# CASE STUDY: ENCRYPTION TOOLS AND THEIR IMPACT DURING WW2

## ENIGMA [1]:

*Figure 1 THE ENIGMA MACHINE [2]*

The main source of secret communication for the Germans during World War II was the ENIGMA machine. It was invented by Arthur Scherbius in 1918. Enigma's encoding process began by typing plaintext characters into the keyboard. A current is passed through the three rotors, hits the reflector then bounces off and passes through the rotor in reverse order and illuminates a lightbulb inscribed with the appropriate letters to be written down to obtain the ciphertext. The plugboard acted like a transposition cipher, providing additional security for encrypted messages. To increase complexity, each rotor shifts its position by one place after a certain number of key presses, creating a cipher similar to the Vigenere cipher. Rings were placed on the left and center discs to determine how many keys had to be pressed before the next rotor was shifted one place. This shift in position meant that certain characters were not always encoded the same way. Attacks by frequency analysis are therefore almost impossible.

The ADFGX cipher, a cryptosystem previously used in Germany, was broken by Allied cryptographers During World War I. Germany was unaware of the work of Allied cryptographers and the German cryptographers thought they still had a secure system. It was only after the war had ended and the British Prime Minister Winston Churchill announced that his army had seized a German codebook containing a list of keywords and algorithms for finding the 5→5 grid used for encoding all German news. The cryptographer was able to read all intercepted messages from Germany. German cryptographers realized they needed a new cryptosystem that could not be compromised even if their codebook is captured.

Enigma became their Primary source for encrypting and decrypting messages. The German government made copies of the codebook and the Enigma and distributed them to the military. The codebook contained the rotor and breadboards initial settings. Every message sent started with a three-letter keyword, which was not encoded. This keyword was used to indicates the rotational position of each rotor. The next 6 letters were scrambled to include a 3-letter codeword that was repeated twice to ensure accuracy. When the target audience received the message, the operator typed the following six characters into the machine after the key to reveal the codeword. This codeword tells the operator the specific initial position of the rotor to decode the rest of the message.

The Germans thought their machines were indestructible, and it seems that was the case for some time. France was the first country to attempt to defeat the Enigma. Cryptographers thought that buying a commercial Enigma could give them insight into how the German military encrypted their messages. This

was of little use as the commercial version had different number of rotors and moreover had no plugboard. In 1931 France finally got the help it needed when Hans-Thilo Schmidt, a German working with a German cryptographer, sold the Enigma Machine documents and keys to France. The extreme number of possible settings for the Enigma that the Germans had to cooperate with Indicates that the Germans had a system that was almost impossible to break. But the Germans didn't make the most of this machine. German troops usually had rotors in the same position with each other for up to 3 months. Allied cryptographer could determine the position of the rotors and need not recalculate them for up to three more months.

In 1939 Poland knew that Germany would soon invade the country. Polish cryptographers and the government decided to hand over all the knowledge they had about Enigma and the replicas they made to France and the British government. The British government soon hired the best math, science and engineering personnel to work at the Bletchley Park facility to deciphers German messages. Alan Turing has planned to simplify Polish machinery. He believed that the machine would work more efficiently if it was built to check the expected text patterns. Many of the intercepted messages contained cilies, allowing Allied cryptographers to guess what the first three characters were decrypted by the Enigma. A cryptographer who knew this only had to check the settings to encrypt his first three letters of the suspicious key. Instead of looking at hundreds of thousands of possible settings, cryptographers need to test a few settings to determine the key. Once that is done, the cryptanalyst can replica the settings and decrypt the rest of the message. Designed by Alan Turing and known as a bombe, this machine worked by circulating hundreds of possible settings at once. Bombe rotor spins at high speed and checks All positions that encode an encrypted 3-character key into an expected 3-character key. If a possible match is found, the rotor will stop spinning.

The messages that the Allies were able to intercept resulted in several major victories that contributed to the outcome of the war.

## Bibliography

[1] K. Callahan, "The Impact of the Allied Cryptographers," 14 december 2013. [Online]. Available: https://www.gcsu.edu/. [Accessed 30 july 2022].

[2] [Online]. Available: https://www.istockphoto.com/.