BREAKING NAVAL ENIGMA (DOLPHIN AND SHARK)

by Ralph Erskine

This note outlines the methods used by BP's Hut 8 to break naval Enigma. There can be little doubt that the naval Enigma decrypts helped to shorten the war, although it is not possible to give a precise period.

The German Navy's three-rotor Enigma machine (M3) was identical to the model used by the German Army and Air Force, but it was supplied with three additional rotors, VI, VII and VIII, which were reserved exclusively for naval use. However, the German Navy also employed codebooks, which shortened signals as a precaution against shore high-frequency direction-finding, and some manual ciphers. The codebooks most often used were the Kurzsignalheft (short signal book) for reports such as sighting convoys, and the Wetterkurzschlüssel (weather short signal book) for weather reports. The relevant codegroups were super-enciphered on Enigma before being transmitted by radio.

Naval Enigma signals used a number of different ciphers, each with its own daily key (rotor order, ring settings, plugboard connections and basic rotor setting). The principal cipher was Heimisch (known to BP as Dolphin), for U-boats and surface ships in home waters, including the Atlantic. At least 14 other naval Enigma ciphers were used during the war.

Most ciphers had Allgemein (general) and Offizier keys. Offizier signals were first enciphered using the plugboard connections from monthly Offizier keylists. The complete message was then enciphered a second time using the Allgemein key. A few ciphers also had Stab (Staff) keys, which were also doubly enciphered, but had their own special settings. Although BP's Hut 8, which was responsible for the attack on naval Enigma, often broke Offizier signals, albeit often a week or more later, it seldom, if ever, solved Stab.

BP received an Enigma machine and rotors I to V from the Poles in August 1939. Marian Rejewski, the Polish cryptanalyst, had reconstructed the wiring of those rotors using advanced mathematics. A statement in a talk last year that the Poles borrowed a Wehrmacht machine does the Poles a considerable injustice - the borrowed machine was the completely different commercial model. The British recovered rotors VI and VII from the crew of U-33 on 12 February 1940, while rotor VIII was captured in August 1940 - unfortunately no one now knows how or where. After that, Hut 8 had all eight rotors, but it still could not break naval Enigma.

In June and July 1940, using some cleartext and cipher text captured from the patrol boat, VP 26, Hut 8 had solved the naval Enigma traffic for six days in April, with the aid of the first bombe (a high speed key-finding aid). That bombe, which was Alan Turing's brainchild, was much slower than the bombes with the “diagonal board” invented by Gordon Welchman. The improved bombe, with the board, came into service from September on. The electro-mechanical bombes were not computers or even forerunners of the computer, since they did not have anything remotely resembling a computer's internal architecture.

Hut 8 faced three main problems in trying to break naval Enigma, even after the advanced bombes entered service-

> the system for indicating the message key (the rotor starting position for the specific signal) was “operator proof” in that it was a book system, which did not depend upon an operator selecting the message key;

the Navy's eight rotors could be arranged in 336 different ways (8x7x6) and not merely 60 (5x4x3) as with Army or Air Force Enigma. A bombe run using all the rotor order combinations would therefore take over five times longer for naval Enigma than Air Force Enigma - and bombes were always in very scarce supply until large numbers of US Navy bombes became operational in the autumn of 1943;

"cribs" (probable plain text, from which bombe menus were derived) were almost non-existent.

In early 1941, with the help of captures from a commando raid in the Lofotens, Hut 8 broke some naval Enigma for February and April. But few, if any, of the decrypts were available in time for them to be operationally useful to the Admiralty's OIC.

Hut 8 was not able to read the Dolphin traffic without delay until June and July 1941. It did so using keys captured in specially planned "snatch" operations from the weather ships *München* and *Lauenburg*. The resulting intelligence at last enabled the OIC to re-route many convoys to evade the few U-boats (about 20) then in the North Atlantic. Re-routeing convoys on the basis of Ultra (or "special intelligence") saved many lives and hundreds of thousands of tons of vital shipping, although one assessment that 1.5 to 2 million tons were saved in the second half of 1941 is over-simplistic.

The June and July decrypts gave Hut 8 enough insight into the traffic to break Dolphin cryptanalytically from the beginning of August 1941. In finding Dolphin keys, BP was helped because the order in which the rotors were inserted in the machine changed only every two days. On the second day, a bombe run on the first day's rotor order would therefore find the second day's settings in under 20 minutes - if a crib for a bombe menu was available. This halved BP's work on the naval keys, saving it a considerable amount of precious bombe time. The capture of indicator books from U-110 on 9 May 1941 also greatly assisted in developing a method ("Banburismus") of working out which rotor was the "fast" rotor in the right hand slot in the machine, which much reduced the number of bombe runs required.

Without cribs, the bombes were useless. Although in many respects the Kriegsmarine used Enigma more carefully than the other services, some units were not issued with Enigma. Some messages were therefore enciphered using manual systems as well as Enigma. Decrypts of the hand-enciphered signals provided cribs if the same signals were enciphered on Enigma.

Sometimes minelaying operations (known as "Gardening") were carried out by the Royal Air Force in order to afford Hut 8 cribs. The Germans had to send signals about the re-opening of sealanes after they had been swept for mines. The signals about the cleared channels were often sent in naval Enigma and a manual cipher known as the Werftschlüssel ("dockyard cipher"). When BP broke the Werftschlüssel, Hut 8 had plaintext if there was an identical Enigma signal. Without help from the section in BP's Hut 4 which solved the Werftschlüssel, there would have been much less intelligence from Dolphin.

Manual ciphers broken by BP's weather subsection, based in Hut 10, provided the other main source of cribs. Short weather signals were transmitted by Atlantic U-boats as an essential part of the German war effort. The signals were encoded on the Wetterkurzschlüssel before encipherment on Enigma. From February 1941 on, Hut 10 broke the naval meteorological cipher, which used the U-boats' reports. In early May 1941, BP received a copy of the 1940 edition of the Wetterkurzschlüssel from *München*. Hut 8 could now reconstruct the exact text of the U-boats' encoded weather signals - and so had a second source of cribs.

BP suffered a massive reverse on 1 February 1942 when a new Enigma machine (M4) came into service on Triton (codenamed Shark by BP), a special cipher for the Atlantic and Mediterranean U-boats. Although BP had found the wiring of the new rotor in M4 in December 1941, the combination of M4, a separate cipher (Shark) and the introduction of a second edition of the Wetterkurzschlüssel proved devastating. Deprived of cribs, BP became blind against Shark.

Fortunately, M4 was not a true four-rotor machine. The fourth rotor (beta) was the right-hand half of a split reflector and was not interchangeable with rotors I to VIII. Beta could be set as part of the message key, giving M4 the equivalent of 26 different reflectors, but M4's rotors could still only be mixed in 336 (8x7x6) different ways - not 3,024 (9x8x7x6). But without the Wetterkurzschlüssel cribs, Hut could not attack Shark.

However, at one setting of beta, M4 was completely compatible with M3, which was M4's undoing. Eventually, the second edition of the Wetterkurzschlüssel was seized from U-559 on 30 October 1942, before it sank near Port Said. After hundreds of bombe runs, Hut 8 found that beta was at neutral when enciphering the weather reports: M4 was being used only in M3 mode. A three-rotor bombe run on, say, 60 rotor combinations would therefore take only about 17 hours instead of the 442 hours (18 days) it would have required if M4 had used its full potential.

On 13 December 1942, BP sent teleprints to the OIC setting out the positions of over 12 Atlantic U-boats as established from Shark weather signals for early December. Hut 8 had penetrated M4 Shark with the help of the met broadcasts broken by Hut 10. The subsequent intelligence from Shark, although sometimes badly delayed, undoubtedly played a critical part in the Battle of the Atlantic, probably helping to save from 500,000 to 750,000 tons of shipping in December 1942 and January 1943 alone.

Hut 8's use of the Wetterkurzschlüssel against Triton was to be short-lived. A 3rd edition of the weather short signal book came into operation on 10 March 1943 - again depriving BP of Shark cribs. BP had feared that the change would blind it for several months, but by using short signal sighting reports (made by U-boats in contact with convoys and encoded from the Kurzsignalheft) as cribs, Hut 8 re-entered Shark again on 19 March and broke it for 90 out of the next 112 days before 30 June. The Kurzsignalheft short sighting reports also used M4 in M3 mode - and U-559 had yielded a copy of the Kurzsignalheft.

British and US Navy four-rotor bombes entered service in June and August 1943, respectively, but some July and August keys still took up to 26 days to solve. However, from September on, Shark was generally broken within 24 hours, although doing so was never plain sailing. At the end of 1943, work on Shark was transferred to the US Navy's Op-20-G codebreaking unit in Nebraska Avenue, Washington, because the US Navy had so many bombes (50 in operation by mid-November, with a further 30 installed), and they were more reliable than the British model.

Hut 8's attack on naval Enigma was led by Hugh Alexander, with his best known colleague probably being the mathematical genius Alan Turing (called “the Prof.” by his colleagues, although he was not a professor). Others included Jack Good, Leslie Yoxall and Shaun Wylie. When decrypts became available, they were translated by Hut 4, which then sent their full text by teleprinter to the Admiralty's Operational Intelligence Centre (OIC) in London. Unlike the other service departments, the Admiralty received the decrypts themselves, and not mere summaries.

The main role for Ultra from naval Enigma was probably in the re-routeing of convoys, but it had, of course, many other uses. Ultra helped in the sinking of the *Scharnhorst* in

December 1943. Armed raiders, such as *Atlantis* were tracked down and sunk with its assistance. And the US Navy employed Ultra offensively in 1943 in its many sinkings of the important U-tankers, which applied a multiplier effect to the U-boats by refuelling them at sea.

While the work of many people at BP and elsewhere was of vital importance in breaking of naval Enigma, it required something approaching a minor miracle before Shark succumbed. Without the bravery of Lieutenant Anthony Fasson, Able Seaman Colin Grazier and 16 year-old Tommy Brown in retrieving the Wetterkurzschlüssel and Kurzsignalheft from U-559, Shark could not have been broken before four-rotor bombes came into service in June 1943 - if then. Tony Fasson and Colin Grazier were posthumously awarded the George Cross, and Tommy Brown (who survived) received the George Medal. Without their bravery, Shark would not have been broken for many months, if at all. The Allies would not then have established naval supremacy in the Atlantic until the second half of 1943 at the earliest and the invasion of Europe would probably have been delayed until 1945. Few acts of courage by three individuals can ever have had so far-reaching consequences. Without Ultra from Shark, the U-boats would still have been defeated in the long run, but the cost in human life in the global conflict would have been even more terrible than it was.