How Mathematicians Helped Win WWII

The 1930s saw a reinvigorated Germany begin to re-arm under the leadership of the Nazi Party and Adolf Hitler. This included continuing to build on efforts begun in the 1920s to create secure communications. Germany had suffered significant losses to its submarine fleet in World War I (1914-1918) because of the ability of the Western allies, especially France and Great Britain, to take advantage of weaknesses in the codes and ciphers the Germans had used to try to protect the secrecy of their communications. In addition, a primary reason for the entry of the United States into the war had been the ability of the British to read a secret German diplomatic cable (the Zimmermann Telegraph). The Germans were determined to correct this problem and make sure that in any future war they would be able to pass messages amongst themselves while keeping others from being able to read those messages.

Figure 1 A four-rotor Enigma machine used by the German navy, the kind of machine Alan Turing was most concerned to solve.

The German military decided in the late 1920s to use a machine that had been built for use by businessmen and made changes to it that would make it more secure, more difficult for an enemy to take advantage of. The machine they used was called the Enigma, and it had been invented by a German engineer named Arthur Scherbius. It originally consisted of a keyboard, a display panel of letters that would light up, and a series of rotors through which electric current would pass. Depressing one of the keys on the keyboard would cause an electric current to pass through the rotors which would rotate in a predetermined fashion and then would cause one of the letters on the display panel to light up. The lit letter would be the cipher value for the letter whose key had originally been pressed.

Because the rotors moved each time a key was depressed, a repeated letter would not be converted to the same cipher letter. For example, the first time an "a" was used it might convert to an "n" and the next time an "a" was used it might convert to an "h." As we will see, the number of possible variations the machine could produce was very large.

The German military made the Enigma machine more challenging by adding a plug board and by increasing the number of rotors they could choose from to operate the machine (there were usually three rotors in the machine at a time, except for the German Navy machines which used four, but there were as many as eight rotors those three or four could be chosen from). These modifications made the machine apparently very formidable. The theoretical number of possible configurations the machine could generate was 3x10 to the 114th power. As a matter of perspective, there are only about 3x10 to the 81st power atoms estimated to be in the entire observable universe.

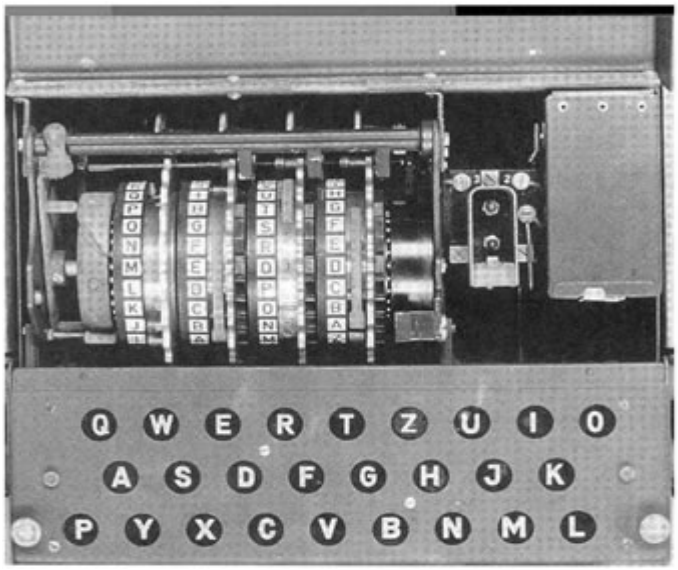

Figure 2 A view of the inside of a German naval Enigma, showing the four rotors in place.

The countries most concerned with possible attacks by the German military turned the problem of solving messages sent using this machine over to mathematicians. The Poles, the French, and the British all began to work against the Enigma machine, but it was a Polish mathematician, Marian Rejewski, who made the initial breakthroughs. He applied the permutation theory and, after numerous failed attempts, was able to determine the electric wiring of each of the rotors used by the German military in the 1930s. He was helped by the fact that German operators did not always use the machine to its full capability, thereby introducing weaknesses that could be used against it. The Poles had made a critical first step, but this did not solve the puzzle posed by the ability the machine gave the Germans to change the position of each rotor, to alter the way the rotors shifted each other, and to vary the way the plug board was used.

Rejewski was then joined by two other Polish mathematicians, Henryk Zygalski and Jerzy Rozycki, and together they were able to overcome many of these difficulties and could read some German Army and Air Force messages by the time World War II began in 1939. The Polish Army was quickly overrun by the Germans, however, and the Poles who worked on the problem fled from Poland through Southern Europe and made their way to France by early 1940. There they continued their work with the French until France itself was defeated by the Germans in June 1940. Many of the Poles then fled through Spain and Portugal and went to Great Britain where they served out the war continuing the fight against their German enemy. They passed on what they had learned and accomplished, making it possible for British mathematicians to take up their work.

The British, led by Alan Turing, built on the initial Polish successes, but faced a more serious challenge. Just before the war began, the Germans increased the number of rotors they could choose from to select the three they would use each day, increasing the possible variations that had to be dealt with. Turing is considered one of the two or

three best mathematicians of the twentieth century, and spent the entire war working in cryptanalysis. He and his colleagues used their mathematical skills to improve on a machine the Poles had first built called a "bombe" that enabled the British to compare, in a relatively rapid fashion, the numerous possible keys with portions of messages they thought the Germans were sending. Success was neither total nor assured, but the British and later the Americans were able to read enough German messages to provide great assistance to their armed forces and helped them defeat Nazi Germany.

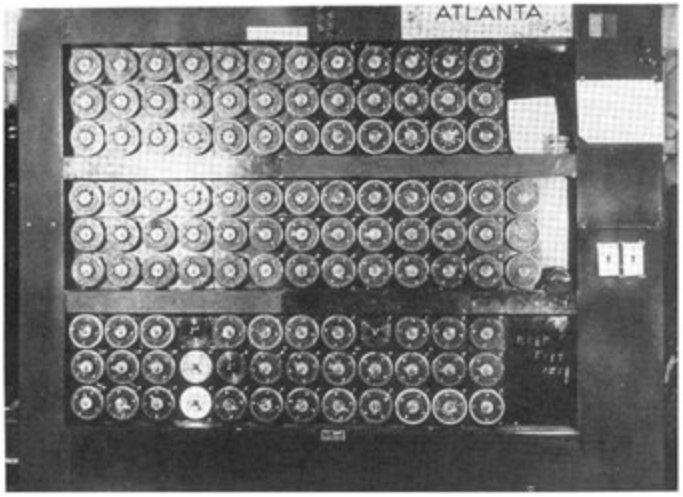

Figure 3 Front view of the British bombe.

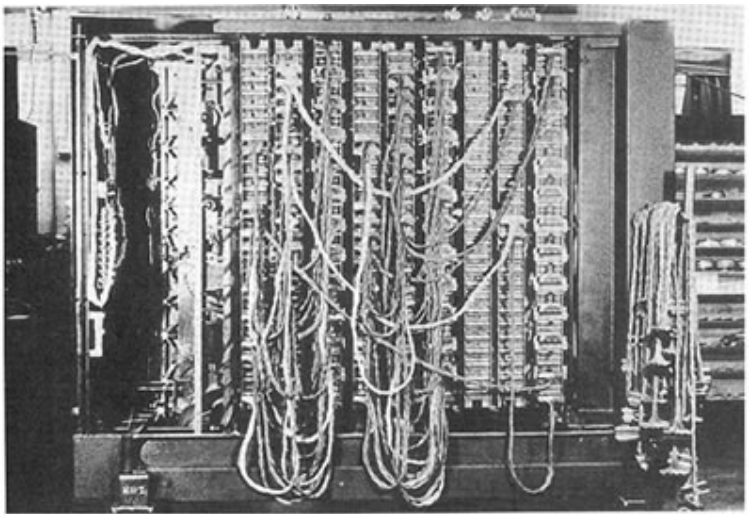
Figure 4 Back view of the British bombe showing the mass of cables necessary for the machine to work.

Figure 5 Adolf Hitler receiving the salute of German troops in Warsaw following their conquest of Poland.

Figure 6 Arthur Scherbius, the German engineer who invented the Enigma machine.

Figure 7 Alan Turing, the British mathematician who devised the bombe to recover Enigma keys.

Figure 8 U.S. Army unit moving through captured German town.