MTV

Richens

81

~~TOP SECRET~~ ~~CANCEL~~

(Floods file)

Reference: X/569/3444

Date: 13th August 1953

Copy No.: 3.

~~MA~~ AJB
~~MATHEW~~
~~MHIACE~~
~~MHV~~ JWW in particular see (89)
~~MHC~~ J.B.C.

HIGH SPEED ANALYTICAL MACHINERY FOR D.S.B.

Written by Dr Gerry Morgan

Please return as quickly as possible with any comments you have.
H.C.R.
10/9/53

Distribution

1. Director, D.S.B. - Copy on 8/10/49
2. Mr. Moriarty
3. MH
4. SUKO
5. Director GCHQ, AD1
6. H
7. HE
8. HR
9. X
10. XR
11. XE
12. X23
13. Mr. Robinson
14 - 20 Spare

~~TOP SECRET~~ ~~CANCEL~~

~~TOP SECRET~~ ~~CANOE~~

Reference: X/569/3444
Date: 13th August, 1953.
Copy No. 3

High Speed Electronic Analytical Machinery for D.S.B.

1. D.S.B's official interest in this subject is first recorded here in a letter of 30th October, 1951, from Mr. R. N. Thompson to Sir Edward Travis. Three reasons are advanced for this interest: the present application of such equipment to current tasks undertaken by D.S.B., the likely extension of applications to future problems, and the desirability of having a second Commonwealth Centre with such equipment and knowledge. The attachment of Australian engineers to G.C.H.Q. was suggested as a first step.

2. In reply G.C.H.Q. warmly welcomed the interest and recognised the soundness of the reasoning and the suggestion. The several machine projects planned in this country were of very different degrees of generality, and there was no doubt here that the one which most fully satisfied D.S.B's interests was the improved form of COLOSSUS which we have taken to calling COLOROB. It was particularly well suited to numerous of the most important attacks on the HAGELIN problem, was essentially of a high degree of cryptanalytic generality and was at least as well calculated as any other to serve as a sound first exercise in establishing an Australian tradition in cryptanalytic machinery. We have subsequently stressed the necessity to attach (mathematical) methods staff to benefit from our experience in using machinery and translating cryptanalysis into machine processes and programmes.

3. It may have been misleading to refer at times to COLOROB as a machine. It is much more than that, being a strategy in the first place, and a class of machines in the second. In fact it would not be far wrong to think of COLOROB as cryptanalytic MECCANO. The meaning of this is amplified in the next part of this paper. Part 3 contains a more detailed discussion of the logical basis of COLOROB, leading to Part 4 which deals with some engineering aspects. Part 5 contains information about some cryptanalytic applications; and the paper is concluded in Part 6 with suggestions towards D.S.B's case for entering the field of electronic equipment.

~~TOP SECRET~~ ~~CANOE~~

Reference: X/568/3444
Date: 13th August, 1953.

Part 2

4. It has long been known that the enormous and complex structure of mathematics can be built up by using a very few types of bricks, the basic concepts and operations of the science. It has been claimed, with a great deal of justification, that an adequate set of bricks can be found within the strictly logical domain, with which logic and mathematics can be constructed. On the practical plane it is well-known that computers are being built to carry out any mathematical calculation (which is a combination of arithmetic and logic) subject to limitation of size, by means of a quite small set of operations. It is important to recognise that the size of this set is considerably optional: it can be more or less redundant, or luxurious. A small set of orders will result in a small, and maybe simple, computer; but orders outside that set will have to be built up out of it, as what are called 'sub-routines'. To do so amounts to paying in time and complexity of programme for the advantages of a simple machine (cost and reliability).

5. What is true in the wider domain is true of cryptanalysis. Explicit cryptanalytic techniques can be expressed in terms of arithmetic and logic, and carried out mechanically in terms of a more or less arbitrary system of operations. As always, cost in equipment has to be balanced against cost in time. It must be admitted right away that, always within limitation of size, cryptanalytic techniques can be carried out on a general purpose computer; but, just as a calculation involving a high proportion of multiplication would take a long time to perform on an equipment which did not provide multiplication as a basic order, so many cryptanalytic operations take an inordinately long time to perform on equipment not built intentionally to cater for them. Cryptanalytic processes do involve a very high proportion of operations which, in terms of logic, programme or equipment, are very complicated. Considerations of time, however, make it desirable and even essential that these processes are available as fundamental operations or orders.

6. Another very significant generalisation applies to cryptanalytic method, distinguishing it from much of mathematics. The latter is mostly and traditionally deductive. The former is made, by the intention of the

Reference: X/569/3444
Date: 13th August, 1953.

cipher maker, to depend on solution by exhaustion; on trying every combination of the variable data until suddenly and without any forewarning a 'success' is achieved. In practice this usually amounts to the repetition, to a large number of times, of the same 'operation' or 'sub-programme' on a series of data which can be adequately or even fully specified in advance. There are important sophistications in which the operation or data, or both, may change in a way which cannot be explicitly determined in advance, but this can be dealt with as a development of the fundamentally simple serial repetition. To achieve rapidity in this repetition we have to aim at the most rapid serial presentation of the data, and the utmost compression of the operation. Ideally we aim at the presentation of the next set of data and the completion of the operation thereon, each time the machine 'ticks'.

7. The first of these aims, fortunately, does not present very great difficulties in principle. In practice we may meet difficulties in the large total amount of data to be analysed or in the large quantity of data entering into each single operation. This involves various forms of 'parallel working', and means that equipment is made large by reduplication. When we come to analyse the second aim it is apparent that, at greater or less cost of equipment, any particular operation can be encompassed in a 'tick', but that cryptanalytic generality is at variance with engineering practicability within one equipment.

8. The strategy of COLOROB is to fulfil the aim of rapid analysis by a resolution of this contradiction between generality and practicability. It does so first by following the precedent referred to above, and expressing cryptanalytic operations as complex structures made up from what we may call 'basic operations', selecting the basic operations for which there is extensive need and then setting out to realise them as engineering units. According to the formula for a complex operation in terms of basics we shall need to connect together the same units in a great variety of different ways. It is a prime requirement that the output of all units shall be the same, and acceptable as an input to each unit. The nature of some of these basic operations and engineering units is expounded more fully in following sections. For the

Reference: X/569/3444
Date: 13th August, 1953.

present we may vaguely speak of units of kinds A, B, C, ... and to carry out a particular task needing a of A, b of B and so on, and of connecting them together according to a formula deriving from the methods staff. We therefore envisage COLOROB as a reserve of an unspecified number of various units A, B, C, ... from which, for a particular, set-up we draw a of A, b of B and so on for appropriate interconnection. For this we provide a racking of unspecified extent into which (to speak somewhat crudely and rashly) any unit will fit in anywhere. Rather more accurately the racking will consist of a two dimensional repetition of a rectangle into one (or more) of which any unit will plug. From the racking each unit derives power supply and clock-pulse (defining the 'tick' of the machine). All inputs and outputs on the units are on the 'front' of the units, and are brought into operation by plugging connections between the units according to the formula.

9. Those unfamiliar with COLOSSUS will wish to know in what way these ideas are related to it, and in what ways they provide a generalisation of it. This is best expressed by saying that COLOSSUS consists of a certain number of units A, B, ... E permanently attached to a rack from which they derive power and clock-pulse, and that inputs and outputs are brought out to a large central plugboard on which the formula is set up. The range of different units is fixed, the available number of a particular kind is within a fixed upper limit. It may be a major difficulty of layout to extend these ranges in what was designed without much intention of the kind. For some tasks much less than the whole range of COLOSSUS's units are needed, but we cannot make use of the rest for another task at the same time.

10. It must be admitted that among the advantages claimed for COLOROB that of economy, of making the fullest employment of a given stock of units, has more force in a large machine division where several tasks (identical or otherwise) are being carried out simultaneously on equipment of this kind. An advantage, of great significance on any scale, which ought to be achieved is the separation of maintenance from operation and the consequent increase in hours available for the latter. Once diagnosis of fault has localised it to a particular unit, exchange of unit for a tested spare enables operation to be resumed.

Reference: X/569/3444
Date: 13th August, 1953.

Further testing and making good the faulty unit can proceed independently, as can all routine maintenance. We aim to make the testing of units as cut-and-dried an affair as possible.

11. We have referred to COLOROB as a cryptanalytic MECCANO. As a start, for a compact and restricted class of problems, a certain set of units would be wanted; just enough to provide enough of each kind for each problem and spares to allow for maintenance. The posing of new problems would call for additional units of the same kind, pure repetition work for the engineers, or sometimes the design of new units to perform different basic operations. We envisage some units of such size and complexity that we should dispense with the spare for maintenance. We aim at the great advantage of being able to attack new special problems without constructing a special machine for the purpose; but of being able to assemble it from general units already used in a variety of previous problems and assemblies. This aim will not always be completely fulfilled, for sometimes there will be an inescapable requirement for a new unit, probably of some size. The new unit will be justified both by a reasonably great economy of equipment and (more often) by a very great economy of time in operation. A very important example will illustrate what is meant: we may assume that an appropriate set of units has been built and used on many different aspects of the Hagelin problem, and it is now desired to have a machine to do key breaking in a code and additive system. The control and arithmetical part of the machine is ready to hand in the reassembly of units already made, but it is necessary to have a rapid access store containing an adequate amount of information about code groups and their frequencies. Such a store we call a "dictionary", and it would have to be a new and separate unit, and a very major one at that. It is referred to again later, in para. 16.5.

Reference: X/569/3444

Date: 13th August, 1953.

Part 3

12. COLOROB will perform its operations in synchronism with a clock. To enable quite elaborate calculations to be performed during one "tick" of the clock, its period has been chosen at 10 μS. (100,000 pulses per sec.)

13. Each COLOROB unit will have a number of inputs and outputs: it is fundamental that every output shall be compatible with every input on the same or any other unit. This compatibility will involve standardization of timing as well as voltage. More specifically all data, including controls and instructions, will be in a standardized binary form. This will probably be pulse for 1, no pulse for 0.

14. Numerical operations will normally be carried out in binary arithmetic. In a complex logical operation on binary numbers, the reverse of a number (0 for 1, 1 for 0) is as likely to be needed as the number itself. It is advantageous to have a simple means of reversing inputs or outputs, but there is no need to do both. An early plan was a reversing switch on every input, but the change to pulse techniques may make it easier to use double-wound transformers, both windings being accessible.

15. No list of COLOROB units can ever be complete, because it is a basic principle that when necessary a new type can be built, limited only by the need that its inputs and outputs shall conform to the standard. There is still uncertainty concerning the best choice of units, but those listed below would constitute an acceptable COLOROB. They are classified as:-

(i) logical

(ii) memory

(iii) mixed

(iv) original input

(v) final output or recording of results.

Reference: X/569/3444

Date: 13th August, 1953.

16. Logical Units

An early idea for a single style of chassis varied only by plugging has been abandoned because the proportion of unused elements would be too high. Now the following units are contemplated.

A batch of 10 independent logical circuits.
A set of associated Boolean "and" circuits.
A translation.
A matrix.
A Dictionary.

16.1 Batch of independent logical circuits: These should provide either the Boolean "and", or mod 2 arithmetic; but the precise arrangement is likely to be settled on an engineering basis, and will depend on the result of experiments currently in progress.

16.2 Associated "and" circuits: The output is only zero when all inputs are zero: the same effect can be produced by a series of simple "and" circuits, but not with quite the same speed of operation.

16.3 Translation: There are two types. In one, 5-unit coding is translated into 32 letters: there is one output for each letter, and this output has the value 1 when the appropriate 5-unit code is presented to the input. The other type performs the converse operation.

[redacted]

Reference: X/569/3444
Date: 13th August, 1953.

16.5 Dictionary: In many processes connected with code and additive problems it is necessary to be able to "look up" code groups with rapidity and discover their meaning, or frequency of use or score based on frequency. The latter is the most generally useful and, fortunately, the least bulky item to store. It may be desired to store several hundred or even several thousand code groups each with appropriate score or meaning. The input to the dictionary is in the form of a hypothetical group, the output is the appropriate score (or otherwise) if that group is stored. The output is required to occur "immediately" so that it may be used in a calculation occurring within one 'tick'. Such dictionaries, as these stores are called, have been made; it would be a matter of considerable debate and probably research to decide how best to design one for COLOROB.

17. Memory Units, i.e. accessible stores of information
No single type will suffice, and the matter is a technical one. A rapid improvement in magnetic core memories might render CRT memory unnecessary. Of the following only Trigger and Drum will definitely be included:

Trigger: access to all bits always, and all at once.

CRT: access to all bits always, but only one at once.

Delay line including Drum revolver: access to only one bit at any time.

Drum: access to only bit at any time, but the delay is necessarily the period of revolution of the drum.

17.1 Some 10 elements of trigger memory will be built on a single unit. As on COLOSSUS, these may be linked to form a chain, such that the input at any time appears in the first output one tick later, at the second output two ticks later, and so on. The individual element will have two inputs and two outputs. When one of the inputs, the control, is 0, the output cannot change; when it is 1, the input will appear at the output one tick later.

Reference: X/569/3444

Date: 13th August, 1953.

17.2 Details of the drum are now being settled with Ferranti's. We are asking that up to 64 tracks may be read at once and up to 32 may be written. This will, in particular, enable two texts, each of whose elements is expressed in up to 32 binary units, to be read simultaneously and to be processed so that they are compared at all staggers. The 32 binary units will suffice for a 5-letter group in a 64-letter alphabet, with two spares. At the other extreme the whole drum may be treated as a single sequence of about 600,000 binary units.

18. Mixed Units Here we refer to three types of unit: accumulator, counter and "stay-put".

18.1 The accumulator will accumulate by addition (binary arithmetic) the numbers presented to its principal input (5 stages) and shew the result on its output (10 stages). A second set of inputs will reset the output to an arbitrary value.

18.2 The counter is similar but can accept additive inputs of 0, 1 only. It will be made to count to an arbitrary modulus. Counters will be numerous because they are to be used for control of operations.

18.3 "Stay-put" is a local name of merely historical significance for an important transfer element. This is a device with two inputs A and B, and an output. The output is constantly 0 until A = 1; it then becomes 1 and remains so until B = 1 when it reverts to 0 until A = 1; and so on. It could be assembled from trigger memory and simple logical units, but not so economically.

19. Original Input

The intention to use more than one form is deliberate, but they will be added one by one.

19.1 Paper tape (5 - 7 unit) at 200 letters/second.
19.2 Hollerith cards
19.3 Magnetic tape.

The first is already developed and in use with us; the second is under development. The third is developed for COLOSSUS speed (5kc/s) and will be a matter of study for COLOROB speed.

Reference: X/569/3444

Date: 13th August, 1953.

20. Recording of Results: At least until magnetic tape is available the standard form will be punched cards. The output mechanism will have standard COLOROB inputs so that data can be taken from any part of the machine, e.g. interesting synthetic text may be recorded. It will be necessary to include optional means of converting from binary to Hollerith code.

21. Wheels: No special "wheels" are provided. The intention is to use instead a counter, with arbitrary modulus; and to translate the counter output to dots and crosses, or, more generally, to "letters". If the counter is replaced by an accumulator, motion can be extremely irregular.

22. Control: Ordinary circuits are to be used for control: the only special control devices are manual switches. Two simple examples will suffice.

22.1 A wheel is to move regularly during each scan of the text and to start each scan in a different position, say 1, 2, 3 ----- in turn. Two counters will be used: one represents the wheel as explained in the preceding paragraph. The other has 1 added to it at the end of every scan, and then transfers its contents to the wheel counter.

22.2 The letters A, B, C ------ are to be counted in successive scans of the text. For this a counter has 1 added to it at the end of every scan, and its output is translated according to the table

0 1 2 3 4 ----

A B C D E ----

23. The Calendar: It was implicit in the examples of control that ordinary units are operative not only during the scanning of text, but also during the interim between successive scans. In such runs four conditions arise:

spring, when conditions are set up for the next test
summer, when the test is made
autumn, when results are recorded
winter, testing is suspended when results appear too rapidly for recording.

Reference: X/569/3444
Date: 13th August, 1953.

These conditions will be derived from perfectly ordinary units, but will perhaps be led to all units. Winter will not occur in every year (which shews how suitable COLOROB is for Australian conditions). Alternatively all seasons except winter may be simultaneous: this would be the case, for example, when applying short cribs to a text.

24. Part 5 of this paper is devoted to our opinions about the suitability of COLOROB to various cryptanalytic problems. It is anticipating that section no more than has been done already to say that it is particularly suited to Hagelin problems. We append provisional figures of the units required to carry out the letter counts and Fourier methods appropriate to [redacted] Hagelin; they would cope with parity methods as a special case.

6 wheels with means for stepping, envisaged as 12 x (counter + translator)

2 further (counter + translator)

2 matrices

1 accumulator

25 "and" circuits

25 mod 2 circuits

10 stages of shift register

1 magnetic drum and associated circuits
for input and internal reading and writing and switching

output circuits

Reference: X/569/3444
Date: 13th August, 1953.

Part IV

Some Engineering aspects of Colorob

25. The concept of Colorob as a machine to be built up of units has necessitated the development of a number of techniques new to G.C.H.Q., but based on our previous experience and that of the computer field. Because of the degree of interchangeability required it has been necessary first of all to establish some standards.

26. Colorob may be divided roughly into three parts, the information store, the logical operations, and the output device. A large information store was a first requirement and a Ferranti Magnetic Drum was the only piece of equipment commercially available that was in any way suitable. The principle of the magnetic drum had been proven and circuits were available for reading and writing bits of information at 100Kc/sec. We therefore decided, having adopted this drum, that our clock should be 100Kc/sec. since embarking on this project, Ferranti's have found it necessary to redesign the drum to overcome certain technical difficulties, but the size of the store was increased. However the original planned size of store, 256 tracks each of 3072 bits (total 786,432 bits) has been retained. The additional 64 tracks available on the drum are an insurance against magnetic failure of the other tracks.

27. The operational requirements for handling the stored data were to be able to read up to a maximum of 64 tracks in parallel and rewrite on a maximum of 32 tracks in parallel. To make the maximum use of the drum under varying operating conditions a flexible track switching arrangement was necessary. As this was closely concerned with the reading and writing on the drum it was decided to give Messrs. Ferranti Ltd., a development contract. This was described in X/4845/8329 and drawing B6671. This is under revision at the moment to incorporate modifications which would reduce operational plugging.

28. Writing data into the store initially can obviously be done via the switching circuits to be provided above, but would no doubt require a replugging for operational use. To overcome this, additional writing circuits

~~TOP SECRET~~ ~~CANOE~~

Reference: X/569/3444

Date: 13th August, 1953.

are to be provided as part of the development contract, so that the information source is telegraph tape, Hollerith card, or (in the future) magnetic tape.

29. Data will pass between the magnetic drum and the logical operations and between the latter themselves by connecting cables set up by the operator. To have flexibility in the arrangement of the logical units and use of data, any output must be capable of feeding any input. Much work has been done on the form of standard input/output. It has now been decided to use a pulse transformer amplifier output. The two states of 1 or 0 will be represented by pulse and no pulse. The pulse will have an amplitude of about 20 volts (from a 0 15-volt level to +5 volts) and duration 5 μsecs. An additional pulse output in antiphase (i.e. from a +5 volt level to -15 volts) will probably also be available. If only one phase is available then phase splitting transformers on the inputs of logical circuits will be required. This is because the inputs to "and" and "or" gates must be of the same polarity for an output. Thus to get an output for "A" and "not B", or "B" and "not A", as in the mod 2 sum of A and B, the "not A" and "not B" are plugged from the antiphase outputs of A and B.

? -15v. to +5v.

30. The data pulse period from the drum will occupy the first 5 μsec of each 10 μsec clock period. As the data is processed through a number of logical circuits the leading edge of the pulse will be delayed, and the maximum that can be tolerated will be of the order of 3.5 μsecs. The number of circuits in series is a function of the problem, somewhat indeterminate at any stage on a universal machine, and therefore it is obvious that circuit delays in each logical circuit must be made as small as practicable. Present experiments indicate that it may be possible to have ten logical circuits in series before trouble arises. Before the end of the pulse, i.e. at 4 - 4.5 μsec the resultant pulse, or no pulse, will be sampled for counting etc. To reduce the intended delays in individual circuits it is intended to use germanium diodes wherever possible for switching, and valves as amplifiers.

31. To provide for the assembly of various logical units for any problem, a standardised form of chassis and rack has been adopted. This will be our first experience

Reference: X/569/3444

Date: 13th August, 1953.

with interchangeable chassis and teething troubles may be expected. The unit rack is 7' high, 2' wide, and 1' 6" deep. The chassis is in the form of a welded angle framework box with the component "deck" inside, being vertical and parallel to the rack front. The variable size is height being a multiple of 7". The rack is fitted with horizontal runners every 7", so that a single or multiple size chassis can be fitted into the rack at any position. It is hoped to mate the plugs and sockets for power supplied, clock etc., automatically when the chassis is pushed home. The components are available for easy inspection by the removal of the top front cover plate from the chassis, all input/output sockets appearing on the bottom fixed front plate. Valves are accessible from the rear of the rack. Cable racking etc. and miscellaneous facilities are provided on the racks. The racks may be assembled in any number of units together. The top of the racks then forms a trunking for air extraction, intake being at the base through filters.

32. Logical diagrams for a number of units have been issued, but these are being revised in the light of recent work. Mr. Robinson's 1/2/REP of 18th April refers; the revisions have not been sent.

33. The output from Colorob will take the form of punched cards, and perhaps in the future magnetic tape. No special difficulties are anticipated with output unit, a standard Hollerith Gang Punch or Reproducer. Work is proceeding on a Selsyn driven cam unit for control purposes so as to reduce modifications to the actual machine.

34. The state of progress at the moment may be briefly summarised. Messrs. Ferranti Ltd., have commenced theoretical work on the circuits of their part and production should commence shortly. Delivery is expected to be completed by March, 1954. Design work on the logical units is under way and production of these will commence at G.C.H.Q. in about December 1953. The number and types required will depend upon operational requirements. Work will commence shortly on the design of the recording circuits.

Reference: X/569/3444

Date: 13th August, 1953.

Part 5

A Sketch of Some Cryptanalytic Applications

35. It would be pleasantly tidy to be able to give a brief description of the sort of cryptanalytic processes for which COLOROB is particularly suited and to be able to compare it quantitatively with, e.g. tabulating equipment or a general purpose computer. It is unfortunately in the nature of the case that this cannot be done, and for a variety of reasons. Cryptanalytic method is sufficiently diverse and COLOROB by its intention so variable and extensible, that no answer can be attempted other than by the accumulation of examples, particular in respect both of the crypt problem and the range of COLOROB units actually available.

36. Thus, treating COLOSSUS as a particular collection of COLOROB units (and not forgetting that its speed is only 1/20th that of COLOROB) we are in a position to make comparison in respect of setting Hagelin messages. We find, when parity counts are used, a very widely spread order of merit - COLOSSUS, FERRANTI Computer, Tabulating. COLOROB would be faster still, by a factor of 20 if sufficient units are provided to carry out the same multiple testing as with COLOSSUS. If, as is often the case, the wheel breaking is done by parity counts then the same order of merit obtains: COLOROB leading the field by a long way. If, in less favourable cases, it is necessary to have recourse to [redacted] to carry out wheel breaking, then the computer pulls a long way ahead of COLOSSUS but is possibly still a little slower than COLOROB. It should be understood here, of course, that in mentioning COLOROB we have a particular set of units in mind - namely the least set which will carry out the runs in a sensible manner. A partial increase in the set, particularly a more generous supply of accumulators would, by means of 'multiple testing', increase the speed far more than proportionately to the cost.

37. It is fair to say, therefore, that for all statistical solutions of the HAGELIN problem COLOROB will have to look further afield for a competitor. It might be found as a general computer either of increased pulse speed (from 100kc/s to megacycle or more) or of parallel instead of serial operation, or both; but such machines are not available as present alternatives. A preliminary opinion is that a serial magacyclic machine is not likely

Reference: X/569/3444
Date: 13th August, 1953.

to be much better than COLOROB, if at all, for this type of problem.

38. The HAGELIN problems amount to performing a sequence of operations (logical, arithmetical or statistical in nature) throughout the length of a cipher text, in conjunction with another 'text' which is constructed from wheel patterns and counters. This way of looking at the work points to another wide class of problem in which it is required to examine texts one against another at all off-sets, making a more or less arbitrary calculation throughout the examination. It includes the classical process of looking for depth by repeats, but much more flexibly than in card methods which start from a reasonably solid repeat. The minimum set of equipment for the HAGELIN work would enable scoring to be provided for repeats of one, two, etc., characters and even to provide scoring on monograph or digraph differences. For example, if a set of 50 Hagelin messages of up to 1,000 characters each are to be examined for off-set depth the operation would take some four hours on a COLOROB of more or less the size already spoken of. No allowance is made in this for variable slide. The method would be that of scoring differences, a much more effective method than depending on a tetra repeat which may not occur, among some 3,000 random ones that will!

cf. "Connie"

39. Another example of comparison is to be found in the [redacted] digraph substitution system. If this is crudely described as a collection of sub-messages each in one of a set of digraph substitutions, a basic cryptanalytic requirement is to identify a collection of sub-messages in the same substitution; aiming at sufficient volume to facilitate some identification. The general problem of examining messages each against each and counting the number of digraph repeats regardless of position is one quite appropriate to COLOROB, and the method is likely to catch cases which would escape notice in a search for longer repeats. We do not become specific as to COLOROB units needed, or time involved, in the absence of more specific information about the problem. But by the token of the

Reference: X/569/3444

Date: 13th August, 1953.

previous paragraph a few hours would suffice to compare a large number of sub-messages.

40. A quite different application is to give assistance in breaking depth in such a cipher as HAGELIN. We instance the possibility of dragging say 500 pentagraph cribs across 200 positions of a depth and using a recognition list of 2,500 pentagraphs, and completing the test in the order of an hour (without multiple testing). As cribs and recognition list are to be written on the drum in a matter of a few minutes from tape this facility combines flexibility and cheapness. It is not claimed to be fast.

41. In considering the [redacted] problem we begin by contemplating a vast mass of enciphered four figure code with more hope than belief that depth exists, and even so some fear that depth may occur with a change of code. Crude and convincing repeats of cipher groups might be looked for; but more hopefully it is believed that certain pattern repeats of groups may occur frequently. In either case it seems more appropriate by far to use tabulating equipment to sort for repeats of cipher or cipher difference groups. (It is not within the present conception of COLOROB development to incorporate electronic sorting). It is difficult if not fruitless to speculate about the stages of progress that might lie between initial discovery of depths and the relatively advanced state in which the cryptanalyst has some knowledge of the code(s) and some, presumably shallow, depths which await breaking. Very powerful machinery can be designed from COLOROB units to assist this breaking, and all these units are employed in the HAGELIN problem except the "dictionary". It is known how to construct a large dictionary, and in more than one way, and there are radically different ideas which have not yet been tried out. Both these problems, the cryptanalytic and the engineering, must be regarded as belonging to the future. They are mentioned because of the inherent importance of code and additive, and because of the significance that units built, perhaps, to solve the HAGELIN could later be employed to attack this other job.

~~TOP SECRET~~

~~CANOE~~

Reference No: X/569/3444

Date: 13th August, 1953.

PART 6

PRACTICAL CONSIDERATIONS

42. It is too early to offer an exact figure for the spatial extent of COLOROB equipment.

The particular nature, layout and size of units is not yet settled; the amount of electronic switching of drum tracks can be considerably less than what GCHQ would allow itself and still probably adequate for immediate and prospective DSB tasks; the choice of output is not yet settled. One rack, of base area 2' x 1½', will hold 9 pluggable units; and the various COLOROB units specified above will occupy 4 racks. The drum, with pre-amplifiers will be housed in a cabinet of 5' square base if the present Ferranti design is repeated. A 'full' complement of switching circuits, as well as input and output, we estimate at (10) racks. An adequate beginning might be made with as few as (6) racks. Power equipment, transformers and fuses, we reckon at 4 racks.

43. When additional equipment is reckoned in - tape reader input, output (typewriter/tape punch/card punch) desk, mobile test equipment - it will be seen that a room 24' x 18' would be too tightly filled. We would recommend that a space 24' x 36' be provided, with provision for evacuation of hot air.

44. The cost of the initial set of COLOROB equipment can be given only in rough figures. We have arrived at the following:

a. Ferranti production contract

10" Drum and 256 reading and writing heads	£3,600	
256 Pre-amplifiers	£2,500	
		£6,100

b. Material cost of rest of equipment

Track plugging	£ 800	
4 Colorob racks and 36 single units (or equivalent)	£5,000	
4 Power racks (transformers and fuses)	£1,000	
(8) (say) racks for input, electronic switching of tracks, and output	£10,000	
		£16,800

c. Labour cost of construction wiring and assembly at GCHQ wage rates; say 4 skilled craftsmen and 9 semi-skilled wire bodies for one year £4,100

£27,000

~~TOP SECRET~~

~~CANOE~~

Reference No: X/569/3444

Date: 13th August, 1953

45. We would mention briefly, but emphatically, at this stage that the equipment can be given a much wider range of usefulness at a disproportionately low cost. Most of the £27,000 is an initial expense; extensions are largely in respect of COLOROB racks, and another £5,000 spent there would make a big difference. This is put in to anticipate the question about continuing development cost. We mention also that the price of £27,000 is deceptively low in making no allowance for any form of overheads or even supervision.

46. There is, of course, auxiliary equipment for input and output, and preliminary and terminal tape and/or card equipment. Much of this may already be at hand in DSB and at any rate partially available. A minimum list includes: tape perforator, autotransmitter, punch and Ferranti high-speed reader; and choice of tape punch (possibly a Ferranti high-speed punch), an electromatic typewriter in parallel with a telegraph punch, or a Hollerith gang punch. We are investigating the extent to which the greater versatility of COLOROB would enable it to dispense with some of the more elaborate tape preparation equipment required for COLOSSUS.

47. As a basis for Australian authorities considering how best their equipment would be made we give present ideas on the timetable to be followed in the further development and construction of GCHQ's COLOROB equipment.

1953	1954			
Sept.	Jan.	April	July	June 1955
Development continuing				
	Prototype units from workshop			
	Delivery of drum input and switching			
		Engineering Testing		
			Production of final units	

Reference No: X/569/3444

Date: 13th August, 1953.

Accordingly it would be around Christmas 1954 when there would be sufficient units available to attempt the first operational use of COLOROB.

48. There would appear to be every reason to begin construction of Australian COLOROB units at the same time as British, that is July 1954. The task splits up into these parts:

a. repetition of the Ferranti contract for drum, heads and pre-amplifiers.

b. reproduction of the input and switching circuits being developed and constructed for GCHQ by Ferranti.

c. reproduction of the COLOROB units and output arrangements being developed and constructed at GCHQ.

d. power supply.

It has always been assumed that a) would be a contract with Ferranti. We do not suggest otherwise. The last item, d), is mostly a purchase of transformers. The second and third parts require more thought. If b) is to be repeated by Ferranti then something like another £10,000 must be added to the cost. We find convincing arguments against b) and c) going, even in part. to any other contractor in England or Australia. The estimate in paragraph 44 indicates the scale of effort if Department of Supply is to undertake the construction. We put forward the suggestion that there would be considerable economies of time, skill and overheads if parts b) and c) were carried out at GCHQ in conjunction with our own programme.

49. The last practical consideration is that of the posts that will be needed to make use of COLOROB. There is first an officer to plan the work and keep an eye on its progress and difficulties. It is not likely to provide full time occupation and is perhaps well combined with crypt research in the person of a man with both theoretical and practical ability. There is need, probably, for three operators to run jobs, including the preparation of tapes. There may be need for more, depending very much on the particular problems being worked and the extent to which help can be obtained from communications tapes. At least one of the operators must be intelligent and educated up to good GCE level or even advanced level. There is need for maintenance staff, which cannot be put below two posts, nor below experimental officer level until more experience has been accumulated. It might be put at one

Reference No: X/569/3444

Date: 13th August, 1953.

experimental officer and one assistant if a stand-in for the experimental officer can be sent from Salisbury.

50. By mutual agreement DSB joined with GCHQ on a large scale development project. The initial expectation was not that it would speedily be possible to construct analytical equipment to make a radical change in DSB's output; and the progress of COLOROB has followed the typical pattern of being slower than early estimates. We now hope, with more firmly based conviction to be ready to start production by the middle of 1954.

51. There was never doubt in GCHQ, ~~and~~ nor we think in DSB, that the first justification of this joint venture was the long term one. An extended role in high grade cryptanalysis, particularly in time of war, necessarily demands electronic equipment. The precondition for having, using, modifying and finally designing such equipment is that there are engineers and cryptanalysts/mathematicians with the right knowledge and experience. That is perhaps the first importance of Robinson's and Watson's attachment to GCHQ. The training of a mathematician in the methods of planning work should have begun by now. This investment in persons is not only as important as the equipment but a necessary prerequisite.

52. We recommended that Australia should participate in the GCHQ project which combined greatest present relevance with generality and long term value. That project we believed, and do so still, to be COLOROB; and the detailed reasons for that opinion have been given above particularly in part 5. We feel that it is for those with intimate knowledge of the current problems and their trends to estimate how fully a COLOROB could be used. Some estimates of times have been given and we should be glad to try to give figures for other runs. But it is misleading to quote ~~f~~ir times until a job is accurately specified.

53. It is for consideration whether there might be some tasks, more particularly of a research nature (where communications delays would matter less) in which GCHQ would welcome part-time assistance of an Australian COLOROB. The Director, GCHQ, would begin to examine such a proposal with a favourable bias.