Cryptanalysis[edit]

During the Second World War, Turing was a leading participant in the breaking of German ciphers at Bletchley Park. The historian and wartime codebreaker Asa Briggs has said, "You needed exceptional talent, you needed genius at Bletchley and Turing's was that genius."[59]

From September 1938, Turing worked part-time with the Government Code and Cypher School (GC&CS), the British codebreaking organisation. He concentrated on cryptanalysis of the Enigma cipher machine used by Nazi Germany, together with Dilly Knox, a senior GC&CS codebreaker.[60] Soon after the July 1939 Warsaw meeting at which the Polish Cipher Bureau gave the British and French with details of the wiring of Enigma machine's rotors and their method of decrypting Enigma machine's messages, Turing and Knox developed broader solution.[61] The Polish method relied on an insecure indicator procedure that the Germans were likely to change, which they in fact did in May 1940. Turing's approach was more general, using crib-based decryption for which he produced the functional specification of the bombe (an improvement of the Polish Bomba).[62]

Two cottages in the stable yard at Bletchley Park. Turing worked here in 1939 and 1940, before moving to Hut 8.

On 4 September 1939, the day after the UK declared war on Germany, Turing reported to Bletchley Park, the wartime station of GC&CS.[63] Specifying the bombe was the first of five major cryptanalytical advances that Turing made during the war. The others were: deducing the indicator procedure used by the German navy; developing a statistical procedure for making much more efficient use of the bombes dubbed *Banburismus*; developing a procedure for working out the cam settings of the wheels of the Lorenz SZ 40/42 (*Tunny*) dubbed *Turingery* and, towards the end of the war, the development of a portable secure voice scrambler at Hanslope Park that was codenamed *Delilah*.

By using statistical techniques to optimise the trial of different possibilities in the code breaking process, Turing made an innovative contribution to the subject. He wrote two papers discussing mathematical approaches, titled *The Applications of Probability to Cryptography*[64] and *Paper on Statistics of Repetitions*,[65] which were of such value to GC&CS and its successor GCHQ that they were not released to the UK National Archives until April 2012, shortly before the centenary of his birth. A GCHQ mathematician, "who identified himself only as Richard," said at the time that the fact that the contents had been restricted for some 70 years demonstrated their importance, and their relevance to post-war cryptanalysis:[66]