MQR 5a

MINUTE PAPER

COPY NO. 4...

REF. NO: 8/10/31

H GROUP

INFUSE

1. As you are all probably aware, DSB is getting an electronic computer. The code name of this computer is INFUSE. The objects of this minute are to give you some general information about INFUSE, to explain how it will fit organizationally into DSB and to try to answer in advance some of the queries which I think may occur to you.

2. INFUSE is not a commercially available machine. It is the twin brother of COLOROB, a machine designed and constructed at GCHQ specifically for use in cryptanalysis. COLOROB is now almost operational at GCHQ. INFUSE was built at GCHQ; the components are being shipped out to DSB and are now in process of being assembled in Room 10, N Block. Installation and testing are big jobs and will take a long time but we hope that INFUSE will be operational soon after the middle of next year.

3. INFUSE is made up of several pieces of equipment. The main ones are: the power supply, consisting of 24 Westat Power Units (each is approximately a 2 foot cube) which are used to convert the mains current to DC; two suites, of equipment, each measuring approximately 10 feet long by 8 feet high by 4 feet wide - these contain almost all the electronic circuitry employed in the machine and mainly consist of logical and memory units.- each suite has two 'faces', each face has 6 'racks' and each rack 7 'chassis' (each rack with its 7 chassis looks very much like a 7 drawer filing cabinet); the other main item of equipment is the magnetic drum, which is used, when the machine is in operation, for storing data. Because of the number of electrical components in the machine (including some 3½ thousand valves), a considerable amount of heat is generated while INFUSE is working and the operations room will therefore have to be air-conditioned (the structure added to the outside of N Block is to house the air-conditioning plant which will be installed early next year).

4. Information is fed to INFUSE on 5 or 7 unit paper tape; it is there stored on the magnetic drum and operated on by the various logical and memory units at high speed. The answer will be printed on a paper-roll by an electric typewriter or punched on paper tape. As I said in the previous para graph, these logical and memory units are contained in the chassis - each chassis has a set of circuitry which performs a basic logical or memory function - the use of this circuitry can be controlled by plugging from the outside of each chassis. The directions given to a machine to tell it how to operate on the data fed to it in order to produce a required answer are known as the 'programme' (IBM jobs have to be programmed,too). An INFUSE programme must therefore specify in the minutest detail the set up of the machine required to produce an answer in the most economical and efficient way. A complicated programme such as FOGLE (referred to later) could take one person 2 months or more to write and check.

5. This may be an appropriate place to note how INFUSE differs from some other sorts of electronic computer. The main kinds of electronic computers are general purpose computers (which may be designed primarily for data processing, or for numerical computation)

and special purpose machines(such as a machine specifically designed to assist in the solution of aeronautical research problems - or a Hagelin analogue). Now though INFUSE is in a sense a special purpose machine, in that it was designed as a tool for cryptanalysts, it is nevertheless, completely flexible because it consists of basic logical units with which all kinds of processes can be performed. It has been called 'cryptanalytic Meccano'. One practical consequence of this is that the INFUSE programmer can not, as with other general purpose machines, give an instruction such as 'Multiply' and merely press the 'Multiply' button - he must design a logical circuit which will perform the process of multiplication & plug it up. In some ways, therefore, each new programme creates a new machine.

6. Probably the best way of giving some indication of the speed at which INFUSE works is by some examples of typical programmes:-

(a) A letter count of a 3000 letter text takes about one second (that is the actual running time on the machine and does not include time for setting up the machine, punching on tape, loading the data into the machine and printing the result). Actually a programme as simple as this would not be economical on its own but might form part of a larger programme.

(b) Programme MANGER. This is a [redacted] programme for setting Hagelin messages on a known machine.

[redacted]

a [redacted] in 1 hour 50 minutes running time
a [redacted] in 14 minutes running time
a [redacted] in 4 minutes running time

(c) Programme FOGLE. This is a programme for Hagelin wheel

[redacted]

[redacted]

FOGLE produces [redacted] in 4½ minutes running time.

6. As you can see, then, INFUSE works very fast - so fast that the present input and output will find it hard to keep up with the processing (if a result is ready before the output typewriter is able to accept it, the calculation is repeated over and over again until it can be printed). For example, with the letter count mentioned above, it might take the typewriter up to 15 seconds to print out the answers obtained by the machine in one second. In order to use the machine economically, therefore, the types of problem for which INFUSE is best suited will be those in which a comparatively small amount of data is needed on which a large amount of calculation will produce a fairly short answer.

7. Before leaving INFUSE itself I would like to stress that, because of its flexibility, INFUSE provides us with an excellent basis for future development. GCHQ for instance are currently planning the use of a 'core storage' (a newer and more readily accessible form of storage) to supplement the magnetic drum. One of the first things we are proposing to do in this direction (with the help of T Group) is to instal special plugboards which will enable programmes to be changed more rapidly. Other developments are planned and will doubtless materialize in due course.

8. Because of its unique design it is not possible to give an exact comparison of the size and speed of INFUSE with commercial computers, but it could be said in very broad terms to compare favourably with any computer now in Australia but not with some of the most modern available overseas.

9. The installation of INFUSE is being supervised by Mr E.T. Robinson of T Group (who is also TLO). Mr Robinson (together with Mr K.H. Watson, also of T Group) took part with GCHQ scientists and engineers in the design and early development of COLOROB when he was at GCHQ two years or so ago. During the installation, Mr Robinson will be assisted by engineers and technicians from L Group who will later be responsible for that most essential factor in a machine's successful performance, that is, its maintenance. The technicians now helping with the installation are Mr D. Singleton and Mr R. Robson.

10. A new section of H Group, MHX, has been created (as from 10th September) to be responsible for the overall operational control of INFUSE. MHX will be headed by Mr A.C. Eastway who has just returned from a two year tour at GCHQ where he studied the operation and programming of COLOROB and of other electronic machines.

11. It is clear that writing programmes for INFUSE, adaption of existing cryptanalytic techniques for presentation to INFUSE and making the best use of INFUSE to help with the solution of new problems will all require research of a very high order. Although it would be possible for people to write programmes in accordance with the requirements given them by those who had done the cryptanalytic

5 D)

and/or mathematical research, I feel that the two aspects are so closely intertwined as to be regarded as one, and that there are considerable practical advantages to be gained from having the one section (in many cases, the one individual) responsible for carrying out the initial research, following through the programming stage and keeping an eye on the eventual production process. MHX will, therefore, have the additional responsibility for supporting cryptanalytic and mathematical research.

12. Initially the staff of MHX will be:

Mr A.C. Eastway O.I.C.
Mr J. Duffill
Mr P. Grouse
Miss D. Hills
Miss B. Beeson

13. I hope in the future that there will be a regular interchange between members of MHX and other MH sections.

14. And now to discuss one or two points which may occur to you on the effects of INFUSE and the MHX organization.

15. What will we be able to do when we have INFUSE that we cannot do now? Broadly speaking, INFUSE is well fitted to carry out two types of task, one being mathematical calculations, the other repetitive processes (often of a fairly simple nature in themselves). This,then gives a clue to the sort of use we expect to make of INFUSE - to enable us to carry out sophisticated mathematical attacks on problems such as Hagelin machine breaking; and less complex but equally valuable tasks such as testing a number of messages suspected of being in depth at all required offsets, calculating number of repeats expected, and printing any result where repeats exceed a certain threshold.

16. In general, therefore, we may expect INFUSE to provide us with a powerful tool for applying advanced and complex mathematical techniques (either existing or yet to be devised) to the solution of cryptanalytic problems and for carrying out very rapidly simpler processes which are completely impracticable with our present resources.

17. INFUSE will therefore enable us to undertake cryptanalytic tasks,requiring more complicated techniques for their solution than we have been able to employ in the past; it will also assist us to carry out our existing tasks more rapidly and efficiently. Remember, however, that INFUSE will not work magic or solve cyphers by itself; it will only return us value in proportion to the hard work and skilled effort put into it - in research, programming and interpreting results.

18. How will the research effort in MHX fit into the existing MH organization? In very general terms, MH sections will concentrate on current production and MHX on supporting research. Nevertheless, sections will continue to have full responsibility for any research on assigned tasks which can be carried out without assistance; for suggesting lines of research to MHX and cooperating in the carrying out of this research and in the resulting development of techniques; and gor processing and interpreting the results obtained from machine programmes. Tasks to be undertaken by MHX will normally be decided after consultation and discussion between the section head concerned, MHX and myself. Typical tasks of this kind might be:

Crypt tasks foreseen but not yet current - e.g. Hagelin C-52 analysis, teleprinter cyphers,

Now Developments in existing tasks - e.g. statistical attack on Hagelin [redacted]

Other tasks where improvements in techniques of solution and/or exploitation may be possible - e.g. [redacted]5 by 5 with no information available from indicators.

19. In carrying out this research, members of MHX will frequently be located in and work with the crypt sections.

20. I would like all crypt section heads to start thinking now about possible tasks for INFUSE and discussing them informally with MHX who will always be available for this purpose.

21. How will INFUSE affect our existing IBM punched card equipment? At present and in the foreseeable future, electronic and punched card machines at DSB are complementary, not exclusive - we have more than enough work for both. Our IBM machines, too, provide essential facilities for data processing with which INFUSE is not designed to compete. We are continuing with a programme of modernizing our IBM equipment which will enable MHK to handle a yet greater volume and variety of work than at present. There will certainly be many borderline cases where we (MHK, MHX and myself) shall have to decide whether INFUSE or IBM is the more suitable - there will often, too, be tasks in which the processing will be shared between IBM and INFUSE.

22. Can INFUSE be used for work other than cryptanalysis? Yes, though initially it will primarily be employed on 'H' work. Electronic computers can of course be used for all sorts of purposes and although INFUSE is designed to be a cryptanalytic tool, it would be available for any other suitable task, subject to overall DSB priorities.

23. What information is available in DSB on electronic computers; what further information will be given on INFUSE? I have not attempted here to go into details of the working of electronic computers in general or of INFUSE in particular. DSB library has acquired several books on the subject of computers - anyone who is interested should see Mr Eastway for advice on general reading of this kind or for further information about INFUSE. In addition, formal courses will be given as required for cryptanalysts participating in research for or evaluation of results from INFUSE.

24. I should like to conclude by stressing that, in order to achieve the successful results which we are confident we shall get from INFUSE, the combined efforts will be needed not only of the operating and engineering staffs, but also of crypt section heads, cryptanalysts and everyone else connected with the machine in any way whatever.

R.D. Botterill

(R. D. BOTTERILL)
MH

1st October, 1957.

J E

8/10/31

DISTRIBUTION

MH	1 & 2
MHX	3
MQR	4

Information Copies to:

DIR	5
AD	6
DQ	7
MS	8
MP	9
MT	10
TLO	11
MLE	12
MQ	13 → Distribution No 13
SUSLO/M	14
AUSLO(W)	15
CJSO	16
GCHQ (H)	17
GCHQ (M)	18
GCHQ (W)	19
(Attention W 65)	