

ACADEMIA

XYZ

Prof. Włodzimierz Zawadzki

Institute of Physics, Polish Academy of Sciences
zawad@ifpan.edu.pl



Mathematicians are important, and not just in wartime.

This story begins sometime in the early 1930s, when the Poles and the French first took an interest in breaking the code generated by the Enigma encryption machines. The Enigma was a German-made electro-mechanical device that looked a bit like a typewriter with little lights, and prior to WWII they were available commercially. The decision to crack the Enigma code proved far-sighted when the machines underwent a complex and classified redesign for military purposes in the run-up to the war.

Codebreaking challenges had earlier been handled by linguists, but the Enigma's rotor-encrypted codes required codebreakers with a mathematical background. The Polish Cipher Bureau, an intelligence outfit located near Warsaw, set up a task force consisting of Marian Rejewski, Henryk Zygalski and Jerzy Różycki. Gustave Bertrand, an intelligence officer working for France's *Section du Chiffre*, kept the Polish team fed with spy documents from Germany. Together, they formed the seed of the "XZ" community of intelligence personnel working against the Nazis (the letters were a classified acronym meaning Paris and Warsaw). Throughout the 1930s the Germans kept perfecting the Enigma design, with Polish codebreakers playing catch-up. In 1938, Rejewski constructed what he called "the bomb": the first machine capable of cracking the new Enigma code. In late July 1939, a month before the start of the war, members of the British and French intelligence arrived in a Polish village called Pyry (now part of Warsaw) for a secret meeting in which the Polish team shared their progress with the Allies. Ironically, the meeting was at first hampered by communication problems: the Polish team did not speak English, and Britain's chief codebreaker Alfred "Dilly" Knox was skeptical. However, Knox soon had a change of heart, and a "Y" was added to the acronym to reflect British participation in the Enigma project.

Following the outbreak of the war and the military defeats of Poland and France, the British were left standing alone in the face of the Nazi threat in Europe. Breaking the military codes was now a top war priority. A dedicated site was created at Bletchley Park to decrypt enemy messages intercepted on different fronts. One of the people working at Bletchley Park was Alan Turing, who would later play a major role in

developing programmable computers. Knox informed Turing about the progress made by the Poles, and Turing built a sophisticated machine of his own that was capable of cracking the increasingly complex Wehrmacht codes. In a nod to the Polish pioneers, Turing too called his device "the bomb." Despite the urgings of British intelligence, Bertrand was reluctant to get the Polish team out of Nazi-occupied France and into Bletchley Park. The team ended up in southern France and, at one point, in North Africa. Despite their continuing insights, the Polish team's direct contribution to the breaking of the Enigma code diminished.

When the United States joined the war, one of the most difficult aspects of Enigma decryption focused on the communications of the German U-boat fleet, which harassed American supply convoys crossing the North Atlantic on their way to Britain. At stake were not only American lives, but also hundreds of thousands of tons of matériel and other supplies Britain needed to survive in isolation from the continent. Success in the war itself hinged on the success of the project. The Americans joined the effort of developing Turing's machine further, and the American engineer Joe Desch incorporated some key electronic elements into the design. World War II was also a war of codes, and the Poles were the first to fight on that front. The Polish contribution is now believed to have shaved off at least a whole year from the time it took the Allies to crack the Enigma code, an opinion recently corroborated by Professor Dermot Turing, a nephew of the great Alan.

After the war, the lives of the Enigma codebreakers took very different paths. Alan Turing was pushed to suicide when he faced criminal prosecution as a homosexual in England. Gustave Bertrand was decorated in France for his contribution to the Enigma project. Marian Rejewski returned to Poland, Henryk Zygalski stayed in Great Britain, and Jerzy Różycki died during the war when a French ship he was travelling on was sunk. A memorial in the Polish city of Poznań celebrates the achievements of Rejewski, Zygalski, and Różycki. There is also a statue of Rejewski in his native town of Bydgoszcz. It's a pity statues are not often dedicated to mathematicians. They are important, and not just in wartime. ■