Shouzab Khan

Skhan6

Alan Turing’s Contribution to Cryptanalysis

Like the traditional Hollywood stories, the story presented revolves around the early attempts to decipher the German Enigma code. The story starts in 1938, with Britain not knowing anything about the inner workings of the Enigma system. Six weeks after the start of World War II in September 1939, regardless of their lack of knowledge, there were talks of building machines to decode Enigma settings. The story takes an exciting turn when important people are introduced, especially Schmit, a German World War I soldier who tries to sell secret documents to the British Embassy after getting access to them. The task of evaluating Schmit falls to a retired criminal with connections to intelligence, Rudolf. As the story goes on, Gusta, the head of French military intelligence, becomes involved in the plan. During a meeting in Belgium in 1932, they talked about the German elections while secretly taking photos of books regarding Enigma. These publications include crucial secrets about the inner workings of the Enigma machine, hidden within the Enigma edition.

The story then turns to Polish mathematician Marion Rejewski, who starts deciphering Enigma signals that are intercepted in the Polish corridor in the 1930s. He uses mathematical equations connected to group theory to explain the inner workings of Enigma. Based on his knowledge of German theory, he guesses about the Enigma machine's possible wiring. This leads the Poles to manufacture fake Enigma machines, which is a significant development.

The automated Bomba machines are created by Polish engineers to help decrypt Enigma settings. However, new rotors introduced by German practice made it more difficult for the Poles to operate Bomba machines properly. A meeting in July 1939 between Polish codebreakers and French and British intelligence personnel led to the exchange of important Enigma-breaking technology as tensions increased throughout Europe.

The story ends with German soldiers pursuing the Polish codebreakers as they escape France. Some make it to safety in Britain, where they aid in the ongoing efforts to crack the Enigma. The narrative highlights the rapid developments in understanding the workings of the Enigma system as well as the cooperative efforts of Polish, French, and British intelligence in the years leading up to World War II.

Alan Turing's contributions to cryptanalysis were very big,

Alan Turing played a significant role as a cryptanalysis leader during World War II. While based at Bletchley Park, he applied his mathematical and cryptologic skills to break the German ENIGMA cipher, an extremely complex encryption method used by the Axis powers. "The bombe," a unique electromechanical device that Turing and his colleagues invented, is used to recognize ENIGMA configurations. This invention allowed the Allies to gain important data by enabling them to crack encrypted German military messages. Turing and his group not only defeated ENIGMA but also the Naval ENIGMA system, assisting the Allies in the Battle of the Atlantic in avoiding German U-boats. Turing is known for having saved thousands of American and British lives, and the success of the Allies was greatly helped by his contributions to cryptanalysis. His work at Bletchley Park was a turning point in the war and proved the usefulness of cryptanalysis in military intelligence.

REFERENCE:

1. <https://www.cia.gov/stories/story/the-enigma-of-alan-turing/#:~:text=Whereas%20cryptographers%20write%20encryption%20systems,powers%20to%20decipher%20German%20encryptions>.
2. <https://www.youtube.com/watch?v=qn_BBQEjCxI>