Breaking Germany's Enigma Code

By Andrew Lycett (Obtained from the Internet)

Germany's armed forces believed their Enigma-encrypted communications were impenetrable to the Allies. But thousands of codebreakers - based in wooden huts at Britain's Bletchley Park - had other ideas. This author investigates how successful they were, and the difference they made to the war effort.

The Enigma "typewriter"

In 2001, the release of the feature film *Enigma* sparked great interest in the tweedy world of the boffins who broke Nazi Germany's secret wartime communications codes. But not all who watched Dougray Scott in the film's lead role realised that the title referred to a machine like a typewriter, which encrypted secret messages.

Fewer people still knew that this piece of spook hardware was invented by a German (based on an idea by a Dutchman), that information about it was leaked to the French, and that it was first reconstructed by a Pole, before it was offered to Britain's codebreakers as a way of deciphering German signals traffic during World War II. As a result of the information gained through this device, it has been claimed, hostilities between Germany and the Allied forces were curtailed by two years.

The importance of signals intelligence became evident during World War I, as staff in the British Admiralty's Room 40, under Captain Reginald "Blinker" Hall, worked at intercepting German communications.

Among these, famously, was the Zimmermann telegram - a message from the German foreign minister to his ambassador in Mexico City informing him of plans to invade the United States. On being notified of these plans, officials in Washington were understandably perturbed, and hastened to affect the entry of the US into the war.

Stealing secrets

After the Treaty of Versailles in 1919, the German defence establishment was eager to improve its compromised communications system, and recognised the potential of a signalling device that had originally been made for the business market.

Dr Arthur Scherbius had developed his "Enigma" machine, capable of transcribing coded information, in the hope of interesting commercial companies in secure communications. In 1923 he set up his Chiffriermaschinen Aktiengesellschaft (Cipher Machines Corporation) in Berlin to manufacture this product, and within three years the German navy was producing its own version, followed in 1928 by the army and in 1933 by the air force.

Enigma allowed an operator to type in a message, then scramble it by means of three to five notched wheels, or rotors, which displayed different letters of the alphabet. The receiver needed to know the exact settings of these rotors in order to reconstitute the coded text. Over the years the basic machine became more complicated, as German code experts added plugs with electronic circuits.

Britain and her allies first understood the problems posed by this machine in 1931, when a German spy, Hans Thilo Schmidt, allowed his French spymasters to photograph stolen Enigma operating manuals, although neither French nor British cryptanalysts could at first make headway in breaking the Enigma cipher.

It was only after they had handed over details to the Polish Cipher Bureau that progress was made. Helped by its closer links to the German engineering industry, the Poles managed to reconstruct an Enigma machine, complete with internal wiring, and to read the Wehrmacht's messages between 1933 and 1938.

Ultra intelligence

With German invasion imminent in 1939, the Poles opted to share their secrets with the British, and Britain's Government Code and Cipher School (GC&CS) at Bletchley Park, Buckinghamshire, became the centre for Allied efforts to keep up with dramatic war-induced changes in Enigma output.

A host of top mathematicians and general problem-solvers was recruited, and a bank of early computers, known as “bombes,” was built - to work out the vast number of permutations in Enigma settings.

The Germans were convinced that Enigma output could not be broken, so they used the machine for all sorts of communications - on the battlefield, at sea, in the sky and, significantly, within its secret services. The British described any intelligence gained from Enigma as “Ultra,” and considered it top secret.

Only a select few commanders were made aware of the full significance of Ultra, and it was mostly used only sparingly, to prevent the Germans thinking their ciphers had been broken.

Despite providing some otherwise inaccessible information, it was some time before Ultra made any significant contribution to the war effort. Although, thanks to the information from the Poles, the British had learned to read parts of the Wehrmacht’s signals traffic, regular decrypts only became possible in the Norwegian campaign - and then they were of marginal operational use.

Within a wider context, two Luftwaffe ciphers were broken, but the information gained was of little effective use. Similarly, Ultra’s role in the Battle of Britain was limited: better grade intelligence came from prisoners, captured documents and improved air reconnaissance.

Only in 1941 did Enigma decrypts pay dividends. In the spring they provided evidence of a German military build-up prior to the invasion of Greece, although the Allies did not have a large enough military force to exploit this breakthrough.

In March, Bletchley’s reading of the Italian navy’s Enigma material helped Admiral Cunningham’s Mediterranean fleet defeat the Italians at the Battle of Matapan. And in the autumn, the cryptanalysts broke ciphers used by Marshal Rommel’s Panzer army, both within its own units and in communications with Rome and Berlin, giving the Allies an important advantage in North Africa.

Pinching the codes

By then the greatest threat to the Allied war effort came from attacks on their ship convoys in the North Atlantic. As a result, Bletchley’s resources were concentrated on breaking Enigma codes used by German U-boats in this sphere of war. If the Allies could find out in advance where U-boats were hunting, they could direct their ships, carrying crucial supplies from North America, away from these danger zones.

So began one of the most exciting periods of Enigma code-breaking. Even in 1940 Bletchley had had some success in breaking Enigma keys used by the German navy.

It soon became clear that the best way of keeping up with rapid changes in ciphers and related technology was to capture Enigma machines and code-books on board German vessels.

In the Admiralty, where the Operational Intelligence Centre (OIC) was a leading user of Ultra, Commander Ian Fleming, Personal Assistant to the Director of Naval Intelligence, showed his talent for fantastical plots when he suggested a plan (known as Operation Ruthless) to crash-land a captured German plane in the English channel, and to overpower the patrol boat that came to rescue its supposed survivors, thereby gaining access to Enigma materials. The plan was never implemented.

A break-through came in March 1941, however, when the German trawler Krebs was captured off Norway, complete with two Enigma machines and the Naval Enigma settings list for the previous month. This allowed German Naval Enigma to be read, albeit with some delay, in April, by codebreakers at Bletchley.

Around this time, Harry Hinsley, a Bletchley codebreaker, suggested that German weather and supply ships, as well as war ships, probably carried Naval Enigma details. This idea was proved correct when, in May 1941, the German weather ship München was attacked and found with Enigma code-books for June on board.

The capture of the supply ship Gedania and weather ship Lauenburg in June yielded codebooks for the following month, and opened the way to the reading of Naval Enigma almost concurrently with events.

The ambush of three German U-boats off Cape Verde in September, however, coupled with a dramatic fall in the number of Allied ships sunk in the North Atlantic, led the German Admiral Karl Dönitz to question if the navy’s cipher had been compromised.

Although he was dissuaded by his experts, the Germans redoubled their efforts to tighten Enigma's security, and the Bletchley Park codebreakers, realising what they were up against, wrote to British Prime Minster Winston Churchill complaining that they were not being given enough resources. Churchill replied with a famous "Action This Day" memorandum: "Make sure they have all they want on extreme priority and report to me that this had been done."

Shortening the war

In February 1942 the Germans hit back by introducing a new fourth wheel (multiplying the number of settings another 26 times) into their Naval Enigma machines. The resulting "net" was known to the Germans as "Triton" and to the British as "Shark." For almost a year Bletchley could make no inroads into Shark, and Allied losses in the Atlantic again increased alarmingly.

In December 1942 Shark was broken, but German innovations meant that the Allies had to wait until August the following year before Naval Enigma was regularly read again. By then the Americans were active combatants, providing much-needed computer power to Bletchley.

By D-Day in June 1944, Ultra was no longer so important. But still no one wanted the Germans to sense that Enigma was being read. When, a few days before the Normandy landings, an American task force captured a German U-boat with its Enigma keys, Admiral Ernest King, US Commander in Chief of the Atlantic Fleet, threatened to court-martial the officer in charge for endangering "Operation Overlord," as the plan for the D-Day landings was known.

By how much did Ultra intelligence, gained from reading Enigma ciphers, shorten the war? Harry Hinsley, based at Bletchley during the war, suggests it was a significant asset. If it did not keep Rommel out of Egypt in 1941, it certainly did so the following year, by preventing him exploiting his victory at Gazala.

As General Alexander put it, "The knowledge not only of the enemy's precise strength and disposition, but also how, when and where he intends to carry out his operations brought a new dimension to the prosecution of the war."

The loss of Egypt in 1942 would have set back the re-conquest of North Africa and upset the timetable for the invasion of France. According to Hinsley, Overlord would probably have been deferred until 1946.

But by then the Germans might have hit back with V-weapons and worse. Enigma successes always needed complementing with other intelligence material, but the fact that the Allies kept Enigma secret until 1974 shows how much it meant to them.

enigma machines. okay, that machine on the right, it looks a bit like an enigma machine. but there is a jumble of wires at the back. that's the plug board. those of you who are sitting in the front row, can you see that keyboard is all wrong. it's in alphabetical order. it's not in q, w, e, r, t, z, whatever, i spoke american correctly. i said "z," not zed. there may be some canadians in the audience who would understand. okay. so that is an enigma machine. it's a polish fake enigma machine. it's not a fake. it's a reverse engineered analog if you like o The Germans had been using Enigma cyphers to scramble their intelligence and military communications and thought Enigma was unbreakable. But work by master codebreakers at Bletchley Park, a secret installation about 45 minutes outside London, eventually proved the Germans wrong. At the same time, the Nazi high command was sending coded messages using a device called the Lorenz. To solve that, Bletchley Park's code breakers came up with a machine called Colossus (a reconstruction is pictured here). CNET reporter Daniel Terdiman visited Bletchley Park as part of Road Trip 2011 . And last ye Breaking Germany's Enigma Code. By Andrew Lycett Last updated 2011-02-17. Germany's armed forces believed their Enigma-encrypted communications were impenetrable to the Allies. But thousands of codebreakers - based in wooden huts at Britain's Bletchley Park - had other ideas. Andrew Lycett investigates how successful they were, and the difference they made to the war effort.Â In 2001, the release of the feature film Enigma sparked great interest in the tweedy world of the boffins who broke Nazi Germany's secret wartime communications codes. But not all who watched Dougray Scott in the film's lead role realised that the title referred to a machine like a typewriter, which encrypted secret messages. The Enigma code was first broken by the Poles, under the leadership of mathematician Marian Rejewski, in the early 1930s. In 1939, with the growing likelihood of a German invasion, the.Â Enigma cipher machine of World War IIThe German navy employed various versions of the Enigma cipher machine during the war, including this four-rotor model.