Part of the "General Report on Tunny", the Newmanry History, formatted by Tony Sale (c) March 2001

INTRODUCTION

This is part of a very large (200 page) document. This section has been tackled first because of the interest in Colossus and the need to fully understand and debate the wartime use of Colossus to enable the completion of the Colossus rebuild by the Colossus Rebuild Project under the direction of Tony Sale.

A complete copy of the original document is held in the Public Record Office, UK.

It was written by Donald Michie, Jack Good and other members of the Newmanry, after the end of World War II and has only recently been declassified.

It was found to be impossible to meet the original objective of a "photo-copy" reproduction because many pages contained over 70 lines of text. As a compromise, Courier Font has been retained, together with the original page numbers. However, a wider page width has allowed re-formatting of paragraphs to "gain some lines" and fit it onto an A4 page.

The document has been produce using Optical Character Recognition (OCR), from photo copies of the original. This is a notoriously error prone task. I am indebted to Frode Weierud, Andrew Hodges and many others for correcting "garbles". Any remaining that are reported would be gratefully received and corrected.

Tony Sale March 2001

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 Nov. 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.45
	(Administration	-	-	1	2	2
	(Cryptographers	2	5	6	20	22
Engineers-	(Maintenance	-	3	9	12	15
	(Construction	-	4	9	11	13
	Wrens	16	16	28	180	273
	TOTAL	18	28	93	225	325

Finally the staff per shift was as follows:

7 Cryptographers : DO in charge of setting (TS note: DO is Duty Officer)
1 Wheel-man in charge of wheel-breaking
1 in charge of Cribs and Robinson work
2 to supervise Colossus setting
2 to supervise Colossus wheel breaking

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

15 computers
1 "Cribs" assistant
5 "Room 11" maintaining contact 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 STAF F

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		5	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 possible 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 men.

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 written up in the Research Logs. In a subsequent 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 instruction 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 V (Category - Special Duties X). No fixed qualifications were required, though a pass in mathematics in School Certificate or apparently "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 17 1/2 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 employment. None had studied mathematics at the university.

On arrival a11 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 conducted 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 basis of the jobs available. The cheerful common sense of the Wrens was a great asset. Several of them showed ability in cryptographic work and several others were trained by the engineers to undertake routine testing of machines.

31F.ENG1NEERS

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 produce 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 months

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 bad 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 systematically till the Education Committee was founded in January, 1945. This committee of four men and 14 Wrens chosen democratically arranged general lectures end "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 mathematical 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, l944 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 set.

(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 (RF) 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. Approximately 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 efforts 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 messages 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. An 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: the copies of each tape perforated were teleprinted from Knockholt. Later on the RF (Red Form) and Master Tape were sent by DR.(Dispatch Rider). 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.

W.S. 31a

M K

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

Q.E.P.	Date	T.S.	T.E.	Freq.	Pages
Trans Date	Time	Pages		Length	Copies
1st 5 Letters	Start	Quality			

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 TAPE MAKING 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 cheeks 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 ofincorrect 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 every 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 through the hand counter and stopped at the calculated position corresponding to the end of each page. The position of the entries 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.

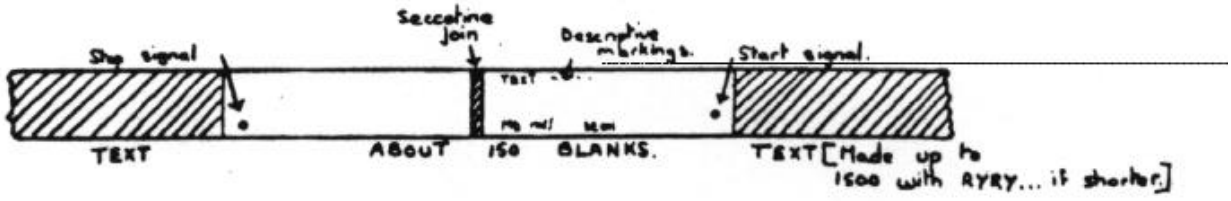
(e) Correction and Doctoring of tapes.

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 overlay of 4 between each part (1-10172, 10169 - 20340, 20337 - end) [see 53B(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 make was stuck for Colossus or Robinson and returned to the Registrar. The Tunny was not stopped during either make.

If the Delta-D 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 20th 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-D 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 Z 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 :- 2-9,62i-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 X2oneback lim) the psis were run against a de-chi tape from which all letters occurring against Total Motor dots were omitted. The contracted de-chi was made on a Tunny on which motors and X2 were set up. A special switch was used and a hand check supplied.

35F WHEEL TAPES AID 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 M37 and M61 and Total Motor tapes (for X2oneback lim) if X2 also set up. Motor tapes were sometimes required for printing the motor over a dechi or for doing motor runs on Robinson. 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 n +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 n +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 Registrar 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.

(a) 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 P5 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 oven 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, decried 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 Sum theta(i,j)^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(tau)^1/2 the WM might start Colossus chi-breaking at once, before the rectangle was converged. If 5.6(v)^1/2<X<7(tau)^1/2 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	19145 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

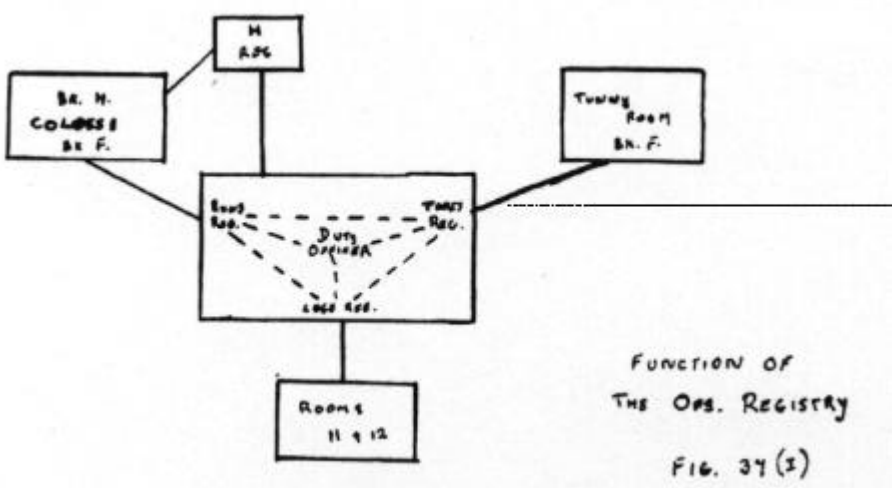
(a) Ops

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 warn 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 wascompleted.

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 Registrar.

After a successful setting job the tapes were returned to Ops with a decode check or de-chi check and Delta-D letter count. If the job was partially successful a Delta-D 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-X5'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 responsible 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 February 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 or 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 occurring 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 priority 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 referred in 37(a) to 'Further Runs'. These were of 5 main types.

(i) Correct Runs, where incorrect runs had been done before.

(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 order to decide if it was worth while, many motor runs were issued with 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 special 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 together. 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 rest 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 P5 limitation was introduced on most of the links normally tried (December, 1943) depths were still occasionally anagrammed on any others that still used X2 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 i944 when X2 PSI1 limitation gradually replaced X2 P5 and X2 lim was reintroduced on several important links. After the start of the daily key change (July, 1943) 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-X5 flag was invented and introduced, the Modern Turingery (with decibans) and later 6 - impulse Turingery for X2 limitation.

Therefore, by 1945, the resources and staff employed in the breaking of chis 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 organisation 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 members 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 Flags.

The flagging of such 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 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 3 1/2 hours.

If the converged combined flag proved significant the Delta-X5 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-X5.

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-X4 flag was made,

(c) the key was issued to Colossus for convergence of 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 mechanically 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 trace of material in Room 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 established in 14A(b). The purpose of this chapter is to describe the organisation in 1945 when there were two major cryptographic commitments.

(1) 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 PSI 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 1 1/2 hours respectively, but more usuallyrather longer owing to unfavourable motor wheels or slides in the text. Messages with X2 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 ???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 through 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.

39 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 actions.

(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 letters 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 letter, in the form of name (Anton, Bertha etc.) which was clearly 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 1,2,3,4,5,6,7,8,9,0, 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 problem 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 the normal alphabet which appeared were those whose first impulse was conventionally a dot. Clearly, owing to some fault in the machine, the 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 clear preambles. For example the sequence a H / I N R I C H and T H / O 3 O R would be recognised as corruptions of H E I N R I C H and T H E O D O R 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 /, were determined.

41B TUNNY SHOWN TO BE A LETTER SUBTRACTOR

The next advance to be made was the demonstration that the cipher 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 Za + Zb 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 construct the sequence Za + Zb , and then to express this as the sum of two passages of plain language, which are assumed to be Pa and Pb . But there is usually no way of telling which of the passages is Pa and which is Pb . 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) The depth "HQIBPEXEZMUG"

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

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 increase 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 attempt 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 depth whose indicators differed only in one or two of the last five letters. 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 periods being small.

In fact the only positive information obtained during the rest of 1941 was obtained by a study of the indicators used. It was 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 there

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 period 23.

(b) Chis, Psis and extensions.

The first success in the analysis or the key was obtained towards the end of January 1942 when it was found almost accidentally 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 or a periodic sequence (of period 41) and of an aperiodic but non-random sequence. We here denote the periodic sequence by X and the non-periodic sequence by PSI.

In order to reconstruct the sequences X and PSI , 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 related; by adding a constant set of five consecutive characters to each of 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 proper order to form a periodic sequence of period 41. This sequence was denoted by X and the result of adding it to the first impulse was denoted by PSI .

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

(1) Consecutive signs in the sequence PSI 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 PSI ,
even when the result (i) was taken into account.

It was then seen that the X 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 PSI, 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 PSI sequence was evidently generated by a wheel of period 43 which sometimes 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 PSI is now denoted by PSI' and the symbol PSI 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 X of period 41, and an "extended" sequence PSI' derived from a periodic sequence PSI of period 43. An ambiguity arose here, for the pattern of X and PSI 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 PSI was still unknown.

The four impulses of the key were next attacked, and they were successfully broken down into X and PSI patterns, just as the first impulse had been. In these cases the periods of the X 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 X1, X2, X3, X4, and X5 respectively, and 43, 47, 51, 53 and 59 for PSI1, PSI2, PSI3, PSI4, and PSI5 respectively.

(c) The Motor

The next problem was to determine the law governing the extensions of the PSI 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 of which each sign was associated with a particular pair of consecutive signs of PSI' , 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 PSI key. When two consecutive signs in PSI' correspond to the same positions of the PSI wheel the corresponding motor-key sign was defined to be dot, and when two such signs corresponded to different positions of the PSI 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 PSI' key. When for example a block of 3 consecutive crosses in the PSI wheel was represented by a block of 5 consecutive crosses in PSI' , 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 PSI' 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 PSI pattern. As there were very few singleton dots, or crosses in the PSI patterns, very few dots could be fixed in the motor key. Sometimes a group of several consecutive dots, or crosses, in the PSI 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 PSI' 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 the 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 X wheel. It seemed probable therefore that the first five indicator letters corresponded to the five PSI wheels in order, and the last five to the five X wheels in order

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 independent motor keys should need at least five

indicators. Hence there was probably only one motor key, controlling all five PSI 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 inconsistencies (or at any rate to no more inconsistencies 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 extensions just as the PSI' keys were derived from periodic sequences.

The pattern of the 37 wheel was readily determined, as was the 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 cryptographic problem presented by the depth H Q I B P E X E Z M U G had now been completely solved. The next 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 X 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 E 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 E 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 most 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 X key of period 23, and an extended PSI 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 E E X E Z M U G, and successful results were obtained in each case. No difficulty was then found in the determination of the motor key.

It was found that the patterns of the PSI wheels in W A O S H were identical with the PSI 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 Q B Z was successfully attacked. All the wheel patterns of this depth, with the exception of these of the two "motor" wheels (with periods 37 and 61 were the same as in W A O S H but these two patterns were different.

From these depths the following conclusions could be drawn:

(i) The order of the wheels was fixed.

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

(iii) The X patterns remain 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 H were taken, so that there could be no serious doubt about the pattern of the X and PSI wheels.

42 EARLY HAND METHODS

42A FIRST EFFORTS AT MESSAGE SETTING

The theory of 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 been decoded for a few letters, that most messages contained the group S P R U C H 9+ + or S 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 8 8 9. In most attempts at message setting therefore, the groups S P R U C H N U M M E R 9 + + or + + Z Z Z 8 8 9 8 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 X wheel was added in all possible settings, and then attempts were made to fit the PSI 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 PSI patterns.

The possibilities were limited by the nature of the PSI 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 or the 10 X and PSI 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, provided 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 29th, 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 ambiguity 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 X 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 PSI 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 X wheels.

The near depth was decoded for about 30 letters and the sum Ka + Kb of the two keys was determined. Crosses (of course) appeared only in the impulses whose X wheels had different settings in the two messages. Both these impulses of Ka + Kb should have shown the periodicity of the corresponding X wheels, and were in 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 X patterns "differenced" at some unknown interval. By repeating the patterns the sequence Ka + Kb 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 up to it.

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

(d) Chis and Psis completed

From the X difference patterns, it was possible to determine the correct X it patterns with some ambiguity. Actually each assumption about the unknown differencing interval led to a different X 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 X or PSI wheel patterns had been made as nearly equal as possible.

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

So the ambiguity of the subtractor keys was resolved, and one impulse of each key was successfully broken down into X and PSI keys. By studying the PSI' key in the impulse it was possible to decide, for very many of the subtractor letters just how many PSI movements had intervened between them and the beginning or the message. As the PSI movement was the same for all five impulses, it followed that for very many letters of the key, the settings of all the PSI 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 X wheel in another impulse. This assumption was legitimate, since the patterns of both X and PSI 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 X wheel, a number of characters in the PSI pattern were obtained, and put at their proper intervals in the PSI pattern, by the use of the relative settings.
From other key characters corresponding to these PSI characters, more X characters were found, and then by continuing this process the complete X pattern and PSI patterns were built up.

Hence all the X and PSI 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 or three and this was successfully set on the X and PSI 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 = 1/2. These values must be compared with those for the patterns for 1941 when a =.703 b < 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 not = 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 PSI wheels, in order, and the last five letters corresponded to the five X 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 X wheel over this period.

The message setters therefore restricted themselves to messages which had for two or more of their X and PSI 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 X wheel was known, the crib, usually SPRUCHNUMMER9++ could be tried in many different positions, and rejected at once in some of them. When the X 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 6th 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 X and PSI wheel patterns remained constant 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 H 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 X 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 X wheels and further that the settings of the 3rd and 4th 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 X patterns changed at the beginning of each month. The patterns of the PSI 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 PSI patterns were used in August as in July of 1941 so it was suspected that the PSI patterns were constant over a period of several months. Three months seemed a likely period, since the first set of PSI 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 X 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 PSI 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 much 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 X wheel and thus permit the breaking of a machine when a depth was available.

A study of the May messages was therefore began as soon as about 10 days traffic had accumulated. The workings have not been preserved, but similar 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 PSI, and X wheels respectively. The row, and also the columns, were lettered in order from A to Z, excluding J, which had never been used is an indicator letter. The fifth impulse of the second letter of a cipher message was entered in the row whose letter was the PSI indicator, and the column whose letter was the X 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 PSI wheel for the second letter was fixed uniquely by the PSI indicator. A very similar 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 PSI 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 X wheels were effective in the encipherment of the first letter.

Similar 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 ZS 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 PSI wheel did not operate in the first place, the nature of the X character in the wheel-setting corresponding to each X 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 X wheel could at once be deduced. It was found to be 11. Of course the count or 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 PSI wheels were now operative. Each cipher character was the sum of a clear character assumed to be x, a X character fixed by the X indicator, and a PSI character fixed by the PSI indicator. However, if a particular X character was assumed to be dot, the values of a number of PSI characters could be deduced from the row of the square corresponding to that X character. Then more X characters could be deduced from these PSI characters, and so on. This process was carried on until it terminated, and so sets of X and PSI characters were obtained. Since these led to very little inconsistency, they were assumed to be the correct ones. Some of the PSI characters were uncertain, since the corresponding rows were almost empty, but all the X characters were obtained with a fair certainty. The first assumption, that a particular X character was x, might have been wrong: it would have then been necessary to reverse all the X and PSI characters finally obtained. This point was settled by using the fact that the number of crosses in the fifth X wheel was 11.

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

We will now summarise 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 X wheel, and to the second letter in the case of a PSI wheel.

The pattern-fragments of the fifth X wheel were known to three places, and the pattern fragments of the fifth PSI wheel were known to two places. A check on the working was now possible, for by the nature of the PSI 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 PSI 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 PSI 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 PSI 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 PSI pattern-fragments were deduced merely from the quality of the corresponding rows. The analysis was completed as for the earlier letters, and thus many PSI pattern-fragments were extended to 3 places, and most X 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 PSI pattern-fragments were used in the fourth place, so one or two X characters, and several PSI 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 X pattern-fragments were easily filled in by using the fact that the fragunts had to fit together to form a wheel. Thus for example the number or fragments four characters long beginning with x.x had to be equal to the nunber 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 X wheels corresponded to an indicator letter. Thus although X and PSI fragments were obtained it could not be decided whether or not these PSI fragments and the parts of the X fragments from the second letter onwards ought to be reversed, and the argument that the X 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 X fragments, and gradually to build up all possible X5 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 X5 indicator letters (and some 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 X5 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 PSI 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 TESTERY 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 quatach 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 X5 had been built up by the time the Germans sent a depth on the 27th.

To meet the introduction of quatach, 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 moon as the full patterns were obtained. The initial stage of setting individual messages (for method see 42A) was therefore more difficult. The last month of the indicator era, October, was broken from a near depth.

43B. TURINGERY.

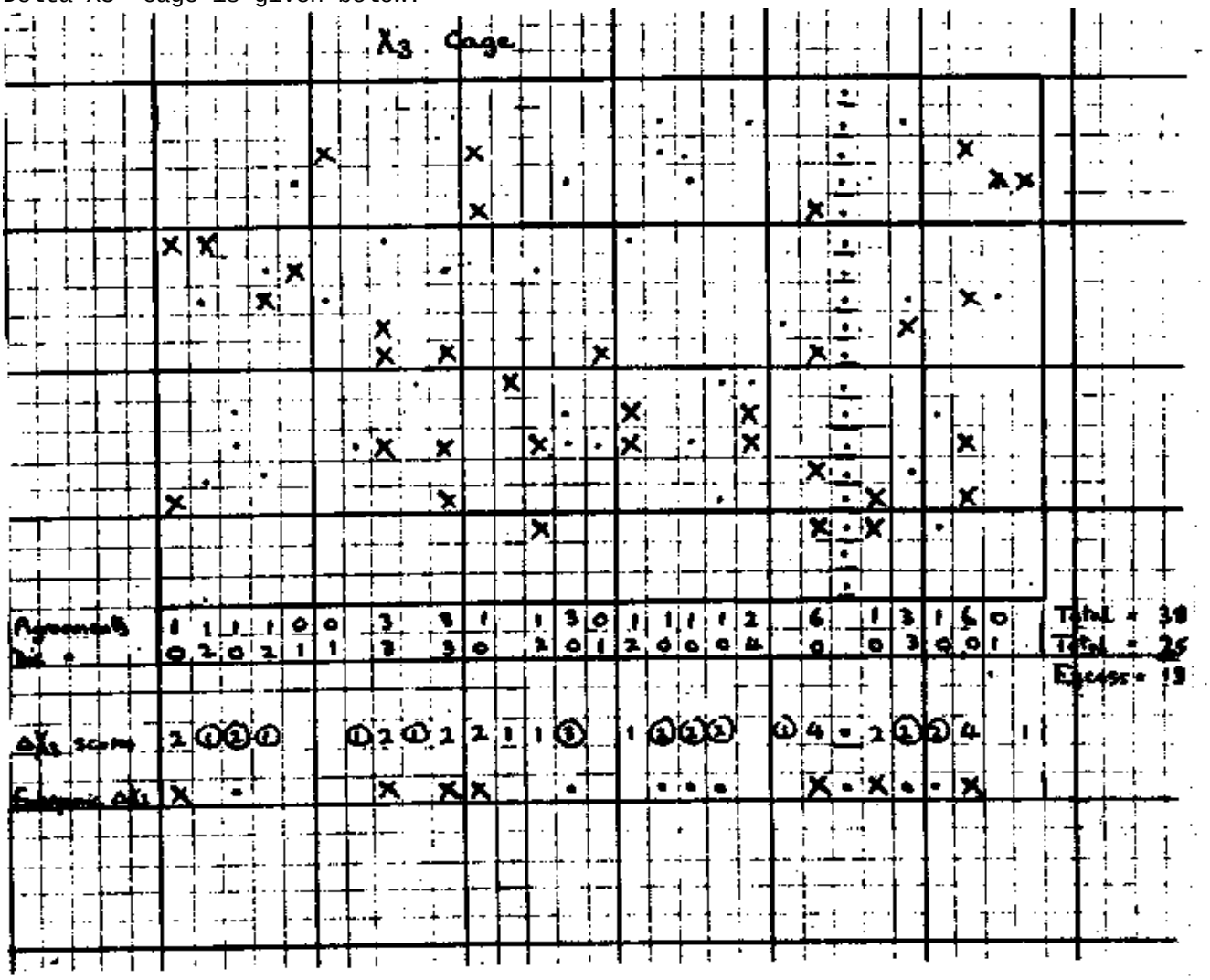
The original method of key breaking clearly became useless as soon as the Germans introduced the condition ab = 1/2. So research was done by A.M. Turing on the key from which the July wheels had been broken by the indicator-cum-depth method, and a method was evolved which produced the correct wheels. The introduction of QSN's (later QEP's) in November i942 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 Delta-K , could yield information unobtainable from ordinary key. This Delta 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 principle involved had not bean studied and understood to the extent that they were later.

The property used throughout is simply P(Delta-PSI'(i,j) = .) = b or in different terms, Delta-K(i,j) -b--> Delta-X(i,j) .

Delta-K 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 or Delta-K 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 Delta-K was the first possible TM dot. At the assumed Delta-PSI'/ position we enter the Delta-X letter in impulses (= Delta-K since Delta-PSI'= /), and the 5 Delta-X signs thus derived are entered on their respective chi-periods throughout the Delta-K. These signs are underlined to distinguish them from other Delta-X signs deduced from them. Now from every Delta-X sign thus entered we can use the property Delta-K(i,j) --> Delta-X(i,j) to deduce one Delta-X sign on each of the other four impulses. For if the underlined Delta-X character is on impulse i and gives Delta-X(i) = Delta-K(i), then in accordance with the above property we deduce Delta-X(j) = Delta-K(j) , for j = each of the other 4 impulses, thus obtaining 4 fresh Delta-X characters which each have probability b provided that the position originally selected is in fact a TM dot. Similarly if we find Delta-X(i) not = Delta-K(i) we assume Delta-X on the other four impulses to be the opposite of Delta-K. These deduced Delta-X signs are written into 5 'cages' of width 41,31,29,26 and 23 respectively. Thus all signs deduced for Delta-X3, from underlined Delta-X signs on impulses 1,2,4 and 5 are written out on a width of 29. An example of a
Delta-X3 cage is given below:



It will be seen that the underlined Delta-X3 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 (1+(beta)^2)/(1-(beta)^2) to the theory that the original position has Delta-PSI'=/ (or Delta-PSI'=8 which merely makes all our Delta-X's inside out). If the result is poor we scrap the cages, erase the workings and take the next Delta-K 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 ~ character being dot or cross (see Fig. (I)). Accepting scores >=2 we form rudimentary Delta-X wheels with which we de-chi the Delta-K 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-X sign. This we assume to be another position where Delta-PSI'=/ , and re-apply the cage teat described above. If the proportion of agreements is poor we try another assumed Delta-PSI'=/ . If it is good we derive Delta-X 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-X's from the combined scores, with which we de-chi the Delta-K to give embryonic Delta-PSI'.

We make a 'count' for Delta-X5, 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-X5 = Delta-K5 at that place. Thus if the Delta-PSI' letter reads x ? . x in the first 4 impulses, and the Delta-K letter is Q we score (1) for Delta-X5 s dot. We write in all these scores through-out the key on a width of 23, and add up the columns to give an improved delta-X5 . with this we de-chi Delta-K5 in place of the earlier delta-X5 used, and count for Delta-X4 . This process continues, going back to delta-X5 after Delta-X1 , until all the Delta-X's are completed. These Delta-X's must obviously integrate into legal undifferenced chis, the even or odd number of crosses in the Delta-X's will tell us whether the original assumption was a Delta-PSI'/ or 8. With the undifferenced chis obtained, from the delta-X's we de-chi the un-differenced K to give PSI', 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,) 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.

K5 is written out and de-chied at all 23 possible settings of X5 to give 23 possible versions of PSI'5 . This process is called 'making a drag' . The problem is to find the true PSI'5. The majority can be discarded immediately because it can be seen at once that they cannot fit the known PSI's whatever extensions are assumed. This process is greatly helped by the fact that the Tunny type Mu61 and Mu37 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 PSI'5 pattern, all TM dots which have to be assumed for the pattern to fit PSI5 are marked. At each of these places we know that Delta-K = Delta-X . So at all X4 settings which satisfy this condition we de-chi K4 and examine the resultant possible PSI'4's. Unless the key is very short (the length normally used is from 14 to 3o) the correct X4 setting based on the correct X5 setting will yield a PSI'4 pattern which when contracted by using the assumed TM dots will fit on the known PSI'4. We then do the same for PSI3 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 26D).

(d) Setting depths on X2oneback limitation

The X2oneback limitation first appeared in February, 1943. The number of dots in Mu37 was doubled to give the same proportion of dots in TM as before. The X2oneback limitation necessitated changes in setting and motor working and caused some changes in Key-breaking methods.

The method of setting depths on X2oneback limitation is essentially the same as with the "No-limitation" motor. But the drag is made on K2 instead of K5 and use is made or the fact that for each setting of X2 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 PSI'2 on to PSI2 . 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 X2oneback limitation on key-breaking

Turing' a original method had already been modified in two respects (see above (c)). With the introduction of X2oneback 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 X2oneback which were finally perfected in early 1945 are described in 26. At the time, however, use was only made of the limitation to obtain X2 after one other chi had been obtained and the psi repeat recognised. This was done by examining the TM deduced from the PSI' already obtained, when written on a width of 31. All TM dote imply X2oneback = x and columns where no dots appear are extremely likely to correspond to a X2oneback dot. This allows us to infer most of X2oneback which is then slid one to the left so that it becomes X2 and is then compared with the Delta-X2 values obtained from the last Turingery count for Delta-X2 to have been made. The combination of the two should give a complete X2 which is then added to K2 to give PSI'2 . This PSI'2 combined with the use of the known X2oneback should place most if not all, of the TM dote 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 X2oneback P5twoback limitation.

The Rome-Tunis link known as Herring operated between Decmber, 1942 and the final collapse of the German forces in Tunisia in May, i943. It was on this link that both the X2oneback and X2oneback + P5twoback limitations first appeared. The method by which the X2oneback + P5twoback limitation was analysed and its method of working understood is described in Ch.44. The X2oneback + P5twoback limitation effectively prevents messages being in depth even when the initial settings are the same owing to the divergence of the two PSI's under the influence of the different P5's. Thus work on Herring was made impossible, until the operational difficulties or passing a great quantity of traffic under pressure using the new P5 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 QRP'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 X's 1,2,4 and 5 and the motor. A print-out of D1245 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's,124 and 5 uniquely. X3 and PSI3 were set as in setting on 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 X3 which gives Delta-X3 = Delta-K3 at all TM dots, and then to add at the correct setting to K3 to give PSI'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 Mu37 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) Delta^2 properties

The next discovery to have an effect on key-breaking techniques was made in September, i943 (see RO pp 53,54). It was that Delta^2 X --> x with probability about 2/3. Unlike the property Delta-PSI --> x the new property was found to lack rigidity. The way in which it is applied Is described in 26B(d).

(iii) The discovery of ^X2 (See 263(b))

The discovery of ^X2 was made on Squid for November, 1943, for which 880 key had been obtained from depth. It had 22 dots in Mu37 and X2oneback limitation. The discovery had far-reaching repercussions. Its ultimate effect on key-breaking is described in (26B(b)), and on chi-breaking from Z in (25E) It led directly to the breaking of wheels from crib. (See 27G) And lastly the level or significance of the ^X2 count or run proved an invaluable test as to (i) whether a given key was on X2oneback limitation or not and (ii) in the case of certainty of X2oneback 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 X2oneback + P5twoback limitation began to be dropped on Western links, and mince 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 i943 on the basis of 16 dots in (see above (b) (i)) were dug up and recalculated on the basis of 18 1/2 dots in Mu37 (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 key (see 26 C) and the 5 by 5 flag (see 26B (a)) were devised, and the Newmanry at the same time invented the powerful X5 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 X2oneback limitation was begun, and after some months of evolution the method reached its final form as described in 26B(b),26E.

(c) The first dc-chis

When the X2oneback + P5twoback 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 dc-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, 1944 were broken within the first fortnight with the comparatively primitive equipment of the time - Colossus I (see 52(c) was not yet in action. Two messages on the same QEP were set on the chis and de-chied. From these two dc-chis, by the method of applying the psis obtained from a break in one to the other de-chi (see 28C(a)) the psi patterns were obtained within an hour. The Mu37 proved to hare 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 Mu37 dottage proved to be only 19, which explained the difficulty encountered. It was now evident that the problem of the X2oneback + P5twoback limitation had been mastered in both sections. A detailed account of psi-breaking from de-chi in given in 28C.

(d) The X2oneback + PSI'1oneback + P5twoback limitation

This triple limitation first appeared in June, 1944 on Codfish and Gurnard. Its action is described in 11B(g)iv); its stay was brief as in December, 1944 the Germans began taking the P5twoback component out of the limitation on the various links; thus it gave rise to the X2oneback + PSI'1oneback limitation (see B(g)(ii), 11B(i)), which became the standard limitation on the majority of links, the remainder reverting to the old X2oneback 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 wheelsetting 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 to 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 X and PSI patterns were changed monthly, and that motor wheel patterns were still changed daily. Here there was one difference from the old Tunny link, for which it had been demonstrated that the PSI patterns were changed only quarterly.

The Germans could not be relied upon to continue to send much a proportion of depths, and in any came 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 warn made early in i942 to set X's and PSI'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 PSI wheels, but it was hoped that the PSI' 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 not = 1/2 but that no success could be expected with ab = 1/2. The reason for this was closely connected with the predominance of changes in the PSI pattern: when the assumed setting of a PSI wheel was one place off the true setting, the resulting sign in the assumed PSI' 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 PSI impulses but an attempt was made to derive a statistical method from a consideration of the other non-random properties of the PSI' key. These are:

(i) All five PSI wheels have the same movement

and (ii) In the unextended PSI impulses, changes are much more frequent than continuation.

These properties, it was thought, could best be expressed in terms not of the actual PSI' key, but of its first difference, which we denote Delta-PSI' . Changes and continuation in PSI' 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 = 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

$$2 ab (1 - b) = 1 - b$$

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 netting should be the differencing of the cipher text and the addition of two impulses of the resulting stream of letters.

All now depended an the properties of Delta-P1 + Delta-P2. Counts

were made on the clear texts at some Octopus messages, and the value .63 was derived for the proportion of dots in Delta-P1 + Delta-P2 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-D12 = .) = •55

and that this property of D was sufficiently marked for it to have been possible uniquely to determine the X1 and X2 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-X1 + Delta-X2 settings had to be devised. The sequence Delta-X2 was added to Delta-Z1 + Delta-Z2 in an arbitrary setting, the numbers of dots and crosses in Delta-Z1+Delta-Z2+Delta-X2 corresponding to each position in the 41 period were tabulated and then this table was compared with each setting of delta-X1. This process was carried out for every setting of Delta-X2. It was found convenient for this process to write Delta-Z1 + Delta-Z2 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 X wheels were set. For later messages it was found sufficient, after X1 and X2 had been set to work only on pairs of impulses for which the setting of one X wheel was known. The settings of the other X wheels would then be comparatively simple with good messages.

(d) Motors and Psis set .

When all the X wheels of the first message had been set, the X key was added to the cipher text, and the sequence D = Z + X , obtained. This sequence was found to have more than twice the random number of double letters. This was presumably because both P and PSI' contained a high proportion of double letters. But nearly all the double letters in the extended PSI 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 analogous 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 PSI wheels should be set statistically, by striking out from the de-chi all letters corresponding to extensions of the PSI-key and then setting the PSI wheels on the 'contracted de-chi' just as the Delta-X 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 PSI 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 much a place, three consecutive letters of the extended PSI 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 PSI 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 developments and his section came into operation later in the year. This section set the X 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 of 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 Delta-Z12 Delta-Z13 and Delta-Z45. The motor was obtained statistically.

Further investigation into Rectangling and other statistical 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 P5 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 using the name 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 X 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 PSI key. The passage was

Z 3 D D D D V Y 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 either agree with, or else be the complete reverse of, the corresponding impulse of the extended PSI key.

The hypothesis was tested by comparing the actual PSI wheels with the various impulses. It was found that complete agreement could be secured by taking the underlying clear language to consist of a long sequence of Z's followed by a long sequence or 9's. The PSI 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-chi 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 P5twoback) and the second X sign of one place back (denoted by X2oneback). This suggested that the total motor key was obtained from the Basic Motor in conjunction with the limitation (P5twoback + X2oneback). This 'basic motor' could be determined whenever P5twoback + X2oneback 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 X2oneback 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 charter.

Such history as is included is a description of development 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 obvious.

The need for efficiency in other copying machines is apt to be overlooked; one of them, Miles, was in fact unduly neglected: in particular the production models of Miles A were vetoed. The 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 existing 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 I counted electronically, in three scales of 2 followed 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 recognised 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 recognised 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 authorised, a most unsatisfactory 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 successive impulses.

Miles (including Miles A) reads the five impulses simultaneously but sends them successively to the reperforator.

Readers which produce five successive impulses are supposed to be called auto-transmitters.

Reperforators which receive 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 or 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 nearly complete
Colossi		4	6		10	
Dragons				2	2	+ 1 under construction
Proteus				-	-	+1 under construction
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 principles should be chosen because

(a) it is easy to make.
(b) 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 impossible conditions were severelylimited.
(viii) The counters were only partly electronic.
(ix) At first Heath Robinson warn 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 (Figs 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 or 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 principle, 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 X2oneback 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 i.

The flexibility of Heath Robinson for experimental purposes made it easy to discover the essential requirements or a 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 shown to be desirable: it was biased towards runs of the form i+j = .: these could be done by switching except in the fifth counter. Moat 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 independently for double testing on X1, but for this it 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.

(r) Colossus 2 and later.

Experience gained from the development of Colossus 1 added to that from Heath Robinson, made possible Colossus 2, 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 chi 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 not = 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 not = 9 but this lost all genuine 9's also (about 1/17 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 specialised gadgets.

The clamour for specialised 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 handi-caps 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 124-128 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 setup 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.

53. COLOSSUS

53 - COLOSSUS

53A INTRODUCTION

The photographs in chapter 58 show the layout both of the whole machine and of individual panels, far more clearly than verbal description, which is therefore omitted.

Colossus makes counts concerning certain streams of teleprinter letters. One, denoted by Z and represented on a punched tape, is wholly arbitrary; the others, denoted by X, Mu, PSI and represented electrically, are specialized and composed from certain fixed periods. These patterns X, Mu, PSI, do in fact represent the 12 wheels of the German Tunny machine, and move in the same way. Their 12 components will here be called wheels. For given "settings" there will be, corresponding to each place on the tape Z, definite positions on all the wheels.

Colossus counts the number of places of Z where a condition involving some or all of these streams is satisfied. An essential feature is that the counts can be made in rapid succession with the various wheels in different relative positions ("stepping").

Colossus cannot count a condition involving two different places in the stream except in a limited way by memory circuits, used mostly for delta-ing.

The sum Q of any number of the three 5-impulse streams Z, X, PSI, either differenced or undifferenced, can be switched into the Q panel: the switches of this panel suffice to impose the majority of the 2^32 app. = 5,000,000,000 combinations of conditions which are theoretically possible. Less specialized conditions can be imposed by the plugboard.

Note 1 Although the streams are named Z, X , Mu , PSI, these are not necessarily used as the real Z, X , Mu , PSI of Tunny. In a short wheelbreaking run (25) the pattern set up in X is really delta X except in the wheel for which the run is made, where it has only one cross and is used merely to select in turn the characters of that wheel.

Note 2 A tape is required in every case, because it controls counting, but Z need not occur in the conditions imposed (e.g. X test runs).

53B THE Z STREAM

(a) The tape

The tape is a continuous loop of five-impulse tape carrying the Z stream, the usual sprocket holes, a start sign, a stop sign, and 150 blanks.

The sprocket holes are utilized

(i) to cause the machine to count if the conditions imposed are satisfied: the machine counts once, at most, for each sprocket hole.

(ii) to maintain the correct motion of X , Mu , PSI.

The start sign is a hole between the 3rd and 4th impulses, which

(i) causes the machine to start counting (the start sign has to be punched 2 1/2 sprocket lengths before the first place to be counted),

(ii) sets X, Mu, PSI, in motion.

The stop sign is a hole between the 4th and 5th impulses, 1 1/2 places beyond the end of the text, which

(i) causes the machine to stop counting, and generally prepares for the next start sign.

(ii) transfers to relays the score which has been counted.

150 blanks between atop and start give Colossus time to prepare for the next start sign.

(b) The Bedstead

The bedstead is a system of pulleys round which the tape is driven by friction at about 40 feet or 5000 sprocket holes per second, so as to pass through a gate where it is scanned by eight photo-electric cells, one for each impulse and one each for sprocket hole, start and stop.

Each Colossus has two bedsteads; while one is in use a tape can be put on the other. An on-of switch by each bedstead controls both its driving motor and its lamp. There is a switch on the selection panel, whereby either bedstead can be selected (near or far), not both at once.

The maximum length of tape which a bedstead can carry is either 11,000 (short bedstead) or, on Colossi 5,6,7,8,10, 30,000 (long bedstead). On a long bedstead the voltage applied to the motor can be adjusted to maintain the correct speed whatever the length of tape and number of pulleys in use.

Although shorter tapes can be put on the pulleys, Colossus does not work well with a tape less than 2,000 long.

53C THE X, Mu, PSI, STREAMS

(a) The triggers

The twelve wheels constituting X, Mu, PSI, are set up in 'triggers' of length 41,31 etc. These triggers, except the wheel-breaking panel, are inconveniently situated at the back of Colossus.

For each character of a wheel there are two small sockets: a cross is represented by short-circuiting these with a U-shaped pin ("putting in a pin"); a dot by leaving them vacant. (Fig 58(xviii)).

There are several alternative triggers for each wheel. The X, PSI patterns have five triggers (a, b, c, d, e) each selected by a switch on the selection panel. X a must be used with PSI a.

The Mu pattern has seven triggers a,b,c,d,e,f,g, any one of which can be used with any X, PSI, trigger. This discriminatory treatment of Mu was arranged when only the Mu's changed daily.

(b) Special Patterns

By using the switch position e' the X, PSI trigger e can be used in a different way as a "special pattern" or "doubting" trigger. Similarly g' is the special pattern Mu trigger.

e' in not added into Q (see Q panel: 53J (a)).

g' does not motorize trio PSI's.

Indeed these patterns appear nowhere except in the seven special pattern jacks on the plug panel, and to have any effect they must be plugged.

These are used in addition to an ordinary trigger.

(c) Wheel-breaking Panel

On wheel-breaking Colossi there is the inestimable boon of a panel on the front of the machine, carrying an ordinary X trigger and a special pattern X trigger: in place of U-shaped pins, easily inserted plugs are used: they are so much easier that they are often used for setting. Each of the 5 X wheels has its ordinary and special patterns adjacent and each is controlled by a 3-way switch whose positions are

(down: ordinary and special patterns in,
(
(normal: all out,
(
(up: single cross in the last position of the ordinary pattern.

(d) Motorization and Limitation determiner switches

The motion of Mu37 and the PSI's is not uniform, but simulates that of the corresponding wheels of the German Tunny machine.

On Colossus the extension of the Mu37 pattern by Mu61 is fixed. The extension of the PSI pattern is naturally adjustable to suit the limitation. The appropriate switches are near the bottom of the selection panel viz

PSI1oneback, X2oneback, PSI5twoback: if one or more of these switches are either up or down the corresponding impulses are added and used as the limitation. At the beginning of the text these, since they refer to places one or two back, are indeterminate: the up and down positions of these switches and of P5twoback impose an arbitrary dot or cross, in these places.

BM C/o is the basic motor cut-out. When it is used the total motor is simply lim.

53D STEPPING AND SETTING

(a) Setting

The setting of a wheel is that character of the wheel which corresponds to the first sprocket hole of Z.

All wheels can be given assigned settings, simultaneously, by putting plugs in the appropriate setting jacks and depressing the switch SU. The setting jacks are arranged below the control panel in 12 rows which correspond to the 12 wheels.

(b) Stepping

Any wheel can be stepped i.e. its setting increased at each revolution of the tape.

This will not of course be confused with the ordinary motion of the wheels at a fixed setting. It should be noticed that increasing settings imply that the patterns move backwards relative to Z. Any number of wheels may be stepped simultaneously.

(c) Stepping Switches

Each wheel has two 3-way switches in the control panel, one in the upper row, one in the lower.

Either of these two switches may be thrown up or down.

Upper switch up) causes the wheel to step fast
or Upper switch down) i.e. to step at each tape
or Lower switch down) revolution.

Lower switch up - causes the wheel to step slowly i.e. to step only when a wheel whose lower switch is thrown down reached the plug in the setting jacks. If in some frenzied fantasy, several wheels have their lower switches down <u>each</u> of them will step a slow stepping wheel.

(d) Repeat Light

When all wheels return to their original settings (strictly to the plug in the setting jack), the repeat light glows. A wheel whose upper switch is thrown <u>up</u> is ignored.

53E DIFFERENCING

Any pattern, except a "special pattern" is available deltaed either on the Q panel (by throwing the Q selection switch to delta) or on the plug panel (by using deltaed output jacks).

The conventional Tunny delta is the sum of present and future i.e. forwards. Colossus deltas by remembering and adding the letter one place back i.e. backwards.

This is immaterial provided that all patterns in use are deltaed by Colossus or all not deltaed by Colossus; but if some are and some not, then those which are, are recorded by Colossus as one place back.

For example suppose that Z is a plain Z tape which is being deltaed by Colossus and added to delta X set up deltaed on the X trigger, the two patterns being level so that the recorded setting is 01.

Opposite the second sprocket hole Colossus produces for delta Z: 1st character + 2nd character.

Opposite the second sprocket hole delta X is plugged as: 2nd character + 3rd character.

It follows that the true setting of X is 02.

This is in many cases corrected by adjusting the settings, whence the phrase "Setting of deltaed wheels should be one back".

A "Special Pattern", however, steps level with the corresponding ordinary pattern, and accordingly when the latter is to be deltaed by Colossus, the former must be set up in the trigger one back, in the sense that the 2nd position of the trigger contains the first character of the wheel.

If the same pattern is used both differenced and undifferenced, the correction cannot be made either by setting or by setting up, but must be made internally by Colossus.

The following are all one back so as to be in the present place when used with wheels deltaed on Colossus
(1) The TM switch at the bottom of the Q panel (including not X2oneback when BM is cut out and the X2 determiner switch is in.)
(2) the jacks not Mu61, not Mu37, not P5, TM on either side of the special pattern jacks.

It will be noticed that the labelling is inconsistent.

53F COUNTING

(a) The five Counters

Colossus counts up to 9999 and then returns to zero.

To increase the speed of operation, Colossus has five separate counters, which can be used simultaneously either for five (or fewer) distinct runs or for multiple testing on a single run. Spanning and stepping must be the same for all runs. The five counters are labelled 1,2,3,4,5, but printed on Colossus records a,b,c,d,e.

(b) Switching into counters

To be effective a condition must be switched (on the Q panel) or plugged (on the plug panel), into the proper counter. In particular in multiple testing the condition on each of the remembered impulses must be plugged or switched to its proper counter.

53G RECORDING OF SCORES

When a count has been completed, i.e. when the stop sign on the tape is reached, Colossus can transfer it to the "display and the printer.

(a) Set Total

To avoid displaying and printing useless scores a "set total" can be imposed so that only scores which exceed, or, alternatively, only scores which do not exceed this set total appear, others being cancelled.

The set total controls for the five counters are independent, and for each of the five, consist of decade switches reading 0000 - 9999 , and a three-way switch "<","off",">". With the off position all scores are displayed and printed. (Fig 58(xiv))

(b) SIP

On Colossus 10 S.1.P. ("significance Interpretation" switch on control panel) causes all counters to print if one

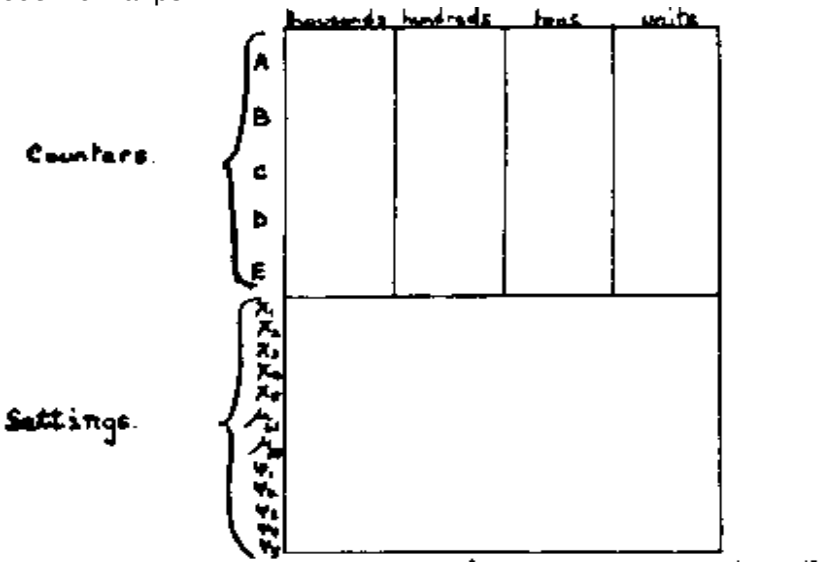
exceeds the set total.

(c) Storage of scores.

Scores which are to be printed, together with the relevant settings are stored on relays and appear on a display. While the next count is being made these relays send impulses to the printer and so clear themselves. If the printing is not completed in time to clear the relays for the next score, stepping is automatically inhibited until the relays are clear: thus no scores are lost.

(d) The Display

The display is a glass screen on which the scores are projected by small electric lamps.



The switch LC/o cuts out the "settings" lamps. The switch ML extinguishes the "settings" lamps when all scores in storage have been printed.

(e) Printing of settings

When the machine is started it prints in a horizontal row the symbols for all wheels which are stepping. In the printed record the settings of these stepping wheels appear before every score. Each below its appropriate heading. when runs are done simultaneously, some of these settings may be relevant to certain runs only. To avoid the printing of confusingly meaningless settings there is a 5 x 12 array of jacks to the right of the X setting jacks, whose rows correspond to the 5 counters, and 12 columns to the 12 wheels: in order that a score on a particular counter shall cause the setting of a particular wheel to be printed, a shorting plug must be inserted in the corresponding jack.

In all cases the name (a, b, c, d, e) of the appropriate counter is printed before each score.

(f) Printing of Scores

After a score is printed there is an automatic carriage return so that each score is on a separate line.

(g) "Print Main Headings". (PMH switch on control panel).

Prints the settings of all 12 wheels, each following its appropriate symbol. Colossus has to be restarted after printing the symbols.

(h)"Letter Count" (LEC switch on control panel)

is for making counts at fixed settings. It stops the machine after printing a batch of scores: without it the same count would be repeated. Whilst one batch of scores is being printed, the next batch can be switched.

(i) Printer Cut Out (PC switch on control panel)

prevents Colossus from sending impulses to the printer, so that stepping ceases [cf. storage if scores in para. (c) above].

(j) Reset (switch on control panel)

clears all scores in storage: in particular if PCO is in use it allows stepping to be resumed.

(k) The Printer

The printer is an electromatic typewriter.

It can be operated manually for the insertion of data (e.g. sigma , S.T. span) not printed by Colossus.

Single, double and triple line feed are available.

The inexplicably assorted founts are not intended for cryptography, but this seems to be no handicap: sigma has appeared as £, @, $.

53H SPANNING

(a) Spanning

is a device whereby Colossus counts only over a selected stretch of the tape.

There are three groups of decade switches (Fig 58(xvi)) above the plug panel each reading 0000 - 9999 labelled

START COUNTERS , START PSIS , END OF SPAN.

If "start counter" is set to m. where m is not 0000, "end of span" to n , Colossus counts only from the (m+1)th to nth places on the tape, inclusive.

If "start counter" is set to 0000, spanning is ineffective, the first place on the tape cannot be included in a span.

(b) The settings

The settings on Colossus refer to the start of the tape, not the start of the span.

Motorizing of the PSI's begins at the place to which "start psis" is set: normally this is 0000, the start of the tape.

(c) On Colossi with long bedsteads

there is a rudimentary 5th decade in the bottom row of the selection panel. Switches are thrown down for

+10,000, up for + 20,000.

(d) on Colossi with short bedsteads

spanning, is unable to distinguish places 10,000 apart so that e.g. 500 - 1,000 cannot be disentangled from 10,500 - 11,000.

(e) End of Span cut-out

The ES c/o switch in the bottom row of the selection panel overrides the end of span switches and spans to the end of the tape.

53J Q PANEL (Fig 58(xiii)).

(a) Q Selection switches

At the top right of the selection panel there are three large three-way switches. Each switch has a neutral position and the active positions are Z, delta Z; X , delta X; PSI , delta PSI . The streams to which these switches are thrown are added together, and their sum appears in the Q panel: the five impulses of this sum are called Q1,Q2,Q3,Q4,Q5.

Note: each large switch is really five switches linked together viz. one switch for each impulse : if necessary these can be separated.

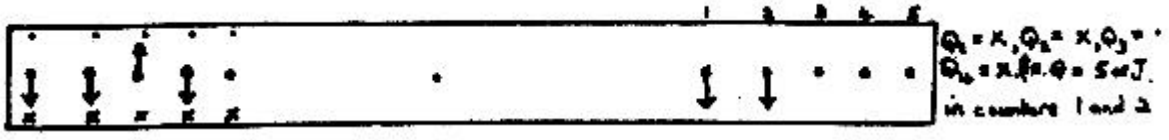
(b) The Layout of the Q panel

The upper part (10 rows) is used for imposing conditions on individual impulses.

The lower part (5 rows) is used for imposing conditions on the sums of impulses.

(c) Conditions on individual impulses

Every row in the upper part of the panel is arranged as follows. At the left there are five 3-way switches, one for each impulse, each of which can be thrown to dot or cross to make the corresponding impulse of Q dot or cross. At the right there are five switches labelled 1,2,3,4,5, one for each counter, to determine the counters in which the condition is to be imposed.



Any number of rows may be used: if conditions from two of them are switched into the same counter, both will be imposed.

(d) "Not" switches

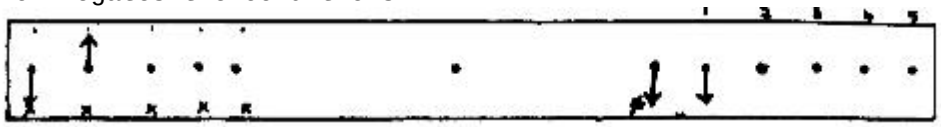
To impose alternative conditions

"either A or B"

is replaced by the equivalent

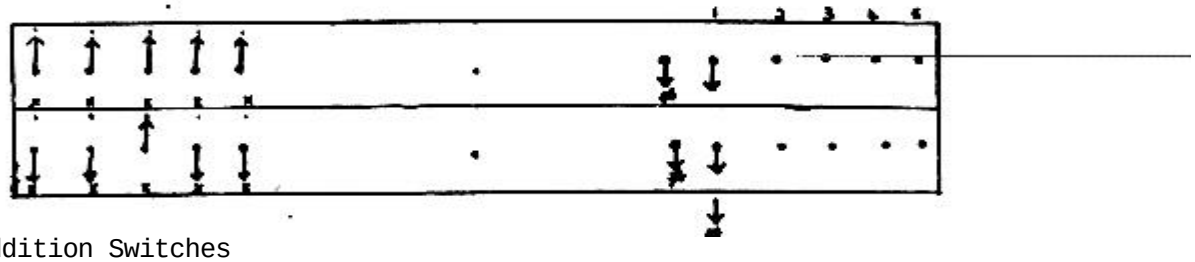
"not (not A and not B)".

Just to the left of the counter switches is a "not" switch labelled not = , which negates the conditions.



means not (Q = x and Q2 = .) : this allows Q1 = . , Q2 = x , or Q1 = x, Q2 = x, or Q1 = . , Q2 = .

At the foot of each column of ten counter switches is another "not" switch, which negates the whole column.
For example: to impose Q = either / or 5
This is equivalent to not (Q not = / and not = 5)



(e) Addition Switches

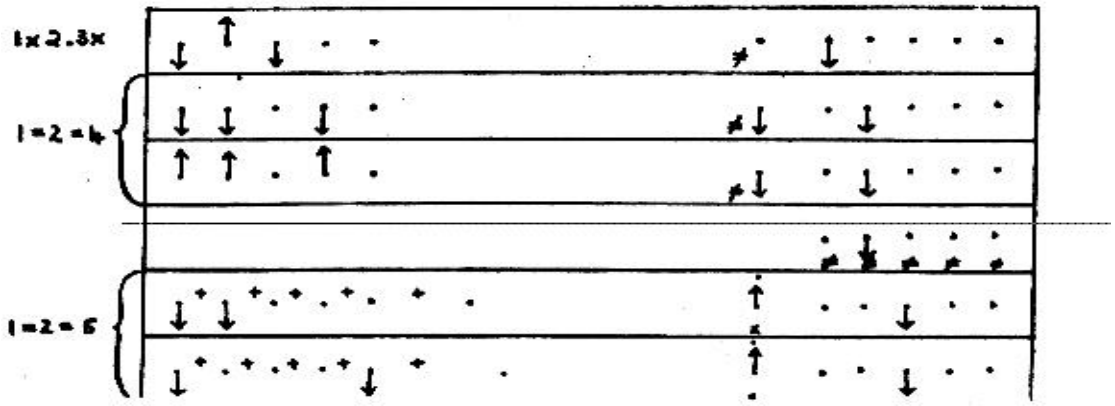
In a row in the lower part of the Q panel the 5 switches at the left which are separated by + signs. can be thrown down only, to make the sum of any number of impulses a dot. There are five counter switches exactly as in the upper part of the panel. The "not" switch is labelled x dot , but it has the same effect.

Footnote: Clearly not(i + j = .) is the same as (i + j = x). These "not" switches actually have a neutral position, but it is not needed and is not alike on all Colossi: on some it causes no condition to be imposed, on others an impossible condition.
The five "not" switches at the bottom of the Q panel labelled not = negate whole columns, not merely the lower part of the panel; in particular they negate the upper row of "not" switches.

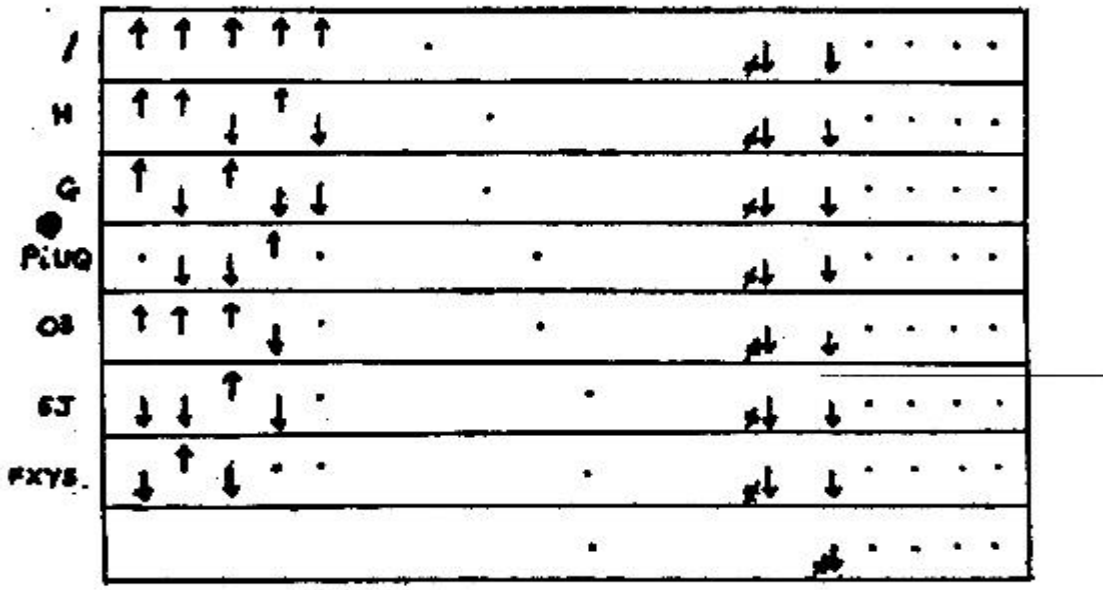
(f) Examples of Switching

It is worthy of emphasis that what is switched is Q, and that Q is whatever is selected by big black switches. In runs to set X's, Q is Delta-Z + Delta-X (though if Delta'd X patterns are set up it is Delta-Z + X so far as Colossus is concerned); in runs to set PSI's it is usually Z + X + PSI . Use has been made of Q as X ,Z , Z + X, Delta-Z + Delta-X + Delta-PSI. The methods of switching on the Q panel are the same in all cases.

(i) 3x/1x2., 4 = /1=2, 5=/1=2 simultaneously on counters 1,2,3 The two runs 4=/1=2, 5=/1=2 would ordinarily be done on the same principle: here, for purposes of demonstration, they are done quite differently



(ii) / H 0 3 G P I U Q 5 J F X Y S as a single run



If this were done in a hurry it would be very easy to overlook that PIUQ can be switched in a single row; if PI, UQ were in separate runs it would not matter, but it is necessary to put some of the fifteen letters together, for there are only 10 rows.

(g) Possible Runs

This suggests the problem of whether all possible sets of conditions can be imposed on Q, i.e. whether it is possible to run for an entirely arbitrary selection of letters from the 32 letter alphabet.

It is obviously possible to run for any ten letters but, for example, R A S H D 0 N 8 L I Z , 11 letters, is impossible.

Despite the aid of the addition switches, 15 rows in the upper part of panel are needed to include all runs.

(h) The R Switches

These are the multiple test switches carrying the impulses R1,R2,R3,R4,R5 [see Multiple Test 53L(c)] : each occurs in two rows in the upper part of the panel and in one row in the lower part.

Evidently the choice of runs will be much more restricted on multiple test than without it.

For examples of multiple test switching see 53 L(1)

(i) Total Motor Switch

In the bottom row of the Q panel is a three-way switch whose active positions are labelled TM . and TM x .

This switch is not used for motorizing, but only for counting against TM = . or TM = x . It is rather more general than this, for by use of the limitation determiner switches TM can be made to mean

BM =Mu37/ : all switches normal
TM : Switches for the appropriate limitation in.
Not X2oneback : BM c/o, X2oneback in

Note: TM is in the present position when used with wheels which are deltaed by Colossus (as it usually will be) compared to patterns not deltaed by Colossus it is TMoneback, i.e. TM one back [cf. differencing 53E].

53K PLUG PANEL (Fig 58(xv))

(a) The Jacks

The jacks in this panel are essentially of four kinds:

1. Jacks carrying streams, (including some combined streams.

2. Addition Field;

3. Common Jacks:

4. Jacks carrying input to counters.

Streams may be plugged into counters, either directly or via the addition field and common jacks. To plug anything into a counter is to equate it to a dot.

(b) Jacks carrying streams are described in paragraphs (c) to (h)

(c) Q Jacks

The whole top row of jacks is really a dependency of the Q panel. Q1, Q2, Q3, Q4, Q5 are the five impulses switched into Q by the selection switches, R1, R2, R3,R4, R5 are the present and remembered items of Qm when Qm is on multiple test. All these have two jacks each.

(d) Z, X, PSI ,

Each impulse of Z, X , PSI , has two jacks, one deltaed and one undeltaed.

(e) Special Patterns

X1 , X2 , X3 , X4 , X5 , Mu41 , Mu37 , have each one each one jack for the pattern set up, independently of the ordinary pattern in use, in the special trigger.

(f) Mu61oneback , Mu37oneback , P5oneback , TMoneback

These are derived from ordinary patterns. If used with streams eltaed by Colossus they are in the present position. If used with streams not deltaed by Colossus they are one back, as labelled [cf. 53E]

(g) Not 99

This is used to inhibit counting at doubtful letters of cipher replaced by Z = 9. Such 9's rarely occur singly. Genuine 9's usually do occur singly. It is therefore only imposed at a 9 adjacent to another 9: at such places this jack carries a cross, elsewhere a dot.

Note: Not 99 is intended for use with a Z pattern which is deltaed by Colossus and therefore, since delta Z is rubbish if

Z one forward is rubbish, it is in use, for each stretch of 9's, from one place before the first 9 to the last 9. Colossus however, because it deltas backwards, treats this as being from the first 9 to one place after the last 9; and accordingly if not 99 is used with Z not deltaed by Colossus one place will be lost unnecessarily at the end of each stretch of 9's.

(h) Start Units

These carry a permanent dot or cross as labelled.

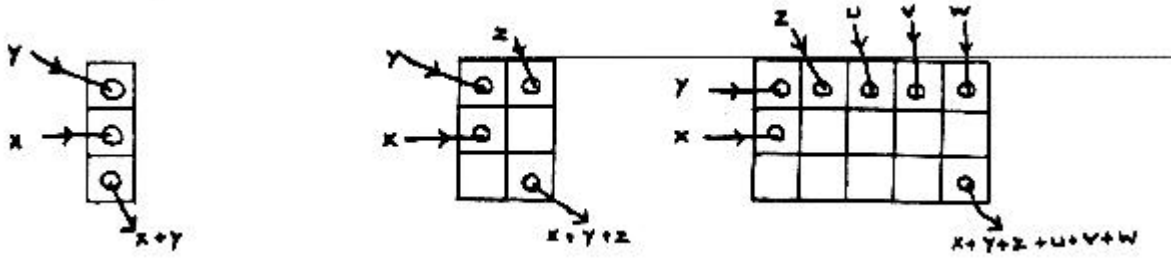
(i) Addition Field

These are of course used to add impulses: there are three rows, 26 columns.

All but one of the impulses to be added are plugged into consecutive jacks in the top row.

The odd one is plugged in the middle row below the first of the other plugs.

The output (sum) is taken from the bottom row below the last of the other plugs.



The columns used thus are isolated so that several additions can be carried out simultaneously.

To plug any impulse to equal a cross, add a cross and plug normally.

(j) Common Jacks

There are on each Colossus six or more commons of five jacks each. An impulse put in can be taken out four times: if this is insufficient common jacks can be linked together.

(k) Counter Jacks

There are 8 jacks for carrying conditions to each counter.

There are also 6 jacks carrying conditions to all counters. One of these is marked TM because it will not work if the TM switch on the Q panel is thrown.

There is a special counter jack (Multiple Test Doubting) used only for multiple testing on special patterns.

(l) Examples of the use of the Plug panel

(1) Before not 99 was available it was usual, on corrupt texts, to switch Q = Z, Q not = 9, and plug all wheel-breaking runs.

(ii) The wheelbreaking run, Delta-X1 + Delta-Z1 + Delta X6 = . is normally done by plugging (delta X6 is usually set up in the X2 trigger).

If the Q panel were used delta Z2 would be switched in along with delta Z1. This could be avoided, alternatively, by splitting the delta Z selecting switch.

(iii) the run i=2=lim (i.e. Delta-D1 = Delta-D2 = X2oneback can be switched and plugged thus

1=2 on the Q panel, multiple testing on X1

Q2 + X + TM = . on the plug panel

TM = not X2oneback on the limitation determiner switches, using BMc/o, X2oneback .

53L MULTIPLE TEST

(a) To save time it is arranged that the same wheel can be examined at five different settings simultaneously, the five scores appearing in the five counters.

(b) Memory circuits

When the multiple test switch for any wheel is thrown, a memory device is switched in, which stores the characters of that wheel 1,2,3, and 4 places back.

Footnote More explicitly Colossus remembers characters of the wheel opposite places on the tape 1,2,3,4, back; in particular characters of PSI' not of PSI . In the first four places of the text some of the remembered characters are really those at the end of the text in the preceding tape revolution; and will give random scores, unless the text length is a multiple of the wheel length: it is customary to span from o4 onwards.

Thus when Colossus is examining a particular place on Z, it has available for comparison:-

(i) on the multiply tested wheel, the present character and the characters 1,2,3,4, back. These are associated with the numbers 1,2,3,4,5 (i back with i+1).

(ii) on Z, and on all other wheels, only the present character.

(c) R1,R2,R3,R4,R5.

Most operators are surprised to find that the remembered characters appear nowhere except as a component of Q, the corresponding five characters of Q are called R1,R2,R3,R4,R5.

e.g. if X is multiply tested and Q = Delta-X + Delta-Z then

R1	=	Delta-Z1 (present)	+	Delta-X1(present)
R2	=	Delta-Z1 "	+	Delta-X1(1 back)
R3	=	Delta-Z1 "	+	Delta-X1(2 back)
R4	=	Delta-Z1 "	+	Delta-X1(3 back)
R5	=	Delta-Z1 "	+	Delta-X1(4 back)

Five counts made simultaneously, with R1,R2,R3,R4,R5, used instead of the corresponding impulse of Q, are evidently equivalent to a count, for the same conditions, at each of the following settings for the multiply tested wheel: present, 1 back, 2 back, 3 back, 4 back.

(d) R1 R2 R3 R4 R5 : Switching and Plugging.

R1 R2 R3 R4 R5, must be plugged or switched in the usual way. The provision for them is less generous than for ordinary impulses. On the Q panel they have two switches each in the upper part, one switch each in the lower part. On the plug panel they have two jacks each: these jacks are part of Q and are controlled by the main Q selecting switches.

(e) R1 R2 R3 R4 R5 : Relation to the Five Counters. (regrettably obscure.)

R1 R2 R3 R4 R5 may of course be switched or plugged into the counters in any order; but Colossus cannot recognise this and therefore always prints the setting. for a batch of five scores in the same order, viz backwards (e.g. 11, 10, 09, 08, 07).

The counters print in the order 1, 2, 3, 4, 5, and therefore if each setting is to be printed opposite the appropriate score, the settings in the five counters must likewise run backwards. (e.g. 11 in 1, 10 in 2, 9 in 3 , 8 in 4, 7 in 5).

The settings corresponding to R1 R2 R3 R4 R5 also run back wards (R1 is resent, R2 one back etc.) and therefore, finally R1 is switched to counter 1 etc.

It may sometimes be profitable to put R1 R2 R3 R4 R5 into the counters in reverse order (e.g. in rectangling).

(f) Manner of stepping

The wheel on multiple test can step either fast or slow [53D (c)] but in either ease it steps five positions at a time, for obvious reasons. The batches of five settings are not arbitrary but must belong to the sequence 02-06, 07-11, 12-16 ..... ending with the batch whose present position is O1 (e.g. X1 ends with 38-01). 1

(g) Multiple Testable wheels.

Multiple testing is provided for all wheels except Mu61 Xs , PSIs were added later and have not been fitted to all colossi. Mu37 has its own switch: the others are in pairs, each pair sharing a three-way switch, viz X1 , X2 ; X3 , X4 ; PSI1 , PSI2 ; PSI3 , PSI4 ; X5 , PSI5.

(h) Mu 37

Multiple testing on Mu 37 has some special features. It can be used only for motor runs in which a count is made against motor = ., or motor = x. It cannot be used for motorizing the psis.

The Mu37 multiple test switch, not only puts the wheel on multiple test, but also puts Mu 37 alone into the switches R1 R2 R3 R4 R5 on the Q panel, where it can be switched in the normal manner. (commonly Mu37' = ., but sometimes M37 + Delta-D12 = .). The effect of these switches is not modified by the limitation determiner switches: they always represent the basic motor. For a total motor run what is required is BM = . and lim = X. BM = . is imposed by these R switches. Lim = x is imposed by the TM switch on the Q panel, the limitation determiner switches being thrown to BM c/o and the appropriate limitation.

(i) No Multiple Test for Motorizing.

It is impossible, in a run involving the psis, to use multiple test on any wheel which influences the total motor, for this would require that the psis should move in two different ways at once. In practice the wheels thus restricted are Mu 37, psi 1, and, with P5 limitation, chi 5, psi 5. It is however, possible to use the multiple test switch merely to step one of these wheels five positions at a time, ignoring four setting out of five. This is useful for PSI'1 because of coalescence [23X].

(j) Multiple Test Doubting (Special Patterns).

Multiple test normally applies only to ordinary patterns, not to special patterns. On Colossi 5,8,10, however, it can be applied to the corresponding special pattern also. The appropriate switch is in the bottom row of the selection panel. As always with special patterns, it must be plugged, viz. from the appropriate special pattern jack to one of the two jacks labelled Multiple Test Doubting . or x : these select places where the special pattern is ., or x, respectively, in all counters.

(k) Checking of Multiple Test Scores.

It is generally undesirable, because of confusion about settings, to check scores with multiple testing in. In place of R1 R2 R3 R4 R5 the ordinary impulse is used, and of course, the wheels must be reset.

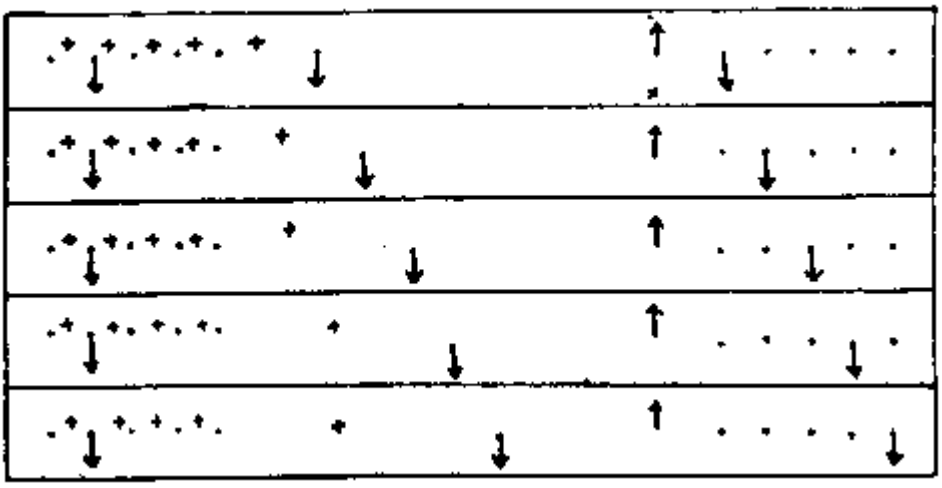
For Mu 37 this means that, in the lower part of the Q panel, what is used is not R1 R2 R3 R4 R5 but TM. In checking a total motor run the BM c/o must be restored to its normal position.

For special pattern multiple test this means that the special pattern shall be plugged into the ordinary all-counters, not into the multiple test doubting jacks.

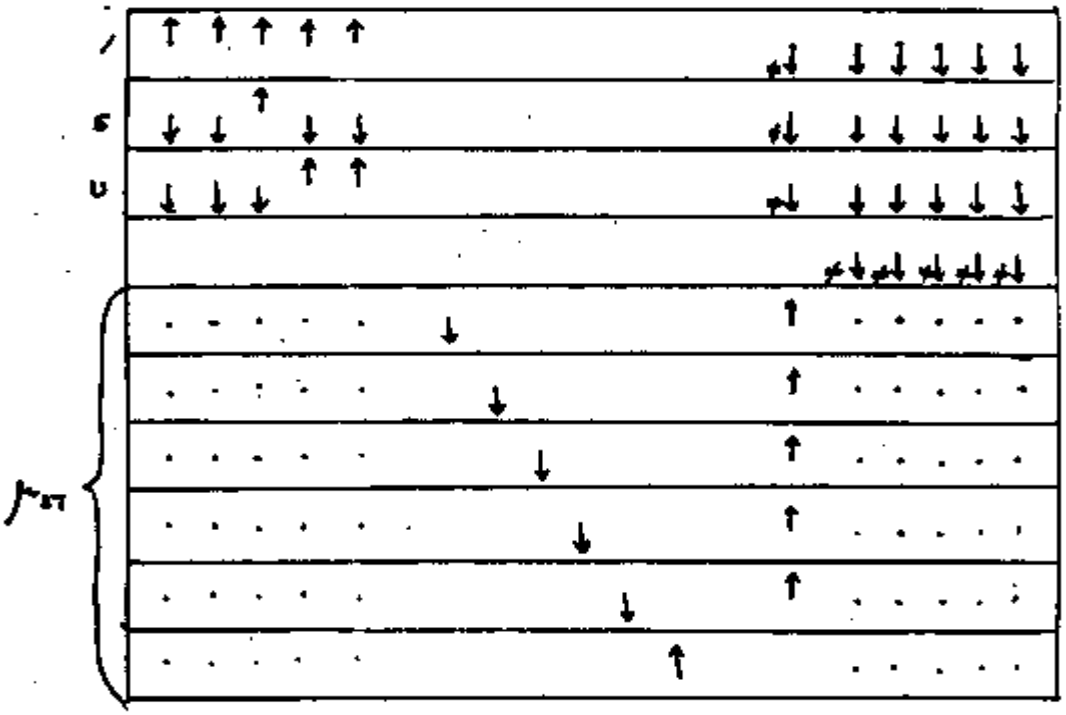
(l) Examples of Multiple Test Switching.

(i) 1+2 = .

Note : this may be either Delta-D12 = . to set X1 and X2,
or P12 = . to set PSI1 and PSI2.
On the Q panel the switching for their two cases is identical.



(ii) Mu 37 = ./5U/1,X2oneback x . A total motor run for M61 M37 when X2oneback limitation is in use, counting TM=., where AD = /,5,U.

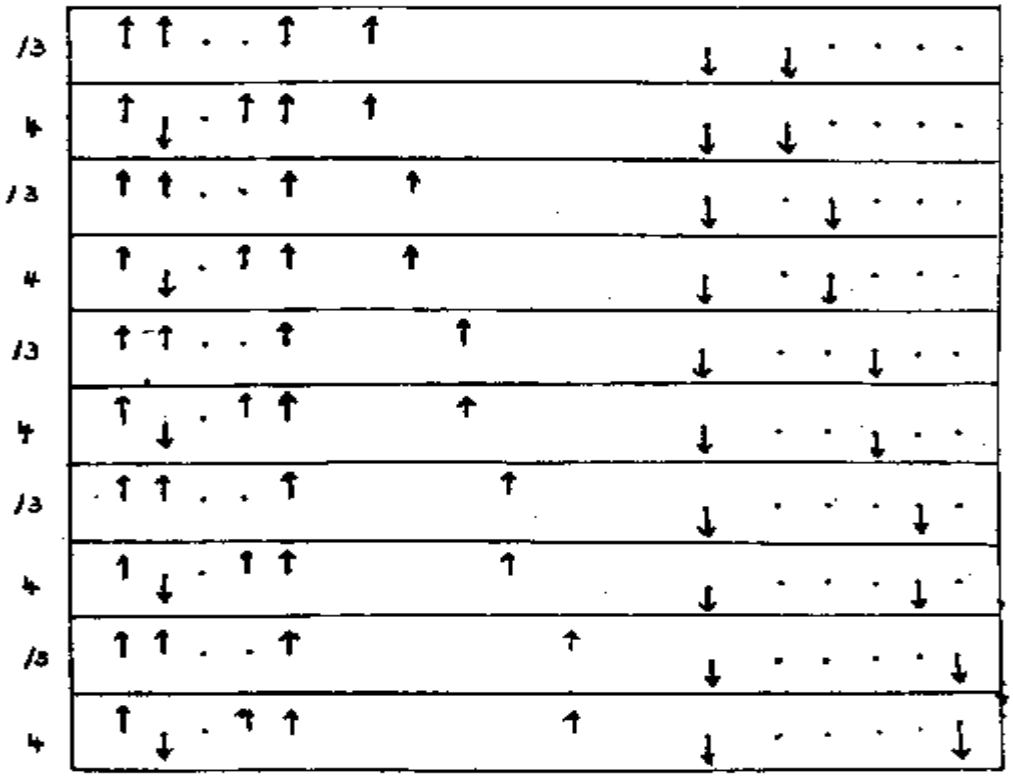


other switching

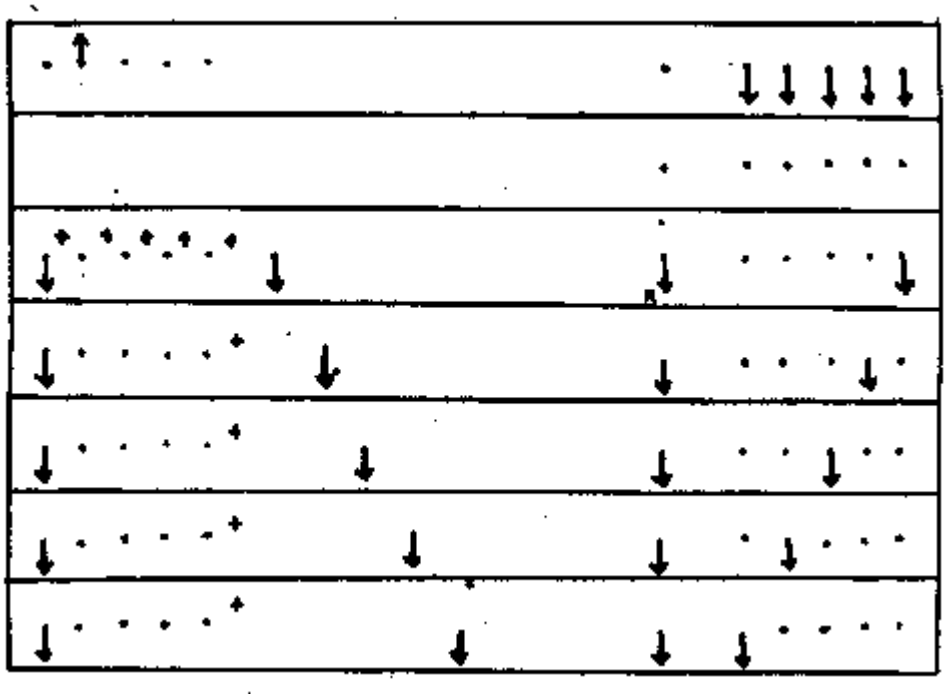
M37 multiple test, step M37 slow, M61 fast.

Limitation determiner switches : BM c/o, X2oneback in. For checking this run see 53L (k).

(iii) P not = /,3, to set Chi 3, Psi 3, with multiple testing on Chi 3, all other wheels being set



(iv) The short wheel-breaking run 3+/1.2. It is not worth while to use multiple test for one-wheel runs, unless the tape is very long, as it may be in chi-breaking. For the reason why 3+1 is switched to cross see 25A.(b) R1 R2 R3 R4 R5 are switched into counters 5,4,3,2,1 so that scores shall be printed An the correct order [53L (c)].



53M. COLOSSUS RECTANGLING GADGETS.

(a) The principle of Colossus Rectangling.

To render the gadget more intelligible the how and why of Colossus rectangling is explained [see also 24B(f)].

Suppose that the Chi 1, Chi 2 triggers each contain one cross, that Q = X ; and that Q is switched : Q1 = x, Q2 = x. This will select a set of places all of which are opposite a particular character of chi1, ands also opposite a particular character of chi 2, i.e. they will belong to the same cell of the rectangle.

Plug Delta-Z1 + DeltaZ2 = .

Throw the lower stepping switches, so that chi 1 (down) steps fast and controls chi 2 (up).

Chi 1 will step, producing a row of the rectangle : when Chi 1 reaches the setting plug, chi 2 will step one.

Chi 1 then atop again, producing the next row, and so on.

(b) The Rectangling Gadget.

If the rectangle were made exactly as above the entries would be printed on separate lines each preceded by the settings of chi 1, chi 2. It is much better to have the row printed as a row. Accordingly a gadget is fitted such that

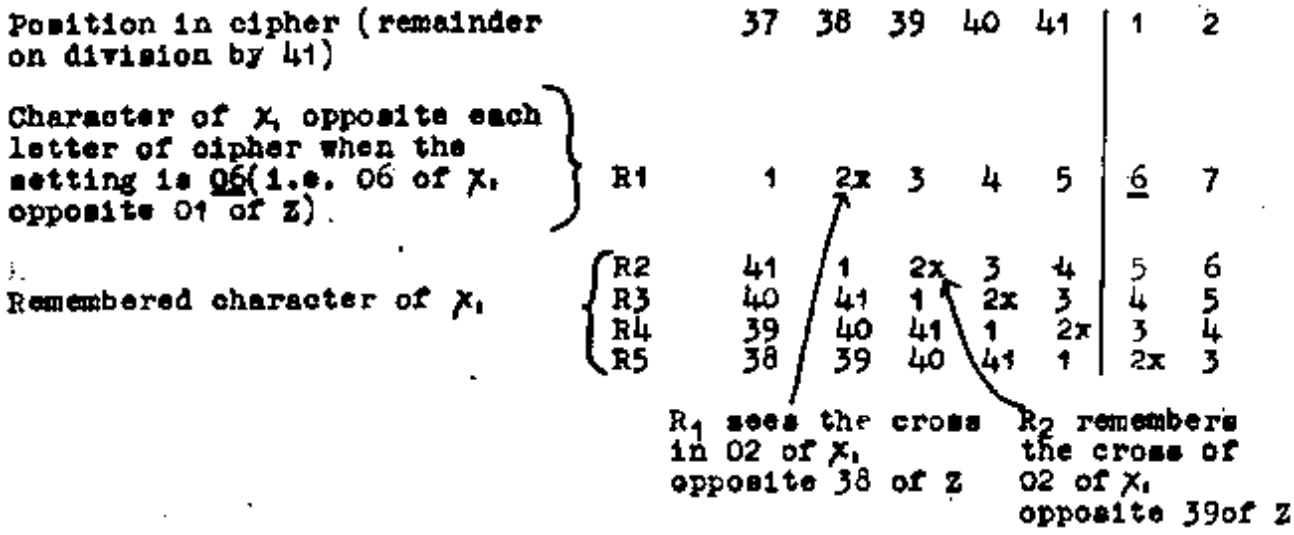
(i) Carriage return is operated only after the completion of a row.
(ii) settings are not printed.
(iii) A score is printed as a single figure.

On Colossus 6 scores exceeding 9 are represented by letters viz. A = 10, B = 11 and so on.

(c) Multiple Test in Rectangling.

To increase the speed of rectangling, multiple testing on X1 is used. Multiple testing always examines batches of settings whose "present" member belongs to the sequence 1,6,11.....41. The first batch of settings in each row of the rectangle is chosen to be 02 - 06, 06 being "present", 02,03,04,05 "remembered". In order that X2 shall step at the correct position of X1, the X1 setting plug must be at 01. If however X1 were actually set at 01, the first row would begin with settings 38, 39, 40, 41, 01. To make the first row begin 02, 03, 04, 05, 06 the wheels are set with the X1 plug at 06 : the plug is then returned to 01 without resetting.

Because the rectangle is made backwards the first five readings should be for the last five cells of the rectangle, which contain places of the cipher whose remainders on division by 41 an 37, 38, 39, 40, 41 so that the required differences (Delta-Z1) are 37 + 38, 38 + 39, 39 + 40, 40 + 41, 41 + 01. Since Colossus differences backwards, the cross in X1 must be against cipher places 38,39,40,41,01. The first batch of settings is 02,03,04,05,06; and therefore the cross must be in position 02:



X2 has a cross in 02, for symmetry, and it follows that its setting is 02.

The last batch of settings is 38,39,40,41 and 01 of which 38,39, 40,41 are also in the last batch but one: the rectangle gadget prevents these from being printed twice.

(d) Print Scores

Done thus, the rectangle would have to be done twice, for Delta-Z1 + Delta-Z2 = ., and for Delta-Z1 + Delta-Z2 = x. Conditional rectangles are done this way; the rectangling switch is thrown to "print scores".

(e) The Subtraction Gadget.

If the depth is constant, which will be the case if the text length is a multiple of 1271 and 99's are not cancelled, the score for Delta-Z1 + Delta-Z2 = . will suffice, for the bulge equals (Delta-Z1 + Delta-Z2 = .) minus depth. A further rectangling gadget performs this arithmetical operation if the rectangling switch

is thrown to "normal", and the appropriate depth switched in on the rectangling panel.

This is the usual Colossus rectangle method : it is often disadvantageous for short texts because so much is lost by reduction to a multiple of 1271.

Note: Although the subtraction gadget can be used independently of the rectangle gadget proper, it is too limited in scope to be of value.

(f) Switching.

the 3-way rectangling switch at the extreme right of the control panel has two active positions : "Print scores" and "normal".

The other switches are on the rectangling panel. Any chi-wheel can be multiply tested for making a rectangle : the corresponding switch of the bottom of the rectangling panel must be thrown. This determines when carriage return is operated and how many surplus scores are cancelled.

The subtraction gadget is controlled by a series of switches labelled 1 to 36, each number indicating the depth to be subtracted.

(g) The Cyclometers.

The Theta(ij)^2 significance test is based on the number of occurrences of each possible value for the entries in a rectangle.

At the top of the rectangling panel is a row of cyclometers to record these occurrences.

Below these is a row of jacks, one for each cyclometer. A pulse here steps the corresponding cyclometer.

Below these again are two rows of jacks labelled 1,2,3.... A score of +- Theta produces a pulse in the jack Theta.

These score jacks can be plugged arbitrarily to the cyclometer jacks.

(h) The punch.

Colossus 6 can make a rectangle in the form of punched tape. A negative score is always represented by a cross in the fifth impulse, but otherwise a score can be represented by an arbitrary letter, selected by plugging from a score jack to a punch jack.

There is a score jack labelled CR which carries the pulse of the carriage return at the end of each row of the rectangle. This is normally plugged to the punch jack labelled 9oneback/ which punches / and adds a cross to the third impulse of the preceding letter (c.f. Appendix 95).

(i) Rectangle not 99.

In any cell of the rectangle containing a place where Z = 9 adjacent to another 9, this replaces the entry by zero. It is useful only for rectangles of depth one.

53N. CONTROL PANEL.

See the photograph.(Fig 58(x))

MAS is the master switch (upper row, second switch from right; labelling obscured in the photograph). Unless this switch is thrown Colossus can neither count nor step. It is however possible to set wheels and to reset counters.

The switches labelled X, Mu, PSI, are the stepping switches 53D(c). The switches labelled mult are multiple test switches 53L(g). X5, PSI5 are oddly placed.

The other switches are

PMH	Print main heading [53G(g)]	PCO	Printer cut-out [53G(i)]
SET ?	Set wheels [53D(a)]	Lc/o	Lamp cut-out [53G(d)]
RESET	Reset counters [53G(j)]	LC	Letter Count [53G(h)]
REC	Rectangle [53M(f)]	KL	Cancel lights [53G(d)]
		SIP	Significance Interpretation [53G(b)]

53P. COLOSSUS TESTING.

Any account of the methods used by the engineers to test Colossi would be entirely out of place in this report, but it is appropriate to refer to the methods used by Wrens, chosen to carry out routine tests.

Owing to the complexity of its operations Colossus can produce results so erroneous as to be useless without arousing suspicion till valuable time has been wasted.

Runs have therefore been selected such that a machine faulty in any respect is unlikely to give correct scores, and these have been done on Colossi known to be in good order, using selected standard wheel patterns and a selected standard tape. One set of triggers on each Colossus is now assigned to these standard patterns, and standard tapes are kept in stock : the runs are repeated on all Colossi at frequent intervals.

A single fantastic run could doubtless be devised to check everything, but it is preferable to use a number of runs, which in themselves will aid in locating faults. Z and X are first tested without PSI.

Of course when there is a fault the ordinary chi and psi tests [23K(d)] will fail, thus providing a crude test of Colossus very frequently.

54 ROBINSON

54A Introduction

54B How scores are exhibited

54C Bedsteads and position counting

54D The Plug Panel

54E The Switch Panel

54F Miscellaneous Counter Facilities

54G The Printer

54H Control Tapes

54J Some Robinson plugging used operationally.

54 - ROBINSON

54A INTRODUCTION

Robinson was made in three versions known as

Heath Robinson.
Old Robinson
Super Rob(inson).

Super Robinson is described in detail: the others, which do not differ in principle, are mentioned in chapter 52.

For photographs see the end of this volume. (Fig 58(iii,iv,v,vi,vii))

Let four or fewer teleprinter streams punched on tapes, with uniformly spaced sprocket-holes, be imagined laid side by side, so that their letters correspond, sprocket-hole by sprocket-hole.

Robinson can count the number of places in the combined stream where certain conditions are satisfied.

Rather more generally, it can count the number of places such that certain conditions are satisfied involving that place, and the place one forward (this includes differencing) together with two conditions involving the place one back, and one condition involving the place two back.

Apart from this it cannot count a condition involving two different places except by using two tapes alike, appropriately staggered.

An essential feature is that the counts can be made in rapid succession, with the various tapes in different relative positions (stepping) : stepping is necessarily uniform though the step between successive counts may be any number of sprocket-holes.

54B HOW SCORES ARE EXHIBITED.

The scores so counted are exhibited in two ways

(i) On display.

(ii) By the printer.

The display is a ground glass screen on which numbers can be projected by small electric lamps.

The four upper digits are the position counter , i.e. they show the relative position of the tapes.

The four lower digits are the score counter .

The printer simply prints all 8 digits in order, without spacing. So that e.g. 25341798, means position 2534 score 1798.

Footnote Display can be switched off either entirely or to show position only. There are more printer details later.

54C BEDSTEADS AND POSITION COUNTING

(a) Bedsteads

A bedstead is a system of pulleys round which the tape is driven by a sprocket wheel at about 2000 sprocket-holes per second, so as to be scanned by photo-electric cells.

There are four bedsteads A,B,C,D: to ensure simultaneous scanning of corresponding places on different tapes, their four sprocket wheels are on a common shaft.

(b) Bedstead Drive

To reduce the tearing of sprocket-holes, two of the pulleys are driven at the correct speed. For the same reason the drive is applied gradually when starting, and removed gradually when stopping (by means of relays).

The tapes are draped loosely on the pulleys, centrifugal action tends to tighten them, and they may need to be slackened. After a long run tapes may stretch.

Between the "Gate" and the sprocket wheel the tape moves past two engraved marks: to ensure that the tape is correctly placed these are aligned with an appropriate pencil mark on the tape [Fig.58(iv)]

The tapes, which are of course continuous loops, are jointed flexibly with Bostick.

One spring switch is used both for starting and stopping: it is thrown down (and released) for start, up for stop.

(c) The Gate

Each bedstead has 13 photo-electric cells which scan the tape as it passes (downwards) through the "gate". The gate is placed as near as possible to the driving sprocket to reduce the effect of stretched tapes.

One of the photo-cells scans the sprocket-holes, permitting the counters to add 1 or 0 at each sprocket hole.

In each position of the tape 10 of these cells scan the 10 dots and crosses in two consecutive places on the tape, the 10 outputs appearing in 10 jacks on the plug panel (the output from each bedstead in the 10 jacks immediately below the corresponding letter), and nowhere else.

(d) Start and Stop Signs

The remaining two photo-cells look for the start and stop signs which are punched in the 4 1/2th and 3 1/2th impulses of the tape, exactly as on Colossus.

A start sign causes the machine to start counting.

A stop sign causes the machine to stop counting, transfer the count to relays, and prepare for the next start sign.

Only one start sign and one stop sign are used as such at any time; these are not necessarily taken from the same bedstead: they are selected by the switches above the plugboard. Start (on A,B,C, or D) by the first four: Stop (on A,B,C, or D) by the second four.

(e) Position Counter

The start signs are used also for finding the relative positions

of tapes. If one (say B) of the right-hand switches above the display is thrown, the position counter shows how many sprocket-holes the start sign on B is behind the start sign used as a start sign.

(f) Period Dials

These are above the display reading 0000 - 9999.
It they are set e.g. to 1271, as soon as the position counter reaches 1271 it returns to 0000 i.e. the reading is always the remainder on division by 1271.

(g) Split Position Counter

If one of the left-hand switches above the display is thrown the position counter is split in two, each half working independently, reading up to 99. The first two digits show the position of the tape selected by the left-hand switch. The second two digits shown the position of the tape selected by the right-hand switch.

Splitting splits the period dials also, e.g. if the dials are set to 4131, the first two digits show the remainder on division by 41, the second two digits show the remainder on division by 61. These may refer to the same or different tapes.

(h) Settings

By convention the setting of one pattern relative to another is the place on the latter against the 1st and not the 0th place on the former. Thus setting = Rob reading + 1.

(i) Stepping

Stepping is effected on Robinson by using tapes of different lengths. If A is m sprocket-holes longer than B, and the original setting is 01, then after a revolution, A will return m sprocket-holes later than B, i.e. the 1st place on A is opposite the (m+1)th place on B, and the setting of A relative to B is +m.

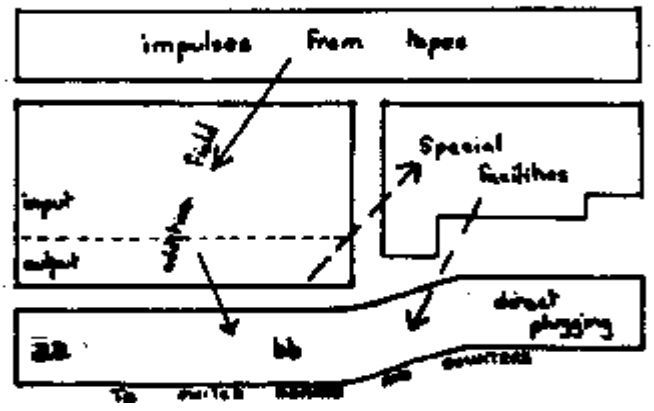
A is said to have moved forward relative to B.

(j) Repeat light

When the position counter returns to its original reading a repeat light appears below the display.

54D THE PLUG PANEL

(a) Layout
The jacks on the plug panel may be grouped thus.



Conditions can be imposed only by plugging both:

1. From tapes to Addition Field input.
2. From Addition Field output to switch panel.

The latter however may be plugged via "Special Facilities". Note that this forbids plugging direct from tapes to switch panel.

Subject to the above rules (and some minor restrictions in the ordinary addition fields) any jack may be plugged to any other. No jacks in the plug panel ate permanently linked except the columns of the addition fields (ordinary and special).

(b) Pulses from Tapes

The arrangement is obvious from the picture.

The upper row is one forward on the tape.

The lower row is present position on the tape.

(c) Ordinary addition fields

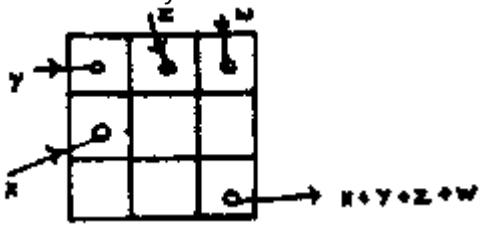
Pulses (one or more) from tapes, plugged into input jacks in any column, appear added together in both the output jacks of that column. For technical reasons there are certain restrictions on the use of these fields. Each of the left-hand five columns has two pairs of input jacks (upper and lower). Each of the right-hand five columns has a single pair of input jacks. Impulses plugged into the two jacks of a pair must come from the same tape. If there is only one impulse in a pair it should be in the upper jack of the pair. Impulses from different tapes can be added only in the five right-hand columns (or in the special addition field). Each column of the addition field has two output jacks from which the impulse may be plugged directly to the switchboard or to some special facility.

(d) Special Facilities

These are special addition, Permanent cross, one back and two back.

(e) Special addition field

This is exactly the same as a Colossus addition field e.g.



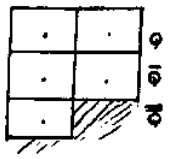
Note: other columns in the addition field are unaffected by this and can be used separately.

(f) Permanent Cross.

The e is a column of jacks to the left of the special addition field: each of them bears a permanent cross, which can be added, in the special addition field, to any impulse. This is useful for making an impulse equal a cross when using "direct plugging".

(g) One back and two back

There are five jacks at the right of the addition field



in each column any impulse plugged into Q

appears one back in Q bar and, in the left-hand column

two back in Q double bar

The notation Q is unfortunate: it is not analogous to Q on Colossus. I would be better.

(h) Plugging into the switch panel.

The output of an ordinary addition field, or of any special facility may be plugged into the switch panel where the conditions, a count for which is to be made, can be imposed.

An impulse plugged into one of the 10 jacks in the bottom row of the switch panel appears on two switches, one labelled x dot, and, immediately below this, one labelled + . The first five jacks correspond to the five pairs of switches aa , the second five to those of bb. The impulses are called (not written on machine) Q1,Q2,Q3,Q4,Q5,Q6,Q7,Q8,Q9,Q10.

Footnote: These are not related to Q,Q bar,Q double bar: they(i.e.Q1,Q2 etc.) are broadly analogous to Q on Colossus, but the impulses plugged into them are quite arbitrary.

The five flacks marked "direct plug" in the diagram have essentially the same function, but are permanently switched to dot.

54E THE SWITCH PANEL

(a) Layout

Without the diagram at the end of this volume, this description will probably be completely obscure; Fig 58(vii).

(b) Q Switches

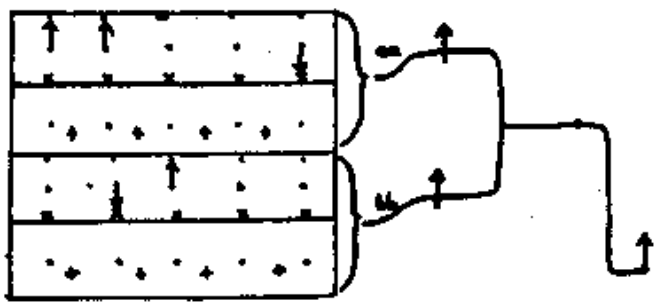
The two rows of switches in the left half of the switch panel will be described first: the conditions they impose may be modified (may even be reversed) by the switches in the right half.

The switches to the left of aa control impulses Q1,Q2,Q3,Q4,Q5.

The switches to the left of bb control impulses Q6,Q7,Q8,Q9,Q10.

A switch labelled X dot can be thrown either to make its impulse a dot or to make its impulse a cross.

If several are thrown, all their conditions are imposed.

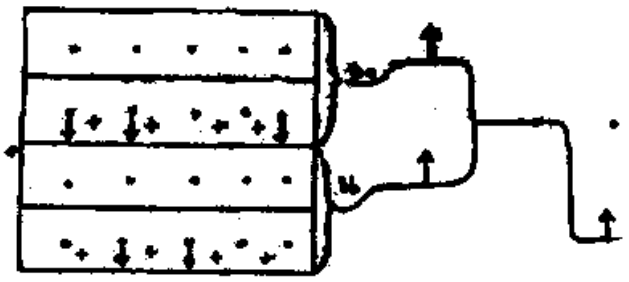


Impose the conditions

Q1 = . Q2 = . Q5 = x

Q7 = x Q8 = .

Switches labelled + can be thrown (down only) to add one or more impulses and equate their sum to a dot.



Imposes the conditions

Q1 + Q2 + Q5 = .

Q7 + Q8 = .

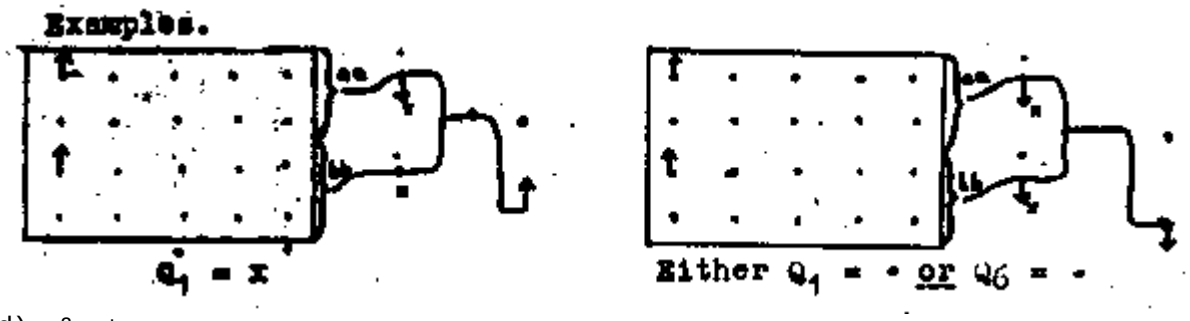
(c) Yes Not Switches

On the right half of the switch panel white lines are drawn: conditions imposed must in effect, pass along these lines.

Switches situated on these lines modify the conditions which pass through them: of these aa, bb and the bottom switch are three-way switches labelled

(. which means : condition is unchanged (yes)
(
(which means : condition in cancelled
(
{ x which means : condition is reversed (not)

The & + and red switches are described later: at present they are supposed to be in their normal positions.



(d) & +

Two conditions reach this switch, from aa and bb.

& means both;
+ means both or neither.

It is intended for use with Q + switches

e.g. Q1 + Q2 + Q3 = . , Q8 + Q9 = . , + , means
(either Q1 + Q2 + Q3 = . and Q8 + Q9 = .
(
(or Q1 + Q2 + Q3 = x and Q8 + Q9 = x

i.e. Q1 + Q2 + Q3 + Q8 + Q9 = .
Obviously any number of Q's can be added.

54F MISCELLANEOUS COUNTER FACILITIES

(a) split score Counter

If the red switch to the right of & + is thrown the score

counter is split into two, each counting independently up to 99.

The 1st and 2nd digits count for conditions imposed in bb

The 3rd. and 4th digits count for condition imposed in aa and direct plugging.

(b) Span Counter

This makes it possible to count on a part only of the text between start and stop.

It controls two sets of decade switches (0000 - 9999) labelled "start", "end", on the panel above the printer.

If "start" is set at m , "end" at n , the places counted on from the mth to (n-1)th inclusive, on the tape from which the start sign is taken.

Note: The position counter continues to work in terms of start signs not in terms of the beginning of span.

(c) Set Total

A device whereby only scores which exceed, or, alternatively, scores which do not exceeded; a fixed score, are displayed or printed. The switches are above the plug panel, viz. a set of decade switches (0000 - 9999) and a three way switch, >,off,<.

54G THE PRINTER

(a) Lost scores

On Robinson stepping is always uniform, so that when scores appear in rapid succession it is not possible to inhibit stepping till they can be printed and scores may thus be "lost". Various devices are used to prevent this.

1. The printer is made to print as fast as possible, without spacing, in fact too fast to print the same figure twice successively. When two or more digits which are alike occur together, the printer replaces all but the last by arbitrary letters (actually a,b,c,d,e,f,g for the first seven digits respectively) for example ab072f39 means 00072339.

2. Two scores can be stored at once (instead of one as on Colossus).

3. The machine is not made to count as fast as it could be.

4. If nevertheless a score is lost, this is shown in two ways.

(i) A light appears below the display (labelled "lost count")

(ii) A cyclometer records the number of lost scores.

The cyclometer can be reset (but only one at a time) by throwing a switch near the cyclometer up to "meter".

(b) PCQ

This switch cuts out the printer: unfortunately if it is thrown to normal during a run it is apt to demoralize the printer and produce rows of dots.

(c) RESET

This switch clears the display and all scores which are in storage.

54H CONTROL TAPES

(a) Definition

A control tape is one used to select a set of places on another tape whereon a count is to be made.

These places may be all consecutive, or in in la ed groups, either regular or irregular.

(b) Spanning by means of control tapes

In particular if all the places are consecutive, and if still more particularly the tape steps in unison with the tape from which the start is taken, a control tape is equivalent to spanning. Spanning by dials has of course the advantage that it can be adjusted rapidly, and if the spanning required is not known beforehand this advantage is overwhelming.

Spanning by a control tape was used for some early versions of mechanical flags and rectangles, in which several different spans are needed: the spans were represented on the control tape by different letters, and selected by means of a letter count which is easier than respanning. This was discontinued when the split score counter was introduced only because it absorbed too many of the conditions which can be imposed on the bb half-count.

A compromise, spanning large pieces of text by dial and subdividing these by a control tape is quite feasible.

Old Robinson has no span counter so that spanning had to be effected by control tape, or more commonly by a control impulse replacing an impulse of the tape to be counted. This was often necessary because the minimum text length was 2,000.

(c) Irregularly spaced selection

Wen the places to be selected are not consecutive a control tape or impulse must be used: the method is obvious: it can be employed to eliminate corrupt letters.

(d) Regularly spaced selection

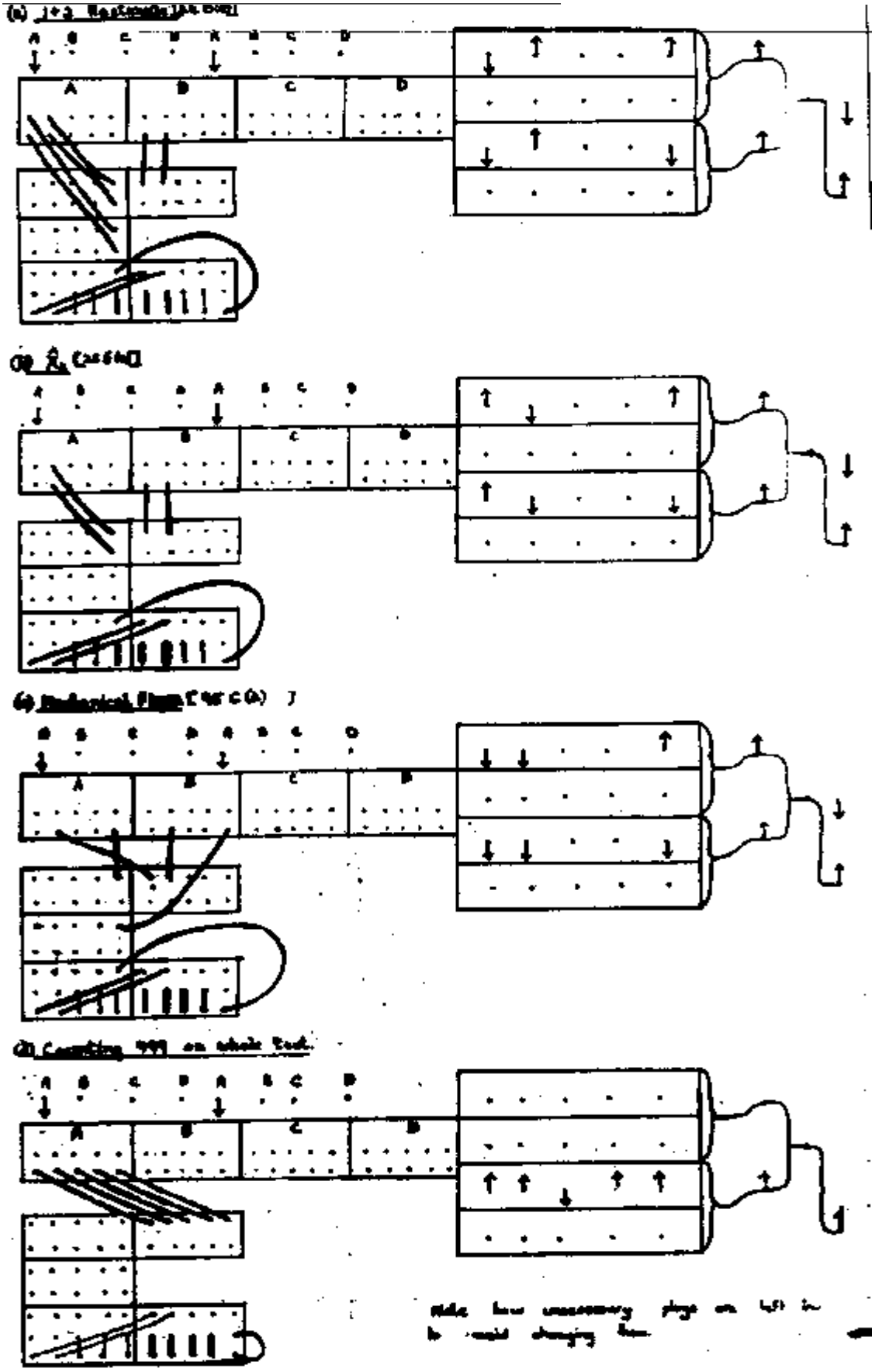
Some simplification is usually possible: the length of the control tape can be any multiple of the cycle which can be put on the bedstead. A proper choice for the length of the other tape will usually suffice for any stepping required. A good example is the 1+2 rectangle [24 B (e)]

(e) Number of different selections made by one tape

A single control tape /9/H/T and so on can, by imposing the conditions Cfwd = 9, C = 9, Cfwd = H, C = H, and so on, be made to select a cycle of 62 or fewer places.

A single impulse of a tape with the pattern xxxx....xx.x..x.. can, by use of Cfwd, C, Coneback, Ctwoback, be made to select a cycle of 16 places.
[R3 p75]

54J SOME ROBINSON PLUGGING USED OPERATIONALLY



55 - SPECIALISED COUNTING MACHINES

55A DRAGON Figs 58(xxvi-xxx) (Details apply to Dragon 2 only)

(a) Purpose and method

The purpose is to set a common crib P, of up to 10 letters, in a given de-chi D, i.e. to find a stretch of D (if there is one) where the underlying plain text is P, so that P + D = PSI' , which when the extensions are removed, yields PSI .

Dragon adds P to a stretch of D in all positions in turn: in each position it contracts P + D, i.e. omits repeated letters, and then compares each impulse of the result, independently, with the corresponding PSI wheel : it all five can be fitted the machine stops and displays the settings of D and all PSI's at the last letter of the crib.

(b) Use of motor or limitation

Although the majority of repeated letters in PSI' are due to extension some are not, and the method will obviously be more powerful if P + D is contracted only at total motor dots.

Dragon 1 cannot do this; Dragons 2,3 can. In practice if the motor settings are known it is unnecessary to use Dragon: the facility can however be used with great benefit to forbid contraction at limitation dots.

(c) Setting up D, PSI, X2, Mu .

(i) The de-chi D is on a tape fed into a tape-reader. Dragon remembers it ten letters at a time.

(ii) The crib P is plugged on a 10 x 5 array of jacks. The length of the crib can be reduced by the top row switches: starting at the left, each switch thrown up cuts out one letter. The only letter which can be cut out from the middle of the crib is the fifth, by throwing its switch down.

There are actually two 10 x 5 arrays, selected by a switch, so that one can be set up while the other is in use.

(iii) PSI . PSI is plugged up as usual: above each jack is a lamp to show the setting at the end at a successful crib.

(iv) Mu, X2 Mu61, Mu37, X2 have each two rows of jacks, the lower for the pattern, the upper for the setting at the start of the de-chi.

(d) The display

When a crib sets, this shews the settings, at the end of the crib, of Mu61, Mu37, X2, D. D is measured in lines of 31.

The display also shows each position (1,2,....9).where P + D has been contracted.

(e) The de-chi display

Above the crib jacks is a display showing, in dots and

crosses, the ten letters currently under examination.

(f) Miscellaneous facilities.

(i) A cut-out switch for each of the five impulses.

(ii) Set total for extensions such that Dragon does not stop unless there is a minimum number of extensions. Switch 5 means 5, switches 5 and i means i .

(iii) Switch for use when setting tapes back, such that the recorded setting of D remains stationary.

(g) Miscellaneous switches

Reset tape, Reset tape and wheels, reset X2, Mu, limitation, single step, de-chi display cut-out, test, start-stop.

(h) Dragon 1

Always contracts a repeated letter.

(i) Dragon 3

A much larger machine; can deal with a 16 letter crib, or with two or three shorter ones simultaneously. It can cope with a gap of up to 5 letters in the crib, trying every possible number of extensions in the gap.

(j) Salamander

This is a "compatibility" gadget for attachment to Dragon [see 28B (d)).

55B PR0TEUS (Fig 58(xxxi))

(a) Purpose and method

Proteus anagrams depths [28A(d)(ii)]

The given depth V is known to be the sum of two plain texts P(a) + P(b) . It is expected that at some position one of these will be a very common group of plain text letters, say one of the six commonest: this is called the crib, P(1); and that at the same position the other is a fairly common group, one of several hundred , called the dictionary P(2).

Then of course P(1) + P(2) + v = /.

What Proteus does is to add P(1), P(2), V in all positions looking for a position where the sum is all /'s.

(b) Setting up, P(1), P(2), V .

(i) P(1) The crib has a length of seven or fewer letters and is set up by plugging. Each letter has 6 jacks: a cross in the 6th means "ignore this letter". Actually six cribs are set up and examined simultaneously but independently.

(ii) P(2) The dictionary is on a tape running on a Colossus bedstead, with blanks between groups.

(iii) V The depth is on a tape fed into a tape-reader.

(c) Operation

Proteus is started: it reads and remembers the first seven letters of the depth, adds them to the crib, and as the dictionary is scanned adds this also in all positions looking for a click consisting entirely of strokes.

If no click is found, the tape reader steps. Proteus acquires the 8th letter and forgets the 1st, so that letters 1-7 are replaced by letters 2 - 8; and so on.

When a click is found, Proteus stops, and displays

(i) The position in the depth (last letter) measured in lines 31 long.

(ii) The successful crib (1,2,3,4,5, or 6).

The place in the dictionary must be found by hand,(by addition).

The anagram can be checked throwing a switch to "rerun", so re-examining the same seven letters of the depth.

To resume stepping throw the switch to "reset".

(d) Other Applications

Proteus is equally applicable to any mod-2-addition teleprinter cipher which has true depths.

55C AQUARIUS Fig 58(xxxii).

(a) Purpose and method

Aquarius sets go-backs [28B(f)] using a de-chi.

In the correct position, the two P's are the same, so that Delta-D(a) + Delta-D(b) = Delta-P(a) + Delta-PSI'(a) + Delta-P(b) + Delta-PSI'(b) = Delta-PSI'(a) + Delta-PSI'(a)

Aquarius adds a stretch of de-chi immediately after the autopause to a stretch before the autopause, differences the sum, and makes counts for resemblance to the sum of two Delta-PSI's. The proportional frequency of each letter depends only on the number of crosses in it. and the six switches are for counting letters with 0,1,2,3,4,5 crosses: throwing more than one switch provides "either - or",

Two counters are provided (generally used for all dots, all crosses.)

(b) Stepping

At first the comparison is made on a steadily increasing, text, thus: first 11 letters after the auto-pause with last 11 before; then first 12 after with last 12 before, and so on.

After the text length has reached 97 there is no further increase, but the 97 letters following the autopause are stepped back relative to the part before the autopause. 97 letters are sufficient: in a long go-back the letters immediately before the autopause may be rubbish.

(c) Setting up the de-chi

The most entertaining feature of Aquarius is that the tape is used only at the outset, to set up the de-chi electrically, viz. on condensers : a charge represents a cross: these are automatically recharged at least once every two minutes, according to the rule "to him that hath shall be given".

The tape is marked at the 97th letter beyond the autopause and (switch: reading position, home, charge operating length, start reader) run backwards through a tape-reader and so transferred to the condensers. It stops automatically at the autopause, where its position is checked. Then (switch: charge comparison length, start reader) 218 letters before the autopause are similarly transferred. Switch: comparison length off, reader off, comparison
position, home.

(d) Running

A set total is imposed on each counter (for /'s and 8's) and the machine is started.

In a position where the score on either counter exceeds set total, the machine stops. The set total is taken off and the switch thrown to "rerun" (i.e. count again without stepping). This checks the score and finds the score on the other counter.

To resume stepping the switch is thrown to "go on".

Because the text length increases, the set total requires occasional adjustment.

(e) Impulse cut-out

Switches labelled 1,2,3,4,5 cut out these impulses, causing them to be treated as all dots.

(f) The Buzzer

This is provided to call attention to imminent catastrophes.

56 - COPYING MACHINES

56A Hand Perforator.
56B Angel.
56C Insert Machine.
56D Junior.
56E Garbo.
56F Miles
56G Miles B C D.
56H Miles A.
56J Tunny and Decoding Machines
56K Tunny
56L Decoding Machines

For general description and classification see Chapter 13.

56A. HAND PERFORATOR.

Operation of the keyboard produces punched tape.

56B. ANGEL.

This simply copies tapes. It consists of a tape-reader linked to a reperforator. To make corrections by hand, it is necessary to stop the machine, and replace the input tape by one bearing the letter to be inserted.

56C. INSERT MACHINE.

(Vulgarly known as the IBM machine)

Functionally this is an Angel with a device for making corrections by hand easily. In addition to the reader and reperforator it has a punch insertion typewriter to which nine special keys have been added, thus

For normal running use "read" : "start" means start and continue to run; "step" means step one letter.

To insert letters, "stop" and
for A to Z use the ordinary keyboard;
for 9 use the space bar;
for 3458/ use the special keys.

To step the reader but not the reperforator use "non-read".

To step the reperforator but not the reader use special key "/";

To correct a letter, use "non-read", and insert.

The tapes produced are unsuitable for Colossus and need to be copied.

56D. JUNIOR.

(a) Function.

Junior prints from a tape. It consists of a tape-reader, a steckerboard, and an electric typewriter.

By steckering any character can be made to print any other character. Any number of characters can be steckered to print the same character.

(b) Details of steckering.

The three upper rows of jacks carry the output from the reader.

The three lower rows carry the input to the typewriter.

Steckering is effected by plug cords.

Letters not steckered are printed normally (as Tunny letters, e.g. 5 as 5 not by actual figure shift).

Different letters to be printed alike are plugged into a common jack and thence to the desired letter.

To common a large group of letters a Ring Common can be used.

The reader output has two jacks for each letter: a mere shorting plug in the upper jack connects the letter to Ring Common RC 1; a plug in the lower jack connects it to RC 2. RC 1, RC 2 can be plugged to any desired letters : if they are left blank the letters commoned into them are printed as . , x respectively.

In a jack carrying input to the typewriter FS means literally figure shift; 5 means 5; similarly for CR etc.

Note : some Juniors have a different and much smaller stecker-board, unsuitable for rapid steckering.

(c) The Typewriter.

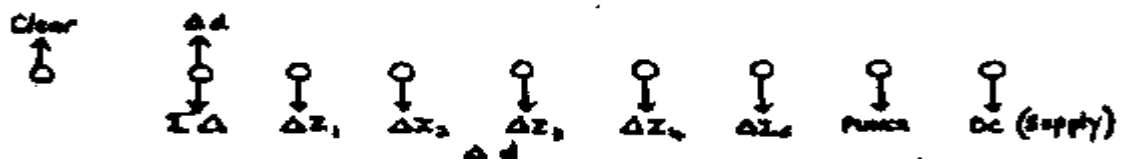
This has three switches : "start"; "stop" and "insert". "Insert" causes the whole machine to stop at the end of each line. The arrangement of these switches varies considerably.

The typewriter can be set to print in any width up to 60.

Letters can be inserted by using the keyboard.

56E. GARBO. Fig 58(xxi).

Everything said about Junior applies to Garbo : the only difference is that, in addition, Garbo has a row of switches for Delta'ing. Garbo always Delta's backwards.



1. If the switch labelled Sum Delta is thrown to Delta-d , each letter is differenced; it may thereafter be steckered.

2. If the same switch is thrown to Sum Delta , and some Delta-Z switches are thrown the corresponding impulses are differenced and added, being printed as . or X : no steckering is needed.

"Clear" merely clears any letter left from the preceding run.

"punch" is thrown if the output is connected to a punch instead of a typewriter.

56F. MILES.

(a) Function.

A Miles is a machine which when fed with one or more tapes produces a tape combining them in some way.

(b) The early Miles.

The early Miles could combine tapes by adding them (in the Tunny sense). Impulses could not be permuted, though an impulse could be cut out. No further description is given.

(c) Miles B.C.D.

These are a development of the early Miles. With no plugging and switches all normal the tapes are merely added. By plugging impulses can be permuted. Differencing is not possible except by using two tapes at a stagger of one. (Details : 56G)

(d) The Mechanical flag Gadget (Miles D) .

This introduced an extension of the notion of combining tapes, viz that one tape can be used to control the stepping of another, or of itself. (Details 56G(m)).

(e) Miles A.

This was designed to be as flexible as possible : nothing is transferred from input to output without being plugged. Plugging is therefore usually more extensive than on Miles B,C,D; but because it is based on a simple uniform principle (56H (c)), it is very easy and can be made quickly.

Differencing, up to eight times, is provided by means of memory circuits. (Details 56H).

(f) Performance of Miles

This has not been entirely satisfactory. These machines could not of course claim the attention devoted to Colossi, but even relatively they have been rather neglected. The design is believed to be sound, but there has been no adequate supply of spare parts. In particular Miles A has been rarely in proper working order, the existing model being the experimental one, not really intended for regular use: this rather than the extra plugging, explains the operators' preference for B,C,D.

(g) Possible Improvements.

The ideal Miles would probably be on the lines of Miles A. It would be desirable to include a generalization of the Flagging Gadget [56G (m)], viz. an automatic stepping control such that any reader or reperforator control could be started or stopped either by pulses from any tape or after a fixed number of letters : one suggestion is two automatic control jacks (stop and start,) on each reader and reperforator control, into which any pulse could be plugged.

If Miles were required to combine letters in accordance with a general combination square, extensive changes would be needed.

The counters would probably be of real use only if they could be reset to zero.

56G MILES B,C,D.

(a) Layout

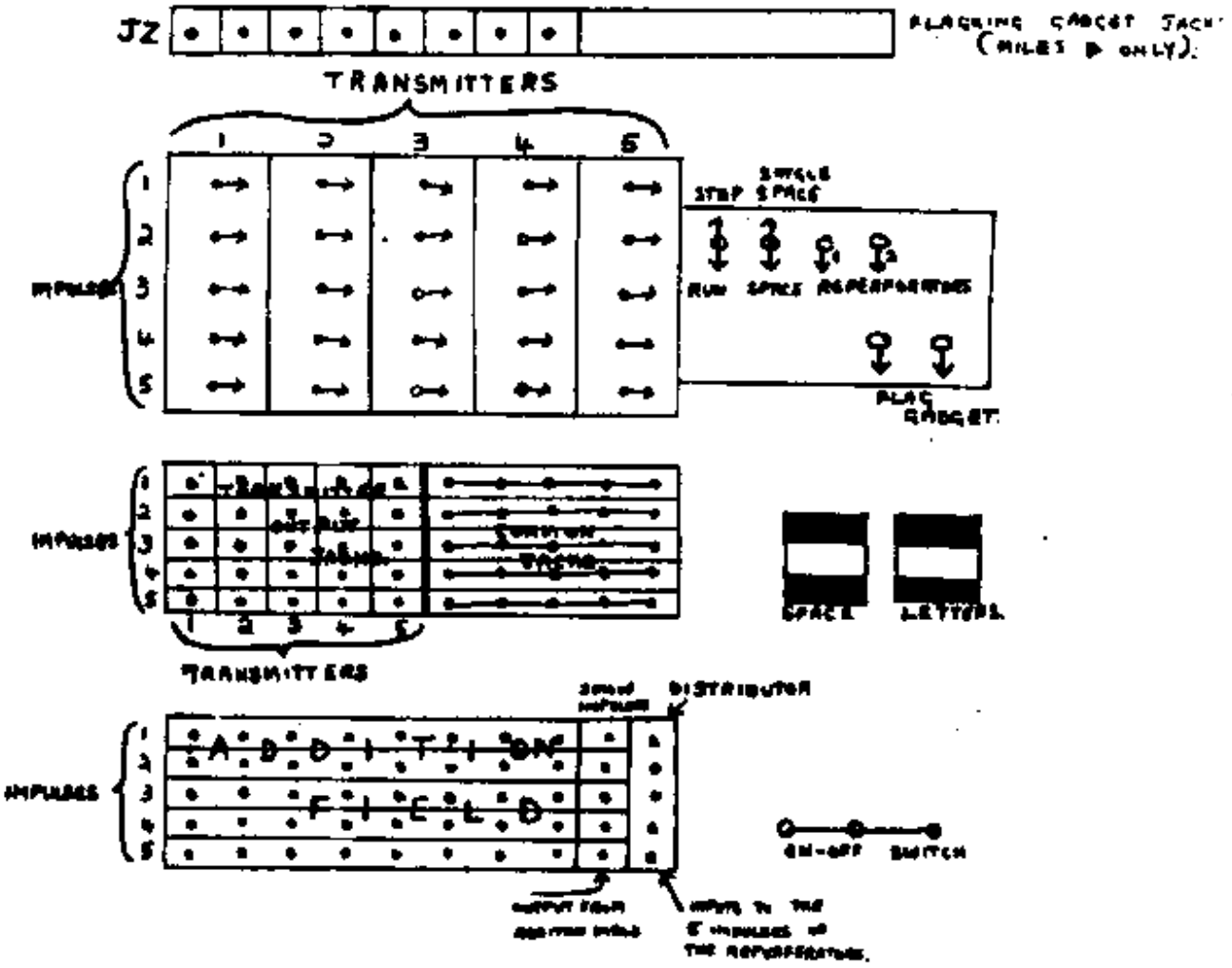
Each of these consist of 5 tape-renders, a plugboard, and 2 reperforators.

B is now incomplete.

The control panel is arranged as in the following diagram.

This may be compared with the photograph (Fig 58(xxii)).

In the description of Miles, tape-readers will be called transmitters, as is customary: these are <u>not</u> auto-transmitters.



(b) The items of the plugboard

1. Transmitter impulse cut-out switches.

2. Transmitter output jacks, each carrying one of the 5X5 impulses for the 5 transmitters.

3. Addition field : this has 5 rows of jacks, one for each impulse.

4. Sum of impulses : these 5 jacks are the output jacks for the 5 sums of the addition field.

5. Distributor : these 5 jacks carry the input to the 5 impulses of the reperforators.

6. Commons : each row constitutes one common jack.

(c) Normal Connection, ie. without plugging.

The first impulses (for example) from all five transmitters are added in the first row of the addition field and taken to the first impulse of "Distributor".

(d) Plugging and Switching.

The more important items are described in paras (e) (f) (g) (h) (i).

(e) Impulse cut-out switches.

Any impulse can he cut out completely by its impulse cut-out switch : if all the impulses of a transmitter are cut out it does not step.

(f) Transmitter output jacks.

Any one of the 25 impulses in the transmitter output jacks can, by the obvious plugging, be transferred to a different row of the addition field. This means that it is :

(i) cut out from its own row

(ii) added to the impulses already in its new row.

For example, if T4 T5 are cut out, and a plug cord is taken from T3(1), the first impulse of T3, to the second row of the addition field the first row now carries T1(1) + T2(1) and the second row T1(2)+T2(2)+T3(2)+T3(1).

(g) Adding a cross.

A shorting plug in a jack of addition field adds a cross thereto.

(h) Permuting sums of impulses.

The outputs from the addition field can be transferred to other impulses, cancelling what is already there e.g. if the 2nd impulse in 'Sum of Impulses' is plugged to the 5th impulse of 'Distributor', the reperforators will have nothing in the 2nd impulse, and whatever is in the 2nd row of the addition field in the 5th impulse.

(i) Common jacks.

These, unlike the other jacks, are not permanently connected to anything else.

Impulses plugged into a common jack are added, not in the ordinary way, but by the rule that the output is a cross unless all inputs are dots (Boolean addition).

Two or more outputs can be taken.

(j) Reperforators.

Either one or both can be used.

(k) Counters.

(Cyclometers) are supposed to record the number of blanks and letters punched : they were used very little and all but one are out of order.

(1) Miscellaneous switches.

Step ("run" on Miles D) causes both the transmitters and reperforators to start and continue to step.

Space causes the reperforators to step, and punch blanks, the transmitters remaining stationery.

Single step , single space can, be flicked on and off for single step or space.

The unlabelled switch to the right of the reperforator switches on Miles C controls an improvised gadget used for making motor tapes when Tunny was disabled by the Fire (See Glossary).

The pair or switches below these on Miles D are for flagging (Next para. 56G m).

The Triple switch is the on-off switch.

(m) Mechanised Flag Gadget (Miles D only).

The basic idea is to control the stepping of transmitters automatically by means of impulses from the tapes themselves.

This may be needed if tapes are to be combined not concurrently, but consecutively, in a large number of stretches.

The gadget was made specially for Mechanical Flagging (ch 95) without much regard to flexibility. Nevertheless, though designed for ordinary flags it proved suitable for combined key flags, when it is used quite differently.

This explains the rather odd facilities available.

The gadget manifests itself as a series of jacks JZ1 - JZ8.

A cross in :

JZ1,2,3,4 starts transmitters 1,2,3,4, respectively.
JZ5 produces a cross in JZ7 and, if
JZ1,2,3,4 are all dots, produces a cross in JZ8 & steps transmitter 4
JZ6 stops transmitters 1,2,3,4 and steps transmitter 5one sprocket hole.

The gadget has two switches : the right hand one switches in the gadgets, the left hand one then acts as an on-off switch.

56H. MILES A.

(a) Layout (see photograph Fig 58(xxix)).

There are
6 Transmitters.
3 Reperforators.
3 Controls (which control the stepping of both transmitters and reperforators).
6 Common jacks.
8 Sets of jacks for differencing an impulse (backwards) or taking an impulse one back.
2 Sets of extra jacks for addition.

(b) All 28 items are completely independent.

Three different tape-making jobs may be done simultaneously, each being started and stopped by its own control without interfering with the running of the others. The allocation of items to each job is quite arbitrary.

At the other extreme one control may control everything, producing identical tapes from all three reperforators.

The linking of items is by plug cords.

(c) Principle of plugging.

Plugging depends on a very simple principle

Each item has a series of corresponding (IN jacks / OUT jacks)

Any impulse plugged into an IN jack appears suitably modified in the corresponding OUT jack.

NOTES. Reperforators have, naturally, no OUT jacks.
Even transmitters have IN jacks.
In a common jack, IN and OUT jacks are the same.
In a control. OUT jacks are common to all 5 impulses.
Corresponding IN and OUT jacks are in the same column.

(d) The effects of the various items on an impulse taken through them.

(i) Any one of the 5 impulses of a transmitter : adds that impulse.

(ii) Common jack : the impulse can be taken out on several cords.

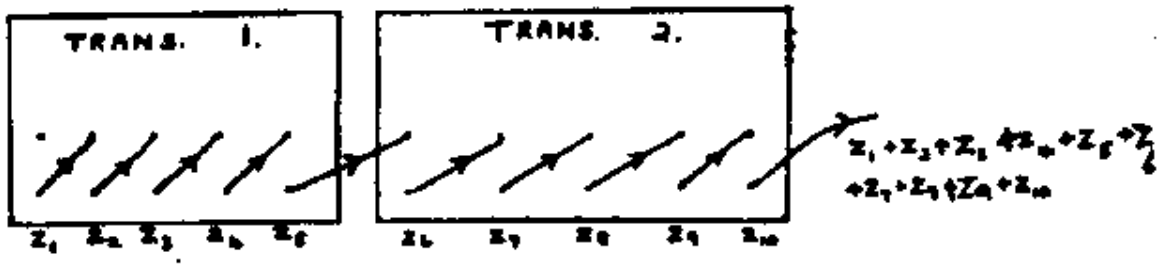
(iii) Delta ; from Ioneback : the same impulse one back.
from Delta-oneback : the same impulse Delta'd backwards (Delta'd).

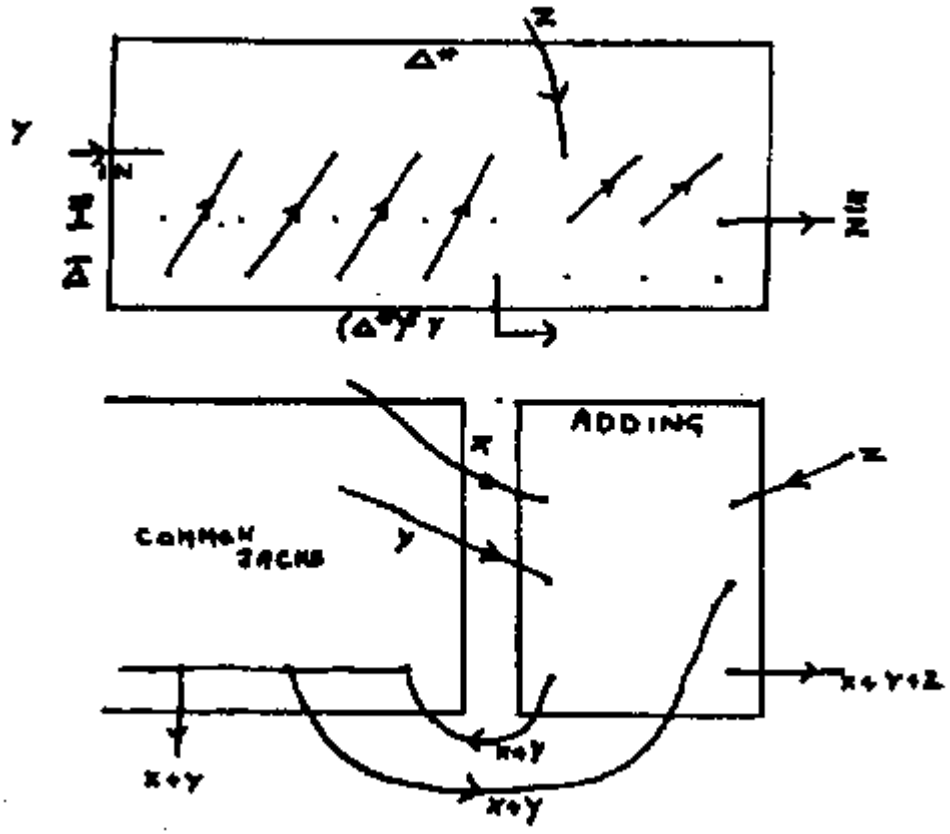
(iv) "Add" : two inputs can be added (may be useful for adding two impulses already complex).

(v) Controls : the impulses plugged into a control can be taken out into reperforators (only one cord for each reperforator) ; each impulse is punched in the corresponding impulse of the tape.

IN and OUT can be continued without restriction as long as there are jacks to spare

(e) Examples :





A good practical examp1e is giyen in 27.

An amusing example is to take an impulse to a common jack thence

(i) to control

(ii) one back (Ioneback) to the IN jack of the same impulse.

This integrates (un-Delta's) the impulse : it can be applied to five impulses simultaneously.

56J TUNNY AND DECODING MACHINES

The original Tunny machine was simply a functional reproduction of the German Tunny machine, operated electrically instead of largely mechanically. It way intended primarily for straight forward decoding. It was developed in two directions:

(i) as a decoding machine improvements were effected and gadgets added for ease of operation, not for versatility.

(ii) as an aid to Newmanry setting and breaking, much more versatile models were produced.

There were several versions of each, some of the early ones being very awkward in operation e.g. patterns were set up by means of U-shaped pins, and wheels were reset by stepping each uniselector switch by hand, one position at a tine, and forwards only. Only the later models will be described.

A weakness common to all Tunnies is that the five impulses of each letter of Z are sent through the machine successively though by different routes, and can be added or permuted only with the aid of remembering circuits. This restriction does not apply to the wheels.

56K THE (NEWMANRY) TUNNY MACHINE (Fig 58(xxv)).

(a) General description of operation.

The tape is fed into an auto-transmitter: chi, psi, unless cut out, are added automatically, and the sum appears on another tape, letter by letter. At each letter the current settings of all wheels are exhibited.

(b) Wheel-patterns.

Each wheel has two rows or jacks, in which shorting plugs can be inserted. The upper row represents the pattern; the lower row determines the initial setting. Each wheel has also one row of indicator lamps to show its current setting.

The "display" shows not the wheel settings but the number of positions through which the wheels have moved: the three rows of figures correspond to Chi, (with Z and Mu61), Mu37, Psi. Each row has a cut-out switch.

(c) Limitation

Switches K P B (for X2oneback , P5twoback , PSI1'oneback,) one or more being thrown determine the limitation.

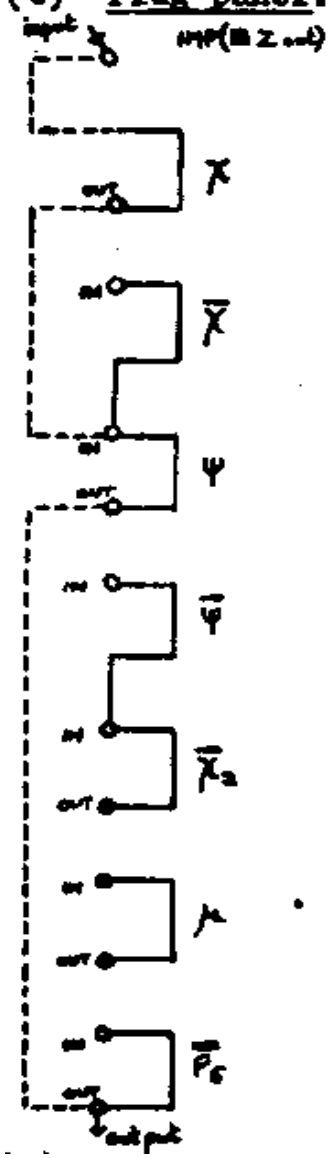
The characters of PSI1'oneback , P5twoback , P5oneback , which are just before the start of Z can be preset by spring switches: P5twoback. P5oneback are set simultaneously by switch positions: .. , .x, x., xx .

(d) Wheel switches.

Each wheel has a separate switch. Unless a wheel is switched in, it has no effect whatever, e.g. if X2 is not in, the limitation will be incorrect and the psis will move incorrectly [c.f. Para (e)].

The chi, psi master switches merely determine whether the wheels move or remain stationary.

(e) Plug panel.



In normal operation the motion of the psis depends on some or all of Z, Chi, Psi, Motor, but only Z, Chi, Psi are added in the resultant tape. It is sometimes desirable to modify this in various ways, e.g. in a total motor tape Mu37 and the limitation are involved in the resultant tape; Z, Chi, Psi are not to be added to it, but Z, Chi, Psi (or X2 at least) cannot be switched out [compare para (d)] because they determine the limitation.

To each or the five impulses corresponds a column of jacks (see diagram : where no suffix is shown, that corresponding to the column is to be assumed). It will be seen that Psi, X2oneback, Mu, P5twoback have each an "in" jack and an "out" jack. Anything put into "in" appears at "out" with the appropriate impulse added to it. Chi has no in jack being normally connected to "IMP", which is in effect, "Z out". Xoneback PSIoneback have no out jacks being permanently connected to PSI X2 respectively. Chi and psi are normally connected both up and down (dotted lines) but a plug inserted in one of their jacks automatically breaks the normal connection to that Jack.

Wheels may be transferred from one column to another, but Z cannot.

There are a few common jacks.

(f) Stop setting.

Decade switches reading 0-9999 can be set so that the machine stops after so many letters of Z.

(g) Contraction.

Because Robinson psi-setting required a de-chi tape contracted by the omission of letters against total motor dots [52 (d)], several Tunnies included a facility for making such tapes.

(h) Miscellaneous facilities .

(i) Reversing one or more of the five impulses.
(ii) Making blank one or more of the five impulses.
(iii) Running backwards.
(iv) Encoding with P5 limitation.
(v) Innumerable switches for cutting out lamps.

(i) Differencing.

Tunnies "1" and "3" can produce differenced tapes.

56L. DECODING MACHINE. Fig 58(xxiv).

(a) General description of operation.

Given a cipher text all of whose settings are known, the appropriate patterns, settings and limitation are imposed, and the machine is started.

As each letter of cipher is typed out on the keyboard, Chi, Psi, are automatically added so that a letter of clear text is printed.

In place of the keyboard an auto-transmitter reading a cipher tape can be plugged in, but its speed is apt to be too great for the machine.

The settings of all wheels at each letter are shown by indicating lamps.

For swift operation some switches are on a control box adjacent to the keyboard.

(b) Wheel patterns .

See 56K(b), but there is no display of positions moved through, only of current settings.

(c) Limitation.

See 56K(c).

(d) Chaser settings .

In early models if it were necessary for any reason, such as typists' error or corruption, to start again a few places back, the position of each wheel had to be calculated and set separately. This is now avoided by "chaser settings" which are stationary during ordinary running, but

(i) the "set reading" switch causes the chaser settings to move forward to current settings (used once per line or so)

(ii) the "reset" switch causes the current settings to move back to the chaser settings.

These switches are duplicated on the control box.

The same lamps are used to indicate both current and chaser settings, but confusion is avoided by "DCL" which extinguishes the chaser settings.

(e) Snaking

On corrupt texts using P5 limitation the psis may be incorrectly motorized. If the SN and the psi cut-out switches are in the active position, then each time SS is shown the psi settings are increase by one. Several versions for ??? and psi settings can be printed: by "snaking" through these the clear text can be found. In practice it was done better by hand.

(f) Chi, Mu, Psi cut-out switches.

These switches (on the control box) cut out a set of wheels completely, including their effect in the total motor.

Cutting out Psi produces de-chi, which may be checked against that provided by the Newmanry.

(g) X2 inside out

This switch interchanges dot and cross in X2.