HOW DOES ENIGMA WORK?

This photo, online via the National Museum of the U.S. Air Force, depicts an Enigma machine in use during World War II. Curators of the museum provide this description: "German forces depended on Enigma machines to encode and decode secret messages transmitted over the radio during World War II. The Enigma machine is on the left. (Photo courtesy of Helge Fykse, Norway)."

After Arthur Scherbius died, in 1929, his Enigma-making company changed hands. By 1933, after the German Army had acquired the rights to make the encryption machine, the manufacturing company's name became Heimsoeth and Rinke.

Although it was still a machine resembling a typewriter, Enigma was now more portable than its earlier models. It also had more rotors - those toothed wheels which were integral to Enigma's success - which its operators could use.

What were those rotors? How did they work? Why did the Germans think Enigma's rotor-produced codes were unbreakable?

Let's begin by answering the last question. Hitler believed his version of the Engima was unbreakable because the chances for a human to break its codes were 150 million million million to one.

That's not a typo. Actually, to be even more precise, the chance of a human deciphering an Engima-generated encryption was nearly 159 million million million to one.

In order to understand what Germany was up to, decoders needed to understand the Enigma machine itself. They got a head start when a new military Enigma device spent a weekend in the hands of Polish decoders in the late 1920s.

By 1932, three Poles - Marian Rejewski, Jerzy Rozycki and Henryk Zygalski - had made great strides toward understanding Enigma's make up. All spoke fluent German, were mathematicians and had completed a cryptology course offered by the Polish Cipher Bureau.

With ingenious analysis and insights, they were able to reverse-engineer Enigma. With help from a German traitor - Hans-Thilo Schmidt, known by the code name Asche - who sold Enigma instruction manuals to a Frenchman (who then passed on those instruction manuals to the Poles), Rejewski and his colleagues worked-out how Enigma was wired and how it operated.

They even produced replicas of the machine itself, including its rotors.

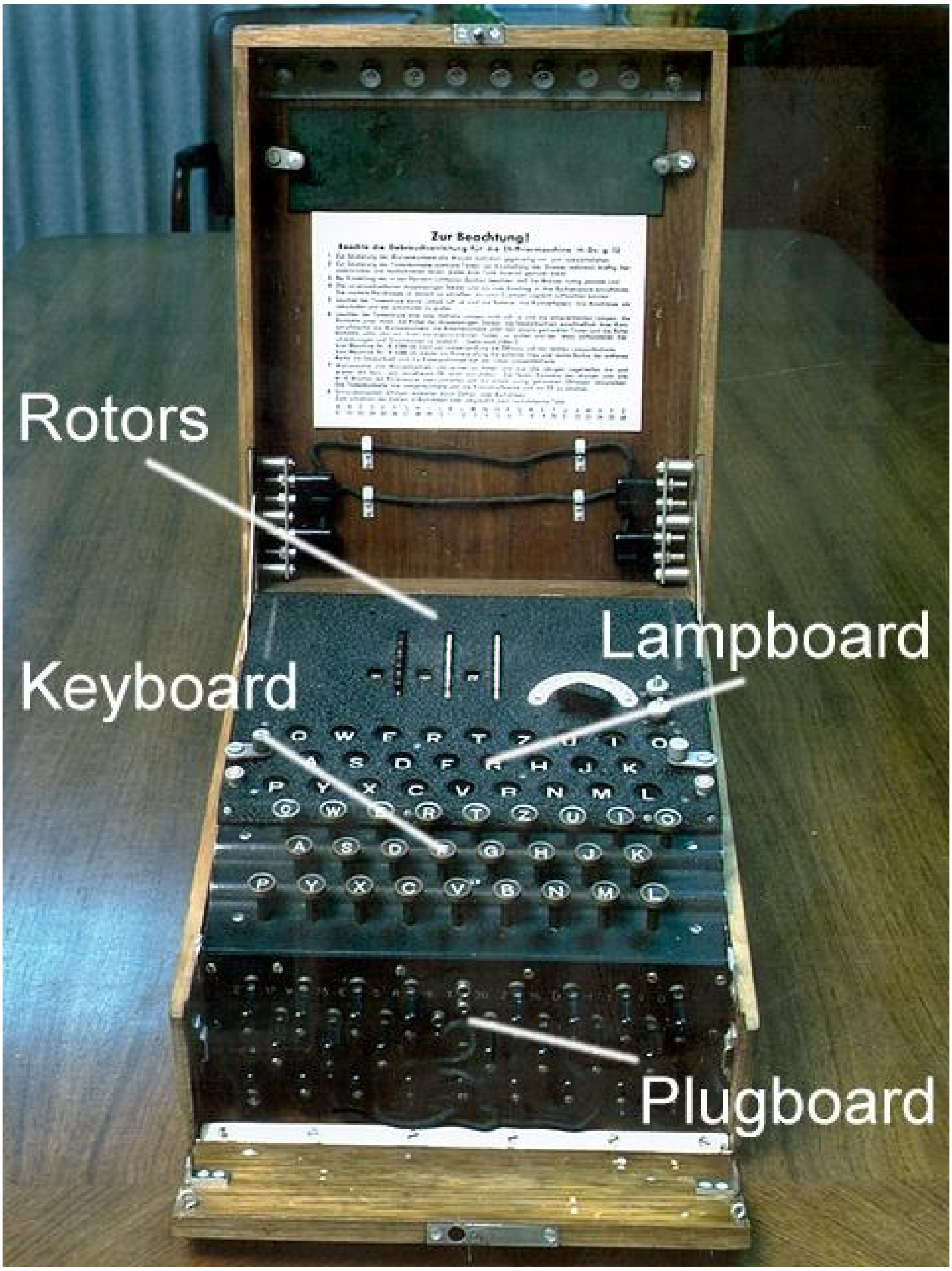
In this Numberphile video, featuring an actual German Enigma machine, Dr. James Grime demonstrates those rotors, the machine in which those rotors function and the many configurations which Enigma operators could use to send encrypted messages.

Rotors were toothed wheels which could be changed whenever needed. German Enigma-operators would change the wheels every day, at midnight.

For code breakers who were unable to decipher messages on any particular day, all the hours of work on that day were lost because different rotors would be used the following day.

Because of the rotors, the original letter typed on the keyboard would change seven times during Enigma's operational process before that original letter became the final transposed encrypted letter. When the transposed letter was selected, it lit-up on another Enigma keyboard (known as the lamp board).

Once the dispatch was fully encrypted, using this process letter by letter, the transmitting operator used Morse Code to send the coded message in groups of five letters.



Enigma could also decode. When an encoded message was received, the same rotors would be in place on the decoding machine, and the process would work in reverse to reach the original letter.

A key to Enigma's unbreakable status was this fact: A single letter - for example "A" - was never used more than once in the coded message. This meant that a code breaker could not find a pattern while trying to break the encryption.

See Alignments to State and Common Core standards for this story online at:
http://www.awesomestories.com/asset/AcademicAlignment/HOW-DOES-ENIGMA-WORK-The-Imitation-Game

See Learning Tasks for this story online at:

Questions 2 Ponder

If the Odds against an Action are Next-to-Impossible, Why Undertake the Action?

If the odds of breaking Enigma—a page of its original patent is pictured here—were around 159 million million million to one—and the code breakers knew that—whatever made them think that they had the slightest chance to break a virtually unbreakable code?

To What Extent Do Human Actions Enhance Computer-Based Inquiries?

Code-breakers, before Alan Turing, had an impossible job. How could it even be possible to break Enigma's code without the help of a machine?

But ... how could a machine begin to help until a human being first invented such a computing machine?

Would human actions improve the code breakers' chance to successfully break Enigma? What role would human actions play?

Media Stream

Marian Rejewski and His Enigma Discoveries

Image online, courtesy Polish Greatness website.

PD

View this asset at:

http://www.awesomestories.com/asset/view/Marian-Rejewski-and-His-Enigma-Discoveries

Jerzy Rozycki

Image online, courtesy Wikimedia Commons.

PD

View this asset at: http://www.awesomestories.com/asset/view/Jerzy-Rozycki

Henryk Zygalski

Image online, courtesy Wikimedia Commons.
In-text image of Bletchely Park Zygalski-sheet demonstration by Toby Oxborrow; license

View this asset at: http://www.awesomestories.com/asset/view/Henryk-Zygalski0

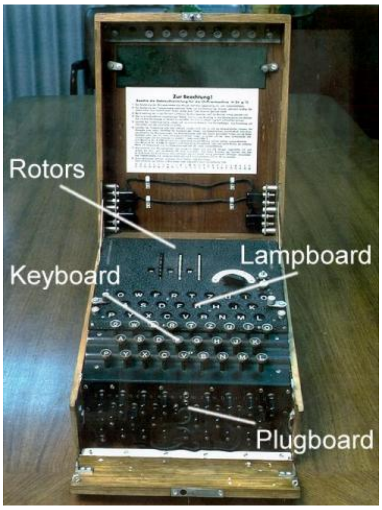
Enigma Machine

This image depicts an Enigma machine (which its German users referred to as an "Encryption Machine").
On the inside cover of the device, we see a list of instructions, written in German.
Translated into English, they state:
To Observe!

Observe the manual for the Encryptionmachine (H. Dv. g. 13)

1. To clean the roller contacts, turn all rolls several times backwards and forwards.

2. To clean the key contacts, press all keys down strongly before turning on power several times and let them pop back up while one key remains pressed.



3. While selection of the characters which are visible in the window, observe that the rollers are in the right position.

4. The "fool proof" [literally: unconfusable] double-pole plugs are to be inserted into the holes all the way. The front wooden panel is to be closed, since otherwise three lamps could be lit at the same time.

5. If no lamps are lit after pressing a key, check battery, contact springs, connectors at the switch and the switch itself.

6. If one or more lamps do not light up with a key pressed, the corresponding lamps, the contacts underneath them, the cables of the double-poled plugs, the plug receptacles including their short circuit panels, the roller contacts, the working contacts underneath the pressed keys and the "resting" (?) contacts underneath the corresponding keys are to be checked and if dirty or oxidized are to be cleaned (see also number 2).

7. Roller axle and roller receptacles are to be kept clean and like any other bearings occasionally slightly oiled with a sap- and acid-free oil. The fixed contacts of the rollers are to be sanded every six to eight weeks with polishing paper and rubbed with a slightly oily cloth. The key contacts, the lamp contacts, and the short circuit panels are to be kept free of oil.

8. Key selection is done through either digits or letters. To translate the numbers into letters, or back, use the following table:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Click on the image for a better view.
Image of Enigma Machine, online via NSA (National Security Agency). Public Domain.
View this asset at: http://www.awesomestories.com/asset/view/Enigma-Machine

HOW DOES ENIGMA WORK?

View this asset at: http://www.awesomestories.com/asset/view/