Virtual Dragon

A computer simulation of the World War II American Dragon cribbing machine used at Bletchley Park.

Introduction

The Dragon was a machine built in America in 1944. It was one of a few machines given the title of Rapid Analytic Machinery (RAM) and was built by the Signal Security Agency (SSA) at Arlington Hall, Virginia. It was created to assist in the breaking of "Tunny", the British name for the Lorenz SZ40/42 cipher attachment.
Dragon was designed at the SSA by Captain George, an expert in telephone switching systems. It was completed on 24th August 1944 and then shipped over to Bletchley Park to arrive on 14th October 1944. The Dragon was placed into Rooms 22, 23 and 24 of Block F which were made into one larger room to accommodate it.

Dragon was a crib dragging machine which would test a guess at a section of text which was believed to be found within the enciphered message being tested. Should such a guess be successful, and a match found, this would give the cryptographers in the Testery the foothold required to begin to break into the message and work backwards to the beginning of the message. Once the start point of the message was recovered, this would give the start positions of the PSI wheels for that message and therefore enable a full deciphering of the message to be generated on one of the British Tunny machines.

A lot of the messages could be deciphered manually by the code breakers in the Testery, but on low dottage days (days where the number of dots generated by the Motor(Mu) wheels and limitation were few), it was much trickier to find a break, and this is where Dragon would be brought into play.

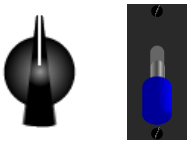
Using the Simulation

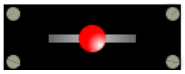
Firstly, the Dragon is a little larger than most monitors, so you will need to know how to zoom in and out using your browser.

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, press the zero key to go back to default 100%. Move around the screen using the scroll bars. For Mac users, it's the same, but use the Command key rather than the Ctrl key.

If you have a touchscreen or tablet, just pinch to zoom in and out and drag to move around the screen.

There are many switches on Dragon, the rotary switches can be switched on and off by just clicking anywhere on them to change the setting. The toggle switches can be switched in three different positions, click above/below or left/right of the switch itself to change them. Most have the same function when set either up or down, but the red Start switch (the one shown on the right here), can be switched either way to give a different function. Click it to the left side for a single letter run or click the right side to run continuous mode until the end of the tape or a match is found.

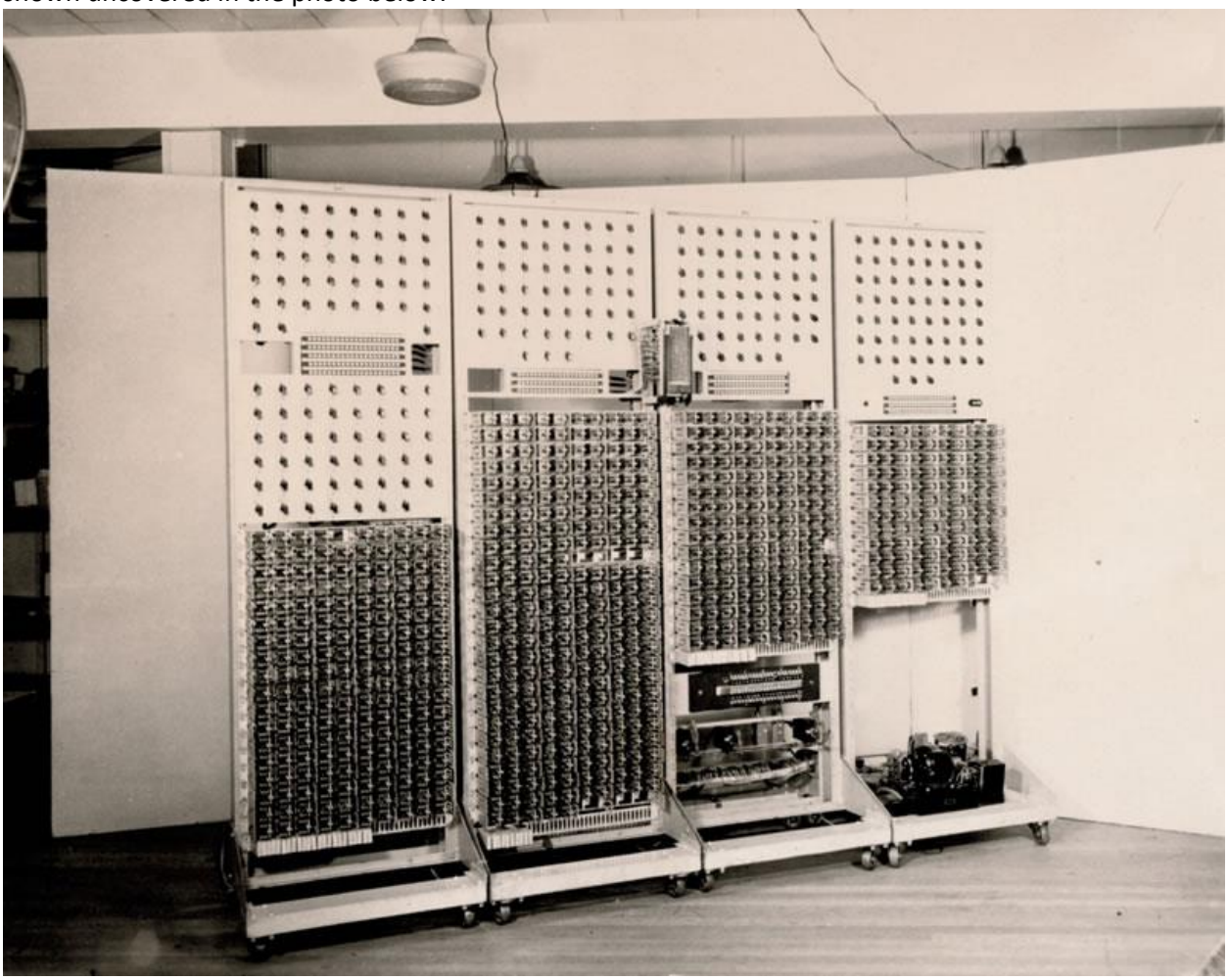




Finally, the crib board is an 8x10 plug board which can have two-pronged pins fitted to make the settings. Just click on a slot or pin to switch in or out.

An overview of Dragon

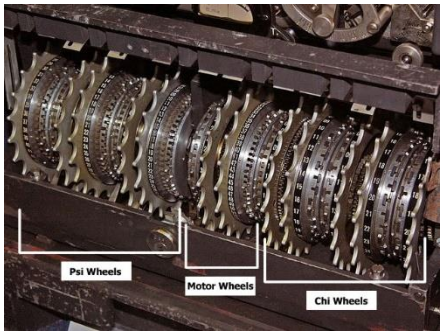
The Dragon is split into four large racks with Bay 1 on the left to Bay 4 on the far right. The top part of each bay houses the controls and displays while the lower half has the numerous relays, ten to a row, shown uncovered in the photo below.



Dragon - Photo courtesy of the National Cryptologic Museum/National Security Agency.

Each bay has the controls and display for at least one of the PSI wheels on the Lorenz, Bay 1 has both PSI 1 and PSI 2 controls whereas Bay 2,3 and 4 have PSI 3,4 and 5.

Each PSI wheel on Lorenz has a different number of small cams or switches around its circumference which change how it enciphers the message. Each wheel has a different number that can be set, PSI 1 has 43 cams, PSI 2 has 47 cams, PSI 3 has 51, PSI 4 has 53 and PSI 5 has 59. The settings for these are replicated on the Dragon panels – you will see that the top panel of Bay 1, called BAUD A, has a total of 43 rotary switches which can be either on or off. These are the settings for PSI 1. The lower panel on Bay 1, BAUD B, has 47 switches, the same as PSI 2 and so on.



The Lorenz SZ42 enciphering wheels

Getting started – the first run

The default settings of the Virtual Dragon should be ready for a test run, but it's worth going through each of the options to make sure it's set correctly.

Setting the PSI wheels

Firstly, we would have been given that days wheel break settings for Lorenz which were calculated by hand by the codebreakers in the Testery. These are the patterns that need to be set on the rotary switches on each PSI wheel. Below is an example of the settings for PSI 1 to 5, an X was written for the `on` setting while a · was written for the `off` setting.

Psi (Ψ) Patterns for KH pattern

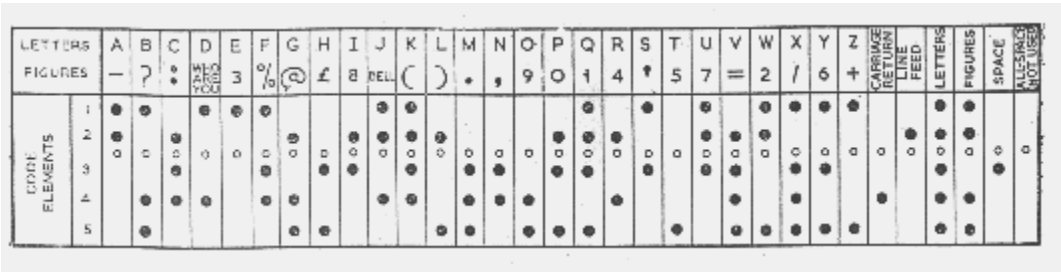
PSI 1 : **X·XX·X··X·X·X·X·X·XXXX·X·X·XXX··X·X·XX···X·**
PSI 2 : **X··X·X·X·XX·X····X·XXX·X·XX·X··X·X·X··XXX·X·XX·**
PSI 3 : **X·X·X··XX·X·X··X·X·XXX··X·X·X·XX·X·X····XXX··X·X·X·**
PSI 4 : **·X·X·X·X·X·X··X·XX·X·X··X·X·XX·X···XX·X·X·XXXX···XX·**
PSI 5 : **·X··X·XX···X·X·XXXX··XX·X·X·X·X·X·X·X·X···X·XX·X··X·XX···XX**

To set these, first pick the PSI 1 settings and look at the top left panel on Dragon, marked BAUD A. Find the first rotary switch (it's the one bottom right – they are numbered down from top to bottom) – it should be set to the on setting. The second setting is a · so switch two should be off and so on through all 253 settings. Fortunately, these were not changed by the Germans for every message!

Rather than having to set each switch manually, we have a quick way to set them. Either from the menu at the top right or by clicking on the "Set PSI patterns" button at the top of Bay 1, you can get a list of a few genuine patterns which were used during WW2. Try selecting No Pattern and you should see all the switches turn off. Select back to KH Pattern to set the switches for this initial run.

Setting the Crib

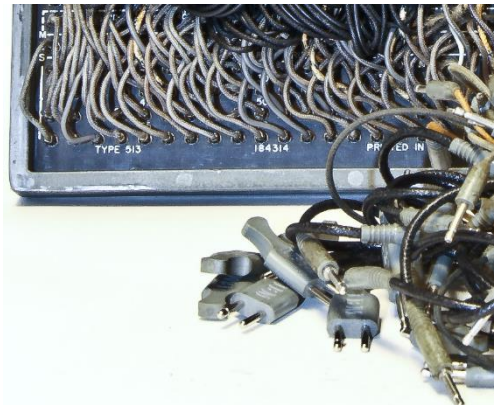
Next, we need to set the crib (the guess at the plain text) that we want Dragon to search for. To do this, we need to know how to set a message in ITA2 (International Telegraph Alphabet No 2) code.



Each letter is encoded as a series of 5 holes punched into a paper tape. To encode a letter A for example, the tape would show holes in position 1 and 2 and unpunched tape in 3,4 and 5. To get numbers and punctuation, a special character code was sent, the figure shift – marked FIGURES above. Once a figure shift code was sent, then any character sent afterwards would show a number or figure until the LETTERS code was sent. For example, to send ABC123 you would send ABC codes followed by the FIG code then the same codes for QWE. The crib we are searching for is within the ITA2 code, so is likely to include some of the control characters not just plain text.

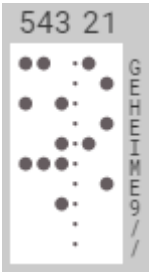
To set the crib, you need to set each of the characters you would like to search for in the plugboard as shown here. This example has the word GEHEIME9 set, geheime translates as the word secret in English. The 9 is how the ITA2 code for space was normally written at Bletchley Park.

The Dragon can search any number of characters up to 10, but the smaller the word being searched, the higher the chance of a false positive match being found.



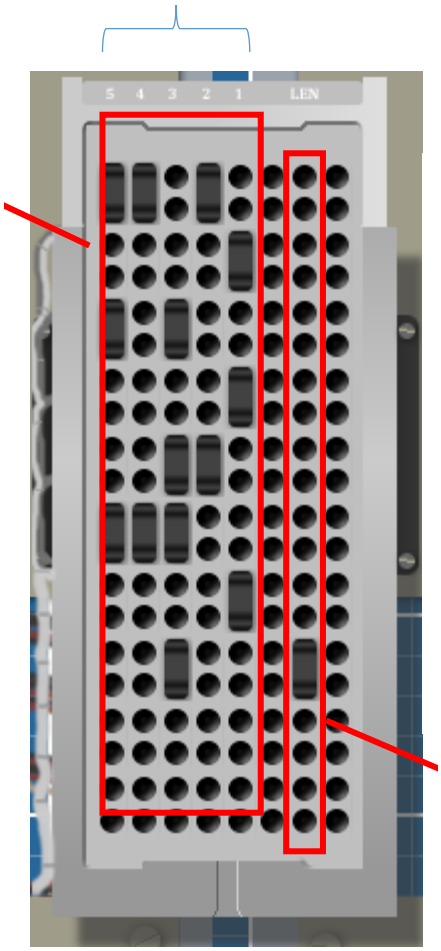
The crib plug board of the sort found on IBM punched card tabulating equipment. The settings were likely to have been set with the type of shorting pins seen here.

The five ITA2 impulses of each character in the crib with space for 10 letters. A plug marks a hole in the tape.



Example punched tape

Note: Impulse holes are set from 5 down to 1 to match the tape orientation



This row sets how many characters are in the crib. Set one plug at the last character (up to 10). This example is set for an 8-letter crib.

If you would rather select a crib or type in one of your own, just click the “set crib” button next to the board or the cribs menu at the top of the screen. You can select a preset crib or type in your own to find. Type in any letter or 3 (CR),4 (LF) ,5 (FIGS),8 (LTRS) or 9 (SPACE) and click set. For our example, make sure this is set to the value GEHEIME9 ready to search our test De-Chi.

Inserting the De-Chi tape

The final step required is to load the enciphered De-Chi tape we want to search through into the Teletype tape reader. The De-Chi tape is generated after Colossus has made the first initial break into the cipher message by calculating the start positions of the Chi wheels. The resulting Chi wheel run can be added to the original cipher to create the De-Chi tape.

Click on the “set tape” button next to the tape reader or on the top menu. Choose one of the tapes listed and click "Load this De-Chi tape” to install it. You can select View De-Chi to see the actual enciphered text of the De-Chi or view the ITA2 or plain decoded text (to find a word to search for). Select Tape 1 section then click the “Load this De-Chi tape” button.

The tape runs through the teleprinter at 50 baud (about 6-7 characters per second) and you can see a close up of the current tape position just above. If you need to take the tape back a few places – you can click or tap on the bottom of the tape to move back a step. If you are using a mouse rather than a touch screen, hovering the cursor over the characters on the tape will tell you which letter is encoded there.

Starting the Dragon

Find the start switch – it's a red toggle switch on the middle right of Bay 4. Click or swipe the switch to the left (or press the letter T on your keyboard) to get Dragon to read in a single character from the De-Chi tape. Let's take a quick look at what just happened.

Firstly, you should see that the teleprinter tape has moved on one character and this has been read into the Dragon's register. The counter display (just above the teleprinter) should be now showing the value 1 and the first character's ITA2 code. The counter display is split into sections from right to left for units, tens, hundreds, thousands and ten-thousands.

Now check the working notes which are listed to the left. These would not have been available to the operator, but it's writing out some notes so you can see exactly what the Dragon is working on behind the scenes.

The De-Chi is read into a bank of relays which store the last ten characters input – you should see the first letter (J) from the tape showing in the first position of the bank with all the other characters showing the null character (written /).

Now set the start switch over to the right to begin the full run (or press Return), each character from the tape will be read in one at a time and Dragon will begin searching for a match by adding the crib to the last ten characters of de-chi loaded.

The first stop should be found at tape position 129 so let's look at the working notes to see what Dragon has found.

```
DE-CHI EGKFZEMUSL <-- input from tape
CRIB   GEHEIME9 <-- set on plug board
PSI'   555NQXXA <-- De-Chi + Crib = PSI'
PSI    5NQXA <-- PSI' contracted ~= PSI
```

This first section shows the ten characters of the De-Chi currently loaded (EGKFXEMUSL) and below it, the crib being checked (GEHEIME9).

The first thing Dragon does is to add each character together (modulo-2 addition, the same as XOR) to give the PSI' (PSI Extended). Adding and subtracting in modulo-2 give the same result.

The Lorenz SZ42 works by adding a letter from the Plaintext to a generated letter from the Chi wheels and to a generated letter from the Psi wheels which gives the resulting cipher letter. The Chi wheels turn once for each letter being enciphered while the Psi wheels stutter and sometimes stay on the same setting, giving the same character each time, and sometimes move on one position.

When referencing the sequence of letters set on the pins of the Psi wheels, we use the term PSI whereas, when referencing the actual sequence of letters generated when running the Lorenz, we use the term PSI' or Psi extended. For example, turning the PSI wheels and reading off the character set by the pins might give the letters 5NQXA (Psi) but when actually running, due to the action of the motor wheels, the actual letters generated may repeat, for example 555NQXXA (Psi').

Therefore:

Plain + Chi + Psi' = Cipher
Colossus was able to break into and work out the sequence of Chi letters being generated and therefore, if that result was added to the cipher text, it would cancel out the Chi wheel completely, giving the De-Chi .

Cipher = Plain + (Chi + Chi $^{\text{cancel out}}$) + Psi' = Plain + Psi' (the De-Chi)

We can then see that if we add our guess at the Plain text (the crib) to the De-Chi and it's actually in the correct position, then we will cancel out the Plain text leaving just the Psi' (Psi extended) text.

De-Chi = (Plain + Crib $^{\text{cancel out}}$) + Psi' = Psi'

Before starting, if you recall, we set the pin settings of each of the five Psi wheels on Dragon, so we know the values of Psi but not Psi'. The assumption that Dragon made was that all repeated letters in our calculated Psi' were due to the stuttering motion of the Psi wheels and therefore, using more relays, it contracted the Psi' value wherever there was a repeated letter. In our calculation above, 555NQXXA becomes 5NQXA. This gives us a possible sequence of Psi characters that should appear somewhere within the settings of Psi we have put into the switches on Dragon.

The next step was that Dragon compared the settings for each impulse of the contracted calculation against all settings of Psi in parallel to check if they were the same – that's a lot of wiring! If a match was found for all five of the Psi wheels, then Dragon would stop for the operator to write down the settings it had found.

The first thing that the operator would have required was the character position that the tape has stopped on. The original Dragon image does not appear to show any way for this to be displayed so it's possible that they just marked the tape and just counted the number of characters to get the position. On this simulation, a counter display has been added – according to a personal communication from Thomas L. Collins, this was a scale-of-31 counter, built at Bletchley Park, using British "3000 type" relays and is likely to be the additional circuitry shown on the later GCCS photo installed at the bottom of Bay 4, the box on the wall and the addition of a new set of switches on the control panel on Bay 2. This shows the current loaded de-chi and the count of the position where Dragon has stopped.

The second item we need is where on the Psi settings the contracted Psi' was found. This is shown on the light displays midway on each Bay. In this example, look at the top row of lights on Bay 1 - this is the result for the first Psi wheel (the switches above on Baud A). You should see that the first impulses for the characters 5NQXA (X•XXX) have been found in two places, from setting 30 to 26 and from setting 21 to 17. The second impulses for Psi 2 are shown on the bottom set of lights on the same panel. These are showing a match in four places. The data for this is shown for you to check on the Dragon working notes page, so you can see exactly where the match was found – the operators at Bletchley Park didn't have that bonus! As an additional option, the characters that had been contracted are shown on the last set of lights on Bay 2's display. This was referenced in the sparse documentation for Dragon 2 built by the G.P.O at Dollis Hill as a value that was displayed so it's been added as an extra feature on this version of the Dragon (as far as I'm aware, there doesn't appear to be any documentation that this appeared on Dragon 1 but it would have definitely been possible to show this).

For your information, click the green “Result” button at the bottom of the working notes page – this will take you to a listing of the De-Chi result as could have been passed on to the Testery for the next decryption step. The De-Chi would have been listed in rows of 31, this being the number of characters on Chi wheel 2 which was used in the limitation of the motor wheels on the Lorenz. The known Chi-2 wheel settings would have been written above the table for the reference of the codebreaker working on the decrypt.

The actual plain text is listed to the right of this table. This is for your information only and would (obviously) not been available to the codebreakers working at Bletchley Park – this is what they are working to decrypt! You should be able to find the word GEHEIME9 listed on Line 4-5 (the position that Dragon found is the position of the last character it discovered - just after the last character 9).
The codebreakers would then use this information to work the wheel settings back to find the start position for the first character of the message – this would then be the start positions that the Psi wheels were set to when enciphering this message. This along with the start positions already found by Colossus for the Chi wheels and the Motor wheels would be set on a Tunny machine and the final decipher could then be read.

Let’s try to see if we can run a second tape. This time, from the top menu, choose the De-Chi Tapes menu and select Tape #2 - this is a longer message on the Bream Psi patterns. Click on the button marked “View deciphered text (plain)”, it will show the already deciphered message so you can pick a word to search for. If you look through the text, you should see the work ROEM written numerous times – this stood for Roman in German which was how the German Army numbered their units (in Roman numerals). The data we actually need to search for though includes the ITA2 codes, probably spaces, full stops and commas so click the “View deciphered text (ITA2)” to see the full decoded text including these characters. If you look through this text, you will see it written in various ways: 9ROEM955 (space, ROEM, space and two change to figure shift codes) and 88ROEM955 (two letter codes, ROEM, space and two figure codes). Let’s choose to find the 88ROEM955 which first occurs about 1295 characters in. Press the “Load this De-CHI tape” button.

Next, we need to switch over to the Bream patterns – click PSI Patterns in the menu and select BREAM Pattern – you should see all of the Psi wheel switches change over. Finally, we need to set our crib to search for, click Cribs and choose the 88ROEM955 button or type this in the section Set my crib and click Set.

Before we start Dragon again, you might notice that we still have letters in the shift register stored from the last tape – we will need to reset the relays to clear these down. Find the Reset Store green switch on Bay 3 and click it once (either way) to reset the store. Now, start the Dragon by setting the Start switch on Bay 4 over to the right.

Remember that the section we’re searching for is 1295 characters along, so it will take around 3 and a half minutes to get to this point – time for a cup of tea or coffee! If all has been set correctly, it should stop at the correct place and you can check the results to see if the plain text matches up … looks like we’ve got a good stop.

Once you’re happy with this stop, let’s try to continue this run and see if we can find another stop further along the tape. Set Dragon running and wait again, after another wait, you should find a stop at character 2643 which takes about the same time as the last run.

Take a look at the results again and see where it stopped. This time, we appear to have stopped where the result is NOT the crib we're looking for! The plain text found seems to be V9ROEM955 which is possibly close enough that the codebreakers in the Testery could work with it, but it's not quite right. Also, we appear to have missed one 88ROEM955 at character 2115 – showing that the way Dragon searches is not infallible.

Try a few different cribs on different De-Chi tapes and see what you can get Dragon to find.

Thank you for trying out Virtual Dragon. I have tried to make it as accurate as possible with the data I have available but if you find an error or can suggest an amend, please do let me know.

Martin Gillow
Twitter: @VirtualColossus
FaceBook: https://www.facebook.com/VirtualColossus/

Shortcut keys

A few quick shortcut keys are available

Return: Start Dragon
Space: Stop Dragon
T: Run one character
1 – 9: Quick set various cribs
Q : Load Tape 1
W : Load Tape 2
E : Load Tape 3
R : Load Tape 4
A : Set No Pattern
S: Set KH Pattern
D: Set Z Pattern
F: Set Bream Pattern