

Alan Turing and World War II Codebreaking



Alan Turing (British mathematician; 1912 - 1954) was one of the twentieth century's most important mathematicians. He did critical work in logic and in the development of modern computer science. Additionally, he played a critical role in the intelligence efforts during the Second World War. In fact, his efforts prompted the mathematician Peter Hilton to remark: I.J. Good, a wartime colleague and friend, has aptly remarked that it is fortunate that the authorities did not know during the war that [Alan] Turing was a homosexual; otherwise, the Allies might have lost the war.¹

Indeed, when his homosexuality was discovered after the war he was subjected to house arrest and a variety of medical "treatments." Soon afterward this highly decorated war hero committed suicide.

1. Find out more about the life and mathematical accomplishments of Alan Turing. Write a brief, two- to three-page biographical essay, addressed to fellow students, that describes your findings.

Polish Mathematicians and World War II Codebreaking

Alan Turing's contributions to mathematics visionary and greatly ahead of his time. His work for the Allies' code breaking efforts were part of a larger effort in which many mathematicians played important roles.

The focus of most of the code breaking work was to discover the secret workings of the German *Enigma machine* a mechanical encryption/decryption machine which worked with a number of rotors and gears. The working of these machines can be described as *permutations*.

¹ Quoted in "Cryptanalysis in World War II – and Mathematics Education," by Peter Hilton, *Mathematics Teacher*, Vol. 77, Oct. 1984, pp. 548-52.



Four rotor Enigma machine (right) and Enigma plugboard (left).

Some of the simplest Enigma machines were decrypted as early as 1932 by **Marian Adam Rejewski** (Polish mathematician; 1905 - 1980).

The work of the Allied mathematicians is celebrated in the Bletchley Park Museum not far from London, England and at the National Cryptologic Museum in Annapolis Junction, Maryland. Additionally, enormous amounts of information about these topics is available online, in print, and in documentaries. There are also numerous novels and movies that present historically-based fiction related to the actual events and accomplishments.

Navajo Code Talkers and World War II Encryption

While the code breaking focus in the war in the Atlantic was on the German Enigma machine, the war in the Pacific had its own important links to encryption. Allied intelligence agents were somewhat successful at breaking Japanese secret codes. The outcome at the Battle of Midway, one of the changing points in the war, was dramatically impacted by U.S. intelligence success in codebreaking.

In sharp contrast, the Axis forces had much less success at deciphering Allied codes. One reason was that U.S. forces encrypted some of their most important messages first by having native Americans, most notably Navajos, translate the messages into their native language first before they were then encrypted using mathematical algorithms. These *Navajo Code Talkers*, as the most well-known group were called, had been secretly enlisted in the Marine's intelligence efforts. Congressional Gold Medals were awarded to the 29 Navajo Code Talkers in December, 2000.

The story of the Navajo Code Talkers serves as the basis for the major motion picture *Windtalkers* (MGM, 2002).

2. Find out more about the Navajo Code Talkers and their role in U.S. intelligence efforts in the Second World War. Write a brief, two- to three-page biographical essay, addressed to fellow students, that describes your findings.