

Recreating the Enigma Machine

Source: <https://nicerc.org/enigma>

Background-

The Enigma was an encryption machine famously used by the German military during World War II. The power of the Enigma came from being simple for the operator to use, but difficult to determine the encrypted letter for any input letter. The number of possible ways to jumble a message through an Enigma was nearly 159 *quintillion*. Thanks to incredible mathematicians in Poland and tenacious work by the British at Bletchley Park, the Allies broke the Enigma code. This gave the Allies the ability to read top-secret communications during the war and greatly disrupt the Nazi German war machine.

The Enigma was an electro-mechanical machine similar to a typewriter. The simplest models had three wheels on top of the case that allowed the operator to set internal rotors into a certain position. The operator would press a key on the keyboard, which would activate an electric circuit and light up a different letter. For example, a letter T might be pressed, but the letter G would light up.

Soldiers in the field and sailors at sea would set their Enigma machines' rotors to the same as the person sending a message. They would copy seemingly random letters via Morse Code from the radio. The Enigma operator would then key in each "random" letter and write down the resulting letter that was lit up on the machine. Each key press on the keyboard would turn a rotor one step and provide a new, different path for the electricity to flow inside the machine.



Thanks to the work of British mathematician Alan Turing, the Allies developed "The Bombe," a top-secret electronic computer used to quickly try every possible combination of letters in order to crack the Enigma code. The Bombe was an incredible feat of engineering and the first electronic computer. However, because The Bombe was classified, the University of Pennsylvania's ENIAC was publicly given the crown of "first computer."

The Enigma remains perhaps the most popular encryption device in history. There are countless stories of other encryption techniques, but none has intrigue and impact that the German Enigma had during World War II. What follows will guide you through the creation of your very own Enigma machine.

Supplies-

- Pringles can (small or large); you can also use a soup can or any other cylinder with a 3" diameter.

- Printed NICERC Paper Enigma page
(Print the page with **Actual Size**; do not select **Fit to Page** or the dimensions of the enigma will not be correct.)
- Scissors
- Clear tape

Construction-

1. Cut each strip of paper along the thin gray outline of each strip.
2. Wrap each strip of paper around the Pringles can.
3. Overlap the tab at the end of the strip and secure with a piece of tape.
4. Ensure each of the paper rings (rotors) can rotate.



Pringle Can Enigma- This example of the smaller can uses only one rotor strip for the middle section. The larger Pringles can will use all three rotors strips to fill in the middle section.

[DOWNLOAD PAPER ENIGMA PDF](#)

Encryption-

The following directions are for the large Pringle can. The small can works the same way, except that you will only be using one rotor. This will result in a starting position where all the A letters are aligned horizontally across the can, as in A-A-A. This is because only three rings are used with the small can. The large can will display A-A-A-A-A, since there are five rings to work with.

There are many start positions each rotor and the reflector can be set for. Align the rotors so all the A letters line up. Aligning the Input; Rotors 1, 2, 3; and the Reflector at Input position A is said to be set to A-A-A-A-A. Later, the start positions of each rotor will change, but for now leave them all aligned with A.

Starting from the left, locate the letter A on the input rotor. Follow the path from A on the input rotor to the letter A on Rotor 1. Follow the path from A on Rotor 1 to Rotor 2. The path leads to the letter C on Rotor 2. Now follow the path from C on Rotor 2 to Rotor 3. The path leads to the letter D on Rotor 3. Now follow the path from D on Rotor 3 to the Reflector. The path leads to the letter G on the Reflector. Follow the path from G on the Reflector to the output letter of the Reflector. The path leads to the letter L. Follow the paths back through each of the rotors. When you get to Rotor 1, the output letter should be L. This means that L is the encrypted letter A.

After you get an output letter, rotate Rotor 3 on letter “up”. The rotors are now A-A-A-B-A. To encode our next letter, locate the letter C on the Input rotor. Trace it across rotors 1, 2, and 3, through the reflector and back through 3, 2, and 1. The output letter should be B.

Shift Rotor 3 “up” one time (because we got our output letter from before). The rotors are now A-A-A-C-A. Encode the letter E by finding it and tracing the path to and from the Reflector. The output letter should be V.

The word ACE when encrypted through this setup of the Enigma is LBV.

Decryption-

Because the message was encrypted with rotors in position A-A-A-A-A, it is important that the Enigma starts with that position. The first letter of the encrypted word is L. Trace the path from the Input rotor from L across Rotor 1 to M on Rotor 2, then to K on Rotor 3, and through L on the Reflector. On the Reflector, L reflects back to G, then to D on Rotor 3, then to C on Rotor 2, and finally to A on Rotor 1 which is aligned with A on our Input rotor. So the decrypted first letter is A.

Remember to shift the third rotor one-step after each output letter. The next encrypted letter is B, which follows the path D to F to B on the reflector, then out from D to G to E to C for the return path. The next *decrypted* letter is C.

Shift the third rotor once then trace the final letter, V, through the path. V connects to S to W to X on the reflector, then out from Z to C to B to E for the return path. The final *decrypted* letter is E.

Notice that the Input and Reflector do not rotate when encoding or decoding. Once those two are in position, they should remain in that position. When you turn the rotor next to the reflector, be sure the reflector has not accidentally turned also. If your message is *longer* than 26 letters, you will have shifted Rotor 3 all the way around. Before you rotate back to A, shift Rotor 2 one time. After another 26 letters, Rotor 2 will turn once more. Rotor 3 will turn the most; Rotor 1 will turn the least. (For every 676 letters, Rotor 1 will turn one time!)

Rotor settings-

If all messages were sent with the same rotor settings (A-A-A-A-A), it would not be difficult to decrypt the message – everyone would have the same encryption mechanism. Designers of the original Enigma knew this and made it so you can set the rotors to whatever configuration you choose. As long as the recipient knows which rotor settings to use, you can decrypt the message.

Try this-

Set the rotors to position **C-Y-B-E-R**. That means to align the letter Y on Rotor 1 with the C on the Input. Align the letter B on Rotor 2 with the Y on Rotor 1. Align the letter E on Rotor 3 with the B on Rotor 2. Align the R on the Reflector with the E on Rotor 3. This configuration is unique to these rotor settings.

Now, just as before, decode the following message and remember to turn Rotor 3 one-step after each letter is encoded or decoded.

The message to decode is **BVHFTD**

The answer is the second word of the first paragraph in the *Background* section. Did you get it?

If you answered that correctly, try the following Practice section for some more challenges.

Practice-

Use your Enigma machine to **decrypt** the following messages.

(All spaces have been converted to an “x” in the decrypted message.)

1.	Rotor Settings	A A A A A
Encrypted —————→	IVWYQDV	
Decrypted?		
2.	Rotor Settings	A A A A A
Encrypted —————→	PVWZARCYHRRCKW	
Decrypted?		
3.	Rotor Settings	C Y B E R
Encrypted —————→	YPELONUPTOZS	
Decrypted?		
4.	Rotor Settings	C O D E S
Encrypted —————→	hufvegZ	
Decrypted?		
5.	Rotor Settings	T U B E S
Encrypted —————→	actrqinxrnqlmvg	
Decrypted?		
6.	Rotor Settings	R A D I O
Encrypted —————→	yedwpqbubbrjhwsetlhden	
Decrypted?		