The Royal Navy captured German U-boat U-110 on May 9, 1941 in the North Atlantic, recovering an Enigma machine, its cipher keys, and code books that allowed codebreakers to read German signal traffic during World War II.

The Enigma machine was an electro-mechanical rotor cipher machine used by the German navy to encrypt and decrypt messages passing from shore to ships at sea. They considered their codes unbreakable and felt safe in exchanging relatively large volumes of radio messages.

On May 9, British destroyers HMS Bulldog, HMS Broadway, and HMS Aubrietia attacked U-110, embarking on what was later called Operation Primrose. The U-boat was seriously damaged and its crew surrendered when it was thought to be sinking. Fifteen men from the boat were killed and 32 were captured. The capture of the U-110 was successfully kept a secret as the boat sunk the next day. The Germans continued to use their codes, assuming their confidential material sank as well.

The recovered materials were taken to Bletchley Park in England, where cryptographers, including computer pioneer Alan Turing, succeeded in breaking the naval code. The codes allowed the U-boat traffic to be read for several weeks, until the keys ran out. Throughout 1941, the British were able to plot the positions of U-boat patrol lines and route convoys around them. Merchant ship losses dropped by over two-thirds in July 1941, and remained low until November. The codes also allowed the British to become familiar with the messages which helped in breaking the new keys.

The machine used by the German army was decrypted as early as 1932 by Polish cryptographers, who later passed their methodology along to the British and French. Breaking the naval code gave the British an advantage in the Battle of the Atlantic.

Naval Enigma signals used different ciphers, each with its own daily key (rotor order, ring settings, plugboard connections, and ground setting). The principal cipher was "Heimisch" for U-boats and surface ships in home waters, including the Atlantic.

The Enigma machine had been around since the early 1920s and is most closely associated with Nazi Germany. It was a combination of mechanical and electrical subsystems including a keyboard,
rotating disks called rotors arranged adjacently along a spindle, and stepping components to turn the rotors when keys were pressed. The parts form a varying electrical circuit, so that pressing the keys completed a circuit with current flowing through the components and lighting one of the display lamps to indicate a letter.

Related articles:

- Design hindsight from the tail-gunner position of a WWII bomber, Part one
- Mechanical analog computers in WWII naval gun directors
- German rocket is 1st to reach space, October 3, 1942
- Cryptography and Network Security—The basics—Part I
- Code Breakers Remembered
- Turing Machine paper is published, November 12, 1937
- Alan Turing, computer science pioneer, is born, June 23, 1912

For more moments in tech history, see this blog. EDN strives to be historically accurate with these postings. Should you see an error, please notify us.

Editor's note: This article was originally posted on May 9, 2013 and edited on May 9, 2019.