Introduction

This tutorial will explain how to use the Bombe Simulator as well as the Checking Machine Simulator for any Enigma encrypted message (and crib; more on that later). It will not go into detail when it comes to explaining why the Bombe works or how it is constructed. The Bombe Simulator aims to be as accurate as possible but there may be differences compared to how a real Bombe would work. The authors are not affiliated with Bletchley Park in any way when it comes to the Turing Bombe, but we recommend anyone with an interest in these things to visit Bletchley Park to see a fully functional Bombe in action.

A Few Words on the Enigma Machine and the Bombe

It is expected that the reader has basic knowledge of the workings of the Enigma machine. However a short overview is provided here to explain some of the terms used when working with the Bombe.

The Enigma machine works by creating an electrical circuit using an input letter from a keyboard, a number of scrambling stages and a lamp showing the resulting scrambled letter. Each scrambling stage swap the input letter for some other letter which is passed to the next stage. The stages are:

- The plugboard. The plugboard provides the possibility to swap up to ten pairs of letters by connecting cables between the letters. If for example a cable is connected between A and E, pressing A on the keyboard will actually send an E to the next stage.
- The rotors. The most common Enigma machines have three rotor slots with eight rotor models, with different internal wiring, to chose from. The rotors are labeled with Roman numerals: I to VIII. Each rotor has a ring with the alphabet printed on it. The rotor can be rotated so that a certain letter is seen in a window on the Enigma. This is called the position of the rotor. The ring can be rotated in relation to the rotor, this is called the ring setting. For more details see the chapter on this below.
- The reflector. After passing the reflector the signal will pass through the rotors and plugboard again, in reverse order. There are three different reflector models commonly used, these are labelled A, B and C.

In order to encrypt or decrypt a message, an Enigma machine operator had to set up a number of things on the machine. These, when taken together, constitutes the key for the message.
The different parts of the key are the following:

- Which rotors are used, and in what order are they put into the Enigma.
- The starting position of the rotors. For example if the starting position is 'HEJ' the leftmost rotor will be rotated to H, the middle to E and the rightmost to J.
- The ring setting of the rotors. This is written in the same way as the starting position: a letter for each rotor.
- The plugboard connections. This is written as a string of 10 pairs of letters.

Assuming that we use a three rotor Enigma with eight available rotors to select from and must use ten cables to interconnect twenty letters on the plugboard, the keyspace will look like this:

Number of possible ways to select rotors and rotor order: 336
Number of possible ring settings: 17,576
Number of possible rotor starting positions: 17,576
Number of ways to connect 10 cables in the plugboard: 150,738,274,937,250

Clearly, the largest contribution to the key space is the plugboard, by far.

The purpose of the Bombe machine is to aid in finding the key used for a specific message, in particular it will help with the plugboard settings. The machine can be seen as a number of simplified Enigma machines connected in a way the will allow it to rule out many impossible plugboard settings and provide the remaining, potentially correct, settings to the user for further analysis. The Bombe can search through all 17,576 rotor starting positions but rotor order and types needs to be tested manually.

More details about rotors and drums

For every key press on the Enigma the rightmost rotor will move one step, when it reaches a certain position it will trigger the middle rotor to move one step. This is called a turnover. In the same way the middle rotor will make the leftmost rotor move. A piece of metal called a “notch” on the rotors will trigger the mechanism that rotates the next rotor. Usually there is only one notch on a rotor, so that it will trigger one turnover per revolution, but some rotors have two notches.

The ring setting on the Enigma rotors does not change the actual scrambling carried out by that rotor. The wiring inside a rotor is always the same for that specific rotor. The ring setting only changes at which position the rotor scrambles one letter to another.
This means that a rotor with its ring set to A, in the position A is equivalent to the same rotor with the ring set to B and the position set to B, except that the turnover position will move one step as the notch is fixed. We will see later how the turnover positions can affect the Bombe process.

The Bombe uses drums that scrambles letters in the same way as the Enigma rotors. However they don’t have a notch or a ring setting. There is still a turnover but it always happens on the “A” position of the drums. The drums are recognised by a distinctive colour, each colour corresponds to one of the Enigma rotors, I to VIII. The drums have similar wiring as their Enigma counterparts but there are differences. Probably by mistake, drums I, II, III, VI, VII and VIII on the Bombe are one letter ahead of the corresponding Enigma rotors. Drum IV is two steps ahead, and rotor V is three steps ahead.

Anatomy of the Bombe

The front of the Bombe has 36 drum banks organised in three rows of 12 drum banks per row. A drum bank consists of three drums representing the three rotors of an Enigma machine. The top drum corresponds to the slow leftmost rotor of the Enigma machine, and the bottom drum to the rightmost rotor. Note that a drum bank is not equivalent to a complete Enigma machine, just the rotor scrambler part, including the reflector.

There are three sets of control logic on the Bombe. These are referred to as chains. The three chains provides the operator with the option of running three different messages or set-ups at once given that the number of drum banks needed for each set-up is not higher than 12.

On the front are also three indicator drums which are used to read part of the possible solution once the Bombe stops. There is also a start and a stop button to control the motorised mechanics.

The reflector of the Enigma machine is implemented as a panel connector on one side of the Bombe. There are three panel connectors, one for each of the 12 sets of drum banks.

On the back of the Bombe there is a number of 26-pole jacks. Cables with 26 conductors (one conductor for each letter in the alphabets) are used to connect the jacks in different ways depending on the analysis of the encrypted message, described below. There are special jacks used to inject a test current into the system as well as display the result.

The other short side of the Bombe has a number of switches used to select on which lead of the 26-pole jack (which letter) to inject a current into the system. There are also some switches for controlling the stepping mechanism (called carry) of the drums on the front. Finally there is a 'letter box' type display which will, once the Bombe stops, indicate which letter is the possible solution for the message currently set up on the Bombe. A lever to the left of the letter box display is used to re-start the Bombe once it has automatically stopped.

Making a Menu From a Crib

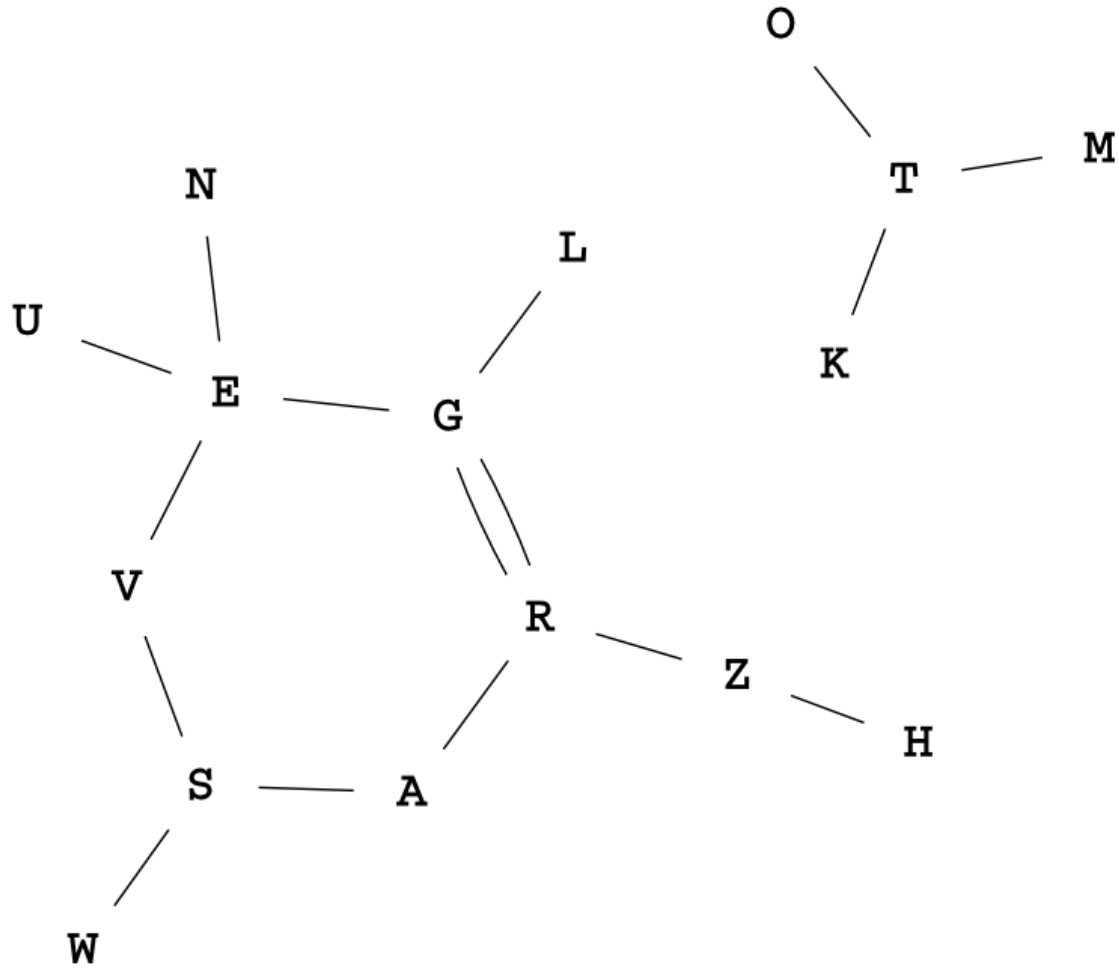
The first step of trying to retrieve the key used to encrypt a message is to create a diagram called a menu. From the menu it is possible to see if the message is likely to be successfully processed on the Bombe. The menu also tells us how to connect the cables on the back of the Bombe for the message in question.
To create a menu we need a piece of the clear text corresponding to a part of the encrypted message. This is called a crib. The analysts at Bletchley Park knew that many messages contained stereotyped phrases, this made it possible to guess the crib. Another fact that helped is that an Enigma machine cannot encrypt a character to itself, so in many cases it could immediately be seen if a stereotyped phrase or word was not present at a specific position in an encrypted Enigma message. If they were able to find the key for a single message received during a day they would be able to read all the messages received during that day, since the same key was used for all messages of a day for a given Enigma network.

As an example of how to create a menu we use the following crib:

Letter Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Clear	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E
Cipher	S	N	M	K	G	G	S	T	Z	Z	U	G	A	R	L	V

WETTERVORHERSAGE is the clear text and means "weather forecast" in German.

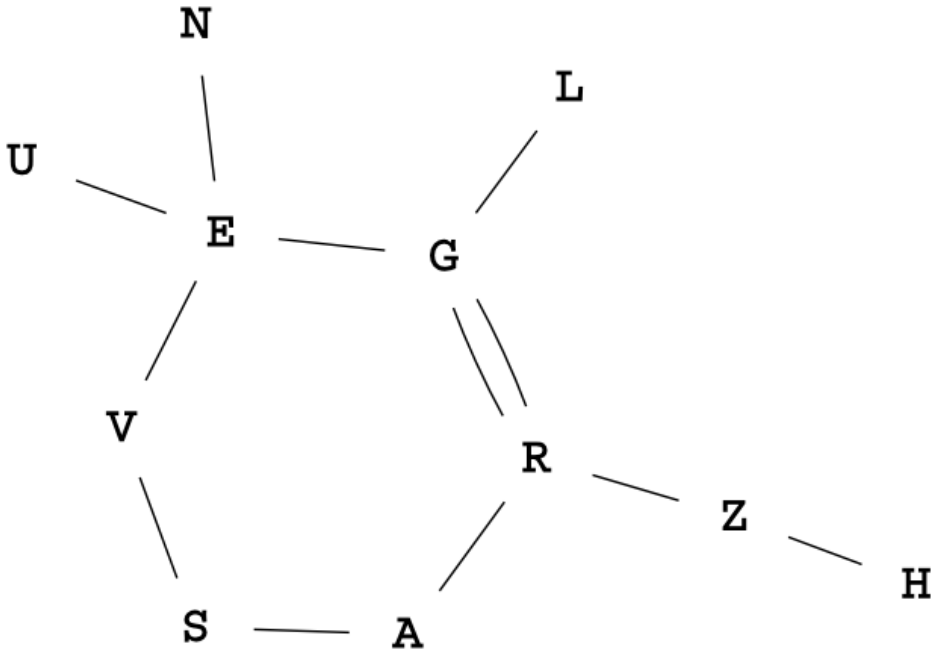
We then draw a graph where links are added between a scrambled character and its clear counterpart.



The aim is to have one connected graph with as many loops as possible. If a menu does not contain enough letters and/or loops there will be many false stops of the Bombe meaning that there will be a lot of work until we can determine the correct key.

The menu now consist of two separated graphs which is generally not wanted. We therefore discard the letters O, T, M, W and K from our menu. It is also convenient to have no more than 12 links in a menu. As mentioned previously, we can test three rotor configurations at the same time if the menu under test uses at most 12 drum banks. We remove the letter W to get only 12 links. Removing W does not break any of the two loops that are present in the menu.

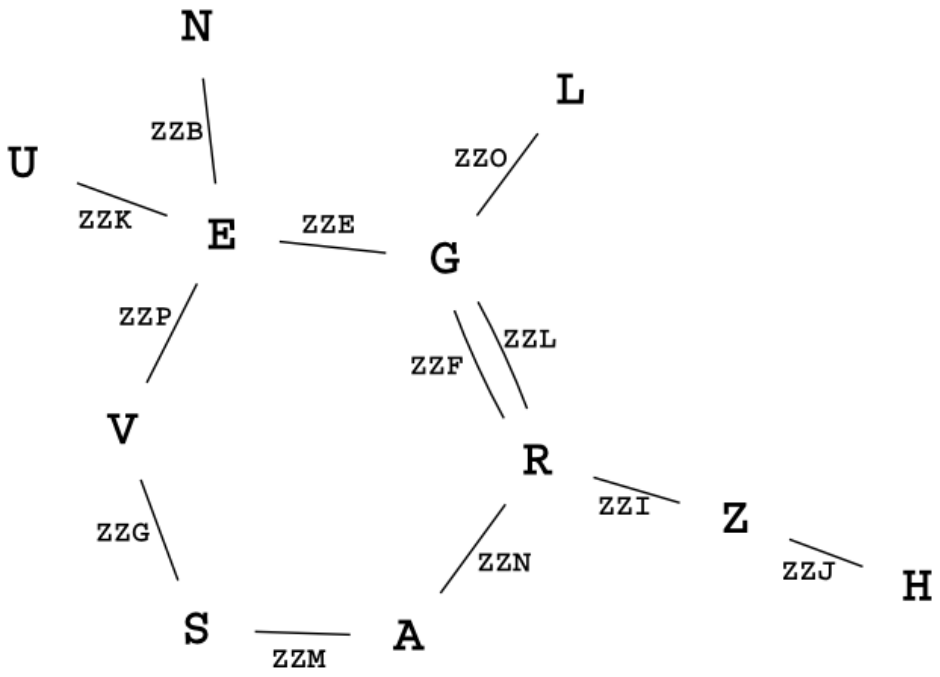
The graph now looks like this:



To this graph we then add additional information. We will assume that the Enigma rotors would be set to ZZZ before the message was encoded, and that no middle rotor turnover had happened. The Bombe considers ZZZ the 'home' position.

Under the circumstances above, the first letter of clear text would have been enciphered with the Enigma rotors set to ZZA, the second letter with ZZB and so on. Write the assumed enigma rotor position for each link in the graph.

The resulting graph:



Assign a drum bank to each link in the graph and write the number of the drum bank in a table together with the assumed rotor position. Try to get a continuous sequence of drum banks following the flow of the graph. This simplifies the way the wires are connected on the back of the Bombe by allowing us to use special bridge connectors that connect the output of one drum bank to the input of the very next one.

We will take the following route through the graph to maximise this effect: U -> E -> G -> R -> A -> S -> V -> E -> N and H -> Z -> R -> G -> L.

Pick a central letter in the graph and denote it 'input'. This is where the test current will be injected. In this case we will pick the letter G.

Finally we make another table where we map each letter in the graph to the connections that are in use on that letter. For example U is only connected to the input of drum bank 1. E however is connected to both the output of 1 as well as the input of 2, and to the output of 7 and input of 8. When a letter is connected to the output of one bank and the input to the next we write that connection within parenthesis. This is a reminder that we can use a bridge connector for this connection.

The last step is to decide which letter to test. It should be a letter that is present in the menu, but not the same or next to the input letter. We choose A and write this on the menu as "Current entry at A".

This completes the creation of the menu which should now look like this:

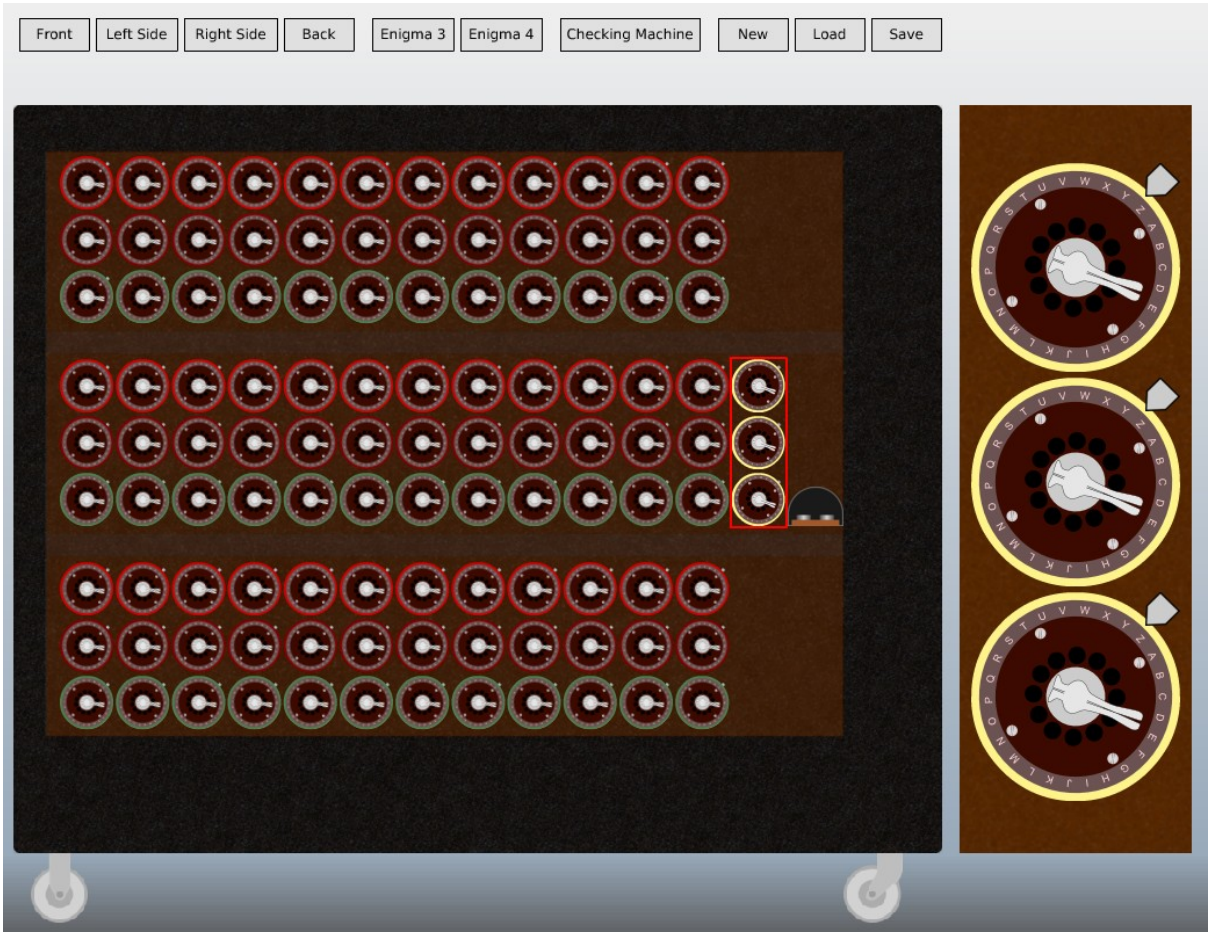
```
1:  ZZK
2:  ZZE
3:  ZZF
4:  ZZN
5:  ZZM
6:  ZZG
7:  ZZP
8:  ZZB
9:  ZZJ
10: ZZI
11: ZZL
12: ZZO

U: 1 in
E: (1 out, 2 in), (7 out, 8 in)
G: (2 out, 3 in), (11 out, 12 in), input
R: (3 out, 4 in), (10 out, 11 in)
A: (4 out, 5 in)
S: (5 out, 6 in)
V: (6 out, 7 in)
N: 8 out
H: 9 in
Z: (9 out, 10 in)
L: 12 out

Current entry at A.
```

This menu will test the hypothesis that A was connected to G on the plug board of the Enigma machine. However, due to the clever construction of the Bombe, even if this hypothesis turns out to be false (which is likely) we will still get the correct plugboard connections.

Setting Up the Menu on the Bombe



First we select which set of rotors we will try and in which order. Since we use no more than 12 drum banks we can try three rotor orders at once if we wish. However, for now we will just try one order; II, V, III, which happens to be the correct one.

Seen from the front drum bank 1 consist of the three rotors at the very top left, number 2 is to the right of bank 1 and so on. Select drum bank 1 by clicking on it. A close-up view of the drum bank is shown on the right hand side of the simulator. Press the circular arrow button next to the close-up of the drums until the right rotor order is in place. II on top, V in the middle and III on the bottom. Click the "copy to chain" button to duplicate this rotor order on all the drum banks in the top chain (drum banks 1-12).

Next adjust the drums to the correct letters according to the menu. Drum bank 1 should be set to ZZK; rotate the top drum to position Z, the middle to Z and the bottom drum to K.

Repeat this for the other 11 drum banks and make sure to set the drums to the letters as per the menu.

By default the Bombe simulator is set to use the B reflector. There are cases when other Enigma reflectors have been used. To change this, click on the "Left Side" button then click

on the reflector panel connector to change it. In our case we should leave it as it is, using reflector board B.

The wiring of the menu is done on the back of the Bombe. Click the "Back" button to see an illustration of the jacks on the back of the Bombe. Each jack can connect either a 26-way cable (one lead for each letter in the Enigma alphabet), or a special bridge connector. A bridge connector connects one jack with the one directly beneath it and it also provides a jack of its own. The jacks labelled "CO1" are all connected to each other. The same goes for "CO2" and so on.

First we place the bridge connectors. These should be placed on the connections we wrote within parenthesis. To bridge the output of drum bank 1 to the input of drum bank 2, click on the jack labelled "OUT1". On the context menu that will appear, click "New bridge". Repeat this for all possible bridge positions in the menu.

We then proceed to connect the entire menu from top to bottom, starting at U. According to the menu U should be connected to the input of drum bank 1. Click on the jack labelled U in the leftmost column of jacks. The three columns of jacks with A-Z-labels are connections to something called a diagonal board. There are three diagonal boards on the Bombe.

The next letter on the menu, E, is connected to two bridges. We therefore need to use one of the sets of common jacks. First connect the E jack to one of the jacks labelled CO1, it does not matter which one. Do this by first clicking on one of the jacks and select "New Cable". A Cable will appear connected between the selected jack and the closest free jack. Click and drag the connectors of the cable so that it stretches from E to CO1. Then create a new cable, this time from one of the other CO1 jacks to the jack on the bridge connector spanning OUT1 and IN2. Add a third cable connecting yet another CO1 with the jack on the bridge connector between banks 7 and 8. This completes the E-line on the menu.

Continue like this for all letters on the menu. The current input, which we selected at letter G, is one of the jacks labelled CH. Select CH1 as input for this menu.

Click on the "Right Side" button. You will now see a section of the right side with a lot of switches, a letter-box display and a lever (next to the letter-box). There are four columns of switches, one for each set of 12 drum banks (chains) of the Bombe, and one auxiliary chain that can be used for more advanced menus. There are one on/off switch for each chain, and then one switch per letter in the Enigma alphabet. This allows the user to select on which of the 26 terminals (A-Z) a test current will be injected. To see the switches in the bottom, drag the red rectangle in the small view to the left. Below the A switches there are three switches. "Carry Home" is used to enable the carry mechanism on all drums until they are in the initial, or home, position. It is a way to quickly reset the Bombe to its starting state. "Double Input" is used, sometimes together with the Aux Chain, for advanced menus and will not be discussed further. "Carry" is enabled to start the regular carry mechanism so that the middle drums advance one step for each full revolution of the fast drums and so on. Switch on the following three switches: "Chain 1" at the top, the switch "A" of Chain 1 and "Carry" at the bottom.

Running the Bombe

The menu is now set up and the Bombe is ready to start working. On the Bombe front, to the right of the three golden indicator drums, are two buttons. The left button starts the Bombe. The right button stops the Bombe. Press the start button and watch as the drums spins; the Bombe has now started to search through a part of the Enigma key space for a setting that satisfies the current menu.

Dealing with Bombe Stops

It is likely (and was actually desired in order to verify that the Bombe was working as it should) that there will be more than one stop before the Bombe has finished searching though the current part of the key space. Only one of these stops will be the correct stop corresponding to what was used on the Enigma machine. The other stops are random; a result of mathematical probability. Each stop has to be checked for validity. We do that with the Checking Machine.

When the Bombe stops the first time the golden indicators show: SNY and the letterbox display on the side of the Bombe indicates the letter D. We write this as SNY:D. Once the stop has been written down the Bombe can be restarted to continue its search. This is done by first pressing the start button on the front (the left of the two buttons), and then briefly lifting the lever to the left of the letter box display on the side of the Bombe. While the Bombe continues to search, the first stop can be tested on the Checking Machine.

The Checking Machine

Clicking the button labelled "Checking Machine" shows a view of the Checking Machine seen from above. The Checking Machine is similar to the Enigma, it has a keyboard, four drums, a reflector and lamps to show a scrambled letter. However, it does not have a plugboard and also no mechanisms to move the drums.

To the left is a cartridge that acts as the reflector. It can be replaced to match different reflectors. Since the B reflector was used for this message and B is the default on the simulator we do not have to change this. Since our message stems from a three rotor Enigma a dummy drum with a one-to-one mapping of the letters of the alphabet is used to the far left. The dummy drum is yellow with no letter markings. Click the arrow above the other three drums until they are set up as the Bombe: II, V, III (from left to right).

On a piece of paper, write down the letters from the menu in a column:

```
U:
E:
G:
R:
A:
S:
V:
N:
H:
Z:
L:
```

Next, set the rings on the drums to the letters indicated on the stop, in this case: SNY. To set the drum rings, hold down the shift key while rotating the drum with the mouse. If you are using a touch device you can hold one finger anywhere on the screen at the same time as you rotate the drum with another finger. The ring setting is indicated with a small black dot on the outer rim of the drum. When you are done the dots should be by the S, N and Y letters respectively.

The Bombe suggested that on the Enigma plugboard the letter G is connected to the letter D. Write the letter D next to G.

On the menu graph, if we want to move from the letter G (our selected input letter), to the letter E we need to set the drums to ZZE. Rotate the drums on the Checking Machine to ZZE. If we now press the D key (the suggested plug board connection of G, also called stecker partner) we will see what the possible stecker partner of E is. In this case P lights up; write P next to E. Using this newly found stecker partner of E we can now use that to check the possible stecker partners to the letters in the menu graph that connects to E and so on. Continue to follow each link in the graph in this manner and make a note of all the suggested stecker partners. If you arrive at a letter for which you already have a stecker partner, the same letter should be the result. If it is not, then this stop is false and we need to go back to the Bombe and find a new one. Remember that a letter can very well have itself as a stecker partner. This is the same thing as an unconnected letter on the plug board on the Enigma and is sometimes called a self-steckered letter.

The complete result for this stop should look like this:

```
U: W
E: P
G: D
R: P
A: X
S: Q
V: I
N: T
H: H
Z: X
L: O
```

Here we have two contradictions: X cannot be connected to both Z and A, and P cannot be connected to E and R.

This stop is therefore false.

The next stop of the Bombe should be DKX:Q. Repeat the procedure on the Checking Machine, this time with the rings on the Checking Machine set to D, K, X and the suggested stecker partner of our input letter G on the menu is now Q. Once all links in the graph are tested the result should be:

```
U: F
E: T
G: Q
R: R
A: D
S: S
V: N
N: V
H: M
Z: P
L: J
```

In this case there are no contradictions. Instead it is reassuring that V has N as a stecker partner and that N has V. This stop, DKX:Q, passes the test and is worth investigating further. Even though we found no contradictions there is a possibility that it still is not the correct solution.

Getting the Enigma Message Key

To investigate a possible key further we will use a simulation of a real Enigma machine. Click on the button labelled "Enigma 3"; this will show a simulation of a three rotor Enigma, seen from above. To the top right of the Enigma machine is a box of spare rotors and another reflector. Under the rotor box is an area where clear and encrypted letters will appear when you type.

First we will set up the Enigma machine as we currently think it should be set up. Click on the grey/red knob that is either left of the P lamp or right of the L lamp. This will "unscrew" the lid and open up the Enigma. Click and drag the rotor until the right rotors, II V III, are in place left to right.

Next we set the ring settings to DKX. First press the "Set Rings" button to enable ring setting mode. Now click and drag up or down on an installed rotor to set the rings to D, K and X respectively.

Close the lid of the Enigma by pressing one of the two grey/red knobs again.

Set the rotor starting position to ZZZ by dragging up or down on each rotor.

Next we will connect the plug board settings we know of. Click on the plug board connectors that can be seen on the bottom edge of the Enigma machine. This should give you a front view of the plugboard itself. Ten cables are available just under the plug board. Connect these as per the results from the Checking Machine: U to F, E to T and so on. Letters that should be connected to themselves (R and S) should be left unconnected. The default state of a letter is to be self-connected.

With all the cables connected, click on a key on the Enigma keyboard (seen on the top edge) to get back to the top view of the Enigma machine.

To compensate for the previously mentioned errors on the Bombe drums (*see page 2*), and given that we are using rotors II, V and III, we translate our assumed starting position ZZZ into YWY.

Now, let's try to decrypt the message! With the starting position set to YWY, take the position of an Enigma operator receiving an encrypted message. Type in the ciphertext SNMKGGSTZZUGARLV. The result is similar to what we want, but not quite right: WETCERVXRHERSAGE. The C and the X are not the expected letters. This is most likely because we do not know of all the plugboard connections yet.
Let's look at C first. We tried to decrypt the letter K and got C instead of the expected letter T. We could then potentially get the desired letter T by connecting a cable between C and T on the plugboard. However, T already has a cable - connected to E. So our next strategy is to find a letter which, enciphered through the rotors alone at the rotor position of this letter (ZZD in Bombe rotors), would be enciphered to E. Since E is connected to T this would result in the desired output. Go back to the Checking Machine and set the drums to ZZD. Press the keys on the keyboard until you find the one letter that enciphers into E. That letter is I. On the plugboard, connect a wire between I and K.
Looking at the next problem, we got an X but wanted an O. Neither X nor O has a cable connected. Connect the last cable between X and O.
Reset the Enigma to YWY and try to decrypt the ciphertext again. We now get the expected result: WETTERVORHERSAGE.

All the letters in our crib are now correctly deciphered. Does this mean that we have the correct key? Yes and no. Since we have all ten plugboard pairs, that part of the puzzle is most likely solved (given that our two guesses proves correct). But the ring setting and the rotor starting positions are probably not entirely correct.
If we had a longer section of ciphertext than just the part of the crib (which must have been the normal case) then at some point it would be expected that the text being deciphered would switch from understandable text to gibberish. If such a sudden switch from clear to scrambled text appears it is fair to assume that what happened was that the leftmost and/or middle-rotor has advanced one step where it should not have. This can happen either on "our" side or it could have happened for the original cipher clerk, but not us. When we suspect that a turnover has occurred at the wrong position, we can adjust the ring and starting position one step at a time until we find the correct notch position. In the worst case we need to do this 25 times per rotor, so this is not an overly difficult process. It should be noted that if a turnover happens in the middle of the crib the process as described in this document will not work.

Summary

We have now seen an example of how an encrypted Enigma message can be broken given a crib. From the crib a menu was created and this menu was then used to set up the Bombe for the message in question. The Bombe stops were checked in the Checking Machine, and the promising stop was further processed in an Enigma machine to get a more complete key.
We cheated a little by knowing in advance which rotors and reflector were used and in which order the rotors were mounted in the Enigma. In practice the same menu would have been

set up on several Bombes. Using three chains on the Bombe it was possible to check three different rotor orders on one Bombe.
This procedure had to be repeated every day and for every Enigma network that was of interest.
A lot of work was needed to maintain this day after day, week after week. But the information retrieved at Bletchley Park was of such great value that it has been estimated that it shortened the war by not less than two years and probably by four years!

Exercise

Here is an Enigma encrypted message that you can try to break using the method described in this document:

QATCTQCNWMTVCOPYVFHOLCQTVGMTWOBRFOUBRMQBRIHLLXDBTZLXLGZUQFC
WPXPOKOLFFADXDAVTJM

Crib: SECRETMESSAGE
Rotors: II I III