

~~TOP SECRET EIDER~~

Folio 12

Declassified by ASD - 2024
National security and/or personal
information removed.

8/10/31

From: DS, DSB.

Date: 4 March 1959

Ref: 8/10/31

To: M23, GCHQ.

INFUSE

Dear Alan,

Thank you for your M/7523/112/1 of 9 February and the information from Ferranti's which Chester sent with it.

2. Generally speaking INFUSE has been running very well. CRADLE I ran until Christmas when it was replaced by MIN which was intended to search for suspected re-use of [REDACTED] MIN was a relatively small program and so it was possible to use a number of chassis to experiment with an elaborate checking system. Tony Eastway will be writing to W65 on this subject but these checks may be of interest to you so I will go into some detail. MIN intended to determine the way in which a four-figure key may have been re-used. The key was punched up in the various likely patterns of re-use and loaded on to one band of the drum. The 97 available messages were punched on one tape and these messages were run against each key version after loading them (in turn) on the drum. Tape input coding was arranged so that all tape symbols had an even number of bits so that a parity check was easily applied. Derived information (putative code) generated a sum check which was written on the drum on an extra track to ensure accurate reading out. These parity checks do not require much equipment and are therefore of more interest than the others. Arithmetic checks on MIN involved repetitive operations: for instance, mod adder operations were repeated by subtracting in one clock period and adding one input to the answer in the next clock period and comparing with the other input. Such checks of course involve more time unless they can be done in parallel with essential operations. Other checks involved more equipment e.g. in accumulating one accumulator added while the other subtracted, and a check was made by adding in a 1 and comparing the one with the complement of the other. Scoring was done in parallel mazes with repeated output to check the print-out. Other checks in MIN were of a more specialised nature and are not of general interest. Fault diagnosis with this program was very easy and we felt that the general principle of inserting checks wherever possible was a good one. Some of these checks have been included in a modified CRADLE program (CRADLE II) which is currently being run; this will be rewritten later to incorporate more checks as a result of experience with MIN.

~~TOP SECRET EIDER~~

~~TOP SECRET EIDER~~

~~TO BE KEPT UNDER LOCK AND KEY AND NEVER REMOVED FROM THE
OFFICE UNLESS TRANSMITTED IN ACCORDANCE WITH REGULATIONS~~

Declassified by ASD - 2024
National security and/or personal
information removed.

8/10/31

4 March 1959

- 2 -

3. I handed over general responsibility for INFUSE on 1 January; I am finishing off the prototype plugboard, looking at the core-store position and tying up some of the loose-ends, before returning to Salisbury on 18 May. Robin Bailey will continue to keep contact and we have had some discussions on how this might be done on a more methodical basis.

4. We have no pressing problems with any of the chassis and so I will not go into any detail in this letter, except to say that we are going to put 6.8 pf cross-over condensers on all the triggers and that the +2 volt modification has been made to all chassis except some of the output shift registers. The fan fitted to the preamplifier chassis keeps the drum bearings cooler and we have not had any further trouble with the sync. hunting late in the day. It is ~~too~~ early to say what effect it has on pre-amp reliability but we have only had two failures in that department.

5. I will be writing to let you know about the results on the plugboard which we are testing this week.

With kind regards,

E. T. Robinson
(E. T. ROBINSON)

DISTRIBUTION

M23 GCHQ
W65 GCHQ
SUKO
DSB (3)

~~TOP SECRET EIDER~~