Library and Information Services

Information sheet no 100

Enigma Machine

The Enigma machine was invented by the Germans in 1918. It was first patented in 1919 and adopted by the German Navy in 1926, the German Army in 1928 and the German Air Force in 1935. It was also used by the railways and other government departments. From then until 1939, and throughout the war, successive refinements were made to the Enigma machine.

The Enigma is an electro-mechanical device which scrambles a plain text message into a ciphered text. It was used solely to encipher and decipher messages. It consisted of a keyboard of 26 letters in the pattern of the normal German typewriter but with no keys for numerals or punctuation. Behind the keyboard was a lampboard made up of 26 small circular windows each bearing a letter in the same pattern as the keyboard that could light up one at a time. Behind the lampboard is the scrambler unit consisting of a fixed wheel at each end and a central space for three rotating wheels. If a key was pressed on the keyboard any other letter could light up and the sequence would only repeat itself after 16,900 (26x25x26) keyings when the inner mechanism returned to the same position. Messages were limited to a maximum of 250 letters to avoid this recurrence which might have otherwise helped the British code-breakers. Thus potentially the number of ciphertext alphabets was vast – and the German military authorities believed in the absolute security of this cipher system.

A secret base had been set up at Bletchley Park, a stately home 40 miles north of London, to attempt to intercept and break enemy military codes. The code breakers were scientists, mathematicians and chess-masters and worked on various projects. The code breakers of Hut Six made a great breakthrough on 22 May 1940 when they broke the Luftwaffe cipher of the Enigma machine. They succeeded by using the first British built Bombe, an electro-mechanical device which could do hundreds of computations every minute (the forerunner of a computer), to break the Luftwaffe's 'Red' key. This meant that all the Luftwaffe's operational and administrative traffic could be read despite the added security devices built into the Enigmas in preparation for the assault on the west. A year later the code breakers received a further boost to their work.

On 9 May 1941, the Royal Naval ship HMS *Bulldog* forced an enemy submarine, *U110*, to surrender south of Greenland. The U-boat's captain, Lieutenant-Commander Lemp, tried to destroy *U110* - which had already been depth-charged by HMS *Aubretia* – but a naval party was able to board the submarine and seize the submarine's Enigma cipher machine and code-books. This enabled the British code-breakers to decipher signals sent between the U-boats and their HQ near Paris. With this information, convoys could avoid U-boat concentrations in the Atlantic. The Germans then developed a modified Enigma machine called M4 and used an additional rotor. This baffled the code-breakers from the beginning of 1942. On 30 October 1942, another enemy submarine, *U559*, was scuttled by destroyers 70 miles off Egypt. While it was sinking, Lt Tony Fasson and Able Seaman Colin Grazier from HMS *Petard* seized two vital code books. However, Fasson and Grazier were unable to escape before the U-boat sank but had managed to pass the books to Canteen Assistant Tommy Brown. For their actions, Fasson and Grazier received the George Cross; Brown received the George Medal, the youngest recipient of this decoration, as it was then discovered

Information sheet no 100

that he had been underage when he had first joined up. They did not receive the Victoria Cross as they had not acted in the face of the enemy.

It took three weeks for the code books to reach Bletchley Park. On Sunday 13 December 1942, Bletchley Park code-breakers finally cracked the cipher used by Admiral Donitz to communicate with his U-boats in the Atlantic. By using the fourth rotor in the neutral position, it made the M4 Enigma machine equivalent to the three rotor Enigma machine used by shore weather stations. The code-breakers learned that the four-letter indicators for regular U-boat messages were the same as the three-letter indicators for weather messages that same day, except for an extra letter. Therefore once a daily key was found for a weather message, the fourth rotor had to be tested only in 26 positions (the number of keys the Enigma machine had) to find the full four letter key. This gave Hut Eight code-breakers at Bletchley Park little difficulty. Later the same day, solutions of the four rotor Enigma U-boat key, called Shark, started to emerge. In the afternoon, Hut Eight telephoned the Submarine Tracking Room to report the breakthrough. Within an hour of this news, the first intercept came through and revealed the position of fifteen U-boats in the Atlantic. Other intercepts arrived in an endless stream until the early hours of the next morning. The breaking of the code enabled the Admiralty's Submarine Tracking Room to once again route British convoys away from German U-boat concentrations, and halved the number of British vessels sunk in January/February 1943.

The Enigma machine on display at the National Museum of the Royal Navy is a type M4 machine. It was probably used by the Norwegian Harbour Police, but is missing the reflector. The first rotor, therefore, has been adapted to enable it to do the reflector's job. This makes the machine an unusual specimen.