Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

VISIT TO NATIONAL CASH REGISTER CORPORATION OF DAYTON, OHIO

Alan M. Turing

Available online: 04 Jun 2010

To cite this article: Alan M. Turing (2001): VISIT TO NATIONAL CASH REGISTER CORPORATION OF DAYTON, OHIO, Cryptologia, 25:1, 1-10

To link to this article: http://dx.doi.org/10.1080/0161-110191889734

VISIT TO NATIONAL CASH REGISTER CORPORATION OF DAYTON, OHIO

Alan M. Turing

INTRODUCTION BY LEE A. GLADWIN

Alan Turing's report "Visit to National Cash Register Corporation of Dayton, Ohio" was written following his visit to the plant in December 1942. It was found by Lee A. Gladwin, an archivist with the National Archives and Records Administration, among some papers recently released as part of the "Crane Collection," Records of the Office of Naval Intelligence (ONI), Office of the Deputy Chief of Naval Operations, Record Group 38. Until its discovery in May, 1999 the report was known only in the brief excerpts incorporated into Op-20-G's "History of the Bombe Project." In that history, Turing's "reaction to the American Bombe design" was described as "far from enthusiastic."[1] Viewed now in their proper context, Turing's remarks, while skeptical at some points, also betray some admiration and surprise at American audacity and the abundance of their resources. His incisive remarks into potential problems demonstrate his command of the technical issues involved, and his ready wit sparkles in what otherwise could be dry reading.

This appears to have been the second of his reports to GC&CS, as a previous report on Navy's bombe is referred to in Turing's third paragraph where he begins commenting upon "minor differences" between American and British bombes. The fact that these differences were considered "minor" again reflects the close liaison and extent of technical exchanges between GC&CS and Op-20-G. Following his descriptions of the differences, Turing comments upon "Cribbing", "Catalogue", "Subtractor machine", "Hagelin", and "Tunny". Most fascinating are references to the history of British efforts to develop machines and methods

[1]Memorandum for Director of Naval Communications, Subject: History of the Bombe Project, From J. N. Wenger, Commander, U. S. N., H. T. Engstrom, Commander, U. S. N. R., and R. I. Meader, Lt. Commander, U. S. N. R., 24 April 1944, in OP-20-G History of the Bombe Project, p. 7; NR 1736, Box 705; Historic Cryptographic Collection, Records of the National Security Agency/Central Security Service, Record Group 457; National Archives, College Park, MD.

to solve Enigma ciphers. These are revealed in Turing's comments on lessons learned by the British.

There may be other reports by Turing yet to be found. Hopefully, they will be.

For more extended commentary on Turing's "Visit to National Cash Register Corporation of Dayton, Ohio", please refer to my article "Alan Turing's Visit to Dayton". (See pp. 11-17, this issue of *Cryptologia*.)

An early undated photograph of Alan Turing.

Photograph from King's College Library.

ALAN TURING'S REPORT

On December 21st I visited the works at Dayton, Ohio, where the Bombes are being made, with Commander Wenger, Lieutenant-Commander Engstrom, Lieutenant-Commander Meader, Lieutenant(jg) Eachus and Major Stevens. The weather held up our train and we arrived six hours late at 2 p. m. so that we did not have quite so long there as we might have had, but probably sufficient.

The plans for the Bombes are on the whole essentially the same as ours, but there are a number of minor differences which should be noted.

(A)

As mentioned in my previous report the machine is intended to step and reverse whenever there is a "stop", and go back to the position of the stop, and there do further twisting. Engstrom and I are still both rather unhappy about this idea. We were given a demonstration of how the motor was able to reverse and be going full speed in the reverse direction in a fraction of a second, with the full load; however this seems to me hardly to prove that all will be well when one tries to reverse the Bombe itself, e. g. the gears might get distorted under the strain. They say that the whole machine is being built sufficiently strongly to withstand such strain. Possibly the real objection to this method is that the time taken over each stop is fairly considerable, viz 15 seconds, and of course it seems a pity for them to go out of their way to build the machine to do all this stopping if it is not necessary. If the machine is made into a Mammoth the stopping and testing feature will be more redundant since most of the testing will already have been done.

(B)

Instead of setting up menus by means of plated jacks (known here as "Jones plugs") it is to be done by switching. The "diagonal board" is wired to a number of uniselectors of 26 positions and 26 wipers each. There is one uniselector associated with the input and one with the output of each enigma. If an enigma corresponds to a pairing GL for instance in the crib, then the input uniselector has its wipers set to position G, and this automatically connects the output of the enigma with the row G of the diagonal board; one sets the output uniselector to position L.

This method sounds as if it would use up an awful lot of wire, but on second thoughts it does not seem quite so bad. I should say it would use up about six times as much wire as we have in the Jones plugs for a Bombe. It eliminates the

need for an independent diagonal board and for commons, and should speed up the plugging-up very greatly.

This system was once suggested by Wynn-Williams. Welchman and I were both very little interested in it at that time, principally because we thought Wynn-Williams ought to be concentrating on speeding the Bombes up and that our present form of pluggings was perfectly satisfactory and need not be interfered with. However at that time I thought also that the method that he was proposing was altogether too elaborate and quite out of proportion, but I am now converted to the extent of thinking that starting from scratch on the design of the Bombe this method is about as good as our own.

(C) Wheel Changing

You may remember that the American Bomb programme was to produce 336 Bombes "one for each wheel order". I used to smile inwardly at the conception of Bombe hut routine implied by this programme, but thought that no particular purpose would be served by pointing out that we would not really use them in that way. However it now seems that this programme has actually affected the design of the Bombes, for, assuming that the wheels would not be changed, they have designed the Bombes with different sizes of wheels for the different positions. This will mean that they will now have to provide a complete set of all eight wheel for each position, which may be a very considerable job, or else the wheels will have to be interchangeable from Bombe to Bombe. This second alternative might lead to endless confusion in the Bombe hut, but we hope to figure out some kind of compromise scheme by which the wheels are only interchangeable between three Bombes, say, and an intermediate number of wheels is required.

I do not really understand the reasons for the various sizes of wheels. I suspect that there is some misunderstanding about it.

(C) Gearing

In our Bombes all the wheels moving at equal speed are directly connected mechanically, and the various sets of wheels connected by a carry mechanism. In the American Bombe however there are independent sets of gears for the various enigmas, and these sets of gears are only related by the shaft which runs at the speed of the high speed wheel. I should have expected that this would have required much more gearing than our method. They say this is not so and that in our method we need to have gearing for each wheel of each enigma, to arrange for the wheel to turn about an axis which is at right angles to the shaft which control the wheels moving at that particular speed, and that this runs one into

just about as many wheels as they use. (Of course this picture of how our wheels move is not altogether correct: there is no controlling shaft for the wheels which do not move uniformly.)

(E) Brushes and circuit breaking

The brushes to be used are not unlike those used by Wynn-Williams. I asked them how they thought they would make out about bounce. They had done some tests on it with a number of contacts in series observing the thing with an oscillograph, and not detected any bounce. They thought that it was easier to eliminate bounce using wheels which, as in our ordinary Bombes, have brushes moving over a plane surface, than it would be with Wynn-Williams' cylindrical commutators. However it now occurs to me that their tests can hardly be considered conclusive as they were not testing for the bounce with the electronic stop-finding apparatus, and moreover such a demonstration was made to Commander Travis and Flowers and myself (using the electronic apparatus) at Malvern, and yet when it came to the point of lining Cobra up for a trial menu, it failed on account of bounce.

On our Bombes the current entering the diagonal board at the input point, and the current through the second coils of the differential relays is cut off by circuit breakers except during the period of "clean contact". (In some forms of the Bombe I believe the circuit breakers take the form of generators which provide square form A. C., but this makes no difference). In the American Bombe there is an extremely interesting alternative method. Instead of the brushes and the contacts being rather narrow they are quite wide, and therefore the period between the clean time in one position and that in the next is a period where too many connections are made through the enigmas rather than too few, and therefore there is no need to make any special provision to avoid the machine stopping in these periods, i. e. one needs no circuit breakers. This has a further advantage. Normally, when there is no stop, the whole of the input row of the diagonal board will be connected together whether one is in a clean time period or not, and so the system will be fairly free from transients, whereas when there are circuit breakers they will set up transients which may mask the transients due to a stop. I think they have got something here, but it remains to be seen how great are the transients which remain and are due to the various paths by which the enigmas connect the points of the diagonal board.

(F) Mammoth plans

The present form of Bombe does not include any Mammoth features, but the inclusion of the Eachus resister board is under consideration.

(G) Drunken Drive

The introduction of gearing, by which the second fastest wheel does not move uniformly, but moves most slowly during the clean time, is also under consideration. Such gearing was demonstrated to Eachus by Keen. It will not be included in the first two Bombes.

(H) Wheel position and wheel speed

It is proposed that the B-wheel should be made the slowest in the Bombes in order that they may be used for 3-wheel problems. The L. H. W. is the super-fast wheel, the M. W. is the fast wheel the R. H. W. is the medium wheel.

With this arrangement one cannot do Hoppity but there is no reason why a few Bombes should not have the R. H. W. as fast wheel instead of the B-wheel, so that they can be used for Hoppity.

Cribbing

The principle of running British made cribs on American Bombes is now taken for granted. I find that comparatively little interest is taken in the Enigma over here apart from the production of Bombes. I suppose this is natural enough seeing that they do not intercept any of the traffic other than the Shark. Apparently it is also partly on security grounds. Nobody seems to be told about the rods or Offizier or Banburisms unless they are really going to do something about it.

Catalogue

A Driscoll-Welchman-Chamberlain catalogue is being made for the 56 wheel orders with 17576 cards in each. There is a dwindling party headed by Mrs. Driscoll that wants to list the positions with a given pairing on separate pages according to B-wheel position. Mrs. D. thinks that this will help when one is looking up positions where there is a turnover, but it won't. We are to get a copy of the catalogue.

Subtractor machine

At Dayton we also saw a machine for aiding one in the recovery of subtractor groups when messages have been set in depth. It enables one to set up all the cipher groups in a column of the material, and to add subtractor groups to them all simultaneously. By having the digits coloured white red or blue according to the remainders they leave on division by 3 it is possible to check quickly whether the resulting book groups have digits adding up to a multiple of 3 as they should with the cipher to which they will apply it most.

A rather similar machine was made by Letchworth for us in early 1940, and although not nearly so convenient as this model, has been used quite a lot I believe.

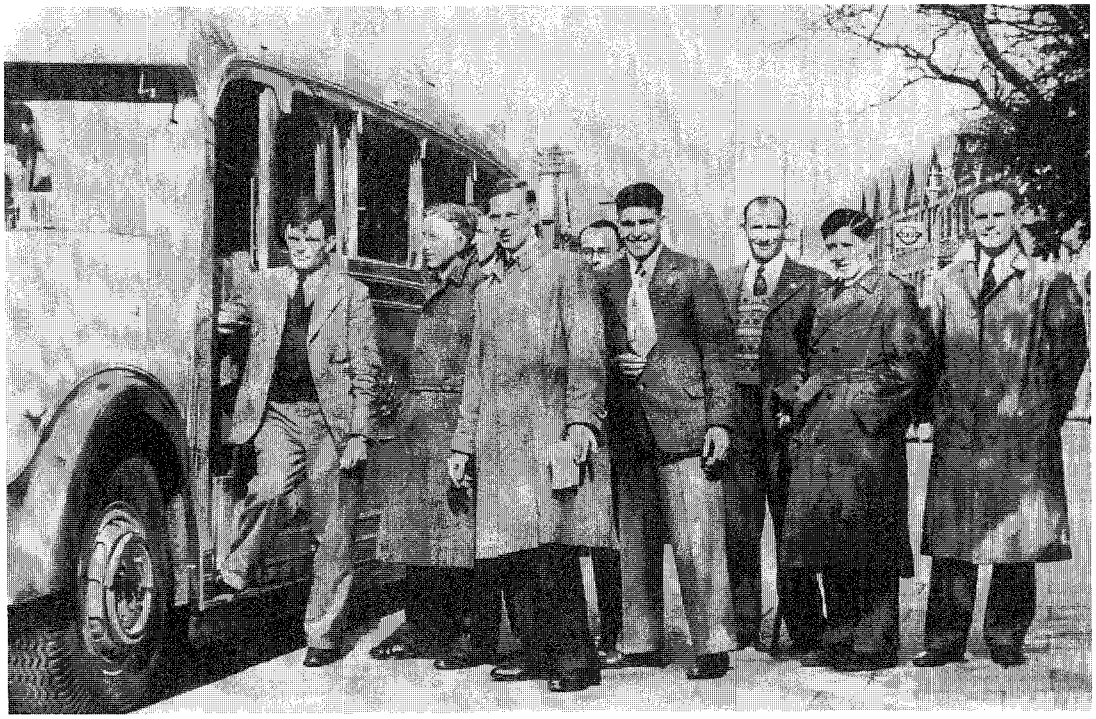
Hagelin

I spent a certain amount of time in explaining what I knew about Hagelin procedure to Borgerhoff the man who is most interested in the Hagelin. We tried to recover the machine from the cipher and clear sent for some September messages, but came to the conclusion that the machine was not being used in the most straightforward way. Each letter seemed to be enciphered with the Hagelin machine, but it appeared that the machine's motion was being interfered with in some way or else that the letters of the message were being enciphered in some unusual order, e. g. enciphering all first letters of the groups and then all second letters. We did not discover exactly what it was. Would appreciate explanation of present procedure.

Tunny

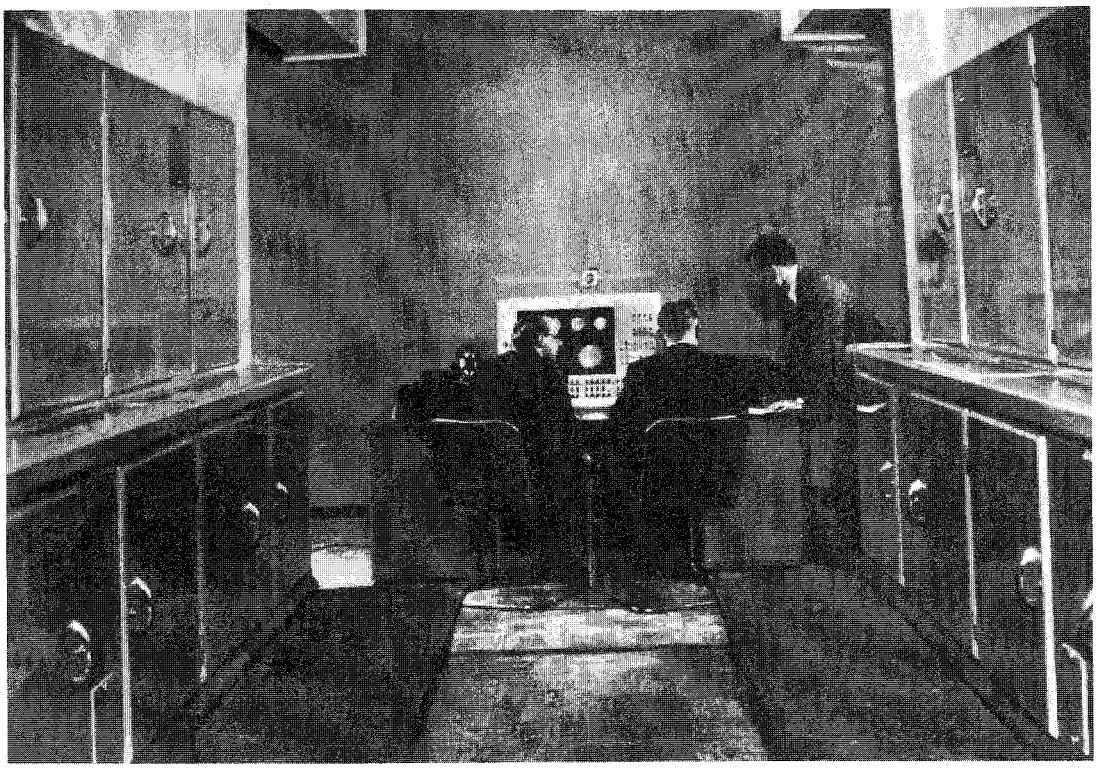
It appears that the long stretch of Tunny key as sent over here for March(?) really could have been broken by Tutte's original method, modified slightly by working entirely in terms of differenced key. Apparently at the time when the first break was made the tendency for the signs in the extended Ψ not to change was so marked that when one wrote out the key in the χ period the pattern of the χ wheel would stand out. It would stand out even more clearly if one wrote out the differenced key instead of the key itself. By March the patterns of the wheels had been improved to the extent that one could not manage without differencing but by April they had been improved still further, so that this method in either form became altogether impossible.

The Ratio Club (London) c. 1949. (L-R) Back Row Standing: Harold Shipton, John Bates, W. E. Hick, John Pringle, Donald Shell, John Westcott, Donald Mackay. Middle Row Standing: Giles Brindley, Tom McLardy, Ross Ashby, Thomas Gold, Albert Uttley. Front Row Sitting: Alan Turing, Gurney Sutton, William Rushton, George Dawson, Horace Barlow. Photograph from King's College Library.



Alan Turing, with colleagues, boarding bus in 1946 when he worked at the National Physical Laboratory in England.

Photograph from King's College Library.



Alan Turing (standing) beside the Universal Electronic Computer (Mark I) installed at Manchester University by Ferranti Limited. Photograph from King's College Library.