Turing’s Report on His Visit to NCR

December 1942

Dr. Alan M. Turing

Editors' Preface

This document was written by the late Dr. Alan M. Turing while he worked as a cryptanalyst at Bletchley Park during the Second World War. The document has been obtained from the US National Archives and permission has been obtained from the Controller of Her Majesty's Stationery Office to publish the paper on the personal Web Page of Frode Weierud. The document has been faithfully retyped by the three editors, Ralph Erskine, Philip Marks and Frode Weierud. The original document was typed and had the style and layout of a typewritten document of that period. To make the re-edited presentation more pleasing the document has been both left and right justified and a more modern type font has been used. The page numbers of the original are given as numbers in square brackets. Apart from these modifications to the layout the document has the appearance of the original.

Where there are obvious typing errors these have been corrected in square brackets. In a few cases a superfluous letter(s) has been removed by putting the letter(s) in square brackets preceded by a slash, e.g. [/s]. The Editors' comments are in square brackets and in italic. Longer and more detailed comments are in numbered footnotes.

The Editors,

Ralph Erskine,
Philip Marks,
Frode Weierud, © September 2000

Source:

National Archives and Records Administration (NARA), Record Group 38, Crane Library, File: CNSG 5750/441.

Acknowledgement:

Our thanks to Stephen Budiansky for finding this report and making it available to us.

Updated: 23 October 2000

[1]

File AM–10 *Dec 1942*[1]

VISIT TO NATIONAL CASH REGISTER CORPORATION of DAYTON, OHIO

On December 21st I visited the works at Dayton, Ohio, where the Bombes are being made, with Commander Wenger, Lieutenant-Commander Engstrom, Lieutenant-Commander ~~Meteur~~ Meader[2], Lieutenant (jg) Eachus and Major Stevens.[3] 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 stop and reverse whenever there is a "stop", and go back to the position of the stop, and there do further twisting [testing ?]. 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.

[2]

They say that the whole machine is being built sufficiently strong 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.

[1] The text in italic on the top and the bottom of the page has been written in pencil.

[2] Meteur has been stroked over and replaced with Meader in pencil. This is undoubtedly Lieutenant-Commander R. I. Meader, U.S.N.R. who was part of the US Navy Bombe Project.

[3] Major Geoffrey Stevens was GC&CS's Technical Liaison Officer at the Signal Intelligence Service (S.I.S). and OP-20-G from June to October 1942. He was then replaced by Major Cheadle. However, Major Stevens' liaison functions did not end in October 1942 as he was active both later in the year and in a large part of 1943.

(B) Setting up of menus. Instead of setting up menus by means of plaited 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 time very greatly.

[3]

This system was once suggested by Wynn-Williams[4]. 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 plugging 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 a Bombe this method is about as good as our own.

(C) Wheel Changing. You may remember that the American Bombe 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 Bombe 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 wheels 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

[4]

wheels are only interchangeable between three Bombes, say, and an intermediate number of wheels is required.

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

[4] This is Dr. C. E. Wynn-Williams who was chief engineer at the Telecommunications Research Establishment (T.R.E.) at Malvern. He was actively involved in Bombe developments and designed the Cobra attachment, a high-speed four wheel Bombe device.

(D) 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 as many wheels as they use. ([O]f 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 this thing with an oscillograph, and not detected any

[5]

bounce. They thought that it was easier for them to eliminate bouncing 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 are not testing for the bounce with the electronic stop-finding apparatus, and moreover such a demonstration was made by Commander Travis and Flowers[5] 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 Bombe 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

[6]

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

[5] Thomas H. Flowers worked at Dollis Hill Research Station of the British Post Office and was involved with Bombe developments. He is also famous for being the chief electronic designer of the Colossus machines used to break the on-line teleprinter cipher machines, Lorenz SZ42.

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[6] features, but the inclusion of the Eachus resistor 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[7]. 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 and the R.H.W. is the medium wheel.

With this arrangement one cannot do Hoppity[8] but there is no reason why a few Bombes should not have the R.H.W. as ~~fast~~ [slow][9]

[7]

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 Shark. Apparently it is also partly on security grounds. Nobody seems to be told about rods[10] or Offizier or Banburismus 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[11] 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

[6] The Mammoth is still largely a mystery device, but it appears to have been used to test a *Stecker* hypothesis. It used large number of relays and could instantaneously reject or confirm the given hypothesis. This indicates it might have been of a combinatorial nature instead of the sequential nature of the Machine Gun, another *Stecker* testing device.

[7] This is H. H. (Doc) Keen of the British Tabulating Machine Co. who was one of the chief designers of the British Bombes. The Drunken Drive was one of his inventions.

[8] Hoppity was a special Bombe menu where the middle wheel (M.W.) would be moved forward one step when the right hand wheel (R.H.W.) came to a designated letter. This type of menu could be run when the Ringstellung of the R.H.W. was known. Usually M.W. turnover was dealt with using a set of Bombe menus.

[9] Alan Turing appears to have become confused here. On the British Bombes, which could do Hoppity, the R.H.W. was the slow Bombe wheel, and this is what he also would like on the US Bombe.

[10] To learn more about rods or any of the other Enigma details Turing refers to please consult the “Prof’s Book”, Turing’s Treatise on Enigma. See the electronic version at: http://frode.home.cern.ch/frode/crypto/Turing/

[11] Mrs. Agnes Meyer Driscoll was one of the civilians employed as cryptanalysts by the US Navy. She broke many Japanese codes and ciphers before the war and was assigned to the naval Enigma problem (on which she made little progress) around mid-1940.

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

[8]

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. enciphered all first letters of the groups and then the 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[12] key as sent over here for March(?) really could have been broken by Tutte's[13] 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

[9]

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.

[12] Tunny was the Bletchley Park (BP) code name for the German on-line teleprinter cipher machine, SZ42, and the ciphers it produced. The BP analogue of the SZ42 also carried this code name.

[13] This is Professor William T. Tutte who was the first person at BP to discover the secret of the SZ42's cryptographic principle. He reconstructed the machine's key generator from a 4000 character message previously broken by one of BP's finest cryptanalysts, Colonel John Tiltman.