Virtual Colossus

An interactive computer simulation of the World War II Colossus computer by Martin Gillow, based on an original version written by Tony Sale.

Introduction

This simulation of Colossus has been created to show how the real Colossus helped in breaking the German Lorenz cipher in Bletchley Park in World War II.

Tony Sale had started the rebuilding of a Colossus in 1993. Only minimal information had been declassified and was available at that time, but a start was made which resulted in the basic functions of Colossus being demonstrated in 1996. But there were still large areas of the code breaking work which were classified. In 2000 the Newmanry report was finally declassified. Although many more circuit boards had been identified and constructed, how they were connected together remained a mystery. Solving these mysteries was achieved by using the original Virtual Colossus to reproduce the code breaking procedures now revealed in the Newmanry report, the report by Albert Small, and the Fish Notes by Walter Fried, Americans seconded to Bletchley Park during the war.

By 2016 the original code, which was written for an older version of Internet Explorer (v6), no longer worked correctly in current browsers. It was possible to get running with a little tinkering, but still had a few issues with some of the control selection.

This is the rebuild of the of that original Virtual Colossus.

A quick overview of Virtual Colossus

Welcome to Bletchley Park Block H.

Before we begin, I assume you've already read and signed the National Security Act? Anything you see and hear from now on is Top Secret and will not be discussed with anyone outside this building … I hope this is understood?

The machine you will be using is called Colossus and to start, we'll just run through what controls are available for you to use on each of the frames you'll have in front of you.

The first thing you'll want to do is to zoom out your browser to see the big picture. If you're using a PC with keyboard and mouse, the easiest way is to hold down the Ctrl key on your keyboard then either use the mouse wheel or press the – key to zoom out, the + key to zoom in or the zero key to go back to default 100%. Move around the screen using the scroll bars.

For those of you with touchscreen devices, just pinch to zoom in and out. Drag to move around Colossus. Note: You cannot drag using a switch so make sure you drag the background if you have trouble moving about. Mac users, use the Command key with -/+.

The first frame on the left is the C Rack. This is the counter control which houses the five 4-decade counter circuits. Near the center is the **set totals panel** with five banks of 4 decade switches.

The second frame in is the relay rack. This is where the count value is temporarily stored before being sent to the IBM **printer** (an early form of double buffering). The small panel in the middle left of this panel only has a couple of active switches which are being used specifically for Virtual Colossus. On the

large section to the right, there is the **display panel** which shows the current counter output at the top and the current setting position of each wheel in the lower section. To the right of the display panel is the main **Control Panel**. Here you will be able to assign which wheels step and to start and stop Colossus. Below this is the **Jack Strip Panel** which has a row for each of the 12 wheels of the Lorenz machine. These are used to set the start position of each wheel.
The next frame along houses the large **K Panel.** Here is where you will find what is known as the Q bus (the first five switches on the left side all the way down), the R bus and the Counter switches. This panel has numerous switches which you will use to set the logic operations for a particular run against a cipher tape. Below the K panel is the χ (Chi) wheel Settings Panel. This is where you can setup the Chi wheel patterns which match the pins around the Chi wheels on the Lorenz.

Next along is the J Rack which has the **Span Panel** and below the **Plug Panel** (not yet implemented) and the **Pattern Panel.**

The two large racks sticking out from the machine next are known as the "Bedsteads". The cipher text punched tape to be checked will be loaded on to one of these and is read at 5,000 characters a second using a set of photo cells. There are two bedsteads, the near and far to enable one tape to be loaded while the other is running to save time.

Finally, around the back (shown to the far right on Virtual Colossus) are the ψ (Psi) Settings Panel where the pin settings for the Psi wheels are setup using small U-shaped pins (one for each of the 5 wheels) and the two μ (Mu or Motor) panels.

Getting started with Virtual Colossus

The first thing we need to do to run Colossus is to load on a paper cipher tape. You can use the menus at the top of the screen for this, but so we get to know a little more about where everything is, find the Bedsteads (two racks of wheels sticking out on the right) and you should see a blue notification box at the lower end. These give options where available for that particular panel and you can also get information on what the panel does. Click on the button "Set Near Tape" and select KHcipher. This will load the KHcipher punched tape onto the bedstead for you. There are a number of pre-defined tapes to choose from, some are original cipher texts, others are original German texts which have been re-enciphered using different settings. The tapes are loaded joining the end of the tape back to the start to create a continuous loop which Colossus reads over and over again. The switch to turn on the tape motor and lamp for each bedstead is a 1940's light switch about 1/3 of the way down each frame – if you have sound active (most current browsers), you should start to hear the tape clicking around.

Next, we need to select which bedstead we want to read from. The Pattern panel just to the left of the bedstead has a number of ganged switches. Find the one marked Near and Far and switch it up to the Near setting.

One of the first basic things we can do to test out our Colossus is to do a count of all the characters on the tape. To do this, we need to route the tape input characters to the main big K switch panel. Head back over to the Pattern Panel (near the bedsteads) until you find the three large ganged switches on the right hand side. These have Q written above them and Z and ΔZ written to the left of the top switch. The Z switch is another name for the input from the tape, so flick that switch up so it's pointing to Z. Well done – you've now set the Z input from the tape to connect to the Q connection at the top of the K

Panel (if you look at the top of that panel, you should see it also marked Q and bit 1 to 5 from left to right). From here, the signal flows down the Q bus and we can pick of various logic tests to find information about the data.

Take a look at the Q bus on the K Panel now. The bank of black switches under the Q bus allow us to check an input bit pattern is set true or false. The switches actually have three positions, up to test for a dot in Bletchley Park terms or down to test for a cross. The centre position means no check will be made – either dot or cross will give true. Thus, only a bit pattern matching the pattern of the switches that are set on the row of switches will give true.

The result of this feed horizontally to the right to the Counter switches (five gray switches labeled CNTRS). These switches allow the true or false result to be switched to any of the five counters in Colossus.

So now, let count some characters coming off the tape. We will first count all the characters so leave all of the black switches set to their middle position (i.e., always give a true result no matter what the bit pattern).

We will count this into counter 1 so flick down the counter 1 gray switch on the top row of Counters.

Now move left over to the main Display Panel (the bank of numbered lights) and check the very first top section - you should get a reading of 2,041. 2 in the thousands set, 0 hundreds, 4 lots of ten and 1 unit. If you want to store this value, you can use the printer by pressing down the LC (letter count) key on the Control Panel. This count should then appear on the printer with the letter “a” in front of the count to show it’s the first counter.

Let’s test that all five counters are working, set all five gray counter switches down in the top row of the K panel move back to the display panel. All five counters should now show 2,041.

How about we do a count of all the letter B’s in the cipher text next? To do this, we need to know the Baudot code for letter B which is **X··XX** (see http://www.virtualcolossus.co.uk/lorenz.html). Setting this on the top row of black switches on the K Panel means putting switches 1, 4 and 5 down to the X setting and switches 2 and 3 up to the · setting. Make sure you have selected at least one counter switch and again, check the Display Panel, there should be a total of 74 letter B’s in the cipher text.

Back at the K Panel, the yellow switch to the left of the five counter switches is a “NOT” switch. It inverts the true or false from the test switches on the left before the result gets counted. Therefore, if we switch the top one down, we’ll get the total number of characters that are not B’s. Try that now – if all is working, we should get 1,967 characters (2,041 – 74). Well done if you’ve got this far.

Getting outputs from the Chi (χ) patterns

One part of Tommy Flower’s genius in designing the Colossus was to get the Chi patterns generated electronically in synchronism with the cipher text on the tape. Originally the Heath Robinson machine which was built before Colossus used two tapes and tried to keep them in sync together but this gave a lot of problems. Let’s take a look at how this was done in Colossus.

We want to setup the Chi and Psi patterns for the wheels. These would have usually already been found out using hand methods from a number of depths elsewhere at Bletchley Park. To assign the Psi patterns, you would normally have to go around the back of Colossus, but to make it simpler, you'll find them on the far right. Select "Set ψ Patterns" and again in this case, choose to assign the KH Pattern option and one of the WRNS will fill these in for you. (WRNS is short for the Women's Royal Naval Service and were the main operators of the Colossus). If you're really up to it, feel free to change these yourself (see Appendix 1) – each board can have U-shaped pins fitted by click on the holes. Pin 1 is at top left and runs down the column to Pin 20 the continues on the next column along 21 – 40 etc.
Setup the two Mu wheels the same way.

Finally, as the Chi wheels generally changed much more often than the Psi and Motor pin settings, the plug board was brought out to the front of the computer to allow easier access. This is found at the bottom of the K Panel (the large black set of switches). Find the "Set χ Pattern" option and again select our KH Pattern.

On this board, Chi wheel 1 is at the top and wheel 5 is at the bottom. Each of the 5 Chi wheels has two rows, the top for standard settings (row 1,3,5,7 and 9) and the second set for special settings (not yet implemented on Virtual Colossus).

If you want to test the Chi wheels are being read correctly, we can switch this into the Q bus by looking at the Pattern Panel and centering the Z banked switch then setting the χ banked switch up. If you want, you can run the letter count and check for letters within the Chi stream in exactly the same way.

An actual wheel setting run

We have seen how to get both the Z (cipher text) and χ (generated wheel pattern) individually into Q, but they can be added together modulo two bit by bit. This is achieved by setting both large Z and χ switches on the Pattern Panel.

However, to do a wheel setting run, based on the calculations done by Bill Tutte, we actually need DeltaZ (ΔZ) and Delta χ (Δχ) added together. The Delta is the difference between the first and second bits down the tape.

Scroll to the large Pattern Panel switches again and set both the Z and χ down to give the Deltas.

Clear all the switches we currently have set on the main K Panel as we're now going to use the lower section with the five rows of five red plus keys on the left. Rather than matching the bit pattern as the above switches, the red switches allow us to add together selected bits.

We are going to run the basic wheel setting algorithm 1p2=· (or 1+2 = dot)

This says we want to count the number of times, throughout the cipher text, where Q bit 1 plus (modulo 2) Q bit 2 = dot. Remember by setting the inputs to ΔZ and Δχ, Q bit 1 is already ΔZ1+ Δχ1 and Q bit 2 is already ΔZ2+ Δχ2. Thus we are executing the famous double delta test: **ΔZ1+ Δχ1 + ΔZ2+ Δχ2** and recording whenever this comes to zero.

To actually run this on Colossus, we need to use the red keys with the + between them. Click down on switch 1 and switch 2 from the left which means the result from Qbit1 + Qbit2 will go left along the row. Ignoring the green switch for the moment, look at the yellow key next along. Clicking this to up will enforce a test for dot while down would check for a cross. For our test, we want to check for dot, so switch it up. Place the result of this into counter 1 by clicking down the next red key along.

Now return to the master control panel, we need to tell Colossus which wheels we want to step on each complete rotation of the tape. What we require is to step the first Chi wheel each time the tape goes around once and the second Chi wheel once the first has completed a full rotation. This means Colossus will check the count of our algorithm using the tape against all possible initial settings of the first two wheels.
To do this, we can use the blue switches on the bottom row of the Control Panel. Click the first key on the left down and the second to up. This tells Colossus we want $\chi 1$ to step fast (every revolution of the tape) and $\chi 2$ to only step when $\chi 1$ has got back to its set up position. A full run is going to check 41 x 31 positions so a total of 1,271 checks.

The start positions to run the test from can be set with the jack strips below. The top five rows are for the Chi wheels, the two below for setting the Mu wheel starts and the final five are for the Psi wheels. You can set the white pin to set the start position but we're going to begin from position 1 so leave these at the start of the jack strip.

When we run this test, Colossus will calculate the result of the algorithm for the whole tape for each wheel position in turn. If the start position for the cipher text is not the correct one that was used to generate the cipher text, we would get roughly an average number count whereas when the position of the wheels is correct, the count will be slightly higher. Therefore, the correct start position for this cipher text will likely be the one with the highest count. Our average score would be half of the number of characters on the tape which we've already found to be 2,041, i.e. 1,020.

If we started now, Colossus would check through and print out the results for all 1,271 positions which is a lot of virtual paper! Let's make this a little easier to read. We can use the Set Totals panel (far left of Colossus) to set a value and only a score greater than this count will be printed. By choosing a fairly high value, only a few counts will be shown.

For our run, let's set this to 1,070. Counter 1 is the first column of switches on the left with Counters 2,3,4 and 5 to the right. We want to set the top 1000 dial to 1, the 100 dial to 0, the 10 dial to 7 and the bottom unit counter to 0.

Now we're ready to go. On the Main Control Panel, press down the SU button once to set the start positions from the jack strips into the computer then press down on the M switch, the Master key is the yellow switch second from the right on the top row.

Check the Display Panel – you should see firstly the count for each run of the cipher tape being displayed against counter 1 and on the lower section, the current Chi wheel settings will be counting up. Each time wheel 1 completes a full rotation, wheel 2 will step on one position.

Next, check the Printer – The initial heading listing the wheels being checked and count should be showing. As each Chi setting is checked against the cipher tape, Colossus will check if the value is greater

than the value we've assigned on the Set Totals Panel (1,070), if it finds such a score, the values for the current wheels will be printed along with the current count.

The first one should listed as 31 01 a1087. Note the letter "a" in front of the count, this shows we're using counter 1 (a for counter1, b for counter 2 up to e for counter 5)

What we're looking for is the highest count above average which could then be a good contender for the original Lorenz machine settings.

Virtual Colossus has been set to try to keep to the real Colossus speed of 5,000 characters per second (this is amazingly fast for reading a paper tape – keep in mind that at the time, 10 character per second was generally standard!). Even running this fast on the tape, remember we need to check 1,271 versions of the tape so if you want to run at actual speed, you'll need to be patient for this to complete.

If you're short on time (or impatient) - let's cheat a little, on our Virtual Colossus, there is a switch which wasn't on the original or rebuilt Colossus which is on the switch panel just above the printer. It is a yellow switch labelled speed. Switch this down and the speed limitation which is trying to match the Colossus tape will be turned off and it will start running as fast as it can. If you're on a recent PC or tablet/phone, then you should find a dramatic increase in speed!

Once you've completed the run, you should find some good contenders at 31 01 a1087 and another at 05 03 a1095. Again, don't forget our average score for this run is 1,020 so these are well above what would be expected if the result was just a random list of characters.

For a real run, we would be expected to check both of these possibilities when checking the next set of Chi wheels. As we continued, one of the possibilities would (hopefully) show to be false. This can be done in more detail in some of the scenarios listed on the website for you to run.

If you want to see the last few results which are still under the printer roller, click the LF (line feed) button on the info box under the printer a few times to space up. To get a new blank page, click the New Page button.

Multiple stepping

When Tommy Flowers built the second Colossus computer, he made quite a few improvements over the first one and this version of Virtual Colossus is based on that second version.

One of the main improvements was to add in "Remembering" circuits which could hold the previous four bits from any of the Chi, Mu or Psi streams. This allowed five comparisons to be made for each cipher character read from the tape which meant that we could step forward in jumps of five wheel positions at a time rather than one. This makes quite a speed difference as we'll now test.

The remembered bits appear as five green switches under "R" on the main K switch panel so scroll over to there now and we'll set this up now.

First, we should currently have the first two red switches still both down – set the first red switch its midpoint and then switch down the green switch to the right (the remembered bit). Make sure we have

the yellow switch up (to check for dot) and then clear the red counter switch 1 and set down counter switch 5.

Next, continue down the next four rows settings each in a similar pattern. Set the second red switch down, the green switch down, the yellow switch up and finally, counter switch 4 for the second row down, counter 3 for the third etc. until we have all five counters being used.

The reason we are putting the first line into counter 5 and going backwards is so the results would be printed in the correct order. Remember, the first green switch gives us the actual X1 bit, the second switch gives us the R bit one character back, the third, two characters back etc.

Next, we need to move over to the Main Control Panel where we need to tell Colossus which wheel to remember. This is done using the red switches – find the one marked χ1 and set it up (6th in on top row).

We also need to set each of the Set Total rotary switches to the same value (1070) for each of the five counters (ie, set 1 on all the 1st row and 7 on all the 3rd row). If you like, scroll down to the printer and press New Page to get a clean sheet of paper, then press SU and then the M start switch to start the run from the main control panel.

Now we're running at an effective processing speed of 25,000 characters per second rather than the actual 5,000 allowed by the tape speed. This allows us to complete what have taken 30 minutes on Colossus 1 in just 6 minutes on Colossus 2.

The values you get will need to be adjusted depending on which letter counter is being printed. For the second reading found 09 03 on counter a, to find the actual wheel setting, you would count back. For counter a, we are actually 4 remembered characters back from the actual setting, b is 3 back, c would be 2 back etc. Therefore, the reading found for counter a in this case is 05 03 as we found earlier.

Once you have the first and second wheel settings values, these would then be set on the Jack Strip Panel and the operator would move onto the next algorithm to run to get further wheel settings. The algorithm to use would generally be selected by the cipher expert in charge and be based upon many varying options including known typing habits of the operators on the particular link this transmission was sent over and the results of previous tests.

Once all the settings positions were known for each of the 12 wheels and were checked to make sure that it was a reasonably high chance of being correct, then the settings would have been passed on to the Tunny machine in another room to do the actual decode and decipher the message.

This is the end of the tutorial – there are a number of scenarios to run on the website which should give more detail on exactly how Colossus was used for real.

Appendix 1

Setting the KH Pattern Manually

Set a plug or pin where you find an X and leave a space for a ·

X or Chi Patterns

X1 : **··XXXX·XX····XXX··X·X···X·XXXX·X·XXX···X·**
X2 : **··XX·XX··X··XX··XXXX·X···XXX··X**
X3 : **·XX·XX··XX···XX···XXX·X··XX··**
X4 : **··X····XXX·XX··XXXX··X··XX**
X5 : **··X·X··X·XXXX····XX··XX**

Ψ, S or Psi Patterns

S1 : **X·XX·X··X·X·X·X·X·XXXX·X·X·XXX··X·X·XX···X·**
S2 : **X··X·X·X·XX·X····X·XXX·X·XX·X··X·X·X··XXX·X·XX·**
S3 : **X·X·X··XX·X·X··X·X·XXX··X·X·X·XX·X·X····XXX··X·X·X·**
S4 : **·X·X·X·X·X·X··X·XX·X·X··X·X·XX·X···XX·X·X·XXXX···XX·**
S5 : **·X··X·XX···X·X·XXXX··XX·X·X·X·X·X·X·X·X···X·XX·X··X·XX···XX**

μ, M or Motor Patterns

M1 : **···XXXX·XXX·XXXX·XXXX·XXXX·XXXX·XXX····XX·XXXX·XXX·XXXX·XXXX·**
M2 : **····X·X···X·X·X···X·X·X···X·X·X·X·X·X·**