US Navy Cryptanalytic Bombe - How to operate the Simulator written by Magnus Ekhall (magnus.ekhall@gmail.com) and Fredrik Hallenberg (fredrik.hallenberg@gmail.com)

Author: Jerry McCarthy, U.K
Issue 1; 24-February-2022.

Introduction.

This document presents a computer simulation of the US Navy Bombe, and explains how to operate it. The US Navy Bombe, an improved version of the British Turing-Welchman Bombe, was predominantly used to break German naval Enigma messages during World War II. This document draws heavily on (Ekhall, Hallenberg, 2018). By using a simulation of a machine to break an example message, it can be seen how the US Navy Bombe could have been operated and how it would have looked when running.

In 1942, with the help of Bletchley Park, the US Navy signals intelligence and cryptanalysis group OP-20-G started working on a new Bombe design. The result was a machine with both similarities to, and differences from, its British counterpart.

There is one single original US Navy Bombe still in existence at the National Cryptologic Museum in Fort Meade, MD, USA. The Bombe on display there is not in working order and the exact way it was operated is not fully known. The US Navy Bombe was based on the same principles as its British version but had a different appearance and thus a different way of operation. The Bombes were used to search through a part of the Enigma key space, looking for a possible Enigma rotor core starting position which would not contradict a given enciphered message and its plaintext (Carter, 2008).

The computer simulation presents a graphical user interface and runs at approximately historically accurate speed.

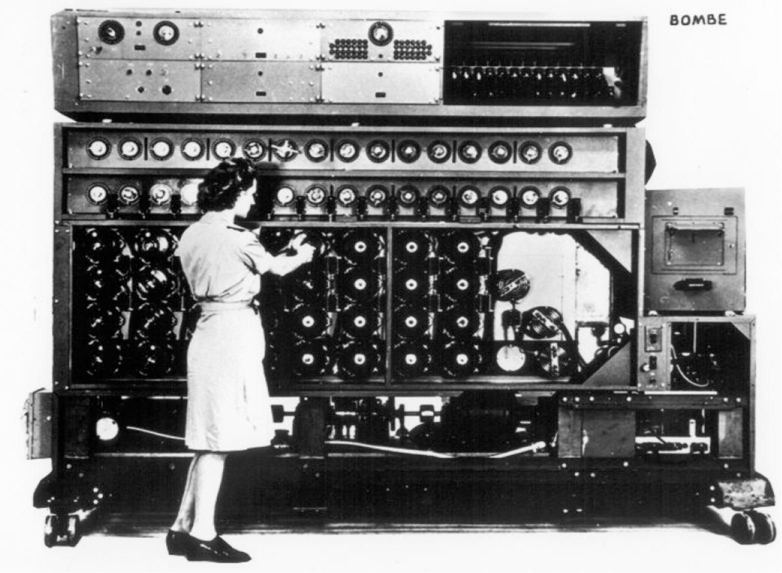


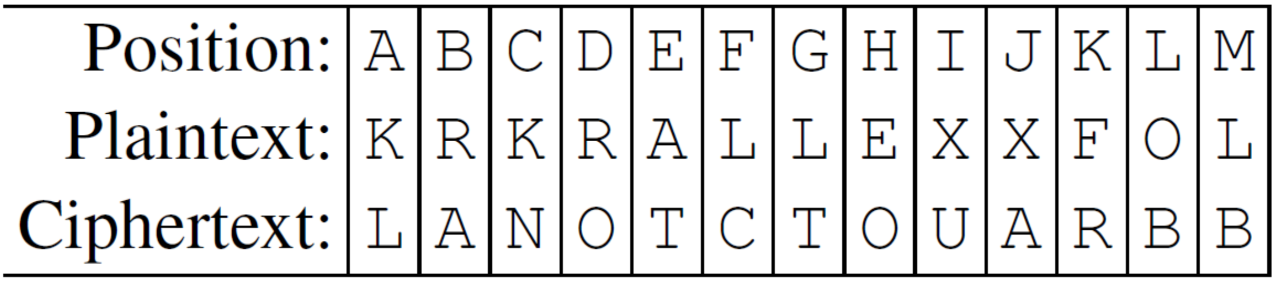
__Figure 1: An operator setting up the wheels on a US Navy Bombe. Source: NSA__

It is assumed that the reader is familiar with the Enigma machine. This knowledge is widely available, for example in (Welchman, 2014).

To find an Enigma message key with the Bombe, it is necessary to have a piece of plaintext, a crib, corresponding to a part of the encrypted message. A crib could be a common word or a stereotyped phrase which is likely to be present in a message, for example, **Wettervorhersage,** which is the German word for weather forecast. The crib is used to derive a configuration of the Bombe, although a guess as to which Enigma rotors were used, has to be made. Once started the Bombe will scan through all possible Enigma rotor core positions and stop when a position has been found that does not lead to a logical contradiction for the given crib (Carter, 2008). If a logical contradiction occurs then the state of the Bombe represents a setting of an Enigma where it would not be possible to encipher the assumed plaintext (the crib) into the ciphertext of the crib. Each stop is subject to further tests after which the Bombe is automatically restarted. If a test is passed, relevant information on the stop in question is printed onto paper (Desch, 1942).

2 Example Message

The Bombe simulation will be tested using a real message sent on May 1st 1945 (CryptoMuseum, 2017) as shown here in Table 1.



Position:	A	B	C	D	E	F	G	H	I	J	K	L	M
Plaintext:	K	R	K	R	A	L	L	E	X	X	F	O	L
Ciphertext:	L	A	N	O	T	C	T	O	U	A	R	B	B

Table 1: Crib and corresponding ciphertext used throughout this paper

In this case, the crib is the first thirteen letters of the plaintext. The wheels used for this message were **Beta, V, VI and VIII**, with the **thin C**-reflector being used. The original Enigma rotor start position was **{CDSZ}**[1]. This means that the leftmost rotor on the Enigma, in this case the Beta rotor, is set to position C, the second rotor is set to D and so on. The ring setting of the rotors for this message was **{EPEL}**. Note that the difference between the ring setting and the rotor start position is 24, 14, 14, 14 positions respectively. This is called the rotor core starting position.

The row labeled ”Position” in table 1 above shows what setting the rightmost Enigma wheel would have had when encrypting a given plaintext letter into ciphertext. The assumption is that the Enigma machine would have been set to **{ZZZZ}** before the message was coded. This leads to the first letter being encrypted at position **{ZZZA}**, the next at **{ZZZB}** and so on. The plug board connectors, Stecker in German, used on the Enigma for this message were:

[1] (this notation will henceforth be used to show positions of the corresponding wheels)

A	B	C	D	H	J	L	P	S	V
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	F	M	Q	U	N	X	R	Z	W

Table 2: Plugboard connections

Note that these Stecker settings were not known at the time the message was intercepted, but are determined as a result of the Bombe run. The letters of the alphabet not listed in the plugboard connector pairs above did not have a wire connected on the plugboard which means that they are electrically connected to themselves.

There were normally ten plugboard cables used in the daily Enigma key, leaving six letters self-Steckered (Copeland et al., 2017).

3 Setting Up the Bombe

Preparing the Bombe to work on a message consists of a number of steps. Firstly, the wheels need to be selected and set to the appropriate starting positions. Secondly, the bank switches need to be set according to the letters in the crib. Thirdly, one or two input switches need to be activated. Finally, some of the printer cables are connected to the diagonal board.

3.1 Enigma Rotor Equivalent Wheels

The Bombe has sixteen wheel banks of four wheels with each wheel bank representing the rotors of an Enigma machine. Eight wheel banks are on the front of the Bombe and eight are on the back.

The Bombe was primarily designed to break messages encrypted with the M4 Enigma which had four rotors. However, it could also work on messages encrypted with a three-rotor Enigma such as the one used by the German Army. For this purpose there is a switch which selects between three- or four-wheel mode. In three wheel mode, the slowest wheel in each of the 16 wheel banks would be stationary (Desch, 1942). By observing how the wheels in a wheel bank are interconnected it can be assumed that the top[2] wheels of each wheel bank would not move in this configuration.

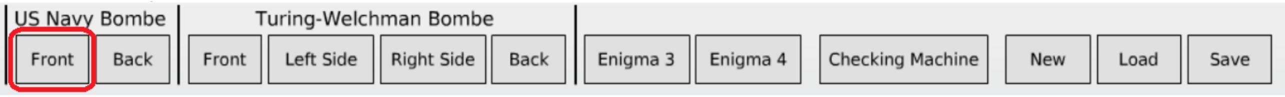
To configure the Bombe for the given demonstration message, a set of wheels which are to be tested has to be installed. As noted above, the wheels are {**Beta, V, VI, and VIII**}**.**

As mentioned in section 2 above, the correct wheel order is already known in this case. The same wheels are loaded onto all wheel banks of the Bombe. Also, the ”thin C”-type reflector cables are connected to all the reflector plugs on the Bombe.

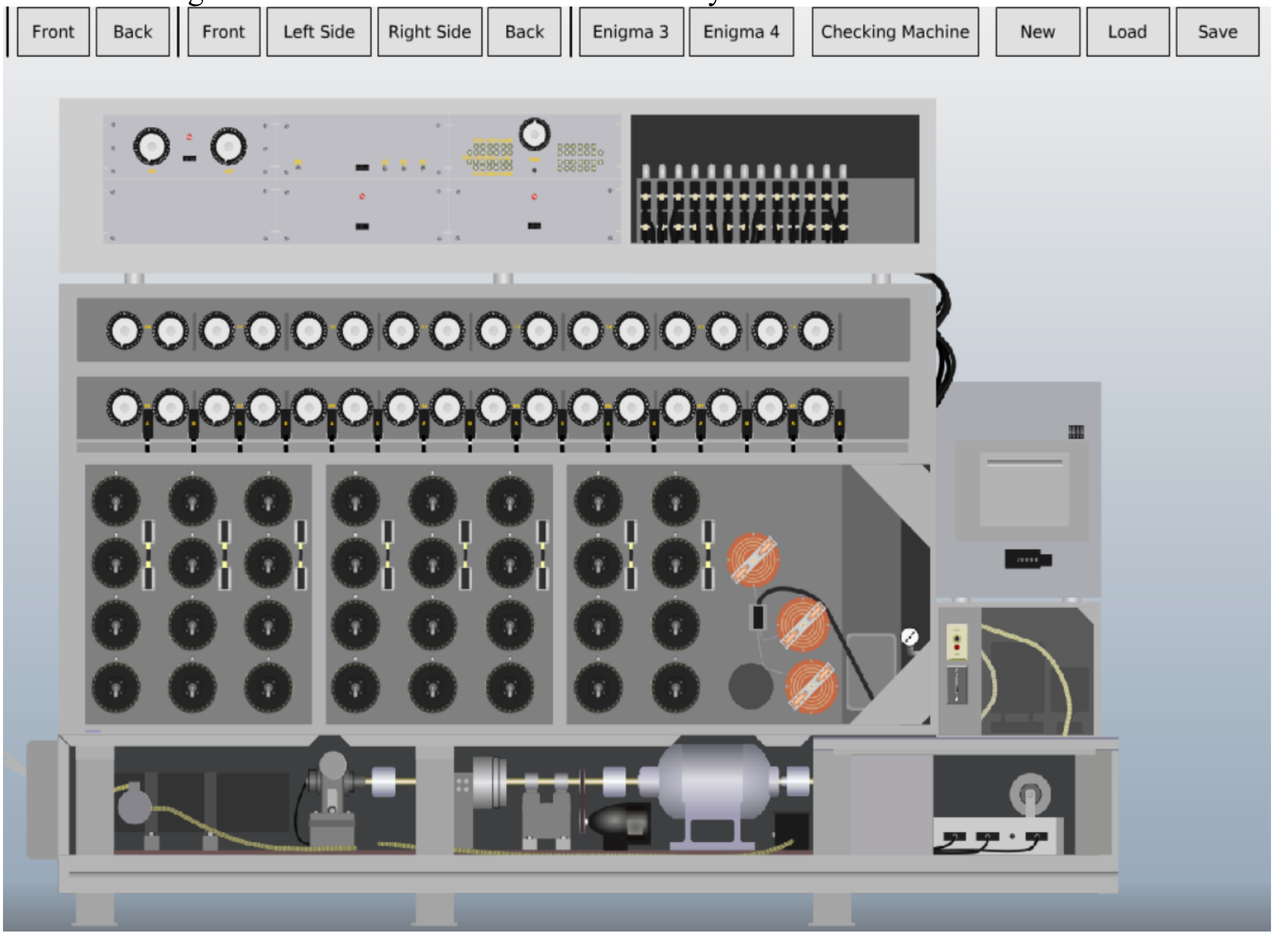
In reality the wheel order was not known but many different wheel orders could be tested in parallel, one wheel order per Bombe. A total of 121 US Navy Bombes were built (Wilcox, 2006).

[2] Note that this observation disagrees with (Ekhall, Hallenberg, 2018).

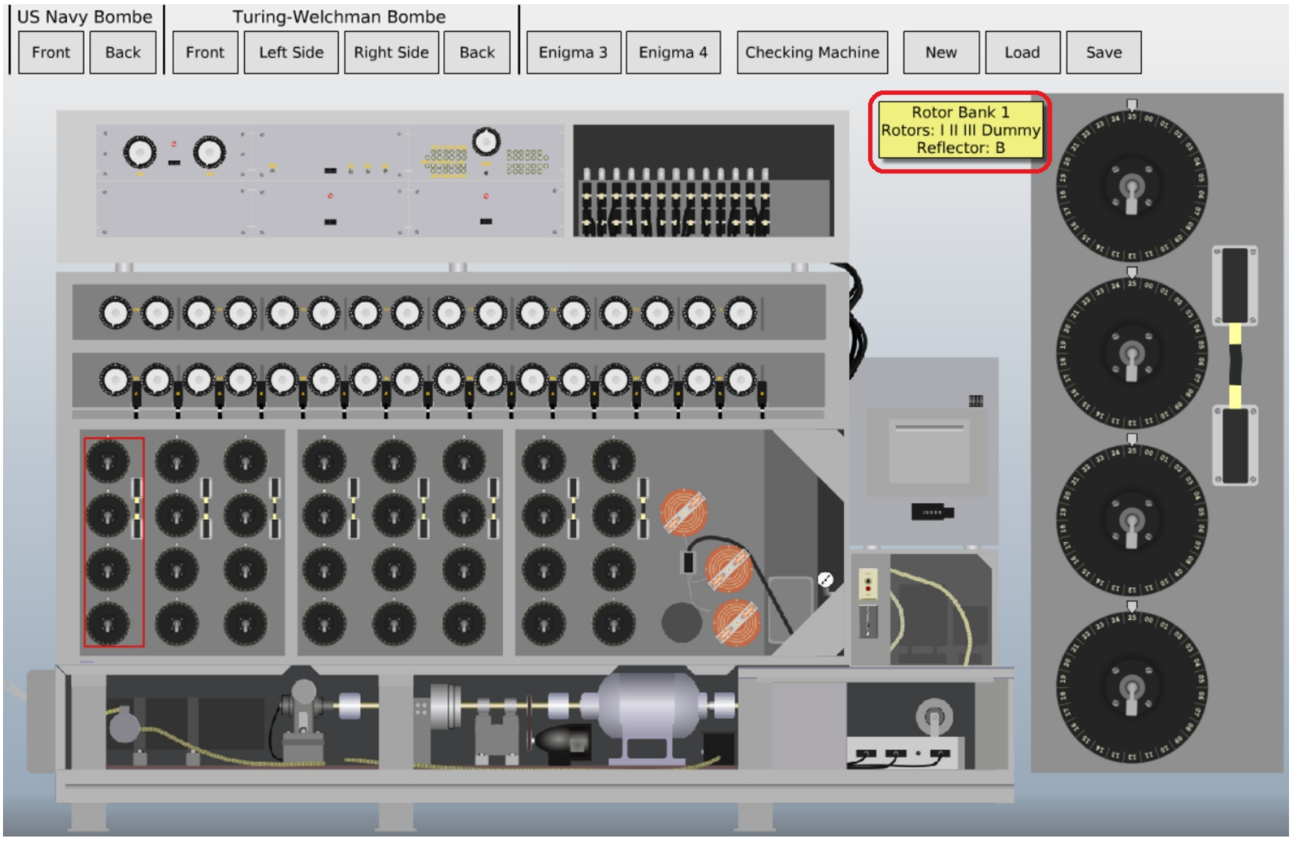
To install the wheels on the Bombe Simulator, first start the Simulator running, and, if necessary, press the US Navy Bombe [Front] button.



So doing will show the front face of the US Navy Bombe:



By default, the wheel order is {**I, II, III, Dummy}** and **Reflector (UKW) B**. This configuration can be seen by clicking on the left-most set of four wheels, at which point a magnified view of those wheels will be seen, with their denominations also visible:



Rotor Bank 1
Rotors: I II III Dummy
Reflector: B

We can now click on the magnified rotors to set them to **Beta, V, VI, and VIII.** Click on the topmost one, until the text "**Beta**" appears, the next one down until the text "**V**" appears and similarly for the next two for their values of "**VI**" and "**VIII**". Note that so doing propagates these settings for all sixteen rotor sets.

Normally, it is assumed that the second wheel of the Enigma does not advance during the crib. Since the second wheel of the Enigma will advance one step once or twice per revolution of the first wheel there is a high probability that this is not the case, and if so, the Bombe will fail to find a possible solution. There are techniques that could have been used if a second wheel turnover was suspected, but such cases are not in the scope of this document.

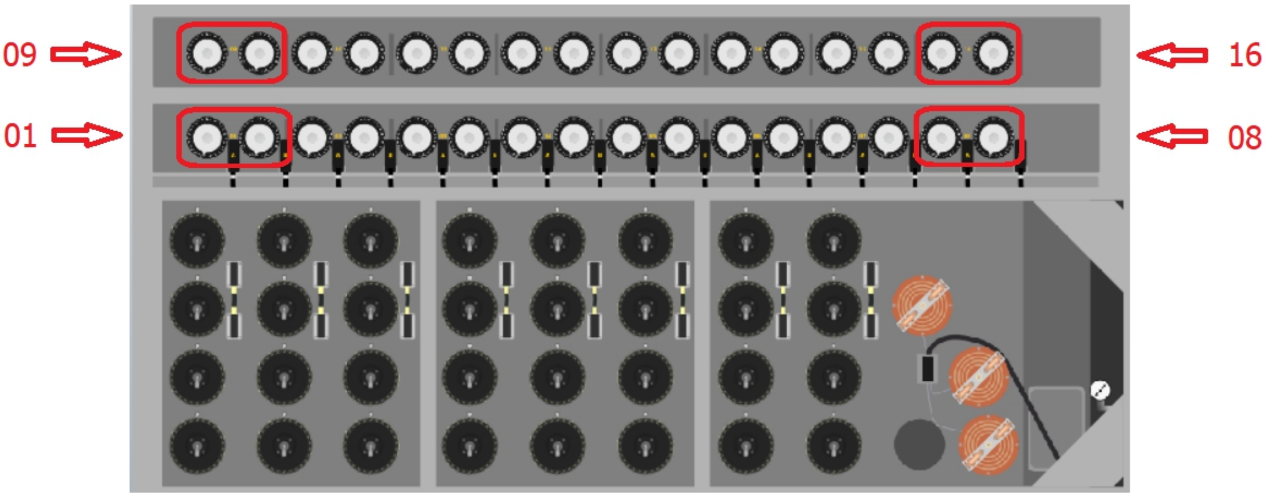
With the example message there was in fact a second wheel turnover before the first letter was encrypted. This knowledge will be taken into account in the following discussion. In practice this could not have been known, but the Bombe would still have found a solution since there is no further second wheel movement during the crib; the entire crib has one and only one wheel position for the second wheel. The difference is that the second wheel now has to be set to A instead of Z which it otherwise would have been assumed to be. Therefore the Bombe is adjusted so that the wheels on wheel bank 1 are set to **{25, 25, 0, 0}; **this corresponds to **{ZZAA}**.

The wheels of wheel bank 2 are set to **{25, 25, 0, 1}** = **{ZZAB}**, wheel bank 3 to **{25, 25, 0, 2}** = **{ZZAC}** and so on all the way up to wheel bank 13 which is set to **{25, 25, 0, 12}** = **{ZZAM}**.

Since the top wheel of the Bombe is connected to the reflector plug it can be assumed that this represents the leftmost Enigma rotor on a physical Enigma which is connected to the reflector of the Enigma. The bottom wheel of the Bombe corresponds to the rightmost Enigma rotor. The set-up of wheel order, reflector plugs and the start position of the Bombe wheels is now complete. The next step is to connect the wheel banks according to the letters of the message.

3.2 Bank Switches

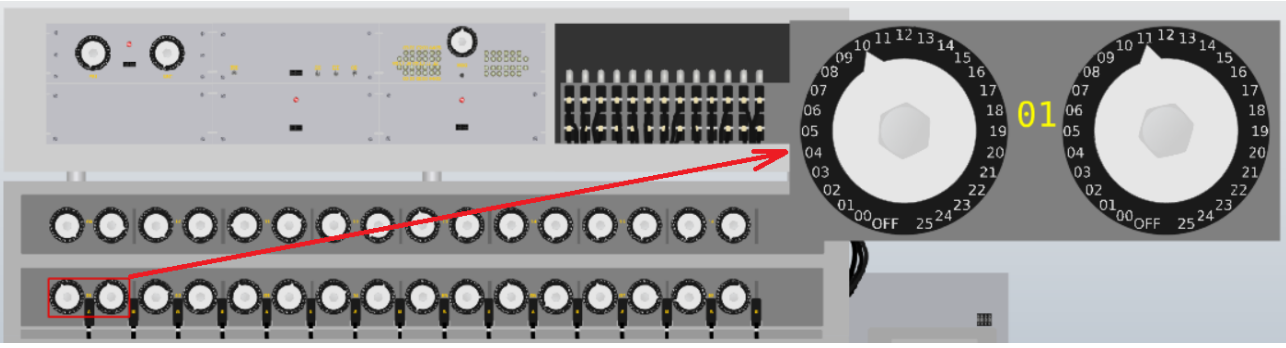
There are two 26-step rotary switches for each of the 16 wheel banks: one switch is for the input letter to the bank and the second is for the output letter. The rotary switch connects the rotor bank to the diagonal board which utilises the symmetrical properties of the Enigma plugboard to interconnect the Bombe wheel banks. All of the 32 switches are located on the front of the Bombe[3], and are numbered as shown here: Bottom row first, left-to-right, and then the upper row, also left-to-right.



The plaintext letters of the message are considered to be the input to the corresponding rotor bank and the ciphertext letters to be the output.

The setting of each bank switch pair is a matter of clicking on one of the bank switches within the pair, which produces a magnified version of the that pair of switches. It is then possible to drag the pointers of the two switches to the required value.

For example, for wheel bank 1 which corresponds to the first letter of the message, the input is K and the output L., but note that the bank switches are assigned the values 0 thru 25, rather than A thru Z. Therefore the left switch of the two bank switches corresponding to rotor bank 1 is set to 10 for the letter K. The right switch is set to 11 for L. The picture below shows the result of setting the switches to K (left switch) and R (right switch).



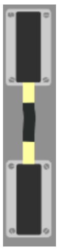
[3] These switches eliminate the need of a plug board as used on the back of the British Bombe and thus makes setting up a crib on the Bombe much faster (Turing, 1942). The British Bombe, on the other hand, could have up to three cribs or wheel orders in use at the same time on one Bombe. The British Bombes usually had 36 wheel banks of three wheels each, thus corresponding to 36 Enigma machines.

Once a given switch pair has been set, it is possible to close the magnified view by clicking somewhere in the empty space just below the right switch.

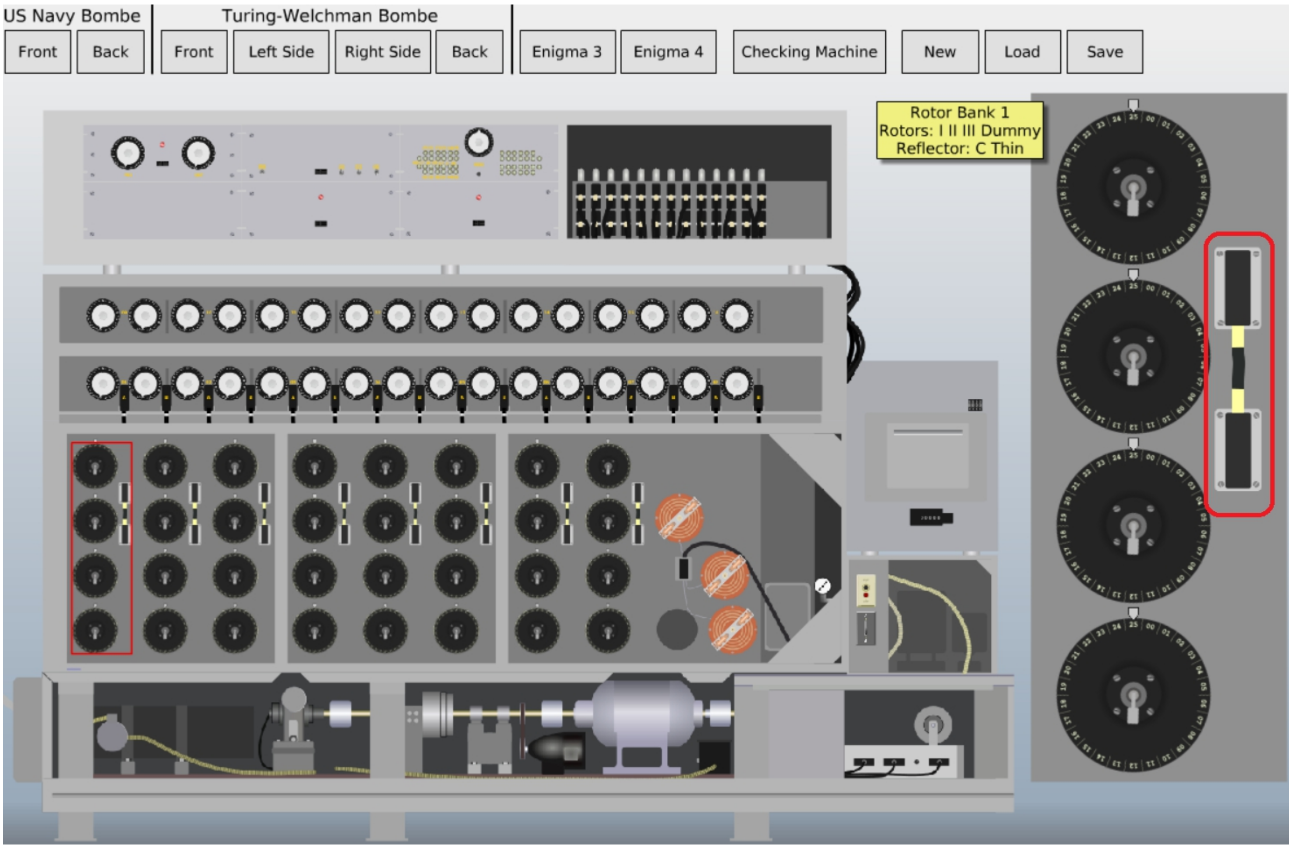
For wheel bank switch 2 the input switch is set to 17=R and the output switch to 0=A, and so on for the rest of the wheel bank switches which are set up in the same way, with the last pair, number 13, set to 11=L, 1=B according to the last letter of the crib (see table 1).

3.3 The Reflectors

Apart from the four wheels in a wheel bank, one for each Enigma rotor, there is also a reflector plug which has the same function as the reflector on the Enigma. The Reflector can be set for all the rotor banks by clicking on any of the rotor banks to create the magnified view, and then clicking on the Reflector image:



Each click on the Reflector image will cycle the Reflector's value through the possible values **{B, C, BThin, Cthin}**. Setting the Reflector for one wheel bank automatically propagates the Reflector setting to all the wheel banks.

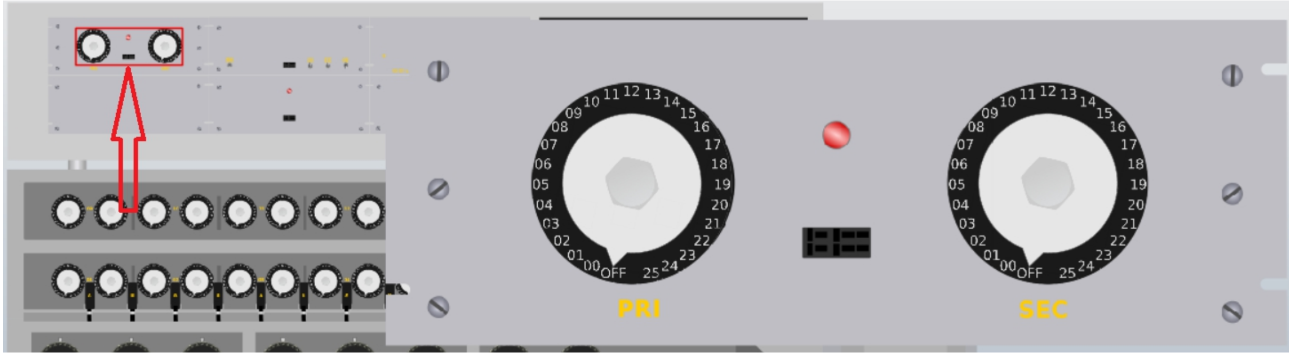


Rotor Bank 1
Rotors: I II III Dummy
Reflector: C Thin

3.4 Input Switches

The Bombe works by injecting a test current into a position corresponding to a certain letter of the diagonal board. This current then propagates through the system and stops the Bombe if it fails to reach all other letters of the alphabet.

To select the letters where the test currents are to be injected, the Bombe has two 26-step rotary switches marked **PRI** and **SEC** (for primary and secondary). Normally only the primary input is set. When using a crib where the letters of the crib and the corresponding ciphertext form two separate graphs, the secondary input would also be needed.


00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 OFF
PRI
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 OFF
SEC

Clicking on one of the two wheels within the indicated area brings up a magnified view of these two Input Switches. They can be rotated by dragging with the mouse to the required setting(s).

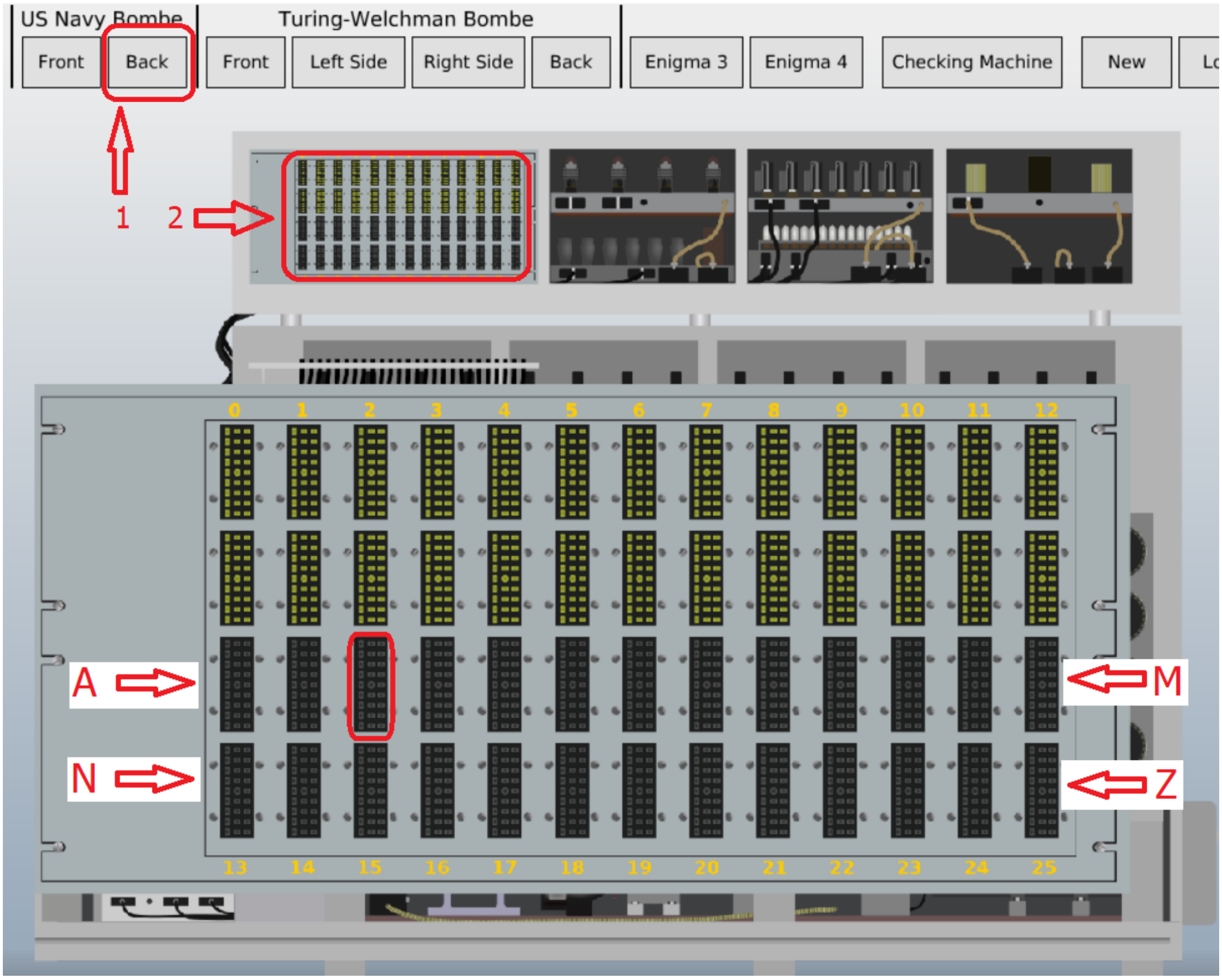
The input should be connected to a frequently occurring letter in the crib. L is selected as it occurs at three places in the example message. The primary input switch is switched to 11 which corresponds to L. The secondary input switch is not needed for the current message example, and should be left at OFF.

3.5 Printer

On the back of the Bombe, the cables of the printer are connected to the diagonal board sockets representing the letters in the crib and in the message. In the current example, the following letters are present: **A, B, C, E, F, K, L, N, O, R, T, U, X**. The printer cables for these letters should be connected to their respective socket on the diagonal board with, again, A=0, B=1 and so on.

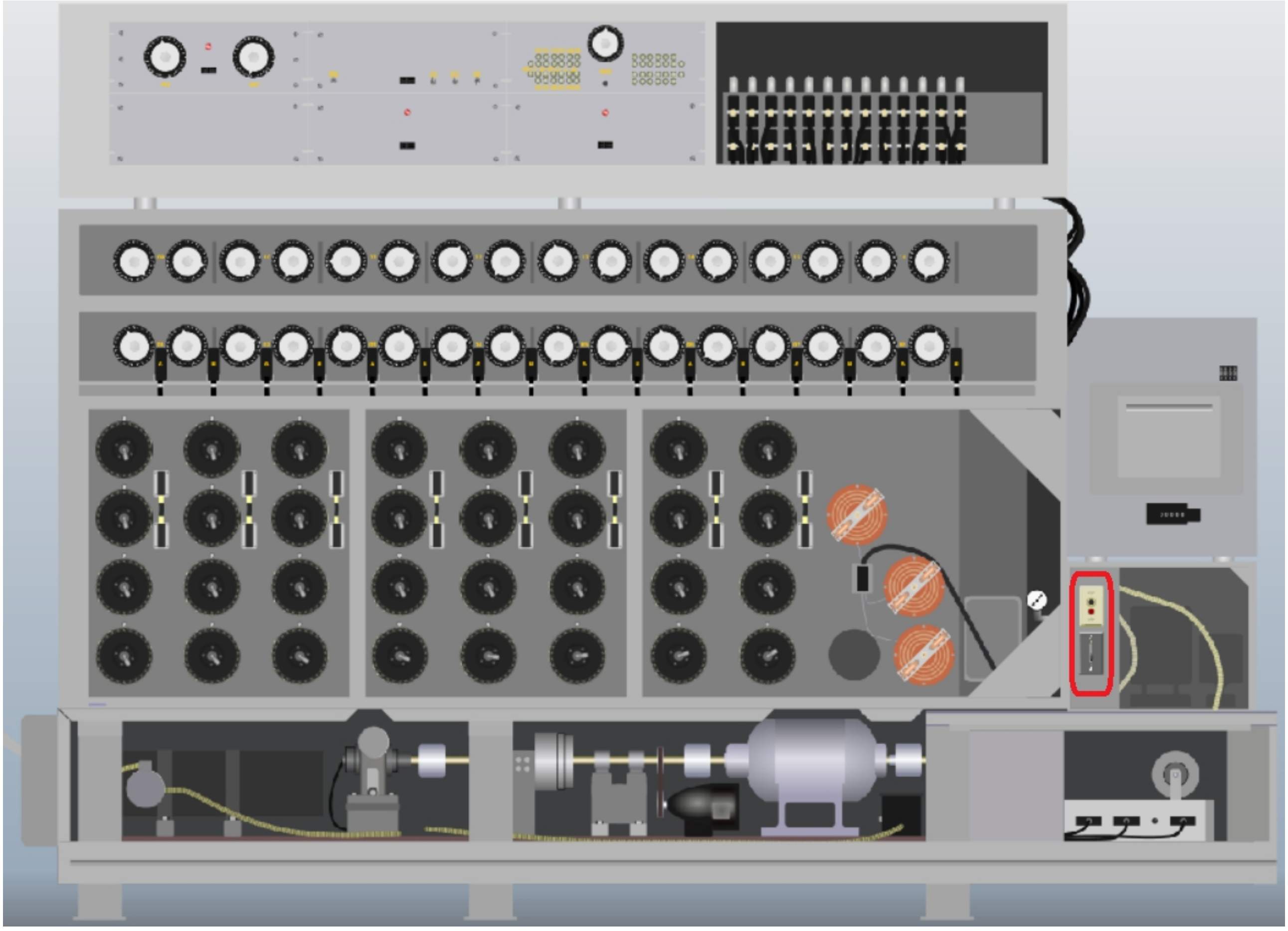
To set these printer wires, first go to the back of US Navy Bombe (using the [Back] button indicated as "1", and then click in the area indicated as "2". Then click on the connectors for the letters required.The Upper Row is for the letters **A thru M**, the lower is for the letters **N thru Z**.

The connector for the letter **C** is specifically highlighted as an example. Clicking on a letter results in a cable appearing; the cable can be deleted by clicking again.

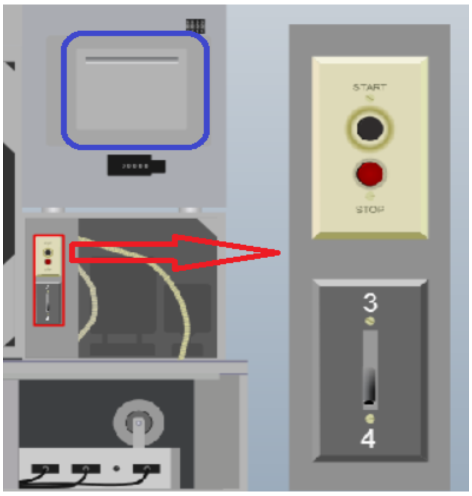

US Navy Bombe
Front
Back
Turing-Welchman Bombe
Front
Left Side
Right Side
Back
Enigma 3
Enigma 4
Checking Machine
New
Lo
1
2
0
1
2
3
4
5
6
7
8
9
10
11
12
A
M
N
Z
13
14
15
16
17
18
19
20
21
22
23
24
25

3.6 Starting the Bombe run.

Once all of the above have been set up, the run can be started. This is done from the front of the Bombe, using the controls in the lower right hand quadrant...

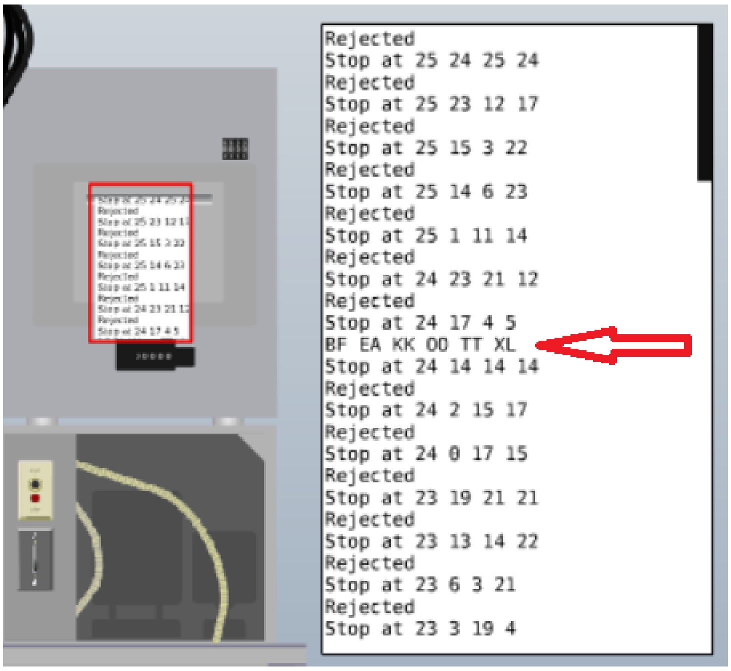


.... which can be magnified by clicking on the area, highlighted with a red rectangle, to result in a display as shown here:



On the white panel, the upper (black) button is the [START] button, and the lower (red) [STOP button can be used to stop a run. On the grey panel below that there is a switch for selecting either a 3-wheel run (switch up) or a 4-wheel run (switch down). By default, the switch is preset to its downward position for a 4-wheel run.

As the run progresses, a paper print-out can be seen emerging from the printer which is shown in the blue highlighted area in the picture above. As the run progresses, the most recent result is at the top of the print-out. The printer with its print-out can be magnified by clicking within the blue area:



```
Rejected
Stop at 25 24 25 24
Rejected
Stop at 25 23 12 17
Rejected
Stop at 25 15 3 22
Rejected
Stop at 25 14 6 23
Rejected
Stop at 25 1 11 14
Rejected
Stop at 24 23 21 12
Rejected
Stop at 24 17 4 5
BF EA KK OO TT XL
Stop at 24 14 14 14
Rejected
Stop at 24 2 15 17
Rejected
Stop at 24 0 17 15
Rejected
Stop at 23 19 21 21
Rejected
Stop at 23 13 14 22
Rejected
Stop at 23 6 3 21
Rejected
Stop at 23 3 19 4
```

This print-out shows a number of "Rejected" stops, and one good stop with the associated plugboard connections.

The simulation of this example message yields 188 stops out of the 26^4 = 456,976 possible rotor core positions tested. Of these, only one stop will pass the hot point test resulting in the following information being printed:

- **Ring setting: 24 14 14 14**
- **Plugboard: B/F E/A K/K O/O T/T X/L**

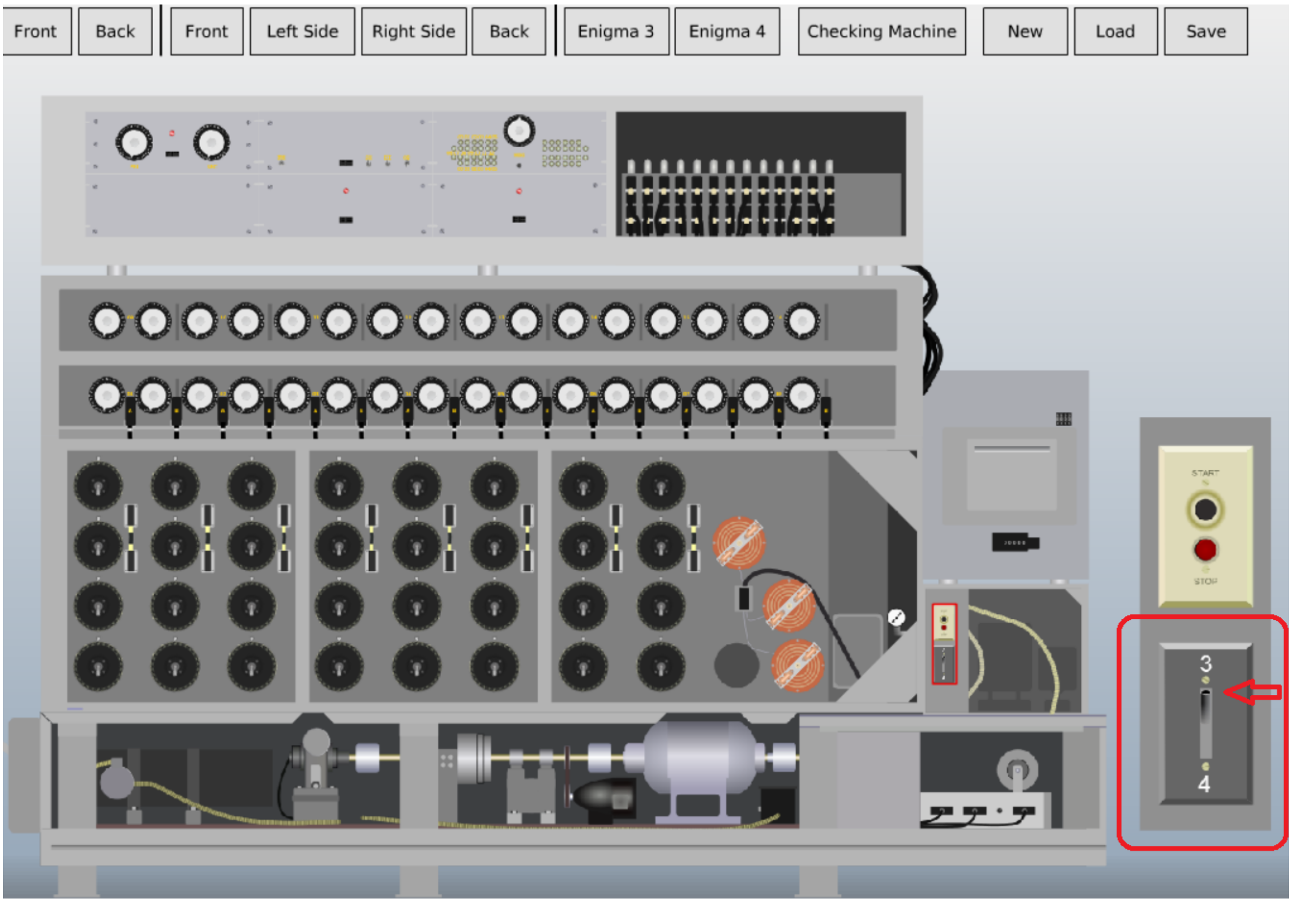
The exact format of the original printouts is not really known. The information in the example above would most likely have been represented by numbers only (Wilcox, 2006) as this is the norm on the rest of the Bombe. This matches the rotor core starting position of the Enigma used to encrypt the message (see section 2). The setting found will be subject to further, manual, tests using a simplified Enigma machine: the M-9 Checking Machine. The output from this process would be either more of the plugboard connection pairs, or the conclusion that the stop was in fact false.

After this there would be a brief set of trial and error tests to find a suitable ring setting that would decrypt the whole message.

4. Three-wheel mode

The US Navy Bombe can also be run in a three-wheel mode, thereby being able to find the message settings for a message encrypted on a three-wheel Enigma.

There are two ways of doing this; however, they both depend on the above-mentioned switch just below the START/STOP buttons; for three-wheel mode this switch needs to be UP, in the "3" position.

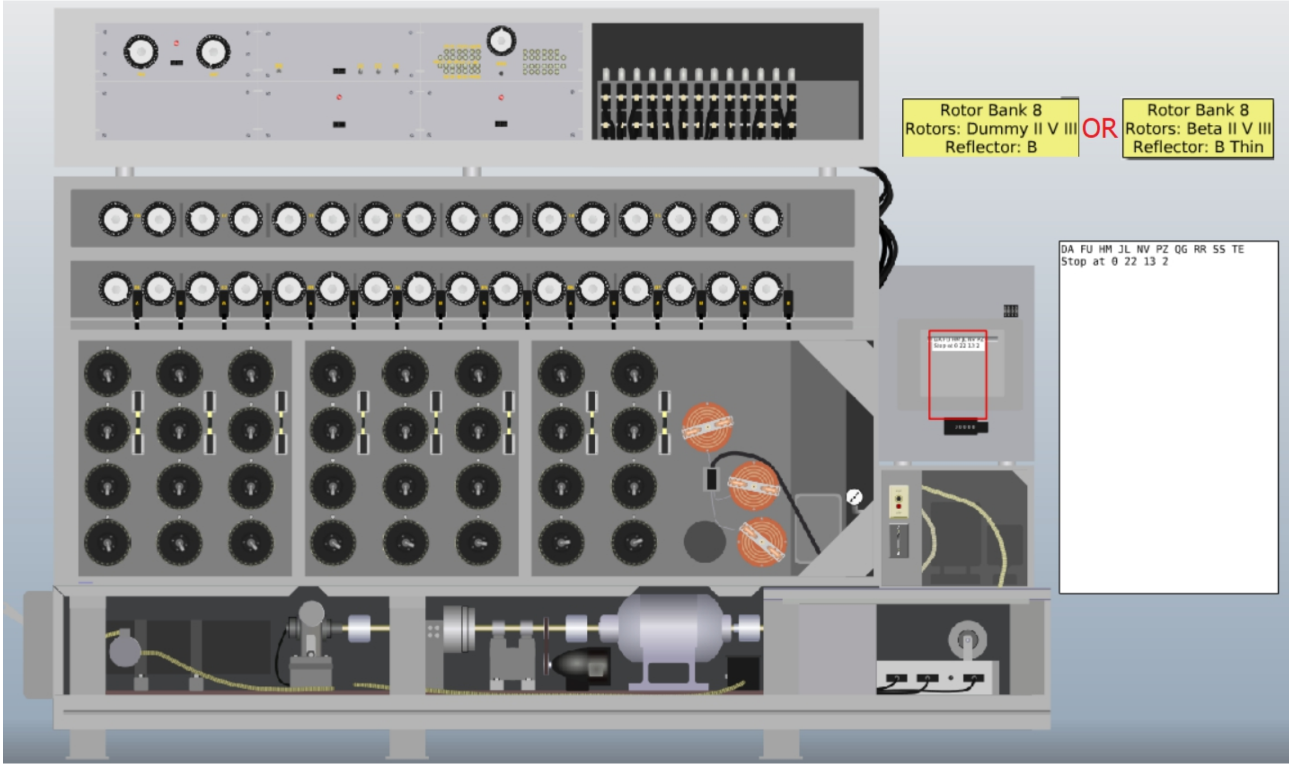


Apart from that setting, it is important to remember that, although a 3-wheel message is being solved, it is still necessary to have four wheels installed on the Bombe. The bottom wheel of each group of four wheels needs have the proposed fast wheel of the three wheel Enigma; the wheel one up from the bottom, needs to have the middle wheel of the Enigma, and the next wheel up would have the slow wheel. There then arises the question of what to do with the top-most wheel and the reflector.

The simple solution is to set the top-most wheel to the **Dummy** and the reflector can then be the standard **B** or **C** as required.

A somewhat educational alternative is to have the 3-wheel Enigma's **B** reflector replaced by the alternative of the **Thin-B reflector** ***plus*** **the Greek Beta wheel**, or the **C** reflector replaced by the **Thin-C reflector** ***plus*** **the Greek Gamma wheel.**

Running the 3-wheel crib for the Wettervorhersage menu as a four wheel mode results in:



Rotor Bank 8
Rotors: Dummy II V III
Reflector: B

Rotor Bank 8
Rotors: Beta II V III
Reflector: B Thin

```
DA FU HM JL NV PZ QG RR SS TE
Stop at 0 22 13 2
```

Note that only the one 'good' stop has been produced on the printer: the false stops produced by the 3-wheel Bombe are automatically discounted.

References

Frank Carter. 2008. *The Turing Bombe.* Report No. 4. Bletchley Park Trust, new edition. ISBN: 978-1-906723-03-3.

B. Jack Copeland, Jonathan P. Bowen, Mark Sprevak, and Robin Wilson. 2017. *The Turing Guide.* Oxford University Press. ISBN: 978-0-19-874782-6.

CryptoMuseum. 2017. *Enigma M4 message.* http://www.cryptomuseum.com/crypto/enigma/msg/p1030681.htm . [accessed 24-October-2017].

Joseph R. Desch. 1942. *Memo of Present Plans for an Electro-Mechanical Analytical Machine.* http://cryptocellar.org/USBombe/desch.pdf . [Published online by Frode Weierud in 2000, accessed 16-September-2016].

Magnus Ekhall, Fredrik Hallenburg. 2018. *US Navy Cryptanalytic Bombe - A Theory of Operation and Computer Simulation.* Paper presented at the 1st International Conference on Historic Cryptology (HistoCrypt 2018), Uppsala, Sweden. https://ep.liu.se/ecp/149/019/ecp18149019.pdf [accessed 6-February-2022].

Alan M. Turing. 1942. *Visit to NCR.* http://cryptocellar.org/USBombe/turncr.pdf [Published online by Frode Weierud in 2000, accessed 16-September-2016].

Gordon Welchman. 2014. *The Hut Six Story.* M & M Baldwin, 6th edition.
ISBN: 978-0-947712-34-1.

Jennifer Wilcox. 2006. *Solving the Enigma: History of the Cryptoanalytic Bombe.* Center for Cryptologic History, NSA.