Feedback

Why is Britain's wartime code-breaking still secret?

Newly-disclosed information about wartime scientific intelligence work on code-breaking is gradually forming a still-hazy picture of the tremendous significance of cryptology to the British war effort. One recent release of official information has briefly detailed the "special purpose electronic computer", Colossus, built in World War Two, and described in last week's *New Scientist* (p 346) by Professor Brian Randell. And the use of the Colossus computer to crack a sophisticated German cypher code-named "Fish" was revealed last week by a BBC series—"The Secret War".

Colossus computers were just one facet —though a vital one—of an intellectual renaissance that took place during World War Two. A formidable number of mathematicians and engineers were gathered together at Station X—Bletchley Park in Buckinghamshire—to work on codes and code-breaking. Station X, which at its peak employed 7000 people, was the government's Code and Cypher School, and was at first a part of the secret service. The work of the establishment, and indeed some of the people who worked there has been widely (but not always openly) credited as being indispensable in winning the war.

The official history of Britain's wartime cryptanalysts still remains classified, however, and as a result the true effects of the intercepted communications and broken codes on recent history remain obscure.

The history of the German Enigma code machine and its analysis has now been well documented. Enigma was an electrically-powered version of a 1920's German commercial machine. About the size of an ordinary typewriter, it was used from the start of the war for communications between German commands.

To substitute a cyphered letter for a letter in "plaintext", the operator pressed a typewriter button and a letter was illuminated on the display panel. The simple electrical circuit between the typewriter key and lamp was scrambled by passing through three scrambling rotors and through a connection panel which further altered the correlation between the original message and the output code. The settings of the scrambling rotors changed after every letter, in a predetermined fashion. The result was that particular sequences reappeared only rarely in Enigma messages.

But like all non-random cyphering techniques there were flaws, which provided a way through the cypher. Breaking the Enigma code was done at Bletchley Park after 1939 when the system was complicated by the possibility of three rotors being selected from a possible five.

The task of cryptanalysis of the extended Enigma system seems largely to have been performed by the late Alan Turing, the Cambridge mathematician whose secret reputation as a cryptanalyst has been said to be as great as his fame in the development of computing. Turing headed the naval section of Enigma cryptanalysts at Bletchley Park and was responsible for the development of an analytical electromechanical device—code-named Bombes—which proved vital in quickly decoding German signals. By 1942, the process of decoding Enigma signals had become regular and automated.

Bletchley Park: Britain's secret code-breaking station

In 1943, the successful cryptanalysis of a special U-Boat version of Enigma (using four rotors instead of three) was another naval code-breaking victory vital to Britain's wartime survival.

There were, however, other high-level German cyphers. And another section of Station X was, in 1942, working laboriously to break one of these systems, known to them as "Fish". From the work of the "Fish" group came the Heath Robinson machines and the Colossus computers.

The "Fish" code machine which Colossus attacked has been officially identified as a Siemens Geheimschreiber (secret writer)—a sophisticated telegraph code machine whose output and input could be directly transmitted along telegraph lines. Geheimschreiber had 10 rotating coding discs, each containing a prime number of different settings. Like Enigma, the settings of the wheel altered after each character coded, determining a different manipulation of the telegraph symbol.

From the section working on the cryptanalysis of Fish came a new proposal for mechanisation, which led to the start of the Robinson and Colossus projects by a team led by Professor Max Newman.

Strangely, however, the successful solving of the Siemens cypher is also claimed in David Kahn's book *The Code-Breakers* by a Swedish cryptologist, Arne Beurling, who intercepted German communications passing on telegraph lines from Norway. Kahn's account given of a solution of Fish-coded messages in two days is irreconcilable with the effort expended on Colossus.

German high command also developed other machines, including a more secure Enigma manufactured by Wanderer Werke. The government's demand that the first production Colossus computer be available in time for D-Day strongly suggests that high-level cyphers other than Enigma were used in critical areas. Nevertheless, the fact that these other high-level cyphers had been broken was apparently kept secret from regular users of Ultra communications intelligence issued by Bletchley.

Despite the acknowledged, and probably still underestimated, role of code-breaking in the British war effort, the fact remains that British or allied cryptographic security was just as poor as the German's. Until mid-1940, easily cracked Admiralty messages gave U-Boats clear information on observations made against them; long telephone calls on transatlantic radio between Churchill and Roosevelt were readily unscrambled by German Post Office technicians; and both the Germans and the British cracked American reports from the campaign in North Africa. One reason for the heavy veil of secrecy still surrounding wartime code-breaking may be the extent of work done against "friendly" countries.

In 1946, a new organisation, Governments Communications Headquarters, took over the cryptographic tasks of Bletchley Park. Despite the vast modern sophistication and virtual impenetrability of current electronic cypher systems, that organisation is certainly the largest scientific intelligence agency of its kind in the United Kingdom. □

Duncan Campbell