(/)

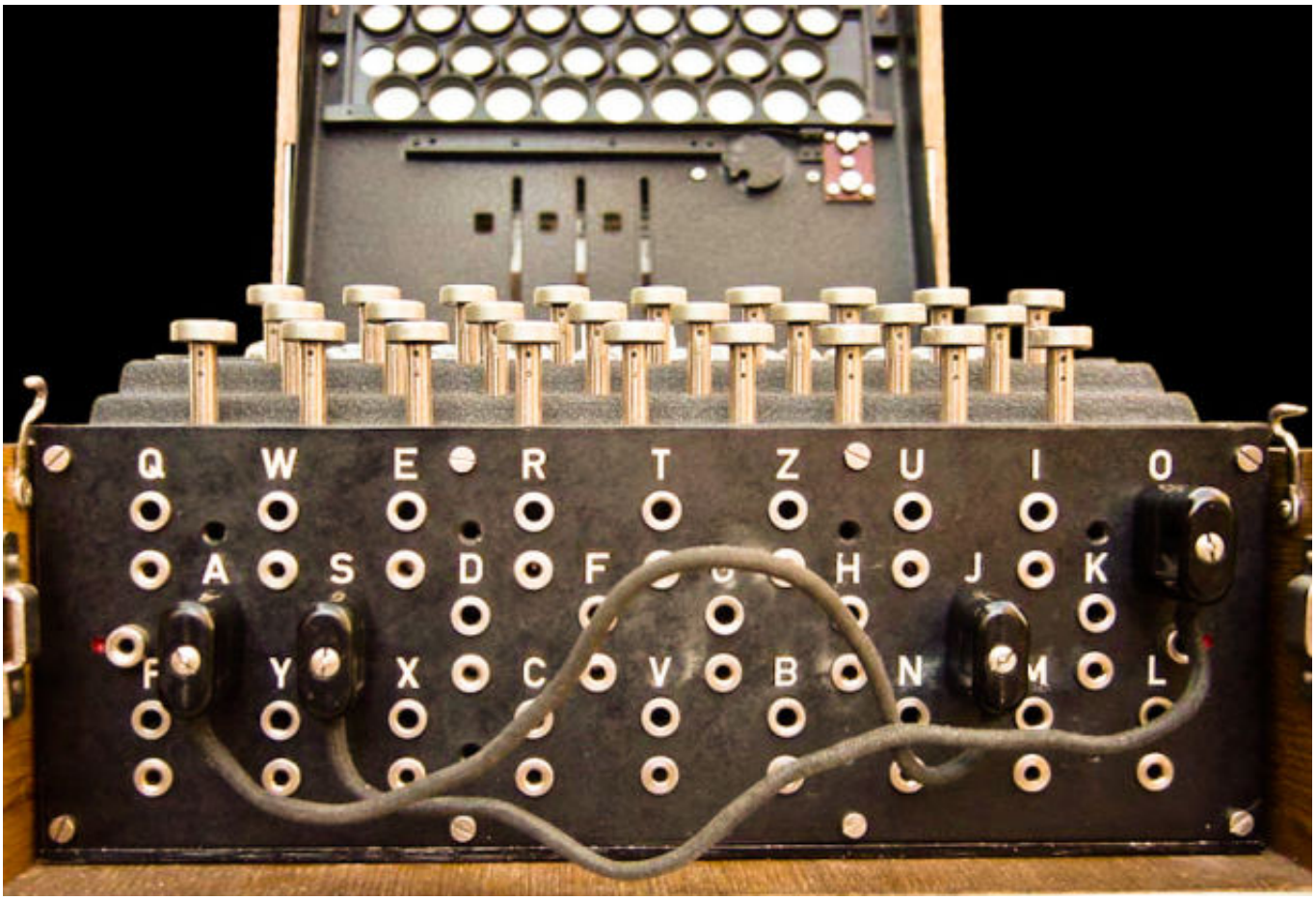
+ FOLLOW

How The Enigma Machine Worked, In One Infographic (http://io9.com/how-the-enigma-machine-worked-in-one-infographic-1658875410)

(http://mark-strauss.kinja.com)

Mark Strauss (http://mark-strauss.kinja.com)
Filed to: CRYPTOGRAPHY (/TAG/CRYPTOGRAPHY) Today 2:40pm (http://io9.com/h

1,512 3



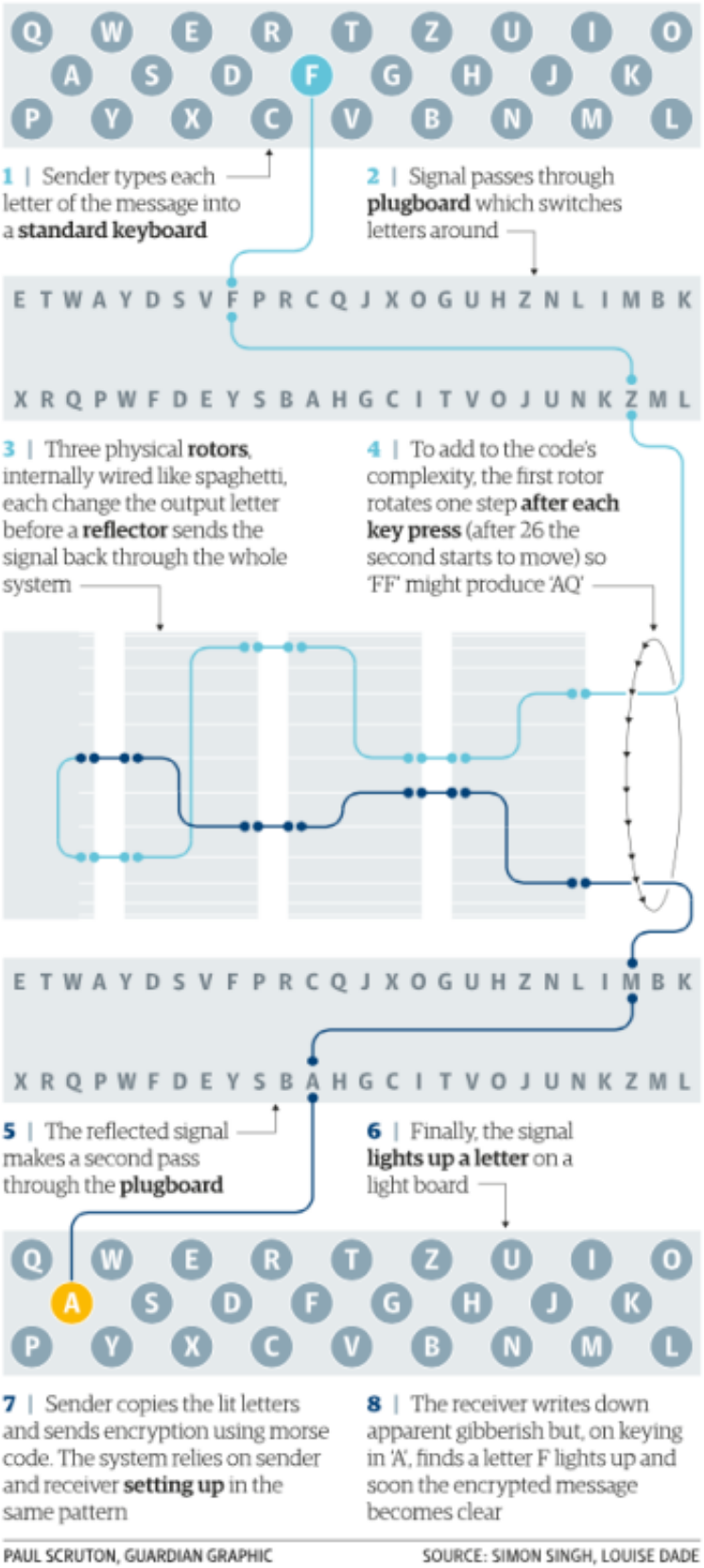
The release of the film, *The Imitation Game*, about the life and work of Alan Turing, inspired the *Guardian* to publish this description (http://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game?CMP=twt_gu) of how the German encryption device worked—and why, like all good cryptography, it was a simple concept that was a nightmare to break.

Part mechanical, part electrical, Enigma looked like an oversized typewriter. Input the first letter of your message on the keyboard, and then a letter lights up revealing what it has been replaced with in the encrypted message:

> *Inside the box, the system is built around three physical rotors. Each takes in a letter and outputs it as a different one. That letter passes through all three rotors, bounces off a "reflector" at the end, and passes back through all three rotors in the other direction.*
>
> *The board lights up to show the encrypted output, and the first of the three rotors clicks round one position – changing the output even if the second letter input is the same as the first one.*
>
> *When the first rotor has turned through all 26 positions, the second rotor clicks round, and when that's made it round all the way, the third does the same, leading to more than 17,000 different combinations before the encryption process repeats itself. Adding to the scrambling was a plugboard, sitting between the main rotors and the input and output, which swapped pairs of letters. In the earliest machines, up to six pairs could be swapped in that way; later models pushed it to 10, and added a fourth rotor.*

EXPAND

Enigma How the machine worked



Thanks to the reflector, decoding was the same as encoding the text, but in reverse. But that reflector also led to the flaw in Enigma, and the basis on which all code breaking efforts were founded: no letter would ever be encoded as itself. With that knowledge, as well as an educated guess at what might be encrypted in some of the messages, it was possible to eliminate thousands of potential rotor positions.

3 ★ 3 Reply

All replies (http://io9.com/how-the-enigma-machine-worked-in-one-infographic-1658875410/all)

The following replies are approved. To see additional replies that are pending approval, click Show Pending. Warning: These may contain graphic material.

SHOW PENDING

Dr Emilio Lizardo (http://dremiliolizardo.kinja.com) ▸ Mark Strauss
52 minutes ago (http://io9.com/the-way-i-understand-it-enigma-was-beaten-because-the-1658995427)
(http://dremiliolizardo.kinja.com)

The way I understand it, Enigma was beaten because the Germans got lazy and reused wheel orders and patchcord patterns, so the Allies could use captured machines to decode messages because the "key" wasn't changed often enough. Many people believe that with good discipline, Enigma would have been secure to the end of the war.

It is also interesting to note that sometimes when men were captured with the machines, Germany was not notified that their soldiers had been taken prisoner so that they would not guess that an Enigma machine had been captured. That was a clear violation of the Geneva convention.

1 ★ Reply

mwhite66 (http://mwhite66.kinja.com) ▸ Mark Strauss
38 minutes ago (http://io9.com/no-letter-would-ever-be-encoded-as-itself-quite-so-1659001175)
(http://mwhite66.kinja.com)

"...no letter would ever be encoded as itself"

Quite so. However, there were other factors that allowed the Brits to crack Enigma, not least that the Germans sucked at using it. The Wehrmacht deployed tens of thousands of the machines in the hands of low-ranking, poorly trained operators. They took many shortcuts, defying protocols, that assisted the codebreakers; they called them "sillies". On one occasion a German operator was ordered to send a long test message; he sent the letter M hundreds of times, giving codebreakers the internal wiring of the rotors. Also, the Germans transmitted reports in the same format every day, giving analysts "depth" to analyze. A key breakthrough was capture of the Weather Short Code Book from a German U-Boat, which gave them the exact format of a weather message sent by every U-Boat every day.

There is a very interesting book about all this called The Hut 6 Story by Gordon Welchman, one of the principles at Bletchley Park. Out of print for a long time, it is once again available, on Amazon.

The movie *Enigma* depicts many of these events in a fair amount of technical detail. There's also middling good spy story and wartime romance thrown in for good measure. Dougray Scott and Kate Winslet star. *Enigma*, Manhattan Pictures International, 2001.

Pictured: interior of Hut 6 in 1941, responsible for breaking the Enigma code every day of the war.

★ Reply