The ‘Ultra’ secret war

Away from the heat and din of battle, both sides fought a war of the airwaves, as each strove to decipher the other’s secret radio signals. The Allies won hands-down – by an inspired combination of courage, persistence and genius.

First on the trail

Poland and France, alarmed by Germany’s increasing militarism, were swift to tackle the baffling new ciphers emerging from that country. The Poles had a first-class cipher bureau – Biuro Szyfrów – where the stars of the German section, BS-4, were Marian Rejewski, Jerzy Różycki and Henryk Zygalski, brilliant mathematicians head-hunted while studying at Poznan University in a German-speaking region. In 1932 they started work on the ciphers, which they correctly deduced were being used on Enigma machine similar to one they had seen in photographs.

Using purely mathematical analysis of the intercepts, with marathon trial-and-error sessions and flashes of intuition, they worked out the wiring pattern of the machine in just 4 months. Later in 1932, a mass of information given to them by Bertrand confirmed their deductions. Bertrand’s source was Hans-Thilo Schmidt, code-named Asché (from the German for ‘ashes’), who worked in Berlin for the German army cipher department. He handed over photographs of hundreds of documents before he was transferred to other work in 1933. Among them were details of non-machine ciphers, operating instructions for Enigma, tables of Enigma enciphering settings – known as ‘keys’ – and a plain text message with its Enigma version.

The Poles designed an Enigma copy and over two years they built 15 such machines. The main breakthrough came at the end of 1932. Ironically, they first began regularly to crack German Army signals in mid-January 1933, just two weeks before Hitler came to power. From then until September 1938 they regularly worked out German Enigma keys, but then the Germans modified their machines, making the task much more difficult. To continue, the Poles needed more equipment than they could produce.

At Bertrand’s suggestion, Polish, French and British cryptanalysts met in Paris in January 1939, but all hung back from revealing how much they knew. They met again in late July at BS-4’s concrete bunkers in a forest near Warsaw. Menzies attended the second meeting – where the British group was thunderstruck at the Polish achievements. It was agreed that the Poles would concentrate on the mathematical approach, the British on the practical side and the French on non-machine ciphers – which were still widely used. The Poles gave their sheet and electro-mechanical scanners (‘bombs’) they had devised for testing possible keys, and promised to send two Enigma copies to Paris. The attaché case brought to Britain by Bertrand contained one of them.

The agreement came none too soon. The German invasion of Poland two weeks after Bertrand’s trip to London forced BS-4 to destroy its work and clear out. Some of the cryptanalysts continued their work in France – even in hiding in Vichy France after the German invasion – until forced to flee again. In 1943, Rejewski and Zygalski reached Britain; Różycki died on board a ship sunk in the Mediterranean in 1942. Others were captured, interrogated and killed. None ever revealed that Enigma had been cracked.

Ultra-Secret Guardian

As a teenager Frederick Winterbotham (1897-1990) travelled widely in Europe – becoming fluent in French – then worked as a labourer in Australia and as a lumberjack in Canada. While in the Royal Flying Corps in World War I, he was captured and spent his time perfecting fluent German. After repatriation, he used his back pay studying law at the University of London. Winterbotham was made head of Air Intelligence Branch in 1929, and built up a network of agents in Germany. But from 1933, Nazism made it increasingly dangerous for them to continue. Winterbotham went to Germany himself, professing to admire Hitler. He made friends with Nazi leaders, picking up valuable information over the years until his purpose was discovered in 1938.

Winterbotham then organised aerial spying. He had an aircraft adapted to pass warm air from the cabin over the lens of a mounted camera. This kept the lens clear of condensation up to 9000 m (30 000 ft), allowing the plane to spy from a safe height. The flights gathered extensive knowledge of Luftwaffe strength. Later, as Chief of the Air Department of SIS, Winterbotham devised and controlled the strict and foolproof distribution system that kept ‘Ultra’ flowing, by way of the Special Liaison Units, to Allied field commanders.

Over to Bletchley

Within days of receiving the Polish gifts and information, Britain’s cryptanalysts were at work. Knowing how the Enigma machine worked was not enough – the key had to be discovered. The Enigma key was changed three times a day during the war – and had to be worked out anew each time. No attempt was made to intercept at least 60 messages in the same key had been intercepted. A section of ‘Y Service’ – the vast wireless interception service – and volunteer radio ‘hams’ operated the secret network of listening posts that gave the Enigma cryptanalysts their raw material. Successive shifts of service and civilian listeners strained to catch the faint Morse signals on special, sensitive American receivers, and took down tediously meaningless groups of letters with absolute accuracy. The messages went by landline or dispatch rider to Bletchley Park, a country house 80 km (50 miles) north-west of London – the centre from August 1939 of the Government Code and Cipher School (GC&CS), now to be renamed Government Communications Headquarters (GC&HQ).

Commander Alastair Denniston was its head and civil servant, Alan Dorothy ‘Dolly’ Knox, was chief of cipher breaking. New versions of the Polish key-scanning ‘bombs’ were made and operators recruited to set them up to check possible decipherments. Brilliant mathematicians were called in to work out the constantly changing keys being used by the Germans, decipherers came to
process messages, translators to turn them into English and a department to evaluate and distribute the information. Eventually about 10,000 people worked at Bletchley Park, in a hotchpotch of hastily built "huts" furnished with trestle tables and folding chairs. Secrecy was strict. None of Bletchley's workers knew who people outside their own section were up to.

PASSING ON THE SECRETS

Information from deciphered Enigma signals ranged from routine situation reports, requests for supplies and mobilisation orders to complete battle plans - and reports from the field back to Berlin. The British gave this most secret - ultra-secret - information the code name 'Ultra'. The problem that now arose was how to prevent the Germans from realising that their radio traffic was being read. At first 'Ultra' was passed onto Allied commanders as coming from SIS spies - but their standing was so low among the armed forces that their information was distrusted.

Group Captain Fred Winterbotham of Air Intelligence set up a network of Special Liaison Units (SLUs) to pass relevant 'Ultra' to commanders it concerned. Only the three chiefs of staff, the three services' directors of intelligence, and the chiefs of Fighter Command and Home Forces received all 'Ultra' as a matter of course. The most important information also went to Churchill. Commanders in the field got 'Ultra' only when it concerned them, direct from their SLU officer - who then immediately destroyed the signal. Nobody was allowed to mention 'Ultra' or raise any suspicion that it was the reason for decisions or reports; sometimes reconnaissance flights or other ruses were used to provide a credible source for information.

The United States shared fully in 'Ultra'. From the start of 1942 and Americans worked at Bletchley Park, but the Russians were never allowed to share in it - though they were sometimes given 'Ultra'-based information. The public did not learn of it until 1974, when Winterbotham was allowed to publish a book.

The Germans never realised that their messages were being read - yet they had a clue. On September 11, 1942, the Royal Navy motor gun boat MGB 335 was captured with documents and charts detailing German convoy movements and mine-free channels. The information could only have come from deciphered Enigma signals, but the Germans never caught on.

Field commanders each had an SLU. Some wanted them constantly on hand, while others snubbed them. Ironically, the existence of 'Ultra' information sometimes proved disastrous for commanders. Generals Sir Archibald Wavell and Sir Claude Auchinleck were in their time both sacked by Churchill after defeats in North Africa, for not acting forcefully on 'Ultra' material they had been given. Montgomery's acclaimed successes in the desert were based on his sounder evaluation of 'Ultra' information. During the Battle of Britain, many of Air Chief Marshal Sir Hugh Dowding's decisions for Fighter Command, based on 'Ultra', were criticised by less well-informed officers - but he could not defend himself without revealing his source.

In other campaigns, 'Ultra' told the Allies where the German forces were weakest - for example, during the landings in Sicily and Italy. However, the codebreakers' supreme contribution was to 'Overlord' - the Normandy landings - and the subsequent breakout, where time and many lives were saved by Allied foreknowledge of German positions.

One of several notable failures when 'Ultra' was ignored was the airborne landing at Arnhem in 1944, which went ahead despite reports that two panzer divisions were refitting in the area - with tragic results. In February 1942, the German warships Scharnhorst, Gneisenau and Prinz Eugen were allowed to break out of Brest harbour despite 'Ultra' warnings of the German Navy's plans.

SIGNAL FAILURES

In Germany, the High Command, the Foreign Office and the SS had separate and rival codebreaking organisations. They relied on linguists rather than mathematicians, even though the ciphers they tackled were problems of permutation theory rather than linguistic analysis. For Britain also had a cipher machine, called the

SOMETHING FISHY

The highest-grade German communications did not go by Enigma but by Geheimschreiber ('Secret Writer'), known to the Allies as 'Fish'. It had ten rotors in two sets of five. One set converted the message into Murray telegraph code - similar to Morse code, but with five-element combinations of 'on' or 'off' switch positions, represented as 1 or 0. The other set of rotors produced its own random string of 1s and 0s. 'Fish' automatically added the two together (two 1s or two 0s gave a 0, one of each gave a 1) and transmitted the result to a receiving machine set to the same key. This reversed the process and turned the string of 100110100110 and the like, into the original message.

To deal with 'Fish', the British designed 'Colossus', a huge primitive electronic computer. Cambridge mathematics professor Max Newman and a Post Office engineer, Dr Thomas Flowers, were its chief begetters, and it started deciphering at Bletchley in December 1943. 'Colossus' scanned the message over and over with a photoelectric reader at 5000 characters a second, automatically subtracting every possible permutation of 1s and 0s to try to recover the Murray code. A cryptanalyst scrutinised the printout until he saw a gradual build-up of recurring letters and letter-groups. This meant the cipher was being solved and had reached the point where the message was readable.

CRUCIAL STEPS

Captain Gustave Bertrand and Major Gwido Langer, heads of the French and Polish cipher bureaux, stand on the top step behind some of their joint team at the Château de Vignolles north of Paris, where the Poles fled as their homeland fell. Using wiring plans worked out by Langer's team in 1932, the AVA Radio Manufacturing Company in Warsaw (right) had made 15 copies of Enigma. One copy gave vital aid to Britain's codebreakers.
TypeX – which, ironically, was also based on the early commercial Enigma. Used with tables that encrypted the signals further – and without the Germans' careless procedures – TypeX proved so secure that the Germans gave up trying to read it in 1941. However, they had considerable success in breaking non-machine ciphers.

The Royal Navy, convinced that its own system was sound, stuck for several years to old-fashioned book ciphers that had been broken by the Germans before the war – with disastrous consequences for the convoys. In 1942, the Germans were reading about 2000 convoy signals a month. A tragic situation developed where convoys were ordered to change course to avoid U-boats pinpointed by 'Ultra'. The Germans then deciphered the convoy orders and gave their U-boats new courses. It was November 1943 before the navy adopted a secure cipher machine produced by the US Navy for Allied convoys.

PACIFIC 'MAGIC'

American cryptanalysts achieved a major success in breaking 'Purple', a Japanese machine cipher first used in March 1939. The Japanese made only 25 of the complex electronic 'Type B' machines that produced 'Purple', which was used for passing highest-grade government information between important overseas embassies. Japan's earlier 'Type A' machine, code-named 'Red', was broken by the Americans in 1935 when Colonel William Friedman became head of a new US codebreaking team. After a burglary of the Japanese naval attaché's office in Washington, Friedman produced a copy of the Type A, which was based on an early Enigma model given to Japan by Germany.

Type B was very different. It had no rotors but a plugboard and a huge assortment of electronic stepping switches resembling a telephone exchange. Friedman and his team took almost two years to fathom it, using mathematics, guesswork, intuitive reasoning, and two deciphered messages – the messages breakable because of predictable formal phrases. The effort gave Friedman a nervous breakdown. The Americans built four Type B copies; one was sent to Britain.

Information from 'Red' and 'Purple' – distributed among the Allies under the code name 'Magic' – gave the Americans crucial information before the 1942 Battle of Midway. And it enabled them to intercept and shoot down Admiral Isoroku Yamamoto's aircraft in April 1943.

MSG RECEIVED? Signals typed on an Enigma keyboard were encrypted for Morse transmission. It also deciphered received messages. The Germans thought it unbreakable – the number of possible cipher combinations totalled five followed by 103 zeros – and they overlooked (or dismissed as boasting) a telltale 1941 newspaper report (left) the British censor missed.
The ins and outs of Enigma

A WEHRMACHT Enigma machine had three rotors or drums on a shaft. Each carried an alphabet around the outside. Inside each was electrical wiring that connected the position for each letter on one side to that for a different letter on the other - transposing B to S, say. Each of the rotors made a different set of transpositions. When the operator pressed a key like a typewriter key, electric current flowed through the three rotors in turn, each of which transposed the letter. The signal was then 'reflected' back through the rotors, which transposed it three more times. It was transposed once more at the plugboard - an array of lettered sockets (below the keyboard) with 13 cables available for numerous possible cross-connections. The current finally lit up a lettered hole on the lampboard.

A second operator noted the letters as they lit up. The message was divided into groups of five letters and transmitted in Morse code. The machine was wired in such a way that it could decode as well as encode, if the sender typed A and R lit up, then A lit up when the receiver typed R.

Each time a key was pressed, the first rotor moved round by one letter. As a result, the letter transposition was quite different. When that rotor reached a certain point, the second rotor moved round a place, so that the positions were changed between the second and third rotors. When the first rotor reached the turnover point again, the second clicked round by another place, and so on. When the second rotor had completed its cycle, the third came into play. No fewer than 17,576 letters could be typed before the rotors returned to their original positions - but that was enough to discern a pattern, so long as there were enough messages using the same key.

ADDED COMPLICATIONS

From December 15, 1938, two extra rotors were issued for each machine, giving the operator a choice of three from the five he now had. Instead of six possible orders for putting the rotors on their axle, there were now 60 and the job of the codebreakers was made much more difficult. German Navy Enigma machines used four rotors instead of three - and these were chosen from a total of eight - making the possibilities almost limitless. (The capture in May 1941 of a German Navy Enigma with its full set of rotors from the sinking U-boat U-110 south of Greenland made it easier for the codebreakers to handle that problem.)

It was not enough to capture a machine in order to decipher the enemy's signals. The 'keys' had to be discovered too: the choice and order of the rotors on the shaft, the position of movable rings on each rotor (which could click to any of 26 positions) and the plugboard connections. This combination of settings applied only to a particular signals network at a particular time, and was called the 'daily key' - although it was changed every eight hours at the height of the war. Daily keys were issued monthly to cipher clerks as printed tables.

With his machine set to the daily key, the operator chose three letters at random (say GLF) and turned the rotors until these letters showed at the small windows over the rotors. Then he transmitted, not in cipher, his call sign and these letters at the beginning of a message. Next he chose three other letters at random (say BMP) as the message key and tapped them twice as the first six enciphered letters of the message - which might come out XOLAVJ. The receiver set his machine to the daily key and with the unciphered key GLF at the rotor windows. He typed the first six letters of the coded message, XOLAVJ. BMPBMP lit up, and he reset the rotors to show BMP at the windows before recovering the rest of the message.

MATHEMATICS AND MIND-READING

The repeating of the message key - a safeguard against mistakes in transmission - was what gave the Polish mathematicians their way into Enigma. They knew from Asch's information that the first and fourth ciphers represented the same letter, the second and fifth both represented another, as did the third and sixth. By analysing the first six ciphers of 60 to 80 messages from the same source on the same day, the Poles made various conclusions: how often the fourth ciphers of one message matched the first of another, or the first and fourth ciphers of one message were the same, and so on. They worked out cycles and chains of letters from the connections and then used theories of permutation and probability to build equations. Finally, tentative solutions to the equations emerged and these were tried out on the message.

Marian Rejewski permuted every possible rotor position and pinpointed some characteristic patterns. He drew up an index of characteristics, called a cyclo-meter; messages were checked against it to give the best starting points for decipherment. Then similar information was put on sheets devised by Henryk Zyglaski. They looked like graph paper with the alphabet running twice along the top and twice down the side, and represented all possible relative positions of the rotors. Holes were made where characteristic patterns occurred. When enough message keys had been analysed to spot their characteristic patterns, the sheets were laid over one another on a light table and moved in certain ways (over 700) to test and reject possibilities. When the light shone through only one set of perforations, a possible key had been found and was tried on a message.

BOMBS AND GODDESSES

In May 1940, the Germans stopped the repeat and the enciphering of the message key. All the comparisons it had offered ended and electro-mechanical 'bombs' were the only way in. They checked at speed whether certain encipherments were possible - but the mathematicians still had to draw up a 'menu' of likely encipherments, and operators had to set a bombe to test them. It clicked through the possibilities and stopped when it had pinpointed a probable key to try out. It was late 1940 before British bombs - nicknamed 'Bronze Goddesses' - were ready. From May until then, mathematicians relied on the operators' bad habits in choosing message keys. They might repeat the same letter AAA, perhaps - or use three consecutive letters of the alphabet, or three that fell next to one another horizontally or diagonally on the keyboard. Guesswork might also hit on the opening phrase or the signature of a message.