . X . X . X . X . X .
. X . X . . X X X . XX . X . X
. X [. . ] X . X . X . X . X . . X . X . XX
A O U 3 U T C
      Q O Q I K
```

back to break A, to assist in discovering the clear which comes in front of this break. Having obtained this clear, the new signs which it gives are projected forward again to Ψ - stream B to assist in getting the clear before break B.

The reason for the stipulation that the original break should produce 17 or more Ψ's may now be clearer. The difference in length between the longest and shortest Ψ-wheel is 16, and 17 places thus gives a complete new Ψ-letter in the projection B (place 60). It is easier if no break is readily visible in the B area of the de-chi, to look for a complete Ψ-letter to give clear when added to the de-chi, than to use only 4-impulse Ψ-letters.

There are two ways in which the breaker can have his work simplified.

(i) By the discovery of "pure Ψ".
(ii) By discovering a go-back.

In (i) the German operator has sent, instead of clear text, a string of /'s, in which case, when the χ wheels have been stripped off the cipher, Ψ' which is usually easy to recognise, forms the de-chi at that point. (The operator has been sending pure key, in fact.) This pure Ψ is the more easily spotted, as the operator usually pauses when he has sent it, and Ψ-breaking de-chi's are usually examined at pauses in the text. But he may send a series of E's instead of /'s, or any other letter. If he sends a string of E's then the last four impulses will fit correctly with the Ψ-wheels but the first impulse will be in reverse (having a cross in the first impulse.) As the breaker never knows which letter has been sent, he has to find a break in the vicinity of the "pure Ψ", write down, in impulse form, the Ψ's obtained from the break, and look for these patterns, or their reverse patterns, in the write-out of the pure Ψ. If he is unable to find a break, then his only alternative is to test the 32 possibilities which the pure Ψ (representin the encipherment of one of the 32 signs of the teleprinter alphabet minus the signs 3 and 4 which do not occur) offers him. Such a method was used with success on at least one occasion. One breaker tested the Ψ write-out with the assumption of / in the clear text, another with the first impulse reversed assuming an E in the clear, and so on.

Case (ii) offers the quickest means of Ψ-breaking and the job has been done in 35 minutes with ease with the aid of a go-back. Usually the operator repeats about 60 letters of his tape in a go-back, which is just the right distance for the breaker. Thus the P of break A, picked up again after a go-back position B, can be expanded by the use of the Ψ signs derived from write-out of the B Ψ-stream. The new clear information is put in at position B, providing new Ψ information for position A. Unless the clear is very awkward, this process carries on quite smoothly until the breaks are linked up and the wheels are complete.

A few points:

(i) Naturally the original Ψ may be projected forwards, or backwards, and any number of times, though the Ψ information gets weaker with each projection, as the impulses get progressively out of phase with each other.

(ii) Use is of course made throughout of the limitation, as in Ψ-setting from de-chi

(iii) After the completion of the Ψ-breaking, the number of dots in the 37 wheel can be discovered as it is in relation to the numbers of crosses in the 5 $\Delta\Psi$-wheels ($ab = \frac{1}{2}$). A chart is used, giving the number of crosses in each $\Delta\Psi$ wheel corresponding to any given number of dots in the μ_{37}. A copy of the chart is given in 22D (c).

It is useful as a second check of the Ψ patterns obtained (the first check being that each Ψ wheel must be an equal number of dots and crosses ± 1), and sometimes as a method of completing an incomplete Ψ wheel.

Thus dottage can be found before breaking the motor and traffic ordered according to the expected ease of difficulty of χ-setting by machinery.

(iv) It should be mentioned finally that about a week after VE-day, a method was successfully used for breaking Motor and Ψ patterns by statistical methods.

28D MOTOR BREAKING AND SETTING

(a) Early Motors

Motor breaking and setting were simple operations with the original Tunny type motors. These had

(i) No limitation,
(ii) 11 groups of crosses in $\mu 37$ separated by singleton dots.
(iii) 11 to 19 singleton dots in $\mu 61$.

Thus the groups of crosses of $\mu 37$ could be numbered in the B.M. modulo 11, a $\mu 61$ dot inferred from every B.M. double dot, and the rest of the $\mu 61$ dots inferred by comparison of the several appearances in the B.M. of the same $\mu 37$ group. This section however deals with the more complex motors universally used after the first few months of the QEP era, in which none of the above conditions was fulfilled.

(b) Motor Breaking

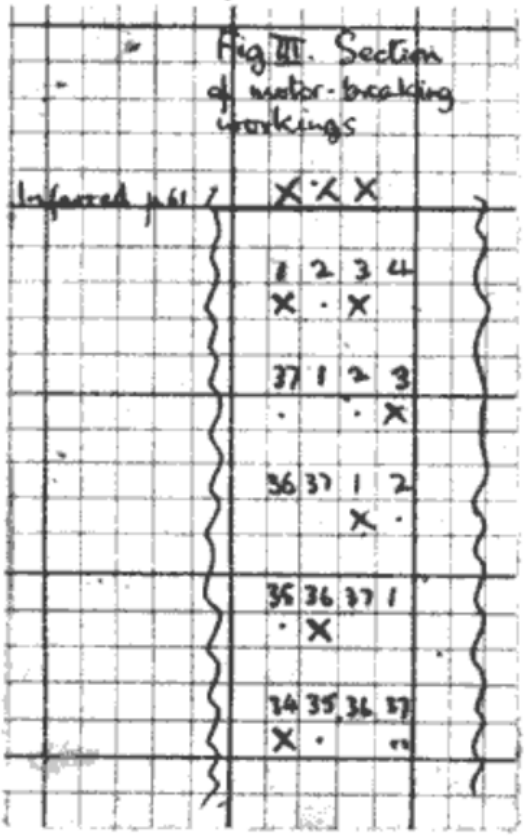
When the first message of a given motor key date has been broken either from depth or de-χ, the χ and Ψ patterns and settings will be known, but those for $\mu 61$ and $\mu 37$ have still to be found. If the χ and Ψ wheels were obtained from a depth then the anagramming necessary to break the motors is already largely provided. Where the Ψ's derive from a de-χ the settings of the χ's may be for the first letter of the cipher and the Ψ settings for (say) the 4,000th. Advantage is usually taken of the plain language and Ψ′ obtained during the breaking of the de-χ, at this latter position and the calculation of the settings for the start carried out after the motor has been broken. When the wheels have been broken by means of a crib, anagramming is unnecessary and the key is de-ciphered to give the required Ψ′. This Ψ′ must be checked against the unextended Ψ. Since only Ψ movements resulting from the B.M. are used to reconstruct the motor wheels, the amount of anagrammin necessary will depend on (i) the type of limitation and (ii) the $\mu 37$ dottage.

In (i) the case of $\bar{\chi}_1$ lim. the longest group of B.M. characters that can appear as T.M. is the length of the longest group of crosses in χ_1.

(ii) The nearer the number of dots in $\mu 37$ is to $\frac{61}{2}$, the greater is the expected proportion of changes of sign in $\mu 37$ and therefore the smaller the amount of anagramming required. Where a Ψ wheel contains undertain characters, the correction of the wheel is done during the anagramming by notin the period in which the wrong letter appears. When the anagramming proves difficult the process of "snaking" is used. An example and explanation of "snaking" is given in 28 Fig V. The anagramming is done on a width of 61 to facilitate the writing out of the B.M. on this width. Motor breaking is begun when a length of from 6 to 12 times 61 has been anagrammed.

First of all, changes of sign (.x or x.) in the B.M. are marked above the first of the pair of signs as a cross in $\mu 61$. It follows that if a block of say 3 consecutive crosses occurs in $\mu 61$, all stretches of B.M. appearing underneath will be stretches of unextended $\mu 37$ (FIG III). If the number of dots in $\mu 61$ is say, 25, $\mu 37$ expands to 62 and the first term of $\mu 37$ reapp on the next line of the B.M. one position to the right, as also positions 37, and 3. The "interval" or "Column difference" is therefore -1, and if each term under the block of crosses is numbered accordingly quite a few terms of

μ37 are revealed and a start can be made on the process of building up μ61 and μ37 as described later. The formula for the "interval" is 61 37 - number of μ61 dots = 24 - number of μ61 dots.



Where the interval is not a small one the inspection of the terms under a block of inferred μ61 crosses is often not helpful, since the terms appearing in the top line may not reappear under the block until many line down, more than have been anagrammed. The finding of the correct interval and thus the μ61 dottage is attempted in 3 ways:-

(i) a simple eye inspection of the columns under a block of inferred μ61 crosses as in Fig III.

(ii) trying out arbitrary intervals and numbering the columns under a block on each assumption.

(iii) looking for a repetition after a gap of 37 - μ61 characters of the columns appearing under a block of crosses (cf BO. p.

As already mentioned (i) only succeeds if the interval is very small. (ii) is very successful when the μ61 inferred crosses are frequent and in large clumps, for by using a card stencil assumed intervals which give contradictions are quickly rejected by inspection. The stencil has a series of openings five characters in width, each opening being numbered according to a particular interval assumption. Intervals from +13 to -7 are provided for.

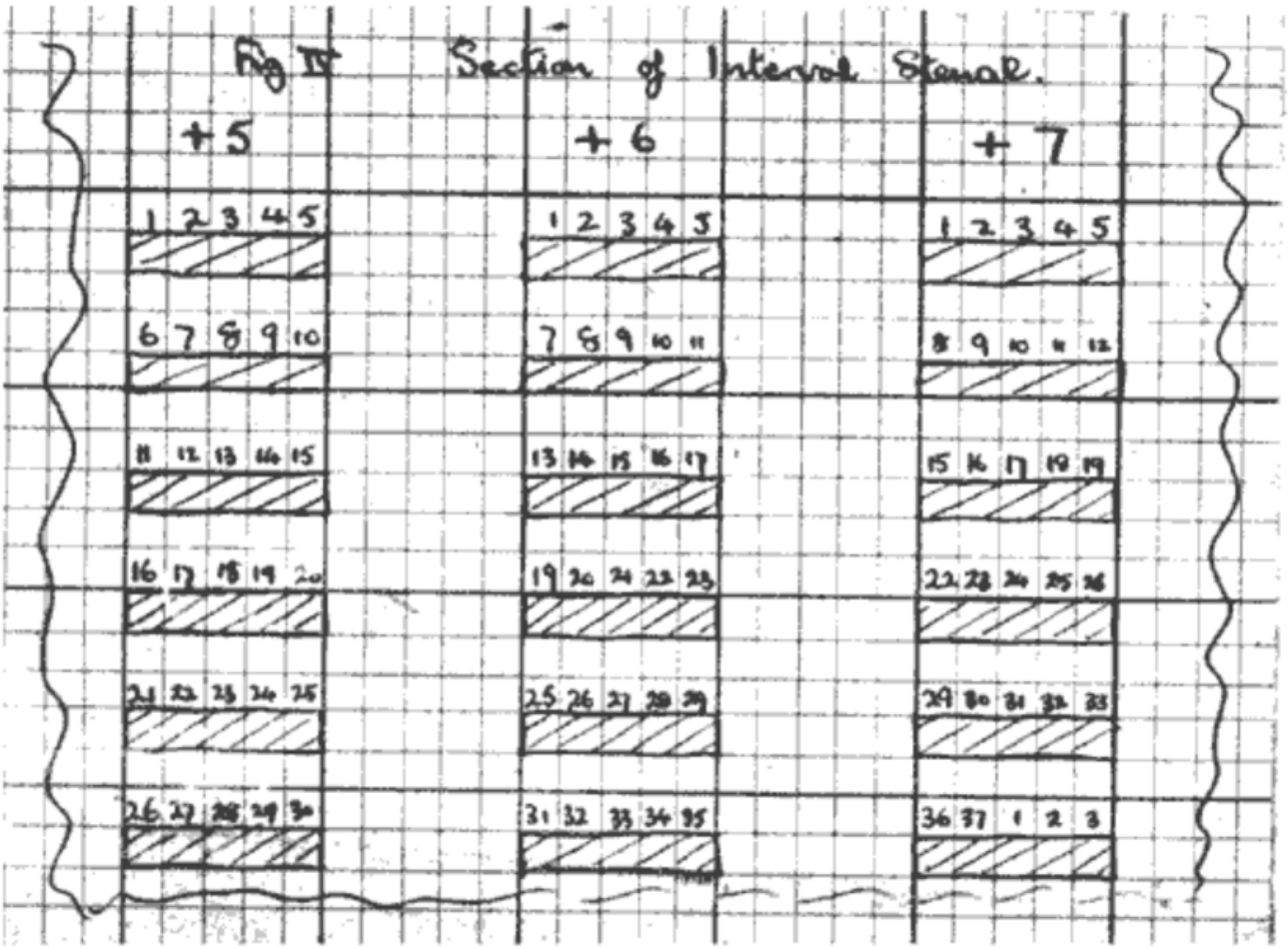
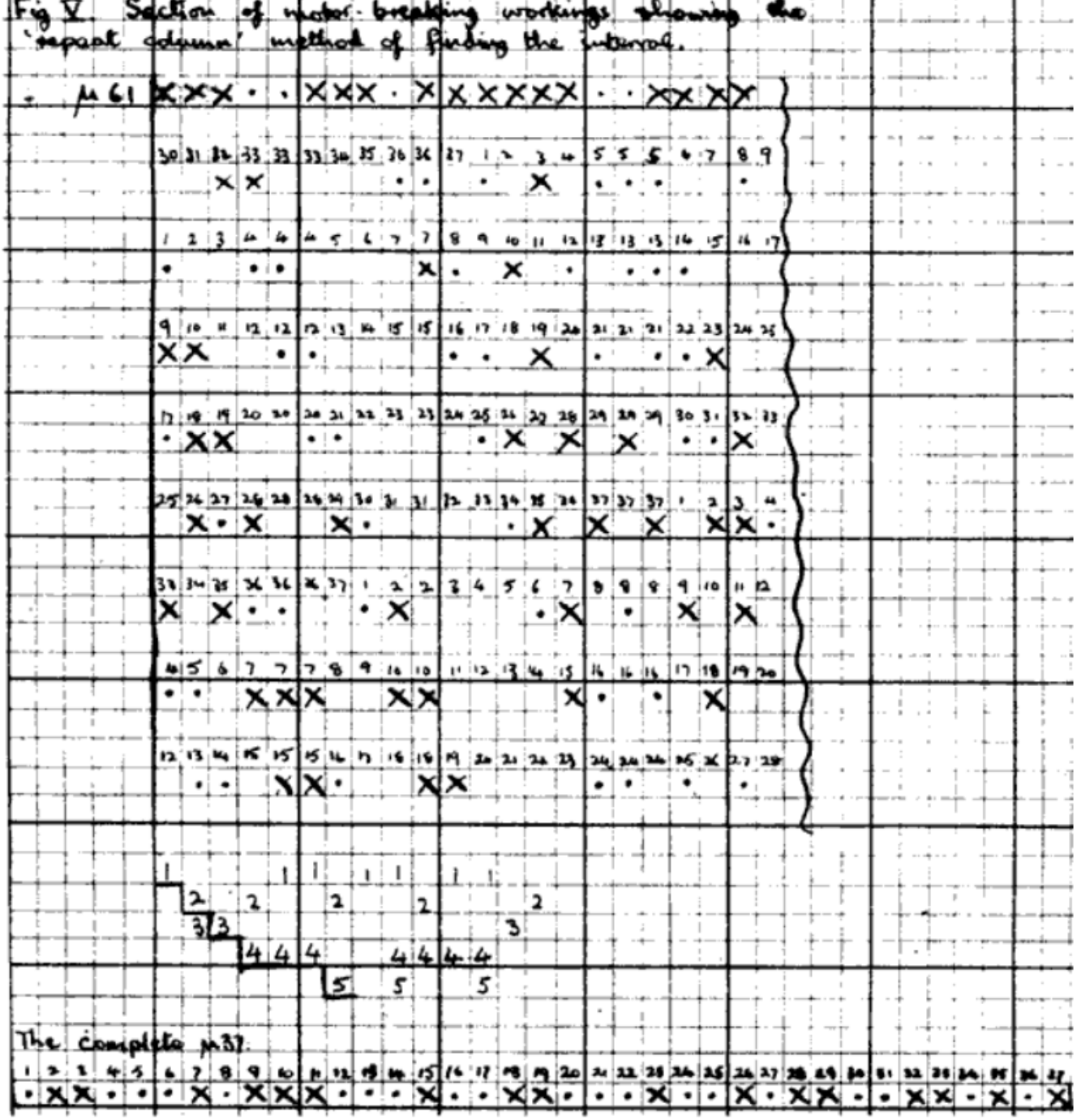


Fig IV
Section of Interval Stenar.
+5
1 2 3 4 5
6 7 8 9 10
11 12 13 14 15
16 17 18 19 20
21 22 23 24 25
26 27 28 29 30
+6
1 2 3 4 5
7 8 9 10 11
13 14 15 16 17
19 20 24 22 23
25 26 27 28 29
31 32 33 34 35
+7
1 2 3 4 5
8 9 10 11 12
15 16 17 18 19
22 28 24 25 26
29 30 31 32 33
36 37 1 2 3

A contradiction is given if a number on the stencil with a sign of B.M. beneath it, reappears in a different row with the opposite sign. The particular interval assumption being made is then rejected and another one tried. When the stencil fits with no contradictions it is replaced by numbering the columns of the B.M. according to the stencil (in pencil) . Then an attempt is made to extend the numbering of the B.M. on all rows backwards and forwards assuming whatever μ61 characters (in the gaps between inferred crosses) are necessary to avoid contradications. This will either yield eventually the entire μ61 and μ37 patterns, with some ambiguities in μ61 (an ambiguity is a short stretch of μ61 where the number of dots is known, but not their exact position) or lead to inescapable contradictions, in which case the interval assumption must be abandoned and another one tried.

In (iii) the repeating columns are identified as follows. A block of inferred μ61 crosses is chosen which has under it a fair number of characters. Column 1 under the block is copied on to a strip of paper which is slid along the columns of B.M. Wherever the characters on the slip give no disagreements with the characters of a column, the figure "7" (for Column 7) is written beneath that column at the bottom of the page. Columns 2,3 etc. are similiarly slid. Examining the results a continuous "staircase" as in Fig.V indicates the repeat, and the length of the gap between the repeat and the original columns gives an idea of the μ61 dottage and therefore the most likely intervals.

Fig V. Section of water-breaking workings showing the 'repeat column' method of finding the interval.



The complete μ37.

According to whether dots or crosses are assumed in positions 9 and 11 of ⊥ 61, the possible intervals in the example are +9, +8, and +7. Assuming a dot in position 9 and an interval of +8, column 10 gives 7, 10 and 18 as crosses - which agrees with the numbering already carried out. Position 11 of ⊥61 must be a cross; if a dot is assumed, then in column 13, 33 would be a dot, whereas it has been accepted as a cross in column 1. Similarly, column 17 must be a repeat of column 16, because 9 is a cross, column 18 a repeat of 17 because 1 is a dot and position 18 of ⊥61 must be a cross, otherwise 1 has to be a cross.

Arguing along these lines, ⊥37 takes shape fairly quickly and in turn enables ⊥61 to be completed.

The expected ⊥37 dottage is given beforehand by the number of groups of crosses in the Ψ wheels. Where the information given by the BM is scanty, the exact location of a dot or cross in ⊥61 may be uncertain. This "ambiguity" can usually be resolved when the message is being decoded, by simple trial and error methods. The process of setting a message on the motor can also result in an ambiguity being resolved.

An elaboration of the "drag-slip" method of identifying the repeated columns is the use of a squared-celluloid sheet which can be laid over the basic motor; the columns under a chosen block of crosses in ⊥61 are copied on to the celluloid with a "chinagraph" pencil. What amounts to a simultaneous comparison of several columns can then be carried out by sliding the marked celluloid over the BM at various points until the repeating columns are found.

As an assumption regarding a dot or cross in the ⊥61 is made, so can extra columns be copied on to the celluloid, thus playing the repeat against the original and vice-versa, until the columns link up.

When the ⊥61 and ⊥37 patterns have been obtained, the ⊥61 setting is given as 1 and the ⊥37 setting is the ⊥37 character which appears or would appear, under 1 in the ⊥61, in the first line of the BM. The χ and Ψ settings ar then the settings for the first χ and ψ characters used to anagram line 1 of the BM.

(c) Motor Setting

When a de-χ or depth has been broken on a day for which the motor patterns have already been broken, the setter is given the depth or de-χ with the Ψ settings at the break. Usually the break is not at the start, so the Ψ settings for the first letter must be found. This is done by calculating approximately the Ψ settings for the start, typing a Ψ stream from these settings, and attempting to fit the Ψ ' on the de-χ near the start, either by 'snaking' or by obtaining breaks in the same way as the breaker does and finding the Ψ' given by the breaks in the typed Ψ strea

To calculate the approximate Ψ settings for the start we multiply the distance from the start to the break by α , and add a small excess for safety. This gives the approximate number of places moved by the Ψ's over that distance. It remains t subtract the number thus obtained from the Ψ settings at the break.

For this purpose a book of subtractors is used, wherein the remainders after dividing this number by the wheel lengths, are listed; e.g. if the Ψ_1 has moved about 2000 places to reach the break the number of revolutions of Ψ_1 in 2000 is 46 with a remainder of 22. The position of Ψ_1 at start is therefore 40 - 22 = 18

When the Ψ's giving clear at the start have been found, anagramming can be carried out, in lengths of 61. When a length of 150 letters has been anagrammed (or less, if the motor wheels are distinctive) the BM is written out as for motor breaking and the compulsory crosses on μ61 written in.

μ37 is next examined for any distinctive feature such as a solitary .x. or x.x or any other characteristic which would enable a deduction to be made regarding μ61. For example, if μ37 has no .xx. every xx in the BM will mean a dot in the 61, or if the largest μ37 group is .xxx. and .xxxx occurs in the BM this will also mean a μ61 dot. When all possible use has been made of the μ37 characteristics the fragmentary μ61 is slid along the actual μ61 until a non-contradictory position is found. The BM is then numbered accordingly, enabling a fragmentary μ37 wheel to be written out. The actual μ37 should fit uniquely on this. The positions on the actual wheels of the first terms of the fragmentary μ61 and μ37 are then the motor settings.

28E DECODING

(a) Organisation

This has been described in the Testery report XII 9.

(b) Operation

The operator plugs the twelve wheel patterns and settings into the Tunny decoding machine and sees that the limitation switches are correctly thro The settings are found written on the red form at the start (FIG. VI). She then types the Z which is printed as P by the machine. If the message has been correctly set and does not have an autoclave limitation, it will decode without difficulty. The operator may find trouble if the cipher text is corrupt owing to poor intercept conditions, bad emendation by the intercept department, or mistakes by the perforating department. Incorrect continuity of the text means that the operator must stop and find the error by means of "sliding" (FIG.VII). The correction is written on the red form (FIG VI). New motor keys which have 'ambiguities' (short stretches of μ_{61} where the number of dots is known, but not their exact position) are sometimes troublesome, but if the ambiguities are correctly marked the operator can solve them by trial and error methods without difficulty.

Messages with an autoclave limitation are much more difficult to decode. In the case of incorrect continuity key cannot be generated and the cipher has to be corrected by means of a 'snake' (FIG VIII). If the cipher is corrupt on the 5th impulse the operator must decide the exact letter which is corrupt, and type through again correcting it. She can easily determine this letter because there will be two clear letters after the corrupt one before the clear breaks down completely.

The finished decode (FIG.IX) has 12 lines of 60 letters to each page with a machine reading of the 12 settings taken at the end of the 12th line and written at the corresponding place of the red form. The first page is headed with message date, the time transmission started and ended, the motor key date, the frequency, the exact amount of the message decoded, the amount (if any) to be decoded, and the serial number. Each subsequent page is headed with the serial number, and all the pages are numbered consecutively. Any clear which has been lost through incorrect continuity or corrupt letters will have been re-constructed by 'slides' and'snakes'(FIG VII and VIII) and is written on the decode. Every letter lost in interception is crossed out on the decode.

This covers normal procedure. There remain messages that are not set at the beginning and those set on the Ψ's and motors by machine. Messages with any limitation except pure $\bar{\chi}_2$ which had to be taken back to the start were passed back to the setters. Those with $\bar{\chi}_2$ limitation were taken back on the machines. The procedure was as follows:-

(i) Subtract the χ_1, χ_3, χ_4, χ_5, ψ_1, ψ_2, ψ_3, ψ_4, ψ_5, break-in settings from the lengths of the wheels + 1.

Subtract the χ_2 setting from the length of the wheel + 4
" " μ_{61} " " " " " " " + 3
" " μ_{37} " " " " " " " + 1 if the μ
setting - 1 = do
+ 2 if the μ
setting - 1 a cr

(ii) Turn the χ_2, μ_{61} and μ_{37} wheel patterns backwards and plug in the transformed settings.

(iii) Tap the number of letters from the break back to the 1st letter and take a reading.

(iv) Repeat (i) with the reading now obtained.

(v) This should give the settings for the first letter.

If however the continuity of the text is incorrect, key must be taken and the cipher slid against it until it 'clicks' into the right place.

28E Page 269

Fig. VI Pages of Red Form, showing settings at start, readings taken every 12th line, cipher corrected by 'slide'.

S.1319. Est. May, 1925 Revd Nov., 1931

W/T RED FORM.

Ref. No. .....
Page K5.5

Ship or Station	Set	Date 7-3-43	Operator's Remarks.*
KNOCKHOLT W/T STATION G.C.N.S.	Opr.	Time Ended G.M.T. 0207/16	Q. S. A. ..... Teleprinter TONE
	To†	Frequency & System.	
	From*	4270 KC/S	

All before the Text

PAGE 1

QSN 1209 CORROTE 2352

Un Un

Text, Time of Origin, Signature, etc. Write ACROSS the page, code and cypher on every third line

Auto =

YGBUV	YGKOX	UM/X94	S3BSZ
YMIRF	UIWQK	4GRVA	MSL8K
BLOVC	/BH/9	3HYA3	/+VSS]
FBQRQ	J/3Z1	L3PUP	JBRXD
AWM3N	KRSND	/KT8M	IL+KC
8APZM	M3CKS	ZNEVH	QHLQU]
QUXX3	9FHKV	AIVBV	ZMV+M
KW+EC	MJRZG	ZJTMA	EH/3J
/HKH+	JH+HL	9VI/H	MHWVB
4UEMV]	DMYQB	/ISJX	QQURL
QWLHO	RKQS9	9BQX8	NUXVX
+KTWL	MGNNQ	QRB8G	PRYWU
TQUI/	/UDZH]	IGKTE	9PZNK
N+OVL	34BPD	/4OVW	R+T/L
H6RHL	Z/HSR	9NM/OU	JNYGB

Do not use Left Margin.

G.03656/25. *Constancy and reliability of signals, quality of operating, interference, atmospherics, etc. †Name of Station; if not known leave blank.
Sta. 1/30.
Sta. 103/31.

S.1311

(5 46) Wt. 3333. D8645. 11/41. 75,000 pads. E. & S. Ltd. 41/1707

286 Page 270

Fig VI (con).

S.1819.
Rev. May, 1926. Revd. Nov., 1931.

W/T RED FORM.

Ref. No.
Page. KS.5

Ship or Station	Set	Date.	Operator's Remarks.*
	Opr.	Time Ended G.M.T.	Q. S. A.
	To*	Frequency & System.	
	From*		

*All before the Text.

Page 6

(12) 19.21.12.22.9.
60.28.
6.38.~~44~~.18.23

Text, Time of Origin, Signature, etc. Write ACROSS the page, code and cypher on every third l

Hand-	LBT8T	A99V8	GIVJ8	XAJKQ
	PPJ8S 9/11 1-SIDE	· IXHF	Y30S+/	V+P Panel
Hand-	EGGVX	PN8LC	WK68P	+UX6B
	X4RQB	TONM+	9YDVU] B	EB6MJ
	UDVO4	MQF/O	3NBJS	VIQPQ
	KKCL/	94JRX	T8UJV	YVQ14
	B8GTB	99HQM	DXSQ/	9HWVL]
	RRBLB	TOBXW	X	Panel
Hand-	MUTTA	DDOHR	/KGDQ	MHORN
	DDUQC	BMLBI	8D/QM	NETTH
	V/LPR	OMLSA	QH/K4W]	RY6IV
	ZZQRON	N14IE	13WPF	MIRNO
	PLOCV	GB2HV	TPJ9Z	QWUHM

Do not use Left Margin.

*Constancy and reliability of signals quality of operating, interference, atmospherics, etc †Name of Station; if not known le

blank.

S.1

Figs VII and VIII

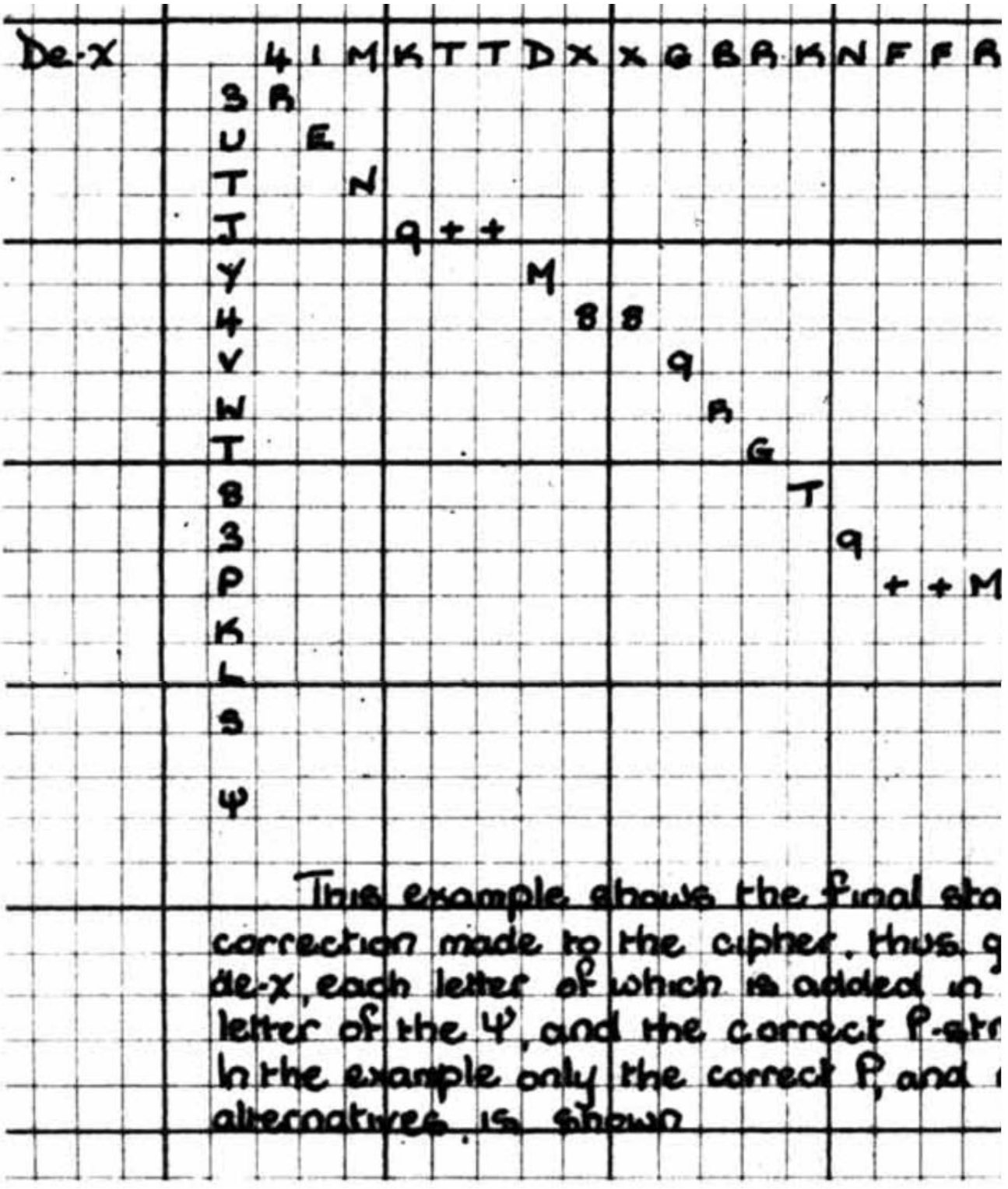
A 'SLIDE'

'Phoney Clear'	W	S	G	O	+	X	M	M	P	Z	X	A	E	D	S	H	D
Cipher	8	3	-	I	X	H	F	Y	3	O	S	M	V	+	P	E	G
Key	N	F	G	V	I	D	Z	D	V	D	O	8	8	L	W	Y	W
Clear	9	-	M	A	L	9	9	E	I	N	9	E	9	9	L	K	L

By omitting 1 letter from t
key we can reconstruct the lost

By omitting 1 letter from t
key we can reconstruct the lost

A 'SNAKE'



This example shows the final sta
correction made to the cipher. thus. q
de-X, each letter of which is added in
letter of the Ψ, and the correct P-str
In the example only the correct P, and
alternatives is shown

Fig. IX

25L Page 272

MACHINE 1

(1)

DATE	TS 0204	FREQ.	MM	DECODED:- 1ST LTR. PAGE 1	TO DECODE	SERIAL NO:-
7-3-43	TR 0216	4270	6-3-43	TOT. END	NIL	K46 590

HRZCHORNSTEINFEGER..ANNA+X-FF.NR+M.YYQ.UMEMRE.VV.KK-.ANN+X-FF

.NR+M.YYQ.UMEMRE.VVLL-.HAVD.NN.HAVXD.++.QIWYR.TMEM.QREP.VV.K

K-.HAVXD.+UQI.WYR.TMEM.QREP.VVLL-..WN.ART+M-.KDR+M-.+.F.-.BEIM

.PZ+M-.AOK.+.ONK.H+M-.GR+M-.SUED.+VV.KK-.AN.ART.+-.KDR+M-.++.

F.-.FEIM.PZ+M-.AOK.+.QN-..H+M-.GR+M-.SUED.+VVLL-..++.W-.SHNEN

N.++.W.-.SCHW+M-.ART+.-.ABT+M.++.UFT.KK-.++.W.-.SCHW+M-.ART+M-

.ABT+M-.++.UFT.LL-.MUSZTE.DREI.ZWOELFTONNER.ZUGMASCHINEN.MIT

.GENEHMIGUNG.HOFH+M-.ART+.-.KDR+M.FPI.KK-.HOEH+M-.AE.NN.ARTM-

.KDR+M-..+EPI.+LL.-.ZUR..++.RM-.PZ+M-.DIV+.M-.+KK+.RM-.PZ+M-

.DIV+MLL-.ASSTEKLEN+M-.ALLE.BEME.NN.BEMUEHUNGEN.DES.BATTR+M-

.CHEFS.+KK-.BATTR+M-.CHEFS+LL-..ZUGMW.NN.ZUGASHCINEN.ZURUECKZU

BEKOMMEN+N-.SIND.A.NN.SIND.GESCHEITERT+M-.BATTR+M-..+KK-.BATT

R1.

38E Page 372 Kb. 590

Fig IX (con).

R+MLL-.BITTET.UEBER.DIE.M+M-.GR+M$_3$..+KK-.M+M-.GR+MLL-.DIE.+.R

M-.PZ+M-.DIV+M-.+KK-.++.RM-.PZ+M-.DIV+MLL--.ZUR.HER.USGABE.Z

U.VERANLASSEN+M-.DA.VERLADUNG.IN.ETWA.+.Y.+KK.YLL-.TAGEN.ERF

OLGEN.SOLL+M-.ERBITTET.BATTR+M.+KK-.BATTR+MLL-..MITTEILUNG+M

-.OB.SIE.DIE.RUECKGABE.DER.ZUGMASCHINEN.SO.RECHTZEITIG.EWWARTE

N.KANN+M-.DASZ.SIE..MIT.TRSP+M-..DER.BATTR+M.KK-.TRSP+M-.DER

.BATTR+MLL-..ABROLLEN.KOENNEN+M-.BATTR+M.KK-.BATTR+MLL-.ISTHZ

U.ERREICHEN.UEBER.AOK.+.W..KK-.AOK.+.WLL-.AUFFAGSTAB..+.YQI.M-

.ROMNY.+PV.KB[illegible]+QFFANGSTAG[illegible]+.YQIN.-.ROM.Y.+MVVLL-..DIENSTSTELL

E.FPN.FM.+[illegible].MPQ.-MRB-HGFZ+M.-IUSCHR+MZZ-.KK-.DIANSTSTELLE.FPN

R+M.EW.WYQ.-.C..GFZ+M-.RSCHR+MZZ.LL-..-.BERICHTIGUNG.+C-.ZUGN

ASCHINEN..VGL+M-.ZUGMASCHINEN.-.QXA.+.+QPPVV--.QXA.+QPPPVVZZ

-KAFFEH Hand

[Slide Out 1]

.....NUN...WIEDER...AWSQ+JUMPSKAPS MAL..EIN.E.. Hand

LKLAEINE. PAUSE..VE
SHBM4QVTBRV+M+PB4

.+B.-..... R2.

31 - MR. NEWMAN'S SECTION

31A GROWTH

In December, 1942 Mr.M.H.A.Newman was given the job of developing machine methods of setting Tunny. In April, 1943 the first machines arrived, a Robinson and a Tunny, pilot models of somewhat uncertain behaviour. Mr. Newman formed his section with one cryptographer, two engineers and 16 Wrens. The section was founded and lived (for the most part) in a single room. After three months two or three messages were set each week.

By May, 1945 there were 26 Cryptographers, 28 Engineers, and 273 Wrens with 10 Colossi, 3 Robinsons, 3 Tunnies and 20 smaller electrical machines. The section moved into Block F in November, 1943, and expanded into a new and additional Block (H) in September, 1944, in which all chi-breaking was done. In the week ending March 31st, 358 messages were set on Chis, 151 on Motors and Psis and 23 sets of new wheels were broken.

The total number of log books used in 2 years was about 500.

31B STAFF REQUIREMENTS

The allocation of staff at 6 monthly intervals is shown in the following table.

		Apr.43	Sep.43	Apr.44	Sep.44	Apr.
	Administration	-	-	1	2	2
	Cryptographers	2	5	6	20	22
Engineers	Maintenance	-	3	9	12	15
	Construction	-	4	9	11	13
	Wrens	16	16	68	180	273
	TOTAL	18	28	93	225	325

Finally the staff per shift was as follows:

7 Cryptographers :
- DO in charge of setting
- 1 Wheel-man in charge of wheel-breaki
- 1 in charge of Cribs and Robinson Wor
- 2 to supervise Colossus setting
- 2 to supervise Colossus wheel-breakin

67 Wrens :
- 7 Registrars
- 17 Tunny Operators
- 2 Robinson Operators
- 20 Colossus Operators

15 Computers
1 "Cribs" assistant
5 "Room 11" maintaining contac
with Knockholt.

5 Engineers and a daily requirement of

2 Research Cryptographers
2 Research Wrens
13 Construction Engineers
6 Administrative Staff.

31C ADMINISTRATION

As the section expanded, administrative problems became considerable. Co-ordinated policy was established through a "Fish Committee" under Mr. Welchman's chairmanship during the period of fastest development (May 1944 - January 1945) to determine the policy of machines to be ordered and staff to be recruited. A good deal of attention was given by this committee to the slip-reading and perforation of tape at Knockholt and every effort was made to encourage the production of material at Knockholt on a scale commensurate with the rapidly expanding capacity at this end.

The administration had to keep in touch with operational results. It did this by collecting and analysing facts about success achieved in each part of the section and issuing suitable reports. The log books kept by all operators provided the required information in addition to making operators conscious of their own efficiency.

31D. CRYPTOGRAPHIC STAFF

The first thirteen men to join the Section as cryptographers were drawn from other sections of GC & CS. In experience and infectious enthusiasm they preserved their lead to the end, and there were few in the section not affected by their keenness. After July, 1944 they were joined by men from other war jobs and men straight from the universities. The qualifications of men chosen are given in the following table:-

Date of Arrival		June 43- July 44.	Aug. 44- May 45.
Professional Mathematicians etc / Research Students		8	4
Other University Mathematicians		3	11
Others		2	1
Previous cryptographic experience		12	3
Enigma		8	2
Fish		3	1
Age on joining	over 30	5	2
	25 - 30	3	3
	20 - 25	3	5
	under 20	1	6
British		11	13
American		2	3
TOTAL		13	16

Cryptographers were not organised into fixed shifts, but worked with different people each week and took it in turn to do research work and the various operational jobs. This system kept everybody in touch with up to date technique and alive to possibl improvements. A weekly change of job led at times to minor administrative inefficiency and the normal term of offices for Duty Officers and wheel-men was eventually extended to three weeks, these two jobs were normally filled by more experienced me

After the Section was fully staffed there were often two research men each week. Most of the important ideas were developed by men as a result of practical routine work and writte up in the Research Logs. In a subsquent research period of a week or more they were at leisure to elaborate their ideas and to tackle any other problems of a pressing operational nature.

Ideas for new methods, and routines for immediate instructio were discussed at the weekly "Tea Party" - a democratic assembly of cryptographic staff.

31E. W.R.N.S.

Wrens were chosen by interview from those in H.M.S.Pembroke (Category - Special Duties X). No fixed qualifications were required, though a pass in mathematics in School Certificate or(a "good social recommendations" was normally considered essential. Though a few of the earlier Wrens were rather older and more experienced, 96 per cent of those who came were between the ages of 17½ and 20. 21 per cent had Higher Certificate, 9 per cent had been to a University, 22 per cent had some other training after school training and 28 per cent had previous paid employmen None had studied mathematics at the university.

On arrival, all Wrens were given up to a fortnight's training in the teleprinter alphabet, the workings of the Tunny machine and (in some cases) in computing. This was followed by a conduct tour of the section and a written test. Wrens (unlike men) were organised in fixed watches and given fixed jobs in which they could become technically proficient. While the section remained small it was possible to try new Wrens at various jobs soon after arrival, but later, allocation was made on the basis of the test held at the end of their initial training period, and on the basi of the jobs available. The cheerful common sense of the Wrens was a great asset. Several of them showed ability in cryptograp work and several others were trained by the engineers to undertak routine testing of machines.

It was decided at the beginning of the association of the P.O. Research Branch with GC and CS that maintenance of equipment would be an increasingly important part of the undertaking. It was agreed to recruit the best available men from the automatic telephone construction and maintenance staff throughout the country, to employ them at Dollis Hill and the P.O.Factory at Birmingham to build the equipment so that they should be thoroughly familiar with it, and to give them, before taking up their maintenance duties, any supplementary instruction that was necessary. As the work developed, the complexity and novelty of the equipment increased and further maintenance training was needed, but the technical staff were often hard pressed to produc the equipment and instruction was neglected. A number of maintenance men made up for this deficiency by their own initiative and exertions, and passed their knowledge on to others Full maintenance efficiency can be achieved only after some month

of experience, and by May, 1945 equipment and maintenance had reached a very high level of performance.

Telephone maintenance work is mainly done by unestablished skilled workmen and skilled workmen Class II. Recruitment for the maintenance force at Station X was made almost entirely from men in these grades aged 20 - 22 years. The first eight men came to Dollis Hill in April, 1942 a number of Chief Regional Engineers having been asked to recommend good men. A selection was made on the basis of paper qualifications, mostly City and Guilds certificates. The selection of the men after the first eight was based solely on their technical qualifications, the type of work on which they had been engaged and (where possible) their performance at the Post Office Training Centre, where men are trained for normal Post Office work. The total number of men engaged in maintenance on "Fish" traffic eventually reached 45.

The allocation of duties to the maintenance men was based on their previous Post Office experience and the aptitude which they had shown for various kinds of work during the time they spent at Dollis Hill. For a long time a rather critical balance of manpower had to be held between maintenance and further construction. The total manpower available at the beginning of 1944 had been so depleted by the demands of the Armed Forces on the Post Office Staff that no further suitable men were available, and the men already engaged - including all the manufacturing force at Dollis Hill and the P.O.Factory worked over 70 hours a week for many months.

31G. EDUCATION

It was the policy of the section that all its members should be encouraged to interest themselves in all its activities and to improve their theoretical knowledge. In practice it became increasingly hard for Wrens to get a complete picture of an organisation in which they might have only done one job. Moreover the mathematical style of the Research Logs made them unreadable for Wrens, and before they (or new men) undertook chi-breaking and Colossus-setting on their own, some other introduction to the theoretical side was needed.

Screeds and lectures on aspects of the work were issued or given from time to time in 1944, but nothing was done systematicall till the Education Committee was founded in January, 1945. This committee of four men and 14 Wrens chosen democratically arranged general lectures and "Seminars" for small parties of Colossus operators or other specialised groups. All lectures and Seminars were given outside working hours and were voluntary. The Seminars for Colossus operators were a complete success. The less mathemati general lectures were also appreciated.

The Education Committee co-ordinated the production of screeds and started a General Fish Series of papers which were duplicated and available in every room.

31H STATISTICS BUREAU

In August, 1944 a permanent Statistics Section was set up employing one or two Wrens. The Statistics Bureau

(i) Collected routine statistics, in particular 32 letter-counts of various types, significant rectangles and numbers of messages a

(ii)Helped the administration to prepare statistical reports.

(iii) Looked after the library and the publication of screeds.

(iv) Helped the research man to complete any statistics that he required.

32 - ORGANISATION OF THE TESTERY

The organisation of Major Tester's Section has been described briefly in 14B (c), and more fully in "Report on Tunny (Major Tester's Section)" and also in the separate report entitled "History of the Fish Sub-Section of the German Military Section". We do not go into further details here as they are of no great cryptographic interest and are not necessary for the understanding of the present report.

33 KNOCKHOLT

33A ORDERING TAPES

The work of Knockholt was the preparation of tapes and Red Forms for Station X and consisted of (i) Interception (ii) Slip Reading (iii) Reperforation. A tape with a single letter inserted or omitted in the middle would almost certainly fail to set, hence the need for accuracy at Knockholt. Approxima 600 people were employed there. Nevertheless there were times when the traffic ordered by us was more than they could handle. Once (Aug.1944) an abortive attempt was made to perforate tapes in Block F.

The priorities of ordering were decided by a morning meeting of various interested parties in Station X. This meeting also decided priorities for machine setting and wheel-breaking. All ordering was done through the 'Control Officer' at Station X by the following procedures:

A procedure Long tapes on unbroken days (according to a link priority list).
B procedure Other tapes for wheel-breaking ordered individually.
C procedure Tapes for setting on broken days.
D procedure Messages required for Crib purposes.
Depths The Control Officer was responsible for ensuring that these were teleprinted at once.

33B TREATMENT OF TAPES

There were 30 receiving sets (in the Set Room). 26 covered priority links and the rest were on directed and general search. Intercepted impulses were automatically recorded on undulator tape and usually on printed and perforated tape. The undulator tape was the most reliable and was used by the "slip-readers" for improving the RF and perforated tape. In March 1945 effots were made to save time by using the automatic perforation (RAW TAPE) when interception conditions were good. Blurred patches were marked by the operator. Sometimes dubious portions were also slip-read. The method of raw tapes is a good one provided that full slip-reading is continued until and if positive cryptographic results are obtained with the raw tape.

Completely slip-read messages were passed to the reperforating room. The final tape was checked against the RF with the use of a 'hand counter', though it was not until Autumn, 1944 that a hand counter was issued to Knockholt. Increased accuracy was immediately noticeable.

There were 10 transmission lines to our section. At its best the reperforation room achieved an average daily output of 400,000 letters.

For further details, including auxiliary interception stations, the report by Sixta should be consulted.

34 - REGISTRATION AND CIRCULATION

(a) Foundation of the Joint Registry

Registration methods were, of course, developed early and in January, 1944 a joint registry was founded for Major Tester's and Mr. Newman's sections. This registry kept track of all material entering or circulating in either section, and itself kept all tapes, or documents for tapes, not being worked on. This avoided congestion and delays in the Newmanry. Few messag strayed and those that did were quickly recovered.

(b) Division of work

Work was divided between Room 12 and Block H. Room 12 dealt with tapes required for setting and the T registry in Room A, Block H, with tapes required for wheel-breaking or Cribs As soon as a days' wheels were broken all tapes and documents for the wheel-day were sent over from Block H to Block F.

(c) Cards and Circulation

The basic system for all procedures was the same: two copies of each tape perforated were teleprinted from Knockholt. Later on the RF and Master Tape were sent by DR. A procedure card was started for each message and a pigeon hole allotted for the tapes and RF (See Fig 34 (I)).

In addition to the procedure card, a card was made out for each message, which accompanied the tapes on their journeys. These were used in Ops or Block H for the registration of various setting and rectangling processes. The "Ops Card" for instance was used for setting messages and it was returned to Room 12 when the message was abandoned or set.

When a set of wheels was broken the relevant material was transferred from the T-Registry to Room 12 and from the H-Registry to Ops. On the other hand if the wheels for a day were not broken within a month the pigeon holes in Block H were emptied, the RF was filed and the master and another tape were stored. The pigeon holes in Block F were not cleared until a setting message was abandoned or completely decoded. In the latter case one copy of the decode was sent to the appropriate intelligence section and one copy was filed in Room 41.

(d) Other Records

Other records kept include registers of:

All tapes intercepted.
'A' tapes and their history.
Tapes for setting on broken days.
Tapes transmitted from Knockholt.
Depths.
Settings of decoded messages.

34 PAGE 283

W.S. 31a.

M K

P.H. No. Decode No. Serial No.

Q.E.P. Date T.S. T.E. Freq. Pages

Trans Date 1st 5 Letters	Time Start	Pages Quality	Length	Copies

Sent to 'H' Registrar

Sent to Ops.

Set on Chis.

Set on Psis.

Decoded

Abandoned

Red Form received from KN

Red Form to Ops.

Red Form Returned

Extra Routine Movements

A.

Fig 34 (I)
Procedure Card

35 TAPEMAKING AND CHECKING

35A INTRODUCTION

The successful working of all parts of Mr.Newman's section depended on the accuracy and efficiency of the Tunny rooms which were responsible for looking after all copying, reading and tape-making machinery.

An elaborate system of checks for all tapes made was found to be essential to prevent the early introduction of mistakes which might be reproduced unnoticed. The importance of checks was not realised at first and it is generally believed that the comparative lack of success in the earliest days was largely due to the use of incorrect tapes.

35B GENERAL RULES

All tapes were made twice independently and compared to ensure that no letters had been inserted or omitted. Before newly-made tapes were returned to the appropriate registrar their text length was measured on a Hand Counter and marked on the tape. All jobs involving the making of tapes (or prints) other than exact copies were sent to Tunny with a Hand Check for the beginning which had been worked out by the Registrar. For every tape made two copies (at least) were ordered to save time in case of damage to one of them. All work was very fully labelled.

35C CHECKING AND ALTERATION OF TAPES

(a) Checking tapes against Red Forms

This was not strictly a Tunny Room job, but may logically be described here. For a long time every long rectangling tape and ever setting tape which failed to set was checked against the appropriate Red Form.

First Method The number of letters on each page of the RF was calculated and the first few letters at the top of each page recorded, The tape was wound throught the hand counter and stopped at the calculated position corresponding to the end of each page. The position of theentries corresponding to the top of the next page were checked on the tape.

Second Method The tape was measured out on a hand counter, marked at every multiple of 1271, and 10 letters after each mark recorded. When the RF arrived, the letters at similar positions on it, were independently noted, and the results compared.This method was suitable for rectangling tapes as it enabled a hand check for the rectangle to be made at once from the tape check.

(b) Comparing two versions of the same tape

It was sometimes necessary to compare two versions of the same tape, (say an original version with its rewrite). The tapes were added together on Miles until the output tape showed that there was a slide. The place at which this occurred was marked on both tapes and the tapes were reset (to account for the slide) and the operation continued. A print-out of both versions was made on Garbo wherever discrepancies had been noted so that Knockholt could be asked to reread the undulator tape at these places and decide which version was the most likely. A composite tape could then be made embodying the best of both tapes.

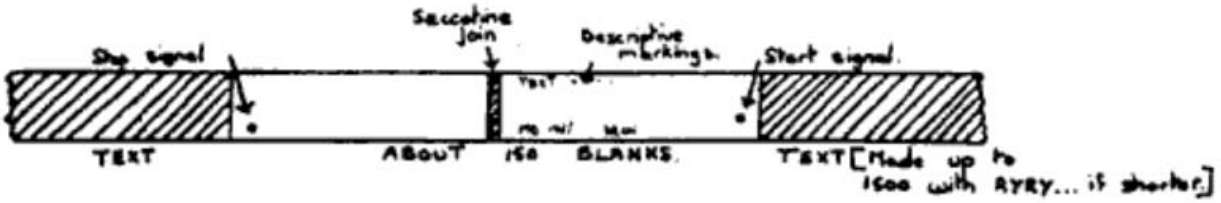
(c) Correction and Doctoring of tapes.

This was normally done on an IBM (preferably) or Angel. The tape to be corrected was marked (with the help of a hand counter) at the places at which a letter was to be inserted or omitted. The IBM or Angel was stopped when the marks were reached and the correction made.

The corrected or doctored tape was compared with the first version by hand and the corrected length verified on a hand counter. It was marked CORRECTED TAPE or DOCTORED TAPE in block capitals.

35D PREPARATION OF MESSAGE TAPES

(a) For Colossus



Tapes were copied (on Angel) if sufficient copies were not available, or if available copies had not sufficient blanks at either end. Tapes issued were stuck into closed circuits as shown, and stop and start signs punched with a special metal gadget. An overlap of two sprocket holes was allowed at the join; the join had to be made with smooth edges and the end (as opposed to the beginning) of the tape on the outside of the circuit.

The text length was measured before the tapes were returned to the Registrar and if it failed to agree with the Knockholt estimate, Knockholt were informed.

If the text length was below 1500, copied tapes were made on which the text was followed by RYRY... till the total length of text exceeded 1500. This was done by feeding a tape reading RYRY.. into the Angel input as soon as the real text had been copied.

For issue to Colossi with short bedsteads very long tapes were stuck in parts of text length 10172 with an overlap of 4 between each part (1-10172, 10169 - 20340, 20337 - end) [See §36(b)]

(b) For Robinson

Message tapes were prepared for Robinson as for Colossus except that a mixture of Bostick and benzene was used for sticking. The tape to be stuck was inserted between two electrically heated plates (a 'hot sticker') and the benzene was evaporated.

35E MAKING OF DE-CHIS

(a) Without Colossus check

The settings and wheels for the de-chi were written on the chit by the Tapes Registrar with a hand check of the first 41 letters of the de-chi. The dechi was made on a Tunny machine twice, and if both makes agreed one was stuck for Colossus or Robinson and returned to the Registrar. The Tunny was not stopped during either make.

If the ΔD count on the de-chi tape checked with that on the Z tape, the dechi tape was returned to the Tunny Room for printing (on Garbo) in rows of 31 with double spacing. To check the print the de-chi tape was marked at positions 1, 621, 1241 etc.

and the start of every 2[illegible]th line on the print verified.

Lines of the de-chi were numbered and the print marked with the 1st 10 letters of Z.

If the $\Delta\Sigma$ count on the de-chi tape did not check the wheels set up on the Tunny machine were checked and if no mistake was discovered the Σ tape was recounted on a different Colossus.

(b) With Colossus check

The Tunny room was supplied with a chit giving setting and wheels and a Colossus check giving the following letters of de-chi :- 2-9, 621-624, 1241-1244, 1861-1864, 2481-2484, 3101-3104 and the last 5 letters. To this the Tapes Registrar had added the settings for letters 621, 1241 etc.

The de-chi was made on Tunny twice. The first make was stopped automatically every 620 letters and the settings checked. This make was printed while the second make was being made. If the two makes were identical, and the print checked with the Colossus check the de-chi was assumed correct and marked and sent over as before.

When the two makes agreed, but the print did not agree with the Colossus check, the Tunny wheels were checked and if correct, the Colossus check was assumed invalid, a hand check made, and the de-chi tape stuck and counted on Colossus.

(c) Contraction of de-chis

In days when psis were set on Robinson (on messages with $\bar{\chi}_2$ lim) the psis were run against a de-chi tape from which all letters occuring against Total Motor dots were omitted. The contracted de-chi was made on a Tunny on which motors and χ_2 were set up. A special switch was used and a hand check supplied.

35F WHEEL TAPES AND TEST TAPES

(a) Chi test tapes

These were made on Tunny. The appropriate wheels were set up at 01 01 01 01 01 and 2002 letters of chi-stream perforated. Before sticking for Colossus every impulse was checked by sliding the tape against itself at a multiple of each wheel in turn.

(b) Psi test tapes

These were made on Tunny with setting 01 01 01 01 01 for Psis and 01 01 for Motors. The limitation appropriate to the wheel-day concerned was used and a hand check of 61 letters supplied by the registrar. Final copies were stuck for Colossus.

(c) Motor tapes

Tunny can be made to perforate Basic Motor tapes from the plugged patterns of μ_{37} and μ_{61} and Total Motor tapes (for $\overline{\chi}_2$ lim) if χ_2 is also set up. Motor tapes were sometimes required for printing the motor over a dechi or for doing motor runs on Robinsons. A hand check of 15 letters was supplied.

35G RECTANGLES

(a) Garbo Rectangles.

The method of making 1+2/ Rectangles on Garbo is described in 24B(c). The following practical steps were taken to ensure accuracy. The tape was measured on a hand counter and positions of the form (1271∞+2) were marked. The second letter of the tape was put in the Garbo (which deltas backwards) and the print-out was started and compared with a hand check prepared for the first few characters. Whenever 1271 characters had been printed and the paper was reset, the tape should have been on the appropriate mark and this was checked. A hand check for the last few characters was prepared, and the position of the last character printed was verified by calculation. Garbo rectangles were only made once.

Different markings of the tape would have been required for a 3+4x/ or 4+5/ Rectangle. These were not made on a routine basis.

A further hand check was applied to rectangles when they were returned to the H Registrar. From the check sheet prepared by her from the Z tape [see 35C(b)] a hand check for the first entries of each cycle of 1271 was made.

(b) Miles and Garbo (Thurlow) Rectangles.

This method of rectangling is described in 24B(d). The tape was measured and marked at positions of the form (1271∞+1). Hand checks for letters 1-10, 1271-1281 etc. of the Thurlow tape were prepared. Marks 1-5 on the Z tape were put in the 5 heads of Miles and the resulting Thurlow tape compared with the hand check. After it had moved 1271 times the Miles was stopped and it was verified that the second mark was in the first head, the third in the second etc. The tape was removed and marks 6-10 put in the 5 heads and so on. The start of each new stretch of 1271 was compared with the hand check.

Thurlow tapes were made twice and measured to ensure that their length was a multiple of 1271 before printing. The positions 2,1273 etc. were marked and the Thurlow tape printed like a Garbo rectangle. The position of the change of depth was calculated from the Z tape, checked on the Thurlow tape and marked on the print out.

A further hand check, similar to that for Garbo Rectangles, was done by the H Reegistrar when a Thurlow Rectangle was returned.

35H OTHER TUNNY JOBS

(a) Hand Perforation.

Hand perforations were most easily checked by printing out the perforated text and checking the print-out against the original.

(b) Cribs.

The various tapes required for Crib work are described in detail in Ch 27.

(c) Other jobs.

Tunny Room machinery was very adaptable and numerous non-routine jobs were undertaken. In certain cases it was necessary for hand checks to be prepared by a cryptographer who (at most) supervised the job in person or (at least) provided a sheet of careful instructions.

36 CHI-BREAKING FROM CIPHER

36A HISTORY AND RESOURCES

(a) Early wheel-breaking.

Mr. Newman's section began as a section for setting messages on wheels broken from depths in Room 41. Wheel-breaking activities came later.

Bream started to use P_5 limitation regularly in the middle of December, 1943, and as there seemed every chance that the use of this gadget would be extended, research activities were devoted to the statistical solution of chis from Z. Tutte's method of rectangles (see Ch.44) was elaborated and from January 1944 monthly keys were tackled operationally.

Significance tests were gradually instituted and methods improved. Soon after Colossus 1 arrived in February 1944 it was discovered that it could be used for chi-breaking. It was this discovery that made large scale wheel-breaking possible even after the introduction of the daily wheel change in July 1944.

(b) The period of expansion.

Between July and November 1944 the number of computers increased from 4 to about 16 a watch, and the number of Colossi from three to six, of which three were fitted with a rectangling device. New Garbos, Miles and arrival terminals from Knockholt were installed in Block H which opened in September and housed all wheel-breaking operators from the middle of November onwards.

From August onwards extensive rectangling was rarely applied to any particular day's messages. A few long tapes on each day were rectangled and it was assumed that when the dottage was high and the interception good the rectangle would be significant. Colossus work on significant rectangles largely replaced the more laborious method of the conditional rectangle, and from the end of August a machine and a man to supervise operation could be spared most of the time.

From the middle of November 1944 to May 1945 the number of machines and trained staff continued to increase, and about 15 sets of wheels broken on rectangles each week. In 1945 there were about 15 Computers per shift, whose main job was to converge rectangles on paper. The head of Computers was called the Rectangles Registrar. A man, called the Wheel Man (WM) was in charge of wheel-breaking operators and there were other men called wheel-breakers, each of whom took charge of one wheel-breaking job on a Colossus.

(c) Checking of tapes.

Needless to say the long tapes ordered on A (or B) procedure for rectangling needed to be particularly carefully checked. Therefore they were checked by us against the Red Form, as described in Ch. 35. However, after Knockholt had been supplied with a hand counter in Autumn 1944, there were so few mistakes that we stopped checking the tapes in Bletchley.

36B RECTANGLES AND CHI2 CAP RUNS

There were four methods of rectangling, described in ch. 24. Priorities were decided by intelligence value, length of tape, supporting tapes and many other considerations. Tapes were often rectangled in parts, in case of a slide in the tape. The $\Sigma \theta_{ij}^2$ test was done when the Colossus had the required meter.

In addition chi 2 cap runs were done on each third and the whole of each message rectangled.

If $x > 7\sqrt{r}$ the WM might start Colossus chi-breaking at once, before the rectangle was converged. If $5{\cdot}6\sqrt{r} < x < 7\sqrt{r}$ the rectangle was given priority. Very rarely the chi 2 cap run revealed a slide in the tape. (See R5 p.98.)

36C TIMES

Here are the average times in hours for various processes and over various periods. The unbracketed figures are for high priority and bracketed for low priority groups.

	1944 NOV-DEC	1945 JAN-FEB	1945 MAR-APR
Time of interception - Arrival in Block H	39(56)	29(41)	25(30)
Time of arrival - Issue of rectangle	5(6)	3(5)	3(4)
Issue - Abandoning	21(26)	11(12)	12(14)
Issue - Significance	11(13)	9(8)	7(12)
Completion of wheels on Colossus	31(27)	15(14)	13(11)

W.S. 33.

Serial No.	Date	TS.	TE.	Lgth.

R/F. Checked

Remake

Ops.

Rectangle

Converged

Significant

Returned to Ops.

Action

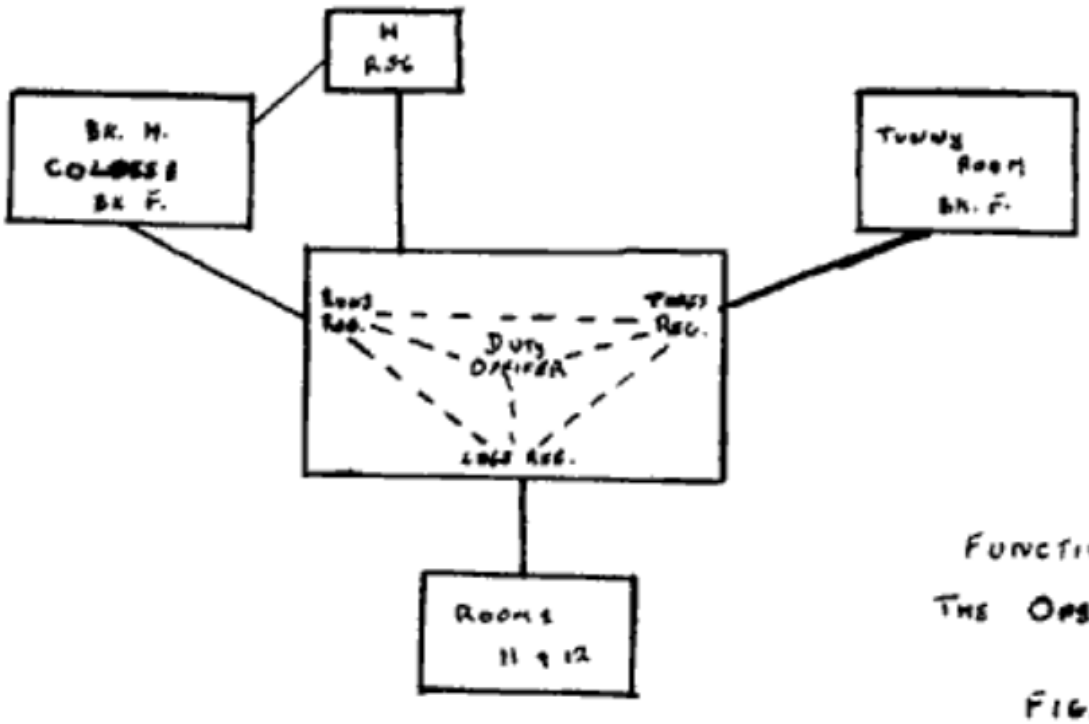
Rectangle card used by H Registry.

37 MACHINE SETTING ORGANISATION

(a) Ops

The following were housed with the Duty Officer (D.O.)

(i) The Runs Registry, which organised jobs for Robinson and Colossi.
(ii) The Tapes Registry, which organised jobs for the Tunny Rooms.
(iii) The Logs Registrar, who maintained liaison with the Joint Registry (Rooms 11 and 12) and the T-Registry (which was the Block H branch of the Joint Registry - see Ch.34) See also Fig.37 (I).



FUNCTION OF THE OPS. REGISTRY

FIG. 37 (I)

In addition there was an H registrar who was effectively the Block H representative of the Runs Registry.

The Runs and Tapes Registrars issued chits with every job ordered. These chits contained accurate descriptions of the job required and were returned with the tapes when the job was completed.

When the Colossus tapes were returned from the Tunny Room the T.R. checked that they were correctly marked, had an adequate join, and stop and start signs in the correct place. To ensure this the first few letters of the tape were checked with those on the Ops. card. The tapes were then passed to the Runs Registra

After a successful setting job the tapes were returned to Ops with a decode check or de-chi check and ΔD letter count. If the job was partially successful a ΔD letter count using as many wheels as possible was provided. When a dossier was given to the D.O. he ordered one of the following: Further runs, Decode, De-chi, or Abandon and returned the dossier to the Runs Registrar.

The Registries had several additional jobs. For example the Tapes Registrar kept an index of $\Delta\chi_5$'s so that any repetition of the same set of wheels could be spotted.

(b) Robinsons and Colossi

In June, 1943, when there was only one Robinson available, each message tried was a research job in itself, and every run

was ordered separately by the Runs Registrar the Duty Officer being consulted if necessary. At this time the D.O. was responsib for all work on messages tried in the Newmanry and it was in Ops. that the psis were first set by hand in November, 1943. After this there was an almost immediate change of policy, Room 41 took over the job of psi-setting by hand, and Robinsons were used to set all five chis on as many messages as possible. This policy remained unchanged for almost a year though spasmodic efforts at machine psi and motor-setting were made.

The Newmanry moved to Block F late in November, 1943: the first 'Heath' Robinson was replaced by 2 production models and others came later. Colossus 1 came in Fenruary 1944 and runs on the new machine took so short a time that it was necessary to decide policy on the spot and a Colossus man was appointed. Colossi soon replaced Robinsons for setting purposes and the duties of the Runs Registrar were increasingly confined to issuing tapes to machines in the right order and seeing that they did not stay there for too long. By the end of August no Robinsons and up to 4 Colossi were used for setting.

As the number of Colossi increased Wren operators were left more and more on their own. A Colossus man was always available for consultation, and the D.O. kept a check on the accuracy of all Colossus work. From July, 1944 onwards the D.O. saw every Colossus dossier as it returned to Ops. and took over the responsibility for abandoning messages and ordering de-chis. This had previously been done by the Colossus man.

By November, 1944 many new Wrens were working Colossi on their own and considerable time was being wasted. Either too many runs were done, or so few that further runs had to be ordered by the D.O. For this reason the runs normally done were standardised, the 'trees' or runs schedules varying according to the type of language and limitation expected. Departures from schedule were only made in consultation with the Colossus man. The new 'rules' had a remarkably good effect and were interpreted in an increasingly liberal way.

In the Summer and Autumn of 1944 there was so much chi-setting to do that psi runs were not done. But in November, when there were 6 Colossi, Motor and Psi runs were done more often, and after December 25th it became a routine to do them on low dottage days. From March 5th, 1945, a new policy of setting motors and psis on Colossus in every possible case was adopted, exceptions only occuring on days of high dottage, or days for which motor patterns were not yet broken. Wrens soon picked up the technique and were able to do motor and psi runs on their own.

The machine resources in 1945 are given in part 5.

(c) Ordering

The D.O. was responsible for knowing what wheel-breaking was in progress, whether on significant rectangles, key, or crib. As soon as it appeared likely that a day would come out, the D.O. (in consultation with the W.M. or head of Room 41) asked the C.O. to order the traffic from Knockholt on C-procedure, and recommended whatever priority and procedure seemed to fit the general priotity of the link, date, estimated dottage, and estimated time of completion of the wheels. The priority of the wheel day was assigned by the morning meeting if it was being worked on when this took place ; otherwise the priority had to be decided from the general priority list or in consultation with Hut 3 (see 33A).

(d) Further Runs

We refered in 37(a) to 'Further Runs'. These were of 5 main types.

(i) Correct Runs, where incorrect runs had been done befo:

(ii) More runs, runs with spanning etc.

(iii) Motor and Psi runs, either immediate or delayed. Messages set on all chis before motors were broken were de-chied, but those set strongly on some chis only, were held for 'delayed motor runs'.

(iv) 4-wheel runs (see 23H(c)). These were done on long messages for which normal methods gave no result, if and when there was machine time to spare.

(v) Runs on a Doctored tape i.e. a tape altered to counteract a message slide discovered by spanning on Colossus.

In all cases it was best for the D.O. to write out quite precisely what he wanted done. As it was often necessary for the D.O. to calculate the expected score of a motor run in orde: to decide if it was worth while, many motor runs were issued wi: E.S. worked out.

Further runs fell naturally into two categories: Runs strongly expected to succeed and runs done because insufficient work had been done to justify abandoning. The first category was marked so that the R.R. could give it suitable priority.

(e) Hut 3 Priority Messages

When Hut 3 believed that messages were of special urgency, the C.O. was sent a chit, requesting that it should be marked Z, ZZ, or ZZZ. If the tapes had not been set the request was passed to the D.O. and Logs Registrar. All documents were marked with the priority sign and treated specially. If other work was plentiful, Z and ZZ messages were run rather more fully than other tapes. If already abandoned when the request arrived, a rewrite was ordered, and run fully. 4-wheel runs were not done. ZZ had priority over Z. ZZZ priority was only ordered in speical cases. All possible runs including 4-wheel runs were done at once on the first tape and a rewrite was ordered. All runs including 4-wheel runs were repeated on the rewrite.

(f) Routine checks for machines

(i) Chi test runs and tapes

Before the first de-chi on a new key day was ordered by the T.R., a chi test tape was ordered from Tunny. This was sent to a Colossus on which the new chis had been set up, and chis and test tape were checked against each other by adding them togethe Test Runs were then done on this Colossus and one other, and if they agreed several copies were made and stuck in each Colossus wheel book.

(ii) Psi Test Runs and Tapes

Psi test tapes were made (with suitable limitation) as soon as psis and motors were known. The routine and uses of psi test runs and tapes were similar to those for chi test runs and tapes.

(iii) Routine Tests.

A routine test (using a general test tape) was carried out on two Colossi per shift. The test took about 20 minutes and was done by Wrens specially trained by the Engineers.

38 - WHEEL-BREAKING FROM KEY, ORGANISATION

(a) Development

In the early days of Tunny work when all monthly keys were broken on depths, the recovery of wheels from key was undertaken in Major Tester's section, either by means of special methods available before the QEP system was introduced, or by 'Old Fashioned Turingery'.

After ρ_5 limitation was introduced on most of the links normally tried (December, 1943) depths were still occasionally anagrammed on any others that still used χ_2 lim. Some monthly keys were broken in this way, but hand methods as practised in Room 41 were rarely strong enough to break wheels from key of under 400 letters. Very long key was sometimes broken on Colossus.

No great advances were made until the autumn of 1944 when χ_2 Υ_1 limitation gradually replaced χ_1 ρ_5 and χ_2 lim was reintroduced on several important links. After the start of the daily key change (July, 1944) it was policy to try as many key days as possible and it became necessary to develop quick and powerful methods on shorter lengths of key. First the $\Delta\chi_5$ flag was invented and introduced, the Modern Turingery (with decibans) and later 6 - impulse Turingery for χ_1 limitation.

Therefore, by 1945, the resources and staff employed in the breaking of ehis and psis from depth key had expanded outside Room 41 and included some or all of the following:-

A skilled key-breaker in Room 41 (and assistant)

The Wheelsman

The Rectangles Registrar and up to 6 computers.

1 Garbo, 1 handperforator and operators in Room D.

1 Colossus with wheelbreaker and 1 or 2 operators to assist him.

(b) Work in Room 41

Work on Turingery in Room 41 involved very little organisati as each job was undertaken by one man with occasional help from an A.T.S.

Certain members of Room 41 took a particular interest in key-breaking and specialised in the work. Most of the older member could undertake the job in the absence of the specialists, and newer members were gradually trained when it appeared that two key-breakers on each shift might be required.

Unfortunately the specialist key-breakers did not work on a three shift basis and were by no means always available. However they were always willing to work double shifts and odd shifts when there were important key-breaking jobs to be done.

(c) Making of Combined Flag.

The flagging of each rectangle was done by one computer, and one computer was employed in adding the flags together, so that 5 or 6 computers worked at once.

It proved profitable for the computer adding the flags to record the entries of each flag on a large sheet

and then to add them. Therefore whenever a few lines of a single flag were completed they were torn off and given for entering to the computer in charge of the adding.

The time for making a combined flag was about 3½ hours.

If the converged combined flag proved significant the $\Delta\chi_5$ pattern was taken through the rectangles and the resulting scores for each character sent to Room 41 with the flag scores for each character of $\Delta\chi_5$.

Results were recorded and further work was normally done in Room 41, unless the key was issued to Colossus.

If the combined flag proved insignificant, all working and entering was rechecked by the wheelsman and if no mistakes were found either:

(a) the key was abandoned

(b) a $\Delta\chi_4$ flag was made,

(c) the key was issued to Colossus for convergenceof a 150 x 150 rectangle in the hope that this might prove significant.

In view of the work involved in making a combined flag and the strain on computers, experiments in making the flag mechanicall started in 1945. These were never successful enough to produce new operational technique and are described in an appendix.

39 - LANGUAGE METHODS

39A CIRCULATION

Circulation of material in the Testery was arranged from Room 12 with the help of the de-chi clerk (in Room 41) who kept track of material in Rooms 40 and 41 and the Supervisor, who kept track of material in the decoding room. Documents for each message worked on in the Testery were circulated in an envelope which included the Red Form (but not the tapes). When the message had been decoded, it was returned to Room 12.

39B CRYPTOGRAPHY

(a) Commitments

Cryptographers in the Testery were divided into two rooms, the so-called 'Breakers in Room 41 and the so-called 'Setters' in Room 40. Room 41 numbered 5 on a shift plus 4 on permanent days, and Room 40, 8 a shift. Room 41 contained the more experienced men and the Head of Room 41 was responsible for all work in the section, on his watch.

The growth of the Testery and the division of work has been outlined in 14A (b). The purpose of this chapter is to describe the organisation in 1945 when there were two major cryptographic commitments.

(i) Recovery and Solution of Key from Depths.

(ii) Psi and motor setting from a de-chi by hand or with the help of Dragon.

(b) Depths

Possible depths noticed at Knockholt were teleprinted at once, not more than 1000 letters being sent. When the interception registers arrived in Room 12 they were carefully examined and a list of other possible depths sent to Knockholt.

(c) De-chis

Before being issued to the Head of Room 41, the annotations "Pause","Auto" and "Hand" were copied by the de-chi clerk from the Red Form on to the de-chi. The head of shift saw that the de-chis were worked on in a suitable order and that psi breaking jobs were given suitable priority. Various aids to de-chi "breakers" existed in the form of decodes and abstracts of message characteristics.

De-chis were passed to Room 40 when sufficient P and ψ' had been obtained to set or break the psis at some point in the de-chi. Room 40 found the settings for the start of the message and worked out sufficient extended psi to set the motor or break the motor patterns. In the most favourable circumstances jobs took 20 minutes and 1½ hours respectively, but more usually rather longer owing to the unfavourable motor wheels or slides in the text. Messages with χ_1 limitation were sometimes set at the position of the Room 41 break and worked back on a specially adapted machine.

De-chis worked on in Room 41 without success and any unworked setting de-chis on low dottage days could be sent to Dragon, which was under the control of members of Room 41. When $\Delta < 19$ it was general practice to send all de-chis to Dragon. A few de-chis were returned to the Newmanry for motor runs.

39C DECODING

Decoding Resources consisted of a Supervisor; 13 machines 10 operators and 3 engineers on each watch. There were occasional interchanges of staff with Room 40.

(a) Supervisor

The Supervisor registered messages to be decoded, and issued them to machines, which had to be set up so that messages could be dealt with, with suitable priority. The supervisor verified from the decodes on their return, that the machines had been set up correctly on all impulses.

(b) Operators

Operators needed to be touch-typists and to be able to recognise P and to be trained sufficiently in Tunny to solve minor breakdown problems. Major breakdowns were passed back to Room 40.

In the later stages, tape decoding was introduced. It was found to be much faster than hand decoding on long messages, but slower on short ones. Corrupt messages were better dealt with by hand methods.

Rewrites of poor or unreliable cipher text could be obtained throught the C.O. from Knockholt, and when necessary a slide run on approximate chi-settings could be done in the Newmanry.

(c) Machines

In the early days decoding had to be interrupted for short periods while repairs and adjustments were carried out,

The number of machines steadily increased to the final total of 13 and during the last 12 months or so, it was possible to have the engineers working on the machines which were not actually required for current work.

39D ISSUING

The Cribs Watch was created, to read decoded material "en passant", and contained 5 German linguists covering three shifts. Its duties were:

(i) To pick out possible retransmissions from incomplete decodes still on the machines, to assist operators in correcting breakdowns by suggesting probable clear text, and to expedite the issue of particularly urgent messages.

(ii) To check the general accuracy of completed decodes, and to route the different messages found in each decode, to the appropriate sections.

(iii) Later, to reread the duplicate copy of each decode (returned from Room 12) with the object of marking any information of interest to Sixta and of informing Mr.Page's Section of any possible cribs.

(iv) To sort amended and typed decodes from Hut 3 and extract and file examples of routine messages for the benefit of Room 41.

41 THE FIRST BREAK

41A EARLY TRAFFIC

(a) A first analysis

The first messages on the "Tunny" link (the name "Tunny" was first given to this traffic in the summer of 1942) to be studied cryptographically were sent out shortly after the German invasion of Russia. They passed between Vienna and Athens. The Hellschreiber method of transmission was used. Some earlier traffic, apparently practice transmissions, had been intercepted in May. This had been sent out in the form of a five-unit code, so it was suspected that a teleprinter was being used. This was confirmed by a preliminary examination of the later traffic, which showed that an alphabet of 32 characters was being employed. These characters were the 26 letter of the normal alphabet, and the six extra symbols 3, 4, 8, 9, + and /

Each message began with a clear preamble in which there appeared first the serial number, repeated several times, and then a set of 12 letters, in the form of names (Anton, Bertha etc.) which was clear a 12-letter indicator. The symbol 9 was used as a separator in this preamble, and a group of five 9's separated the clear preamble from the cipher text. Immediately after the cipher text there appeared a sequence of 8's. The serial number was given in letter form by means of a simple keyboard substitution the digits 1,2,3,4,5,6,7,8,9, being represented by the letters Q,W,E,R,T,Y,U,I,O,P, respectively.

(b) Meanings of teleprinter letters

On the assumption that a teleprinter machine was being used, two problems presented themselves. First, was the correlation of the 26 letters of the normal alphabet with teleprinter signs the same as that of the international convention, and second, what teleprinter signs corresponded to the symbols 3,4,8,9,+ and / ?

Both these questions were answered by the study of a a series of corrupt messages which were sent out on July 22nd. Only sixteen different letters appeared in these messages, and those letters of th normal alphabet which appeared were those whose first impulse was conventionally a dot. Clearly, owing to some fault in the machine, t first impulse of each letter had been transmitted as dot, even when it should have been cross. This effect finally confirmed the hypothesis that a teleprinter machine was being used and answered the first of the above questions in the affirmative.

The second problems was then solved by a study of the corrupt cl preambles. For example the sequence H / I N R I C H and T H / 0 3 0 would be recognised as corruptions of H E I N R I C H and T H E 0 D 0 respectively. Hence it would be deduced that for each of the pairs (E,/) and (D,3) the teleprinter signs differed only in the first impulse. But by convention E is (x....) and D is (x..x.). Hence it was deduced that / corresponded to the teleprinter sign (.....), and 3 to the teleprinter sign (...x.). By this sort of argument the teleprinter sign corresponding to each of the letters 3, 4, 8, 9, +, and /, was determined.

41B TUNNY SHOWN TO BE A LETTER SUBTRACTOR

The next advance to be made was the demonstration that the ciphe was a letter subtractor cipher, and the determination of the law of addition used.

This was made possible by the occurrence of a number of "depths of two", that is, of messages having the same 12 letter indicator. Usually the two messages of such a pair were consecutive, as though an operator had failed to reset his machine between the two messages, but instead had made use of some device for returning all the wheels to their starting points.

The simplest assumptions to make seemed to be that a letter subtractor cipher was being used. The law of addition was fairly

easy to guess and was guessed correctly.

It was argued that if a pair of messages (a, b,) with the same indicators were really in depth, the sum of the two cipher messages must be equal to the sum of the two clear messages, it being assumed that the cipher was a letter subtractor.

Now when the sums $Z_a + Z_b$ were formed for a number of depths of two it was noticed that some pairs of them began with the same sequence of five or six letters. This was regarded as a proof of the assumptions that had been made, namely that the cipher was a letter subtractor, and that the law of addition had been inferred correctly. The effect would be expected to arise if stereotyped beginnings were being used.

The proof was completed when about 15 letters of one of the depths were decoded. When a group ++zzz88, which had appeared occasionally in clear preambles was tried as the clear of one message, the clear of the other message, came out as the first letters of the word S P R U C H N U M,M E R (serial number).

41C A DEPTH READ

(a) Problems of depth reading

The first attempts to reconstruct long key-sequences from depths of two were failures. Depth breakers then had no previous experience of the traffic, and so depth breaking was much slower and much more difficult than it was in later years. Apart from this there was one very serious obstacle in an ambiguity which is inseparable from a depth of two.

For in the process of depth breaking the first step is to constru the sequence $Z_a \rightarrow Z_b$, and then to express this as the sum of two passages of plain language, which are assumed to be P_a and P_b . But there is usually no way of telling which of the passages is P_a . and which is P_b . It can be done when cribs to the messages are known; for example, as in the early days when the serial numbers were given both internally and externally: and it can also be done when the decoding process is carried on to the end of the shorter message, for then the clear message which comes to an end must be associated with the shorter cipher message. But it cannot be done by the depth breaking process alone, without independent evidence.

In the depths which were first attacked, the clear language obtained was not continuous, and the short sequences obtained could not be correlated with one another, so the ambiguity arose fresh in each section.

It is not surprising therefore that for some time little progress was made with the "Tunny" cipher. The construction of long pieces of key was very difficult, and even when it was possible the results were not unique.

(b) <u>The depth "HQIBPEXEZMUG"</u>

On 30th August, 1941, the German cipher operators came to the rescu

On that date two very long messages, with the same indicators HQIBPEXEZMUG were sent out from the same end of the link. When a depth was broken into, it was found that the messages were essentially the same, but the spacing, the mis-spellings and the corrections were different. Evidently the same message had been typed out twice, by hand. As a result the two versions, at the same number of letters from the beginning, would be at slightly different places in the true text of the message. This divergence increased slowly, until at the 3,976th letter, where the shorter message came to an end, it had increas to more than one hundred letters.

This depth was much easier to read than the earlier depths had been, for at any stage the next letter of clear language in the less advanced message could be predicted from the clear language already derived for the other. The messages were in fact decoded over the entire length of the shorter message, so that the ambiguity in the key was resolved. The practice of giving the serial number externally and internally had ceased some weeks previously.

From this depth a length of subtractor key of 3,976 letters was reconstructed (with a few of the letters doubtful, of course). During the remaining months of the year 1941 the Research Section were engaged in attempts to analyse this key, and so discover the nature of the machine which had produced it.

The Germans may have noticed this breach of security, for the traffic almost stopped for a few days, and no more true depths are on record for the remainder of 1941.

(c) Near-depths

Besides the depths in July and August there were a number of "near-depths". These were pairs of messages sent out on the same day whose indicators differed only in one or two letters. One pair whose indicators differed only in the first letter was decoded successfully for 20 or 30 letters on the assumption that the two subtractor keys differed only in the first impulse. Then another pair whose indicators differed only in the first two letters was decoded for a dozen or so on the assumption that its two subtractor keys differed only in the first and second impulses.

It was deduced from this that the first letter of the indicator affected only the first impulse and the second letter only the second impulse of the subtractor key. No further positive information was obtained from near-depths at this stage.

Mention should also be made of some pairs of messages having the same indicator, but not sent on the same day. All attempts to decode the beginnings of these pairs failed.

With luck, we might have had at this early stage a near dept whose indicators differed only in one or two of the last five lett Such a depth, we now know, should have given very important information. However no such depth seems to have been intercepted until March 1942, except for a hopelessly corrupt one in the January of that year.

41D KEY ANALYSED

(a) Study of Indicators

For a long time no progress was made in the analysis of the subtractor key of the depth H Q I B P E X E Z M U G. This was due to concentration on a hypothesis now known to be wrong - that each impulse was the sum of two or more periodic components, the period being small.

In fact the only positive information obtained during the rest of 1941 was obtained by a study of the indicators used. It w found that, in any particular month, there were two letters (apart from J) which could not appear in the twelfth place of the indicator. This pair varied from month to month. One other fact about the indicators was established: the letters most frequently used were those in the middle of the alphabet, and those at the ends of the alphabet were comparatively rare.

The reason for the latter effect remains obscure though ther

is no doubt that it is only a psychological one, and is not necessitated by the nature of the machine and of the indicator system. The first effect suggested that the last letter of the indicator controlled the setting of a wheel of period23.

(b) Chis, Psis and extensions.

The first success in the analysis of the key was obtained towards the end of January 1942 when it was found almost accident that many repeats occurred in the first impulse of the key at intervals which were multiples of 41. This suggested that this first impulse was the sum of a periodic sequence (of period41) and of an aperiodic but non-random sequence. We here denote the periodic sequence by χ and the non-periodic sequence by ψ .

In order to reconstruct the sequences χ and ψ , the first impulse was written out on a width of 41, and for each set of five consecutive columns a count was made of the five consecutive characters which occupied these columns. When two such counts were made it was found that they were closely relate by adding a constant set of five consecutive characters to each the five character sequences in one of the sets of columns, the frequency count of this set could be brought into close agreement with that of the other. It was found that these constant five-character sequences could be so chosen as not only to bring all the frequency counts into good agreement, but also to fit together in their properorder to form a periodic sequence of period 41. This sequence was denoted by χ and the result of adding it to the first impulse was denoted by ψ .

When ψ was examined with the object of determining its non-random properties, the following "local" peculiarities were observed:-

(i) Consecutive signs in the sequence Ψ tended to be equal. In fact there was equality in about 3/4 of the cases.

(ii) The sequences .x. and x.x were significantly rare in Ψ, even when the result (i) was taken into account.

It was then seen that the χ pattern could have been reconstructed by considering only pairs of consecutive columns in the rectangle, and that the power of the method was not appreciably increased by taking five columns rather than three. When the method came to be applied to other depths, the counts were therefore made on sets of three consecutive columns.

The most striking property of Ψ was that it was roughly periodic; it could be regarded as a periodic sequence of period 43 which had been "extended" by replacing some dots by sequences of two or more consecutive dots, and some crosses by sequences of two or more consecutive crosses. The Ψ sequence was evidently generated by a wheel of period 43 which somtimes moved on one place, and sometimes stayed still when the cipher machine moved from one of its states to the next.

We may here introduce a slight change of notation. The extended key which has been called Ψ is now denoted by Ψ' and the symbol Ψ is used for the periodic sequence from which it is derived by extension.

We have now reached the stage at which the first impulse was shown to be the sum of a periodic sequence χ of perod 41, and an "extended" sequence Ψ' derived from a periodic sequence Ψ of period 43. An ambiguity arose here, for the pattern of χ and Ψ could both be reversed (by replacing dots by crosses, and crosses by dots) without affecting their sum, but this was evidently of very little importance.

The law governing the extension of the sequence Ψ was still unknown.

The four impulses of the key were next attacked, and they were successfully broken down into χ and Ψ patterns, just as the first impulse had been. In these cases the periods of the χ wheels were found by booking 7-sign repeats in the first few hundred places of each impulse, factorizing the intervals and selecting the most common, fairly large, prime factor. The periods were found to be 41, 31, 29, 26, and 23 for $\chi_1, \chi_2, \chi_3, \chi_4$, and χ_5 respectively, and 43, 47, 51, 53 and 59 for $\Psi_1, \Psi_2, \Psi_3, \Psi_4$, and Ψ_5 respectively.

(c) The Motor

The next problem was to determine the law governing the extensions of the Ψ patterns. This was attacked by means of the concept of the "motor-key".

The motor-key was defined as a sequence of dots and crosses which each sign was associated with a particular pair of consecutive signs of Ψ', and such that the nth sign of the motor key corresponded to the pair formed by the nth and $(n + 1)$th signs of the extended Ψ key. When two consecutive signs in Ψ' correspon to the same positions of the Ψ wheel the corresponding motor-key sign was defined to be dot, and when two such signs corresponded to different positions of the Ψ wheel the corresponding motor key sign was defined to be a cross.

The motor key corresponding to a particular impulse could only be determined partially from the corresponding Ψ' key. When for example a block of 3 consecutive crosses in the Ψ wheel was represented by a block of 5 consecutive crosses in Ψ', it was possible to say that just two of the pairs of consecutive crosses in this block corresponded to dots in the motor key, but it was not possible to say which two of the four such pairs these were.

A pair of consecutive different signs in Ψ' necessarily corresponded to a cross in the motor key, but the position of a dot in the motor key could only be fixed, when it corresponded to the extension of a singleton dot, or cross, in the Ψ pattern. As there were very few singleton dots, or crosses in the Ψ pattern very few dots could be fixed in the motor key. Sometimes a group of several consecutive dots, or crosses, in the Ψ' key would not be extended at all: each sign in the motor key corresponding to a pair of signs in this block could then necessarily be a cross

A motor key determined from a Ψ' key therefore consisted of a number of isolated groups of one or more crosses, together with a few groups consisting of dots flanked by crosses. These groups would be separated by intervals whose lengths varied from two places up to eight or nine. In each such interval the number of dots, but not their distribution, would be known.

A study of the indicator had suggested the hypothesis that t motor keys of the five impulses were identical. For since the first and second indicators affected only the first and second impulses respectively, it was supposed that each indicator letter gave the setting of a particular wheel in the machine. We have already mentioned the evidence that the twelfth indicator letter gave the setting of a wheel period of 23. This wheel could now be identified with the fifth χ wheel. It seemed probable therefore that the first five indicator letters corresponded to the five Ψ wheels in order, and the last five to the five χ wheels in or

This left only the middle two indicators to govern the motor key. (This would explain why near depths differing in this pair of indicators have proved unbreakable.)

But five indpendent motor keys should need at least five

indicators. Hence there was probably only one motor key, controlling all five Ψ wheels.

The five partial motor keys, obtained from the five impulses were therefore compared, and it was found that the assumptions that they were all partial descriptions of the same fundamental motor sequence led to no inconsistences(or at any rate to no more inconsistences than could be explained by rare corruptions in the text). The five motor keys were accordingly combined to give the true motor key. Even this was not free from ambiguities but most of its signs were fixed.

The Research Section now tried out a number of hypotheses on the motor key, without success, until it was noticed that the key was nearly periodic. It was then found that it was derived from a truly periodic sequence, of period 37, by a system of extension just as the Ψ' keys were derived from periodic sequences.

The pattern of the 37 wheel was readily determined, as was law governing its extension. For the "motor-key" governing the movement of the 37 wheel was simply a sequence of dots and crosses of period 61.

41E TWO MORE DEPTHS

The cryptographical problem presented by the depth H Q I B P E X E Z M U G had now been completely solved. The new problem was to find what changes were made in the machine between the encipherment of different messages. For example, could the wheel patterns be changed, if so how often were they changed? Again, could the actual order of the wheels be changed, so that say, the 41 wheel became the χ wheel of the 3rd. impulse?

The first attack on this problem was made by attempting to set messages of 30th August 1941 and other dates close to this, on the set of wheels found for H Q I B P E X E Z M U G, taken in the same order. In this way it was hoped that the period of time over which these wheel patterns, with this wheel order were valid could be determined. But these attempts at message setting all failed. An attempt was then made to set a depth of July 3rd, the indicator letters of which were D K T N F Q G W A O S H. This depth was usually referred to as "Waosh". Now that a good knowledge of the type of plain language used in the traffic had been obtained from H Q I B P E X E Z M U G, and now that it was known that keys could be broken, depth breaking became a much more rapid and successful process than it had been in July and August, 1941. Two passages of the depth were read, one about 500 letters long, and the other about 300 letters long, and two possible subtractor keys were obtained from each passage.

These possible keys were submitted to the analysis that had succeeded in the case of H Q I B P E X E Z M U G, but the columns were now counted in three, rather than fives. The alternative which seemed to give the more significant results in the fifth impulse, on a width of 23, was retained in the case of each of the passages that had been read. The information given by both passages was now combined, and the fifth impulse was successfully broken up into a χ-key of period 23, and an extended Ψ key of period 59. The ambiguity in the key was now eliminated for all five impulses. The analysis was now applied to the other four impulses on the assumption that the wheel order was the same as in H Q I B P E X E Z M U G, and successful results were obtained in each case. No difficulty was then found in the determination the motor key.

It was found that the patterns of the Ψ wheels in W A O S H were identical with the Ψ wheel patterns of H Q I B P E X E Z M U G, but the patterns of all the other wheels were different in the two depths.

Next a depth of July 21st with indicators K O W P A E N G F B Z was successfully attacked. All the wheel patterns of this depth, with the exception of those of the two "motor" wheels (with periods 37 and 61) were the same as in W A O S H , but the two patterns were different.

From these depths the following conclusions could be drawn:

(i) The order of the wheels was fixed.

(ii) The Ψ patterns remained unchanged over periods which could exceed one month.

(iii) The ϰ patterns remained unchanged over periods of many days.

(iv) The patterns of the motor wheels were changed comparatively frequently.

It could now be assumed that one reason why the attempts to set messages not in depth had failed was that the wrong motor wheel patterns had been assumed. The attempts were now resumed, but no assumptions were made about the motor patterns. Messages intermediate in time between K O W P A E N G F Q B Z and W A O S were taken, so that there could be no serious doubt about the pa of the ϰ and Ψ wheels.

42 EARLY HAND METHODS

42A FIRST EFFORTS AT MESSAGE SETTING

The theory of [redacted] message setting which was attempted in March, 1942, after the breaking of the first three depths is simple. It had been observed from these, and from depths that had only be decoded for a few letters, that most messages contained the group **S I K U C H** 9+ + or **B P R U C H N U M M E R** 9++ either right at the beginning or else preceded only by such groups as 89. or + + Z Z Z [redacted] 8 9. In most attempts at message setting therefore, the groups S P R U CH N U M E R 9 + or + + Z Z Z [illegible] 9 S P R U C H were assumed as the clear language in some position near to the beginning of the message. After the group 9 + + the serial number of the message would be given in letter form. When this was also given in the clear preamble the crib could be extended a little if necessary. (This practice of giving the serial number in clear soon ceased.)

By adding the assumed clear language to the cipher text, a length of about 15 letters of possible keys was obtained. Each impulse of this was treated in the following way. First the corresponding χ wheel was added in all possible settings, and then attempts were made to fit the ψ pattern, suitably extended, to each of the set of sequences of dots and crosses thus obtained. Usually there were two or three sequences which could be interpreted as extended parts of the ψ pattern.

The possibilities were limited by the nature of the ψ patterns, which contained so few singleton dots or crosses. A sequence containing several singletons could be rejected at once.

After this process had been gone through for the five impulses the results were compared to see if the same motor key could be fitted to five of the possibilities, one in each impulse. If so, a possible setting of the 10 χ and ψ wheels had been obtained. It was finally tested by an attempt to decode more of the message. This test depended on the principle that a message can be decoded even when the motor key is unknown, provide that the other ten wheels are correctly set. For suppose we have decoded a message up to the nth letter. Then there are only two possibilities for the nth sign of the motor key, namely cross and dot, and the (n+1)th sign of the subtractor key can readily be calculated for each possibility. By applying these two subtractor letters we get two alternatives for the (n+1)th clear letter, and considerations of sense are usually sufficient to decide between them. Thus the message can be decoded letter by letter, the motor key being built up sign by sign at the same time.

For a long time the would be setters had no success, but at last came the great day when the first single message was set and decoded.

By the end of April several other July messages had been set, and the Research Section was in a position to attack the July indicator system. But then some messages were broken which were only about a month old. The message setters thereupon forgot all about July 1941 and concentrated on March, 1942.

42B MACHINE BREAKING FOR MARCH 1942

(a) Depths in February

Interest in current traffic, dormant for six months, revived at the end of February, 1942. The Hellschreiber method of

transmission had now been superseded by tone transmission in 5 - unit code; near depths were once more appearing. Many of these were corrupt, but the beginnings of some were decoded, and were shown to be of the same stereotyped forms as were those of July and August 1941. Two or three hundred letters of one February depth were read and an attempt was made to break the machine. This failed. A near depth of March 3rd was passed over in favour of the February depth.

(b) A depth of three

On March 25th, an unprecedented phenomenon, the interception of a depth of three, occurred. Attention was immediately diverted to it. Reading in depth of three was found to be very easy, and it was soon carried to the end of the shortest of the three messages (975 letters). It was continued for the other two messages without a break up to the 1060th letter. There was no abiguity about the subtractor key, as there would have been in a depth of two, and there was hardly any possibility of corruption in it, since all three messages were good, and since two messages would need to be corrupt in the same letter in order to produce an error in the calculated subtractor key. No better length of key could have been desired, and all the energies of the Research Section were thrown into the attempt to break it, but without success. Some evidence was found to confirm the hypothesis that the periods of the χ wheels were the same as of old, but that was all. It was supposed that the Germans had taken steps to eliminate the non-random characteristics of the extended ψ patterns. The Research Section did not manage to anticipate Turing's Method of Key Analysis and work on the depth of three had to be abandoned.

(c) A near depth of March 3rd.

However, though depths could no longer be broken, it was thought that a near depth might prove vulnerable. For when a near depth can be read it gives not merely one key, but two closely related, but different keys. Attention was therefore transferred to the rather corrupt near depth of March 3rd. which has already been mentioned.

The two messages of the near depth had indicators which differed only in two of the last five letters, and therefore according to the hypothesis referred to in Section IV the only difference between the two subtractor keys was in the settings of two of the χ wheels.

The near depth was decoded for abouth 30 letters, and the sum $K_a + K_b$ of the two keys was determined. Crosses (of course) appeared only in the impulses whose χ wheels had different setti in the two messages. Both these impulses of $K_a + K_b$ should have shown the periodicity of the corresponding χ wheels, and were i fact found to do so, though the piece of pattern actually repeated in either impulse was of course very short. Hence, both these impulses were assumed to be χ patterns "differenced" at some unknown interval. By repeating the patterns the sequence $K_a + K_b$ could be extended as far as was desired. So from this sequence and the cipher texts the sum of the two clear texts could be derived. This sum was attacked as in the breaking of ordinary depths, and two or three hundred letters were decoded. So two alternatives for the subtractor key of either of the messages were worked out for this stretch of two or three hundred letters.

This success established the validity of the assumptions which led upto it.

At this stage then, not only were two alternatives for a length of key known but also two χ patterns differenced at unknown interval had been obtained.

(d) Chis and Psis completed

From the χ difference patterns, it was possible to determine t e correct χ patterns with some ambiguity. Actually each assumption about the unknown differencing interval led to a different χ pattern, but most of these could be rejected as having too many, or too few, crosses. The justification for this lay in the fact that in July and August 1941 the numbers of dots and crosses in any χ or ψ wheel patterns had been made as nearly equal as possible.

Those few possible χ wheels that remained for one of the impulses were applied in their proper settings to the alternative subtractor keys, and t e resulting sums were examined to see if they were nearly periodic. One of them did indeed prove to be an extended ψ key.

So the ambiguity of the subtractor keys was resolved, and one impulse of each key was successfully broken down into χ and ψ keys. By studying the ψ' key in the impulse it was possible to decide, for very many of the subtractor letters just how many ψ movements had intervened between them and the beginning of the message. As the ψ movement was the same for all five impulses, it followed that for very many letters of the key, the settings of all the ψ wheels, relative to their initial settings could be determined. This was done, and then the value dot was assumed for the first character of the χ wheel in another impulse. This assumption was legitimate, since the patterns of both χ and ψ wheels in any impulse can be reversed without affecting their sum. Then from the characters of the key corresponding to the first position in this χ wheel, a number of characters in the ψ pattern were obtained, and put at their proper intervals in the ψ pattern, by the use of the relative settings From other key characters corresponding to these ψ characters,

more χ characters were found, and then by continuing this process the complete χ pattern and ψ patterns were built up.

Hence all the χ and ψ patterns were determined and then the motor key was analysed just as for July and August, 1941.

The message setting method was then applied to the Key from the depth of three and this was successfully set on the χ and ψ wheels which had been derived from the near depth. The motor wheels were however different.

(e) Value of a and b

When the March wheel patterns were inspected it was seen that there were still 11 dots in Mu 37 (so that a = .703 since there was no lim) and that the value of b was about .7 giving ab = $\frac{1}{2}$. These values must be compared with those for the patterns for 1941 when a = .703 b < $\frac{1}{2}$ so that ab was always less than .352.

The change in the value of b explains the failure of the old method of key analysis on the key from the depth of three. It is worth noticing that the Tunny machine would probably never have been broken if there had been no stretch of key susceptible to the single impulse analysis possible when ab $\neq \frac{1}{2}$

42C MESSAGE SETTING FOR MARCH 1942

The success obtained with the near depth of March 3rd. confirmed the theory of indicators which has been mentioned above It was now taken for granted that the setting of each wheel was

controlled by a single letter of the indicator, that the first five letters of the indicator corresponded to the five Ψ wheels, in order, and the last five letters corresponded to the five χ wheels, in order. The obvious assumption that the same indicator letter in the same place for two messages meant that the corresponding wheel had the same setting in both messages was also made. Justification for it could be found in the fact that the last indicator letter was restricted to the same 23 values over the whole of any one month, which seemed to show that there was no change in the indication of the fifth χ wheel over this period.

The message setters therefore restricted themselves to messages which had for two or more of their χ and Ψ indicators values which had appeared in messages which were already set. The settings of the corresponding wheels could be assumed known, and this greatly simplified the process of message setting described above. In impulses in which the setting of a χ wheel was known, the crib, usually SPRUCHNUMMER9++ could be tried in many different positions, and rejected at once in some of them. When the χ setting was known for two impulses, most of the false crib positions could be rejected.

The process of message setting was very successful, and with each success it became more powerful, since the meanings of more indicator letters were known. In its later stages the settings of the majority of the wheels for the message attacked were known, and the process differed but little from ordinary decoding.

The theory of the indicators was completely confirmed. The results, together with those for April - the two months were soon being attacked simultaneously - also gave new information about the motor wheels. It was found that their patterns changed every day but that the corresponding indicator system, that is the correlation of the indicator letters with wheel positions, was fixed over each month. The 5th indicator letter

controlled the 37 wheel and the 7th controlled the 61 wheel.

It should be noted that the cyclic order of the wheel settings corresponding to the indicator letters was not correlated with the order of those indicator letters in the alphabet.

It was found that the χ and ψ wheel patterns remained contant over each of the months March and April, but changed between these two months.

42 D APRIL 1942

(a) Breaking the wheels

One or two depths were found in April, but no attempt was made to analyse the keys obtained. The break into April was made on a near depth of April 22nd. The indicators of the two messages concerned were

M H S L P E I S V O I U

and

M [illegible] S L P E I . . O I O

Two of the indicator letters in the second message could not be determined, owing to corruptions. By a curious coincidence both were found, after the near depth was broken, to represent different wheel settings from those used in the first message. The fifth χ indicator differed between the two messages.

It was clear at the beginning therefore that the two message settings differed only in the settings of the χ wheels and further that the settings of the 3rd and 4th χ wheels were the same. Moreover the messages were stated in the clear preambles to be 3rd. and 2nd parts of messages (presumably the same message) respectively. From experience with the decodes of July and August 1941, and of March 1942 the clear messages were expected to begin with

DRITTER9TEIL9DES9SPRUCHES9

and

ZWOTER9TEIL9DES9SPRUCHES9

or equivalent phrases, respectively.

The initial problem was to find two such phrases which when added together gave a result which agreed in the third and fourth impulses with the sum of the two cipher messages. This problem was solved without difficulty and the wheels completed. (The screed of the Research Section contains further details of this job.)

(b) Setting

When the wheel patterns had been obtained the April depths were set, and then messages whose clear language was unknown were studied. The process of message setting was carried so far that the indicator system was completely solved.

At this stage, early in May, 1942, it was possible to draw conclusions about the periods over which the wheel patterns remained valid. It was found that the patterns of the motor

wheels changed every day, and the χ patterns changed at the beginning of each month. The patterns of the ψ wheels, it was found, had changed at the beginning of April, and they were constant over each of the months March and April. But it was remembered that the same ψ patterns were used in August as in July of 1941 so it was suspected that the ψ patterns were constant over a period of several months. Three months seemed a likely period, since the first set of ψ patterns had presumably come into force at the beginning of July 1941.

A curious difficulty arose out of the first letter of each message, which never seemed to decode according to the rules. This effect was not understood until the studies described in the next section had been made.

42E THE INDICATOR METHOD

(a) General Tunny position in April 1942.

The Research Section had achieved great success with the March and April messages. The complete decoding of all this traffic would have been possible if suitable machines had been available at the time. (As a result, while this analysis was proceeding, it was decided to have such machines made; the first one came into operation at the beginning of June, 1942).

But the mastery of the problem was not so complete as the March and April success might seem to indicate. No way of breaking a length of key, without independent information was

known, and the only independent information that would suffice seemed to be a knowledge of one of the χ patterns, or of a number of alternatives for such a pattern. The only way of getting a length of key with this additional information, seemed to be by the study of a near depth, for which the two indicators concerned differed only in the last five letters. The Germans could not be relied upon to send such near depths at the rate of one a month.

It seemed possible that a pair of messages whose indicators differed only in one of the first five letters, so that only one ψ wheel was differently set in the two messages, might also be breakable. However there was never any occasion for the Research Section to attempt the feat of breaking such a pair.

One possible line of research would have been the search for a new method of breaking into a length of key, so that wheel patterns might again be derived from true depths. It was not until July, 1942 that such a method was discovered, (by Turing).

Even such a method would have been useless in the case of a month in which no depth had been sent, and there had been several such months.

(b) Idea of using indicators for breaking the wheels, May, 1942

The Research Section sought therefore for a method of machine breaking independent of depths. It seemed possible that such a method could be developed from a study of the indicators and first few cipher letters of a sufficiently large number of messages. Even if the process was not carried on to completion it might give the pattern of a single χ wheel and thus permit the breaking of a machine when a depth was available.

A study of the May messages was therefore begun as soon as about 10 days traffic had accumulated. The workings have not been preserved, but similiar workings for June still exist.

(c) The first experiment

In the first experiment which was made, the fifth impulse of the second letter of each cipher message was tabulated against the fifth and twelfth indicator letters, corresponding to the fifth Ψ and χ wheels respectively. The row, and also the columns, were lettered in order from A to Z, excluding J, which had never been used as an indicator letter. The fifth impulse of the second letter of a cipher message was entered in the row whose letter was the Ψ indicator, and the column whose letter was the χ indicator. Several hundreds of messages were used.

Many of the 625 squares contained more than one entry, but it was very rare to find two different signs in the same square. This confirmed the assumption that almost all the messages began in the same way, and also showed that the setting of the Ψ wheel for the second letter was fixed uniquely by the Ψ indicator. A very similiar effect was found when the fifth impulse of the third cipher letter was tabulated in the same way, but when the fifth impulse of the fourth letter was tabulated, very many cases of different signs appearing in the same square were found. It was deduced that the movement of the Ψ wheel was the same for all messages up to the third letter, but that between the third and the fourth letters the wheel could either advance one place or else stay still.

Another count was made for the fifth impulse of the first letter. This count differed from all the others in that nearly all the entries in any one column were the same. This showed that only the χ wheels were effective in the encipherment of the first letter.

Similiar results were obtained for the first and third impulses. The other two were avoided because they are the ones in which + and Z differ, so that these two impulses would, it was thought, present more difficulty than the others.

The difficulty that had been presented by the first cipher letter in March and April was now explained, and it was no longer a matter of complete indifference whether the wheel patterns of a Tunny machine were reversed or not. This property of the first letter was peculiar to SZ 40 (the first model of the German Tunny machine).

(d) Construction of pattern fragments.

On the assumption that almost all messages began with a group of +'s, followed by a group of Z's it followed that nearly every message began, in the fifth impulse with a sequence of crosses. (At least 6 crosses, to judge by the March and April traffic). Since the ψ wheel did not operate in the first place, the nature of the χ character in the wheel-setting corresponding to each χ indicator could be determined from the count of the fifth impulse of the 1st letter. Since each setting of the 23-wheel corresponds to some indicator letter, the number of crosses in the pattern of the fifth χ wheel could at once be deduced. It was found to be 11. Of course the count of the first letter did not suffice to determine the pattern of the wheel, since the wheel settings were not in the

order of the indicator letters.

The analysis of the count of the 2nd letter was more complicated since the Ψ wheels were now operative. Each cipher character was the sum of a clear character assumed to be x, a χ character fixed by the χ indicator, and a Ψ character fixed by the Ψ indicator. However, if a particular χ character was assumed to be dot, the values of a number of Ψ characters could be deduced from the row of the square correspondi to that χ character. Then more χ characters could be deduced from these Ψ characters, and so on. This process was carried on until it terminated, and so sets of χ and Ψ characters were obtained. Since these led to very little inconsistency, they were assumed to be the correct ones. Some of the Ψ characters were uncertain, since the corresponding rows were almost empty, but all the χ characters were obtained with a fair certainty. The first assumption, that a particular χ character was x, might have been wrong: it would have then been necessary to reverse all the χ and Ψ characters finally obtained. This point was settled by usin the fact that the number of crosses in the fifth χ wheel was 11.

The count of the third letter was analysed in the same way. It was found that the Ψ wheel always moved on between the second and third letters.

We will now summarize the information which had been obtained at this stage. We shall use the term "pattern-fragment for A" to denote a short sequence of dots and crosses in a wheel beginning at the setting which, with the indicator A, corresponds to the first letter of the message in the case of a χ wheel, and to the second letter in the case of a Ψ wheel

The pattern-fragments of the fifth χ wheel were known to three places, and the pattern fragments of the fifth Ψ wheel were known to two places. A check on the working was now possible, for by the nature of the Ψ wheels the pattern

fragments .x and x. should have been much more common than the pattern fragments .. and xx . The pattern fragments actually obtained were found to fulfil this requirement.

(e) Extension of the fragments

The next step was the analysis of the fifth impulse of the fourth letter. This was expected to be more difficult, as either the second or third characters of the Ψ pattern-fragment might be used in any given message. In all the motor keys of March and April the proportion of dots to crosses was 11 to 26, so the effect of the third signs of the Ψ pattern-fragments was expected to predominate.

In some rows of the square it very seldom happened that two different characters were entered in the same small square. This evidently meant that the second and third characters of the corresponding Ψ pattern-fragments were the same. Conversely rows in which there were many cases of different entries in the same square corresponded to pattern fragments whose second and third characters were different. Thus many third characters of Ψ pattern-fragments were deduced merely from the quality of the corresponding rows. The analysis was completed as for the earlier letters, and thus many Ψ pattern-fragments were extended to 3 places, and most χ pattern-fragments to four places

There were more ambiguities this time than there were before, because of the messages in which the second characters of the Ψ pattern-fragments were used in the fourth place, so one or two χ characters, and several Ψ characters could not be determined by this analysis. But it was known that the results obtained did not need to be reversed, (by the argument from the qualities of the rows).

The missing characters in the χ pattern-fragments were easily filled in by using the fact that the fragments had to fit together to form a wheel. Thus for example the number of fragments four characters long beginning with x.x had to be equal to the number of such fragments ending with x.x .

The same kind of analysis was applied to the first and third impulses, but with less satisfactory results, owing to the fact that not every possible pattern-fragment in the corresponding χ wheels corresponded to an indicator letter. Thus although χ and Ψ fragments were obtained it could not be decided whether or not these Ψ fragments and the parts of the χ fragments from the second letter onwards ought to be reversed, and the argument that the χ fragments must fit together, (with others) to form a wheel was not so readily applicable.

It was now possible to get further characters of some of the χ fragments, and gradually to build up all possible χ_5 patterns. There were rather less than 10. These were applied in turn to key from two rather corrupt depths, and the May wheels were completed before the month was quite over. (This was something new). As the settings for most of the χ_5 indicator letters (and som others) were known with certainty, the setting of the other May messages was comparatively easy.

(f) June and July, 1942

The wheel patterns for June and July were also broken by the Indicator method. In June no depth was found and the problem was correspondingly more difficult. It was necessary to extend the χ_5 fragments until only one wheel could be formed from them. In July a good depth (yielding several hundred letters of key) was intercepted early in the month. The analysis was completed

before 18th July and current traffic was read for the first time.

(g) Later uses of the method

Refinements of the Indicator Method, whereby the second and fourth impulses were given equal status with the others, and whereby a complete and systematic determination of the wheel patterns was made possible, even when the Ψ patterns were initially unknown will not be described here.

It may be noted however that analysis by indicators still proved possible and useful, even when the stereotyped beginnings were replaced by arbitrary padding words as was the case from the middle of August onwards. However, after July, Turing's method for analysing key from true depths was available, and wheel patterns for September and October were actually broken on depths and near depths. The indicator analysis was used only for the breaking of the indicator substitution.

At the end of July work on the Tunny cipher by the Research Section came to an end, and was all taken over by a special "Tunny" Section. Later however the Research Section made another contribution in the shape of the Statistical Method.

43 TESTELY METHODS 1942 - 44

43A. BREAKING TUNNY AUGUST - OCTOBER 1942.

The first major job of the newly formed Tunny section (see 14A (b)) was to break the August wheels. The indicator method described in 42E was applied and for the first 10 days the traffic responded well, except for the bad corruption caused by exceptionally poor intercept conditions. But from the 11th onwards only a very few messages seemed to produce the stereotyped openings. By working only from those messages which were using the regular and predictable openings progress was made until it became clear that the others opened with German words, - the padding sentences or quatsch which continued as the invariable preliminary to the message text throughout Fish history. It was often possible to predict the next letter of partially obtained words and thus progress was made, using much more material than required in previous months, until a [illegible] had been built up by the time the Germans sent a depth on the 27th.

To meet the introduction of quatsch, research into German plain language in its teleprinter impulse form was carried out, and it was thought that the indicator method was still possible though immensely slow and difficult. But the findings were never put to the test for on September 5th a depth was sent which provided easily enough key to break the wheels on the recently evolved Turing method (see below 43B). At this stage the position of only one indicator on each wheel was known (that of the depth) whereas the indicator method had enabled a number of indicators to be placed on the wheels

as soon as the full patterns were obtained. The initial stage of setting individual messages (for method see 42A) was therefor more difficult. The last month of the indicator era, October, was broken from a near depth.

43B. TURINGERY.

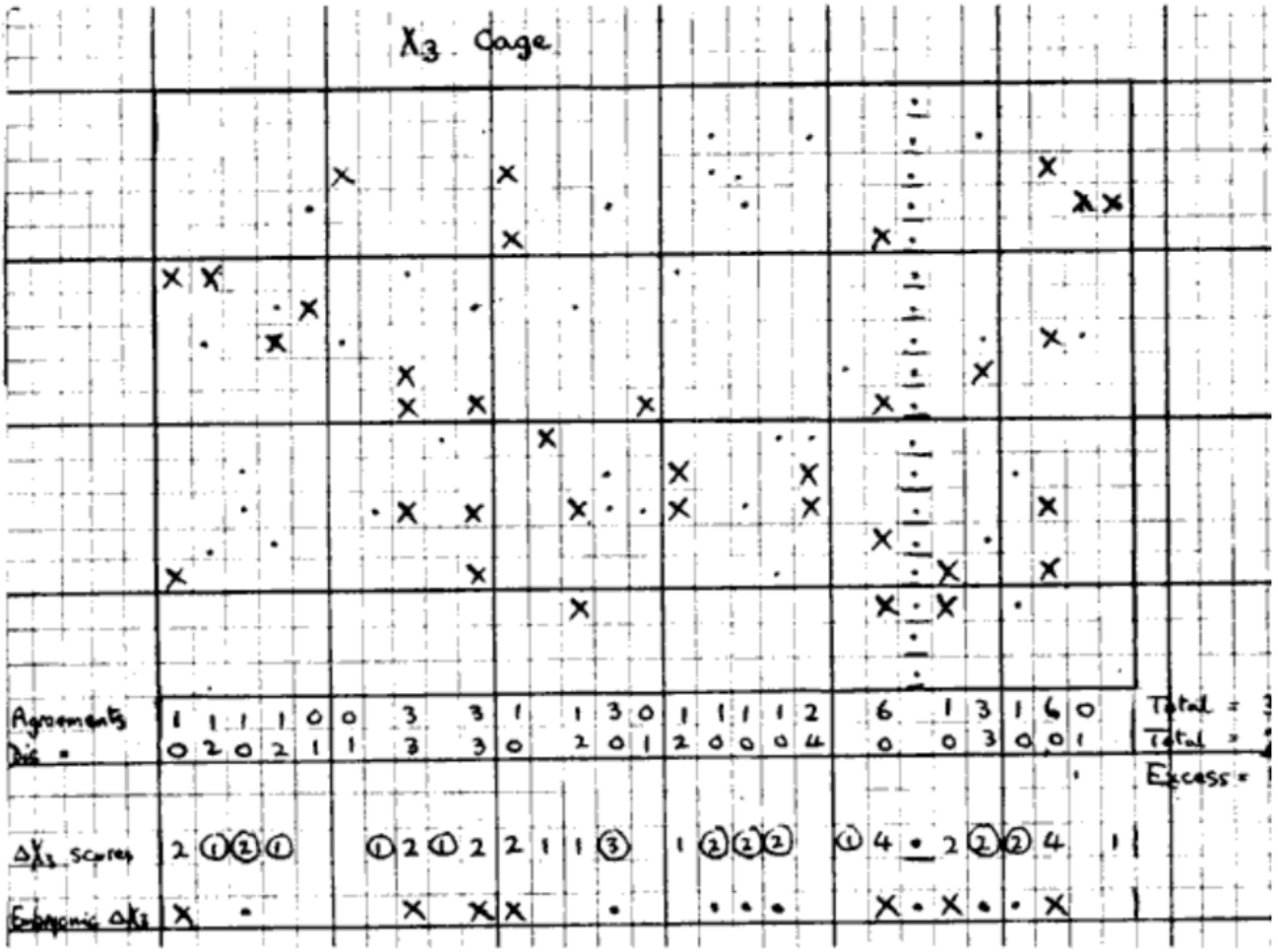
The original method of key breaking clearly became useless as soon as the Germans introduced the condition $ab = \frac{1}{2}$. So research was done by A.M. Turing on the key from which the July wheels had been broken by the indicator-cum-depth method, and a method was evolved which produced the correct wheels. The introduction of QSN's (later QEP's) in November 1942 dealt the death blow to the indicator method and left Turingery as the only known way of breaking wheels.

Turingery introduced the principle that key differenced at one, now called ΔK, could yield information unobtainable from ordinary key. This Δ principle was to be the fundamental basis of nearly all statistical methods of wheel-breaking and setting. Many improvements and refinements of technique have since been made enabling very much shorter lengths of key to be broken than the 500 or more required by original Turingery. The technique of modern wheel-breaking from key is given in Ch.26. The original method is described here. The description gives a certain amount of rationalisation of the process which could certainly not have been given at the time since the principles involved had not been studied and understood to the extent that they were later.

The property used throughout is simply
$P(\Delta\psi'_{ij} - \cdot) = b$, or, in different terms, $\Delta K_{ij} \xrightarrow{b} \Delta\chi_{ij}$.

ΔK is written out in ink on squared paper. The 5 rows

of squared paper beneath are regarded as corresponding to the 5 TP impulses and each impulse is marked off with an upright ink line according to the chi length of that impulse. All subsequent work is done in pencil. A letter of ΔK is arbitrarily chosen and assumed to have $\Delta\Psi' = /$. On the Tunny machine of the time the psis came in at the second letter and moved on automatically from the second to the third place. So the third place of ΔK was the first possible TM dot. At the assumed $\Delta\Psi' /$ position we enter the $\Delta\chi$ letter in impulses ($= \Delta K$ since $\Delta\Psi' = /$), and the 5 $\Delta\chi$ signs thus derived are entered on their respective chi-periods throughout the ΔK. These signs are underlined to distinguish them from other $\Delta\chi$ signs deduced from them. Now from every $\Delta\chi$ sign thus entered we can use the property $\Delta K_{ij} \longrightarrow \Delta\chi_{ij}$ to deduce one $\Delta\chi$ sign on each of the other four impulses. For if the underlined $\Delta\chi$ character is on impulse i and gives $\Delta\chi_i = \Delta K_i$, then in accordance with the above property we deduce $\Delta\chi_j = \Delta K_j$, for $j =$ each of the other 4 impulses, thus obtaining 4 'fresh' $\Delta\chi$ characters which each have probability $\frac{1}{2}$, provided that the position originally selected is in fact a TM dot. Similarly if we find $\Delta\chi_i \neq \Delta K_i$ we assume $\Delta\chi$ on the other four impulses to be the opposite of ΔK. These deduced $\Delta\chi$ signs are written into 5 'cages' of width 41,31,29,26 and 23 respectively. Thus all signs deduced for $\Delta\chi_3$ from underlined $\Delta\chi$ signs on impulses 1,2,4 and 5 are written out on a width of 29. An example of a $\Delta\chi_3$ cage is given below,


X3 Cage
Agreements
Dis •
Total =
Total =
Excess =
ΔX3 scores
Erroneous ΔX3

It will be seen that the underlined $\Delta\chi_1$ sign is also written into the cage each time it occurs as a check against inadvertently sliding the cage to right or left when entering. We now use these 5 cages as a test of the original assumption of a TM dot. For if the original assumption is correct the ratio of agreements to disagreements among the signs in each column of the cage will be $b^2 + 1-b^2$ to $2b(1-b)$, or $(1+\beta^2)$ to $(1-\beta^2)$. We therefore write the number of agreements and the number of disagreements at the bottom of each column (see Fig. (I)) and add up the total excess of agreements over disagreements for all 5 cages. Each excess contributes a factor of $\frac{1+\beta^2}{1-\beta^2}$ to the theory that the original position has $\Delta\psi' = /$ (or $\Delta\psi' = \backslash$ which merely makes all our $\Delta\chi$'s inside out). If the result is poor we scrap the cages, erase the workings and take the next ΔK letter as our $\Delta\psi' = /$ assumption. If it is good we accept the original assumption. In that case the cage entries each have a probability b of being correct and can simply be totted up in columns, and written at the bottom as ringed or unringed numbers according to whether they are scores in favour of the particular $\Delta\chi_1$ character being dot or cross (see Fig. (I)). Accepting scores ≥ 2 we form rudimentary $\Delta\chi$ wheels with which we de-chi the ΔK to give rudimentary $\Delta\psi'$. We examine thus $\Delta\psi'$ to find a character with 3 or more dots, not counting dots generated by an original underlined $\Delta\chi$ sign. This we assume to be another position where $\Delta\psi' = /$, and re-apply the cage test described above. If the proportion of agreements is poor we try another assumed $\Delta\psi'$ / . If it is good we derive $\Delta\chi$ scores as before by summing the columns and combine these with the previous scores by straight addition, provided that the agreement between scores is reasonably good. Again taking a standard of ≥ 2 we form 5 embryonic $\Delta\chi$'s from the combined scores, with which we de-chi the ΔK to give

embryonic $\Delta\Psi'$.

We make a 'count' for $\Delta\chi_5$, which is the shortest wheel and therefore will accumulate the most evidence per character. The system of scoring is as follows. For each $L_{m,n}$ in $\Delta\Psi'$ (considering only the other 4 impulses) (where $L_{m,n}$ is a letter with m dots and n crosses) we score $m-n$ for the theory that $\Delta\Psi'_5$ = dot, and that therefore $\Delta\chi_5 = \Delta\kappa_5$ at that place. Thus if the $\Delta\Psi'$ letter reads x ? · x in the first 4 impulses, and the ΔK letter is Q we score ① for $\Delta\chi_5$ = dot. We write in all these scores throughout the key on a width of 23, and add up the columns to give an improved $\Delta\chi_5$. With this we de-chi $\Delta\kappa_5$ in place of the earlier $\Delta\chi_5$ used, and count for $\Delta\chi_4$. This process continues, going back to $\Delta\chi_5$ after $\Delta\chi_1$, until all the $\Delta\chi$'s are completed. These $\Delta\chi$'s must obviously integrate into legal undifferenced chis, the even or odd number of crosses in the $\Delta\chi$'s will tell us whether the original assumption was a $\Delta\Psi'$/ or 8. With the undifferenced chis obtained, from the $\Delta\chi$'s we de-chi the undifferenced K to give Ψ', from which we derive the psi wheels by taking out the extensions.

43C. THE PRE-NEWMANRY QEP ERA.

(a) Introduction of QEP's.

At the end of October, 1942 Tunny was replaced by Codfish (Saloniki - Berlin,) [redacted] and Octopus (see 14A(b)).

Indicators were replaced by the QEP system. This meant a serious reduction in the amount of traffic decoded because we had to rely entirely on depths. Fortunately the Germans sent frequent and sometimes multiple depths - sometimes as many as 10 messages on the same QEP number (or QSN number as it was at first called). Keys were broken from depths as before, but the wheel settings had to be found for each depth broken for a month for which the chi and psi patterns were known. The method for doing this is described below. The motors constructed in the same way as those used in Tunny.

(b) Setting depths with no-limitation motors.

The P obtained by anagramming the depth is added to Z to form K. Where it is not possible to determine which P belongs to which Z the second possible K has to be tried if the first fails.

K_5 is written out and de-chied at all 23 possible settings of χ_5 to give 23 possible versions of Ψ'_5. This process is called 'making a drag'. The problem is to find the true Ψ'_5. The majority can be discarded immediately because it can be seen at once that they cannot fit the known Ψ'_4 whatever extensions are assumed. This process is greatly helped by the fact that the Tunny type μ_{61} and μ_{37} only have singleton dots and therefore cannot give more than two consecutive dots in TM. The remaining candidates are examined by reference to another impulse in the following manner.

For each assumed Ψ'_5 pattern, all TM dots which have to be assumed for the pattern to fit Ψ_5 are marked. At each of these places we know that $\Delta K = \Delta\chi$. So at all χ_4 settings which satisfy this condition we de-chi K_4 and examine the resultant possible Ψ'_4's. Unless the key is very short (the length normally used is from 14 to 30) the correct χ_4 setting based on the correct χ_5 setting will yield a Ψ'_4 pattern which when contracted by using the assumed TM dots will fit on the known Ψ'_4.

We then do the same for Ψ_3 and so on until all psis and chis are set. It remains to anagram by using the known psis and chis sufficient to break (or, if the motor patterns are known, to set) the motors.

(c) Advances in Key-breaking

Recognising the psi repeat and numbering , were devised in the winter of 1942 and were never discarded (See 26b).

(d) Setting depths on $\bar{\chi}_2$ limitation

The $\bar{\chi}_2$ limitation first appeared in February, 1943. The number of dots in μ_{37} was doubled to give the same proportion of dots in TM as before. The $\bar{\chi}_2$ limitation necessitated changes in setting and motor working and caused some changes in Key-breaking methods.

The method of setting depths on $\bar{\chi}_2$ limitation is essentially the same as with the "No-limitation" motor. But the drag is made on K_2 instead of K_5 and use is made of the fact that for each setting of χ_2 used, we know where the compulsory crosses in TM fall and therefore we know where we are not permitted to assume extensions when trying to fit possible Ψ'_2 on to Ψ_2 . On the other hand we no longer have the useful feature of the old type motor, which precludes more than two consecutive TM dots.

(e) The effect of $\bar{\chi}_2$ limitation on key-breaking

Turing's original method had already been modified in two respects (see above (c)). With the introduction of $\bar{\chi}_2$ limitation a certain amount of use was at once made of this new feature in key-breaking, though it was realised at the time that it should be possible to make very much greater use of it. The powerful methods for using $\bar{\chi}_2$ which were finally perfected in early 1945 are described in 26 At the time, however, use was only made of the limitation to obtain χ_2 after one other chi had been obtained and the psi repeat recognised. This was done by examining the TM deduced from the Ψ' already obtained, when written on a width o 31. All TM dots imply $\bar{\chi}_2 = x$ and columns where no dots appear are extremely likely to correspond to a $\bar{\chi}_2$ dot. This allows us to infer most of $\bar{\chi}_2$ which is then slid one to the left so that it becomes χ_2 and is then compared with the $\Delta\chi_2$ values obtained from the last Turingery count for $\Delta\chi_2$ to have been made. The combination of the two should give a complete χ_2 which is then added to K_2 to give Ψ_2'. This Ψ_2' combined with the use of the known $\bar{\chi}_2$ should place most, if not all, of the TM dots whose position is ambiguous.

The disadvantage of the new modification was that recognising the psi repeat was made much more difficult because the old rule disallowing more than 2 consecutive TM dots no longer held.

(f) A new feature

In the early months of the QEP era a new feature appeared. Messages no longer invariably began and ended with the beginning and ending of transmissions, nor did transmissions beginning in the middle of messages start with "Zwoter (etc) teil . . . ". No serious difficulties were caused, apart

from the greater difficulty of breaking depths, and later de-chis, because we could no longer rely on the starts of transmissions containing stereotyped message beginnings, though a fair proportion still did.

(g) The Herring link and the first appearance of $\overline{\chi}_2 \overline{\overline{P}}_5$ limitation

The Rome-Tunis link known as Herring operated between December, 1942 and the final collapse of the German forces in Tunisia in May, 1943. It was on this link that both the $\overline{\chi}_2$ and $\overline{\chi}_2 \overline{P}_5$ limitations first appeared. The method by which the $\overline{\chi}_2 \overline{P}_5$ limitation was analysed and its method of working understood is described in Ch.44. The $\overline{\chi}_2 P_5$ limitation effectively prevents messages being in depth even when the initial settings are the same owing to the divergence of the two Ψ''s under the influence of the different P_5's. This work on Herring was made impossible, until the operational difficulties of passing a great quantity of traffic under pressure using the new P_5 attachment proved too great (a single fifth impulse corruption in reception would cause a breakdown, necessitating a complete retransmission) and the attachment was abandoned. - (to reappear on nearly all links in December, 1943). From then on the Germans sent an enormous quantity of traffic; the majority was sent in depth (often multiple depth), presumably because they could hardly spare the time to reset their machines. The effort and production of the Testery reached an unprecedented peak, at a time when the messages broken were of great operational importance. In May the section decoded over 1,400,000 letters, a figure which was not equalled until March, 1944, when the Newmanry was in full swing.

43D THE FOUNDATION OF THE NEWMANRY AND AFTER

(a) Early days

In July, 1943 Mr. Newman formed his section, to set messages not sent in depth, by mechanical and statistical methods. Since the introduction of QEP's these messages had not been touched. For the first few months the Newmanry was struggling to put its work on an operational basis. The Testery occasionally helped them by hand-breaking messages set on $\chi'_{1,2,4}$ and s and the motor. A print-out of D_{1245} was provided with TM printed above. A break was obtained opposite a run of dots in the TM and then extending the break both ways with the aid of nearby TM dots until sufficient had been read to set $\Psi'_{1,2,4}$ and s uniquely. χ_3 and Ψ_3 were set as in setting a length of K, described above (43C (b) and (d)). K is produced by adding Z to the P obtained, and since all the TM dots are known it is a simple matter to find the setting of χ_3 which gives $\Delta\chi_3 = \Delta K_3$ at all TM dots, and then to add at the correct setting to K_3 to give Ψ'_3.

(b) Further advances in key-breaking

(i) Accurate scoring

In the summer of 1943 the Germans reduced the number of dots in the Bream μ_{37} from 22 to 16. This made key-breaking by Turing's original scoring system extremely slow and difficult, and stimulated the first attempt to make key-breaking scoring more accurate. Accurate scoring in its final form is described in 26C .

(ii) Δ^2 properties

The next discovery to have an effect on key-breaking techniques was made in September, 1943 (see RO pp 53,54). It was that $\Delta^2\chi \longrightarrow \varkappa$ with probability about 2/3. Unlike the property $\Delta\psi \longrightarrow \varkappa$ the new property was found to lack rigidity. The way in which it is applied is described in 26B(d)

(iii) The discovery of $\hat{\chi}_2$ (see 26B (b))

The discovery of $\hat{\chi}_2$ was made on Squid for November, 1943, for which 880 key had been obtained from depth. It had 22 dots in μ_{37} and $\bar{\chi}_2$ limitation. The discovery had far-reaching repercussions. Its ultimate effect on key-breaking is described in (26B(d)), and on chi-breaking from Z in (25E) It led directly to the breaking of wheels from cribs (See 27G) And lastly the level of significance of the $\hat{\chi}_2$ count or run proved an invaluable test as to (i) whether a given key was on $\bar{\chi}_2$ limitation or not and (ii) in the case of certainty of $\bar{\chi}_2$ limitation a priori, but ambiguous key (see 28A (e)), which of the two alternative keys was the true one.

(iv) Key-breaking rationalised

In the autumn of 1944 the $\bar{\chi}_2 \bar{\Psi}_5$ limitation began to be dropped on Western links, and, since we were now in the era of daily change, (see above (f)) breaking wheels from depth once more came into prominence. The accurate scoring formulae devised in the summer of 1943 on the basis of 16 dots in μ_{37} (see above (b) (i)) were dug up and recalculated on the basis of 18½ dots in μ_{37} (see 26C Y (d)) as being nearer to the average expected dottage and also as giving convenient values for a and b (a = 3/4, b = 2/3). The test for the sign of the k (see 26 C) and the 5 by 5 flag (see 26B (a)) were devised, and the Newmanry at the same time invented the powerful χ_5 composite flag (see 26B (c)). The immediate result of this

work was that the length of key and the length of time thought necessary to break the wheels were divided by about 2 and 4 respectively.

At the same time research on key-breaking for $\bar{\chi}_s$ limitation was begun, and after some months of evolution the method reached its final form as described in 26B(b), 26E

(c) The first de-chis

When the $\bar{\chi}_s \bar{\bar{P}}_s$ limitation was reintroduced in mid-December, 1943 it was no longer possible with the equipment of that time to set the motors and psis mechanically, and at the same time the main source of decodes and the whole source of employment for the Testery, dried up, since depths could no longer occur. So the Testery had to master the art of setting the psis by hand from the de-chis prepared by the Newmanry, and this became their main job. But, more important, the month's wheel patterns could no longer be broken from depth, and the task of breaking the wheels from Z had to be attempted. The Bream chis for January, 194. were broken within the first fortnight with the comparatively primitive equipment of the time - Colossus I (see 32(e)) was not yet in action. Two messages on the same QEP were set on the chis and de-chied. From these two de-chis, by the method of applying the psis obtained from a break in one to the other de-chi (see 28C(α)) the psi patterns were obtained within an hour. The χ_{s3} proved to have 26 dots which helps to explain this remarkably short time.

The breaking of the February Bream chis was greatly helped by the use of Colossus I. No pairs of messages on the same QEP were available, and attempts by the Testery to break the psis from the de-chis sent over were at first fruitless.

Finally however the psis were broken with great difficulty and effort from one de-chi. The Ψ_3 dottage proved to be only 19, which explained the difficulty encountered. It was now evident that the problem of the $\bar{\chi}_2$ $\bar{\bar{P}}_5$ limitation had been mastered in both sections. A detailed account of psi-breaking from de-chi is given in 26C

(d) The $\bar{\chi}_2$ $\bar{\Psi}'_1$ $\bar{\bar{P}}_5$ limitation

This triple limitation first appeared in June, 1944 on Codfish and Gurnard. Its action is described in 116(g)(iv) ; its stay was brief as in December, 1944 the Germans began taking the $\bar{\bar{P}}_5$ component out of the limitation on the various links; thus it gave rise to the $\bar{\chi}_2$ $\bar{\Psi}'_1$ limitation (see 116(g)(i), 116(g)), which became the standard limitation on the majority of links, the remainder reverting to the old $\bar{\chi}_2$ limitation. It did not cause any new difficulties apart from slightly complicating the process of de-chi breaking.

(e) Daily Change

The introduction of daily change of all wheel patterns in the summer of 1944 meant that the time and energy previously expended to release a whole month's traffic for setting now only released one day's traffic. The emphasis in the Testery as well as the Newmanry changed from wheelsettin to the much more difficult job of wheelbreaking. But the concerted efforts of both sections met with such success that the production figures for August, 1944, the first month with daily change on all links, was higher than ever before, and the figures continued to rise steadily month after month.

44 - HAND STATISTICAL METHODS

44A INTRODUCTION OF THE QEP (QSN) SYSTEM

(a) Codfish and Octopus

At the end of October, 1942, there was a complete change in the nature of the Tunny traffic. The Tunny link itself closed down, and it was for a time supposed that the Germans had abandoned the "Tunny" cipher machine. Two other teleprinter links (called Codfish and Octopus) came into operation at this time, and it was shown, by the analysis of depths of three that both these links were using the "Tunny" machine. These links did not transmit twelve letter indicators, but only a "QSN" number (QSN was later replaced by QEP). Messages having the same QSN number on the same day and belonging to the same link were, it was found, in depth.

(b) Depths

Messages were soon being sent in greater numbers than ever, but now only those messages which were in depth with others could be read. So during the first half of the year 1943, the Tunny Section confined itself to the reading of depths.

Fortunately the German operators began to send depths in great profusion, and so on many links it was still possible t read a fairly large fraction of the traffic. (From this

time on, many new links were coming into operation, or were being discovered.)

Codfish was one of the links which gave a large proportion of depths. Depths of more than a dozen messages were not unknown on this link. Octopus depths were much rarer.

(c) The New Cryptographic Problem

It was found that each link had its own set of wheel patterns, that χ and ψ patterns were changed monthly, and that motor wheel patterns were still changed daily. Here the was one difference from the old Tunny link, for which it had been demonstrated that the ψ patterns were changed only quarterly.

The Germans could not be relied upon to continue to send such a proportion of depths, and in any case the single messages presented an urgent problem. The wheel patterns for a link could be obtained from the depths but there seemed to be no way by which single messages could be set on these patterns.

It was clear that single messages had now to be considered in isolation, for it was no longer possible to relate them to one another by means of their indicators, as in the method of analysis described in 42E. Had there been reliable cribs, the method of message-setting described in Section VI could have been employed, but the Germans had now taken precautions against the use of stereotyped beginnings, the chief precaution being the use of padding words. Sometimes a fairly reliable crib for a link would be found, but positions of the crib in the message was then so variable that the method was still not practicable.

The only hope left was that it might be possible to set messages by using the statistical properties of the plain language, or extended psi-stream.

44B SETTING - STATISTICAL METHODS

(a) First ideas - P characteristics.

An attempt was made early in 1942 to set χ_s and ψ_s for a message by using the observed fact that dots predominated markedly over crosses in the fifth impulse of ordinary Tunny plain language. This was not successful but the possibility of using this effect was again investigated. The chief difficulty was the irregular movement of the Ψ wheels, but it was hoped that the Ψ' key could be approximated to sufficiently closely by using a standard motor key instead of the unknown true motor key. The theoretical investigation showed that success might just be possible with $ab \neq \frac{1}{2}$ but that no success could be expected with $ab = \frac{1}{2}$. The reason for this was closely connected with the predominance of changes in the ψ pattern: when the assumed setting of a Ψ wheel was one place off the true setting, the resulting sign in the assumed Ψ' key was more likely to be wrong than right.

(b) $\Delta\Psi'$ characteristics.

In another investigation, no attempt was made to use the periodicity of the unextended Ψ impulses but an attempt was made to derive a statistical method from a consideration of the other non-random properties of the Ψ' key. These are:

(1) All five Ψ wheels have the same movement

and (ii) In the unextended Ψ impulses, changes are much more frequent than continuation.

These properties, it was thought, could best be expressed in terms not of the actual Ψ' key, but of its first difference, which we denote by $\Delta\Psi'$. Changes and continuation in Ψ' are represented by crosses and dots respectively in $\Delta\Psi'$.

At this time, as in March and April, 1942, the Germans always arranged that $ab \doteq \frac{1}{2}$, so that dots and crosses were equally frequent in each impulse of $\Delta\Psi'$. Hence no statistical method could be founded, it was thought, on the statistical properties of $\Delta\Psi'$.

But suppose, it was argued, that two impulses of the $\Delta\Psi'$ key, say the first and second, are added together. The resulting sequence $\Delta\Psi'_1 + \Delta\Psi'_2$ will have a dot in each position corresponding to a dot in the motor key, and in the positions corresponding to crosses in the motor key, the proportion of dots will be $b^2 + (1 - b)^2$, and the proportion of crosses $2b(1 - b)$, if, as an approximation we take the same value of b for each impulse. But then the proportion of crosses in the entire sequence will be

$$2ab(1 - b) = 1 - b$$

and therefore the proportion of dots in the sum of any two impulses of $\Delta\Psi'$ will be equal to b and about 70%.

It was deduced that the first step in any statistical method of wheel setting should be the differencing of the cipher text and the addition of two impulses of the resulting stream of letters.

All now depended on the properties of $\Delta P_1 + \Delta P_2$. Counts

were made on the clear texts of some Octopus messages, and the value .63 was derived for the proportion of dots in $\Delta P_1 + \Delta P_2$ averaged over these messages. This effect seemed to be due, largely to the high proportion of double letters in Octopus clear in which long drawn out punctuation signs such as+++MAA8889 were used.

It followed that, for the sample taken.

$$P(\Delta D_{12} = .) = .55$$

and that this property of D was sufficiently marked for it to have been possible uniquely to determine the χ_1 and χ_2 settings for one of the Octopus messages whose P had been counted.

(c) Chis set successfully

An attempt was then made to set an unbroken message by this new method of the " 1+ 2 Break In". A systematic method of testing the 1271 possible $\Delta\chi_1 + \Delta\chi_2$ settings had to be devised. The sequence $\Delta\chi_2$ was added to $\Delta z_1 + \Delta z_2$ in an arbitrary setting, the numbers of dots and crosses in $\Delta z_1 + \Delta z_2 + \Delta\chi_2$ corresponding to each position in the 41 period were tabulated and then this table was compared with each setting of $\Delta\chi_1$. This process was carried out for every setting of $\Delta\chi_2$. It was found convenient for this process to write $\Delta z_1 + \Delta z_2$ diagonally into a rectangle, of sides 31 and 41.

A message of length about 4000 letters, which did not belong to a depth, was taken, and a significant result was obtained for the first two impulses. The same process was then applied to some other pairs of impulses and by combining the best results for all these pairs, the other three χ wheels were set. For later messages it was found sufficient, after

χ_1 and χ_2 had been set to work only on pairs of impulses for which the setting of one χ wheel was known. The settings of the other χ wheels would then be comparatively simple with good messages.

(d) Motors and Psis set.

When all the χ wheels of the first message had been set, the χ key was added to the cipher text, and the sequence $D = Z + \chi$, obtained. This sequence was found to have more than twice the random number of double letters. This was presumably because both P and Ψ' contained a high proportion of double letters. But nearly all the double letters in the extended Ψ key would correspond to motor dots and therefore most of the double letters in the de-chi would correspond to motor dots.

It was found that, by an analysis of the distribution of the probable motor dots the patterns of both motor wheels could be derived. The method used was analagous to that later used for motor breaking on machines with limitation, and described in Ch.28.

A controversy broke out in the Research Section over the problem of the best method of continuing the analysis from this point. Some held that the Ψ wheels should be set statistically by striking out from the de-chi all letters corresponding to extensions of the Ψ-key and then setting the Ψ wheels on th 'contracted de-chi' just as the $\Delta\chi$ wheels had been set on the differenced cipher message. Others held that attempts should be made to guess the clear at some point of the de-chi, and thus to obtain a short stretch of extended Ψ key, on which the wheels could easily be set. The best way to do this, they said, was to consider a place where there were two consecutive dots,

in the motor key. (There were never more than two consecutive dots in the motor keys of those days). For in such a place, three consecutive letters of the extended Ψ key would be identical, and there would be only 32 possibilities for corresponding trigram of the plain language.

In the case of the first message, the Ψ wheels were set by means of the second method, but the first method was also used successfully later on.

(e) Foundation of Newmanry

When two or three messages had been set by the statistical method, it was seen that new machinery, and a new section to operate it, was needed, for the hand methods took far too long to be of much practical use. Mr. Newman was put in charge of developements and his section came into operation later in the year. This section set the Χ wheels of their messages essentially by the method described above at first, but carried out its processes mechanically. The technique of using only runs of form $i+j$ was soon improved upon (see 23 or Part I

(f) Statistical Chi-breaking

Statistical methods were carried further by the Research Section early in 1943 when an example of chi-breaking from rectangles was carried out. 'Wheel-breaking' in the sense of chapter 25 was not used - in fact the message was so favourable that all the chis were obtained from three rectangles, namely ΔZ_{12} ΔZ_{13} and ΔZ_{45} . The motor was obtained statistically.

Further investigation into Rectangling and other statistica chi-breaking methods was carried out by the Newmanry, but it was only after the general introduction of autoclave in Dec. 1943 that these methods were used operationally.

No statistical method for motor-breaking (with limitation) was developed by the Research Section.

44C INTRODUCTION OF P_5 LIMITATION

The autoclave was first used on a single link in March 1943, before the Newmanry came into operation, but it was abandoned and was not used again until December. The analysis of messages showing the autoclave effect was one of the triumphs of the hand methods of statistical analysis.

The first sign that a new device was being used was the sending of a number of pairs of messages on the 'Herring' link the members of each pair having the same QSN number. These pairs should therefore have been depths, but attempts to break them in the usual way all failed. Fortunately this happened in the middle of the month, so the messages were expected to be usi the same wheel patterns as the earlier messages of that month, some of which had been broken. One of the messages in the unbreakable 'depths' was about 6,000 letters long, so the statistical method for setting χ wheels was applied to it. The method was completely successful. The de-chi was obtained and investigated. One passage of this de-chi contained so many repeated letters that it looked like an extended Ψ key. The passage was

Z 3 D D D D V V N A A F G O O E 8 / / / K H R R R

Q Q Q C C C C 3 8 S S W M

It was assumed therefore that in the underlying clear

language the same clear letter was being repeated over and over again. If this hypothesis were correct, each separate impulse of the passage would wither agree with, or else be the complete reverse of, the corresponding impulse of the extended Ψ key.

The hypothesis was tested by comparing the actual Ψ wheel with the various impulses. It was found that complete agreement could be secured by taking the underlying clear language to consist of along sequence of Z's followed by a long sequence of 9's. The Ψ wheels were thus set and the motor key could now be derived by decoding the message.

This was the first example of hand psi-setting from a de-c with an unknown motor key, but the de-chi was an exceptionally easy one.

The decoding process was applied to both messages of the 'depth' on the assumption, soon verified, that the initial settings of the wheels were the same for both messages. The two motor keys were different however, and the difference could only be explained on the assumption that the motor key was a function of the clear language, or cipher, as well as of the initial state of the machine.

The nature of the plain language effect was deduced by studying the actual plain language near the places in which the two motor keys differed. It was found that when they differed, there was always a difference in the two clear texts two letters back, in the fifth impulse.

Further investigation revealed that when there was a difference in the motor key, the motor sign in each message was given by the sum of the fifth impulse of the plain language two places back (denoted by $\bar{P}_5$) and the second χ sign of one place back (denoted by $\bar{\chi}_2$). This suggested that the total motor key was obtained from the Basic Motor in conjunction with the limitation ($\bar{P}_5 + \bar{\chi}_2$). This 'basic motor' could be determined whenever $\bar{P}_5 + \bar{\chi}_2$ had the value cross. The fragmentary basic motor was written out on a width of 61 and broken by the methods already devised by the Testery for dealing with motors having the $\bar{\chi}_2$ limitation.

51 INTRODUCTORY

(a) Character of chapters 51 - 58

This is a strictly functional and non-technical account of the machines used. A technical account is to be prepared by the post office engineers.

Some attempt is made to avoid statements technically false, but none to avoid statements technically vague.

(b) Terminology

The terminology is that of the layman and cryptographer: for example a switch means a lever to be pushed up and down, or a knob to be rotated. As in other parts of the report, an impulse means one of the five streams of which teleprinter letters are composed, but when the meaning is clear from the context, impulse is also to mean electrical impulse, otherwise called pulse to avoid ambiguity.

(c) Scope of the chapters

Such history as is included is a description of developmen and lacks chronology.

Colossus and Robinson receive detailed treatment, for in large measure it is the use of these machines which gives Tunny-breaking its distinctive character.

Copying machines are indispensable but less distinctive, and are treated less fully.

The specialized counting machines, Dragon, Aquarius, Proteus are treated rather sketchily because being specialized most of their functions are adequately dealt with in the description of their applications.

(d) Relative importance of machines

The pre-eminence of Colossus and Robinson is manifest.

The need for a "Tunny" machine to decode messages, or, as an intermediate step towards decoding, to de-chi them, is obvio

The need for efficiency in other copying machines is apt to be overlooked; one of them, Miles, was in fact unduly neglec in particular the production models of Miles A were vetoed. Th supply of spare parts for readers and reperforators generally has been inadequate. The hand counter is very simple and quite indispensable: a long time elapsed before a reliable one was produced. The amount of Colossus time wasted because tapes were delayed or incorrect is difficult to estimate but it is certainly very considerable.

(e) Electronic counters etc.

As a matter of general interest it may be mentioned that on the Griffiths, A counting and stepping machines, counting is in the scale

of 10 (strictly, in alternate scales of 2 and 5) and is purely electronic: auxiliary circuits which can operate more slowly however, use also mechanical relays and uniselector switches.

The earlier Robinsons counted in four electronic scales of 2, followed by four mechanical relay scales of 5.

Colossus 1 counted electronically, in three scales of 2 follc by four scales of 5.

Copying machines, whose speed per letter is much less, generally employ mechanical relays, but Miles A is largely electronic and Tunny and the decoding machines use a few valves.

(f) Use of standard components.

Many features recognized as desirable in Tunny-breaking machinery were not incorporated because they require equipment which was either non-standard or not readily obtainable, e.g. six-impulse tape. Indeed it is a recognized principle that a machine which can be assembled from standard parts, even though more complex, is preferable to a machine requiring special parts. This is due in part to availability, in part to the probability that the special parts will not work properly. This is one advantage of electronic equipment: the amazingly reliable counters of Colossus are of novel design but do not need special parts, being made from standard valves and other standard equipment.

(g) Note on the source of machines

All machines were provided by the Post Office Engineers except the counters of Heath Robinson, and some copying machines due to TRE. The maintenance of the TRE machines by P.O. Engineers was never officially authorized, a most unsatisfacto

state of affairs, in consequence of which, despite their relatively simple character, they are less reliable than Colossus.

(h) Readers and Reperforators.

There is one example of technical vagueness in this account of which warning must be given. The five impulses which constitute a teleprinter letter are transmitted over distances successively, not simultaneously, for otherwise five separate wires or other carriers would be required. Within a terminal office, however, there is no objection to the use of five wires; in some tape readers and reperforators the five impulses appear simultaneously, in others successively. Both types are used for Tunny cryptography, though for this purpose successive impulse apparatus has no advantage except availability: it is clearly much easier to add and permute simultaneous impulses.

The hand perforator, the Insert machine, Junior, Garbo, and the punch of Colossus 6 use simultaneous impulses.

Angel Tunny, and the decoding machine use succesive impulses.

Miles including Miles A) reads the five impulses simultaneou but perforates them successively.

Readers which produce five successive impulses are supposed to be called auto-transmitters.

Reperforators which punch five impulses simultaneously are supposed to be called punches.

(i) Typewriters

Similarly "typewriter" and "printer" are used indifferently for various types of electric typewriters, regenerative and non-regenerative.

(j) Impressions of Colossus

It is regretted that it is not possible to give an adequate idea of the fascination of a Colossus at work: its sheer bulk and apparent complexity; the fantastic speed of thin paper tape round the glittering pulleys; the childish pleasure of not-not, span, print main heading and other gadgets; the wizardry of purely mechanical decoding letter by letter (one novice thought she was being hoaxed); the uncanny action of the typewriter in printing the correct scores without and beyond human aid; the stepping of display; periods of eager expectation culminating in the sudden appearance of the longed-for score; and the strange rhythms characterizing every type of run : the stately break-in, the erratic short run, the regularity of wheel-breaking, the stolid rectangle interrupted by the wild leaps of the carriage-return, the frantic chatter of a motor run, even the ludicrous frenzy of hosts of bogus scores.

Perhaps some Tunny-breaking poet could do justice to this theme; but although an ode to Colossus and various fragments appeared, all seemed to have been composed in times of distress and despondency, and consist almost wholly of imprecation or commination.

(k) Number of machines in use

	MAY 1943	MAY 1945				NOTES
		BLOCK F	BLOCK H	TESTERY	TOTAL	
Robinsons	1		2		2	+ 2 near complete
Colossi		4	6		10	
Dragons				2	2	+ 1 unde construc
Proteus				–	–	+1 under construct
Aquarius				1	1	On test
Decoding machines	5			13	13	
Tunnies	1	3			3	
Miles			3		3	
Garbos			3		3	
Juniors		4			4	
Insert Machines		1	1		2	
Angels		2	2		4	
Hand Perforators		1	1		2	
Hand Counters		4	2		6	
Stickers (Hot)	3		3		3	
Stickers (cold)		3	3		6	

52. DEVELOPMENT OF ROBINSON AND COLOSSUS

(a) Introductory.

Some of the paragraphs in this chapter will not be fully intelligible without reference to the two chapters which follow: 53, 54.

A brief description of the two machines has already been given [15(b)]. The essential difference between them is that on Robinson all streams of letters are on tapes. On Colossus only Z is on a tape, the wheels being set up electrically.

(b) Heath Robinson.

In the experimental stages of Tunny-breaking, though other forms of machine were considered, it was inevitable that one using Robinson priciples should be chosen because

(α) it is easy to make.
(β) it can be adapted to any wheel length by preparing suitable tapes.

The original Heath Robinson was effective, despite what now seem intolerable handicaps:

(i) There was at first no printer: the operators (two in number) had to write down the fleeting figures on display: this was a fruitful source of error.

(ii) The distance between the gate where the tape was scanned and the sprocket-wheel which drove it was six inches, so that the stretching of tapes alone was sufficient to put tapes out of alignment.

(iii) The position counter recorded, not the relative position of the two tapes, but the number of revolutions completed: from this the relative position can be found but with great risk of erroneous calculation.

(iv) Heath Robinson would not tolerate long stretches of dots or of crosses, so that elaborate tapes, with additional opportunities for making mistakes had to be devised to avoid this.

(v) The minimum text length was 2000. If it was less, rubbish had to be inserted in such a way that it was not counted.

(vi) There was no spanning.

(vii) The forms of impos-able conditions were severely limited.

(viii) The counters were only partly electronic.

(ix) At first Heath Robinson was unable to obtain results, even if not itself at fault, because the tapes, not being subject to a proper system of checks, were incorrectly made.

As a direct result of experience with Heath Robinson all the improvements needed to remedy these defects (except spanning, whose value was overlooked till later) were incorporated by stages in Old Robinson and Super Robinson, and incorporated at the outset in Colossus.

(c) Old Robinson (Fig. 58 I,II)

The old Robinson, which followed Heath Robinson, had a special Gifford printer, which should have been far superior to the ordinary typewriter, for it printed all eight digits at once: in fact it caused endless trouble, and its records were barely

legible. The counters were much the same as before. The restrictions on strings of dots or crosses and on minimum text length remained.

(d) The basic weakness of Robinson.

The disadvantages of Heath Robinson listed above were later overcome, but there is one which is inherent in the Robinson priciple . namely, that a pattern cannot be "extended", in particular, in psi-setting, because the psi pattern could not be extended, it was necessary to "contract" the de-chi, i.e. letters opposite a total motor dot were omitted. This wasted evidence, but was quite feasible with no limitation or χ_2 limitation.

A related functional disadvantage is that stepping is necessarily uniform, so that to set wheels arbitrarily is extremely laborious: moreover when a wheel which has been stepping, is to remain at a fixed setting, its tape must be replaced by one of different length.

(e) Colossus 1.

The flexibility of Heath Robinson for experimental purposes made it easy to discover the essential requirements of a Tunny-breaking machine. As a result, Colossus 1, the original experimental model, really lacked surprisingly little for a first model. The choice of runs, though more extensive than on Robinson, was less extensive than Heath Robinson had show to be desirable: it was biassed towards runs of the form $\Delta+j=\cdot:$ these could be done by switching except in the fifth counter. Most other runs required plugging, though there was a single set of five dot and cross switches for "all counters". There were five counters, two pairs of which could be used independentl;

for double testing on χ_1, but for this is was necessary to set up the same wheel twice with a stagger of one. Operation was not very simple because of the lack of symmetry, accentuated by changes introduced without correcting the "signwriting" on the machine. There was no spanning and only a single bedstead.

(f) Colossus 2 and later.

Experience gained from the development of Colossus1 added to that from Heath Robinson, made possible Colossus2 the prototype of all later Colossi, in a form which needed very little modification.

Colossus 2 possessed from the first, quintuple testing, a generous switch-panel (including not-not), a versatile plug-panel, spanning, a double bedstead, and a greatly increased simplicity of operation.

Spanning was introduced originally for P5 limitation, but was soon found indispensable for all setting.

The chief modifications introduced later were the rectangling gadgets, devices to reduce the effect of doubtful cipher letters, and devices to make wheel-breaking easier.

(g) The rectangling gadgets.

These were added shortly after Colossus 2 came into use, and afterwards fitted, with technical modifications, to several Colossi. Score meters were added later; Colossus 6 has some special gadgets for key rectangles.

Colossus rectangling has been slightly disappointing; although the rectangle is produced in the required form, it has been found necessary to copy it onto squared paper for convergence; as a single operation it cannot be used with "not 99".

(h) The use of Colossus for wheel-breaking : not 99.

Colossus was designed for phi and psi setting, not for breaking. The first attempts to use it for chi-breaking consisted of setting up some provisional wheels and changing the characters one by one ; if the score improved the character remained changed, otherwise it reverted. It was soon realized that this was equivalent to the more rapid process of putting only one cross in a trigger, and stepping it, thus in effect using the trigger to select the characters of the wheel one by one. Essentially the same method had already been used on Robinson.

That Colossus (including Colossus 1) should prove suitable for wheel breaking justified the policy of making it as flexible as possible, but immediately demanded further improvements.

(i) Longer bedsteads, because breaking requires longer texts than setting.

(ii) Uncertain letters replaced by 9's are a nuisance in chi-setting and breaking from cipher, even if there is no slide, but it is in chi-breaking from depth key, where missing letters are a substantial part of the text that the problem becomes acute. It was found necessary to use the Q panel for the condition $Z \neq 9$, there being no "not" facility on the plug-board, and plugging all runs, which was intolerably tedious.

In consequence "not 9" was fitted, a device which imposed $Z \neq 9$, but this lost all genuine 9's also (about $\frac{1}{5}$ of the text after differencing), and was replaced by "not 99".

(iii) Multiple testing on doubted wheels is obviously of great value when setting long messages during wheel-breaking.

(iv) Intolerable delays and mistakes during wheel-breaking were caused by the need for setting up pins at the back of Colossus and complaints finally extorted the wheel-breaking panel on the front of some machines

(i) Objections to specialized gadgets.

The clamour for specialized gadgets continues : the objection to it is the difficulty of maintaining Colossi unless they are all alike : a device worth fitting to all Colossi is much more welcome.

(j) Super-Robinson.

Colossus soon replaced Robinson for setting and breaking, but Robinson remained indispensable for crib runs in which two tapes (derived from Z and P), must be compared in all

positions. A successful crib run usually produced key of such length that wheel-breaking was extremely easy. For this reason four Super-Robinsons were ordered to overcome some of the handicaps which persisted on Old Robinson, and to include spanning whose value had been proved on Colossus.

(k) Suggestions for a Super-Colossus.

Many suggestions are made in R4 pp 124-126; fundamental, trivial or even frivolous.

Perhaps the most obvious development is the logical completion of devices to deal with corruption, including spanning, on two or more stretches, slide-correction without doctoring tapes, and not 99 for all purposes including rectangling.

The difficulty of not 99 in rectangling is that the most straightforward (though not the only) method demands the subtraction of a variable number. The most satisfactory scheme would be a general facility so that, on the same counter, some letters score positively and others negatively. A generalization would be that scores from different runs could be added, each multiplied by an arbitrary constant either positive or negative. Given either, wheel-breaking would require no immediate simplification.

A small improvement would be the setting up of wheels by means of punched cards.

(l) Suggestions for Robinson.

The most pressing needs are not 99 and a longer bedstead, but the latter is a difficult mechanical problem. Multiple testing and a much larger plugboard and switchboard are desirable.

(m) Synthesis of Robinson and Colossus.

There have been various suggestions for a combined Robinson-Colossus in which all patterns are set up electrically, being of adjustable and in many cases, very considerable length. These could be set up from a tape (as on Aquarius). A further suggestion is that of making it possible to examine many positions simultaneously (as on Proteus) : this however is more than a mere modification of Colossus, and leads to such flights of fancy as a machine to combine two letters by means of an arbitrary conversion square before counting them.