Leonard Fernando

Professor Paul Lambert

CS-486-01

October 25, 2017

Dropping the Bombe on Enigma

As a computer scientist, it is hard to not know who Alan Turing is. His contributions extend to almost every facet of modern computing, which includes cryptography, mathematics, and computer science. One of his greater achievements in the field of cryptography, cracking the Enigma Machine, was a feat at the time thought to be impossible. Yet, he managed to break the otherwise uncrackable cipher machine and saved millions of lives in the process. His work and the work of his colleagues was not declassified until the 1970's, but since then, cryptographers have uncovered their ingenious implementation of the Bombe Machine, which was used to crack Enigma. So how did Turing's invention help shorten an already long war and help contribute to modern cryptography?

To understand the Bombe Machine, we must first analyze the cryptographic properties of Enigma. On first glance, Enigma looks like a regular typewriter with a few modifications. Its components consisted of a keyboard, a plugboard, a static rotor, regular rotors, a reflector, and a lampboard. The journey through the machine to encrypt a message sounds like an overtly strenuous one, but this journey created a strong encryption. First, a letter was typed into the keyboard sending an electrical signal to the plugboard where the letter would be swapped with another. Then, we send our swapped letter to the rotors where the letter would be swapped about 3 more times through a static rotor, a right rotor, a middle rotor, and a left rotor. After this swapping, the letter, now completely different, is sent to a reflector, where it will start the whole process in reverse. After this second round of swapping, a different letter will light up on the

lampboard for an operator to write down. To understand how strong this encryption really is, I will do some calculations. When an operator received a machine, they could choose 3 rotors from a set of 5. This means there was 5 * 4 * 3 = 60 combinations for rotor placement. We must also factor in the 3 rotor starting positions which is 26 * 26 * 26 = 17,576 starting positions. There are 10 pairs you can make with the plugboard settings or 20 letters you could swap. This gives us 26!/(6! * 10! * 2^10) = 150,738,274,937,250. Multiplying all these combinations together gives us the staggering number of 158,962,555,217,826,360,000 enigma settings.

It would take hundreds of years of brute force attack alone to crack Enigma by hand, so Turing invented the Bombe machine to automate the system. The Bombe was a huge machine that was 7 feet wide, 6 feet tall, 2 feet deep, and 1 ton in weight. It also contained 12 miles of wiring and 97,000 different parts. The reason why it was that big and why it contained so many parts was because it emulated 36 Enigma Machine setting at the same time. Once the machine was switched on, each of the three rotors per machine checked on 17,500 possibilities until a match was found. Still, with the encryption strength of Enigma, the machine needed something more to achieve perfect decryption of each message.

This came in the form of multiple flaws Enigma had that Turing and his colleagues took advantage of. For one, you could not encrypt a letter as itself, so you could eliminate multiple possibilities. Another bigger flaw was that some operators sent messages with repeating patterns such as “wetterbericht”(weather report) or “Heil Hitler.” This human error eliminated even more possibilities for letter encryption.

In simplicity, it seems that the Germans defeated themselves by using predictable plain text in their messages. There is obvious irony in this, but it is important to understand that even with known plain text, it would still take years to decrypt a message by hand. The Bombe Machine helped shorten this process, while also taking advantage of German errors. In terms of

modern cryptography, the Bombe Machine helped cryptographers create better machine implementations of cryptography such as the British X Machine, an improved inspiration of Enigma, and better understanding of plaintext attacks using social engineering. Moreover, Turing's contribution is estimated to have shortened the war by 2 to 4 years. If anything is to be taken away from this short piece, it should be this contribution alone and the recognition of the possibilities cryptography can create.

Sources

- Dade, Louise. *How Enigma Machines Work*, enigma.louisedade.co.uk/howitworks.html.
- Lewis, Katy. "Bletchley Park: No longer the world's best kept secret." *BBC News*, BBC, 18 June 2014, www.bbc.com/news/uk-england-beds-bucks-herts-27808962.
- numberphile. "158,962,555,217,826,360,000 (Enigma Machine) - Numberphile." *YouTube*, YouTube, 10 Jan. 2013, www.youtube.com/watch?v=G2_Q9FoD-oQ.
- *Bombe*, www.cryptomuseum.com/crypto/bombe/.
- *Turing Bombe Simulator*, www.lysator.liu.se/~koma/turingbombe/.
- "Welcome to Py-Enigma's documentation!¶." *Welcome to Py-Enigma's documentation! — Py-Enigma 0.1 documentation*, py-enigma.readthedocs.io/en/latest/.
- "Crypto." *Practical Cryptography*, practicalcryptography.com/cryptanalysis/breaking-machine-ciphers/cryptanalysis-enigma/.