Stories

The Enigma of Alan Turing

April 10, 2015

Innovation and Tech

Alan Turing—an English mathematician, logician, and cryptanalyst—was a computer pioneer. Often remembered for his contributions to the fields of artificial intelligence and modern computer science (before either even existed), Turing is probably best known for what is now dubbed the "Turing Test." It is a process of testing a machine's ability to "think."

The basic premise of the Turing Test is that a human judge would be placed in isolation and have two conversations -- one with a computer and one with another person -- except the judge wouldn't be told which was which. If the computer could fool the judge and carry on a conversation that is indistinguishable from that of the human, the computer is said to have passed the Turing Test. *No computer has passed it yet.*

Less is known, however, about Turing's intelligence work during WWII when he used his mathematical and cryptologic skills to help break one of the most difficult of German ciphers, ENIGMA.

Codes and Ciphers

Though often used interchangeably, the terms codes and ciphers are very different. A code changes the meaning of a word or phrase by replacing it with a different word or phrase to make a message secret. A cipher, on the other hand, makes a word or phrase secret by changing or rearranging the individual letters in a message. Together, codes and ciphers are called encryption.

ENIGMA was a cipher machine—each keystroke replaced a character in the message with another character determined by the machine's rotor settings and wiring arrangements that were previously established between the sender and the receiver. For additional security, the German military services usually double-encrypted their messages by first substituting original text with code words and then enciphering the encoded text.

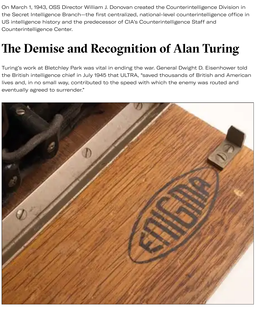
Reproduced with kind permission by Bletchley Park Trust.

Breaking ENIGMA

In the early years of WWII, Turing worked at Britain's code breaking headquarters in Bletchley Park. In addition to mathematicians, Bletchley Park also recruited linguists and chess champions, and attracted talent by approaching winners of a complex crossword puzzle tournament held by The Daily Telegraph.

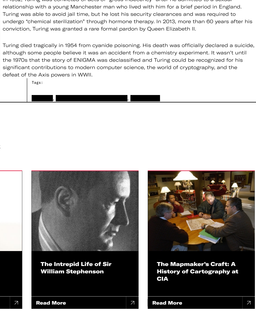
Turing's mathematical and logic skills made him a natural cryptanalyst. Whereas cryptographers write encryption systems, and cryptologists study them, cryptanalysts like Turing break them. In 1939, Turing created a method called "the bombe," an electromechanical device that could detect the settings for ENIGMA, allowing the Allied powers to decipher German encryptions. Turing and his colleagues were also able to break the more complicated Naval ENIGMA system, which from 1941-1943 helped the Allies avoid German U-boats during the Battle of the Atlantic.

Poland was actually the first to realize that the solution to breaking ENIGMA would most likely be discovered by a mathematician. Polish cryptanalysts as early as 1932 could decode German ciphers and, by 1939, they were able to successfully decipher messages written with an earlier version of ENIGMA using a replica machine like "the bombe" that could emulate the way ENIGMA worked. When Poland was overrun by Germany in September 1939, the Polish as well as French cryptanalysts shared what they knew about ENIGMA with the UK, which allowed the cryptanalysts at Bletchley Park, including Turing, to finally crack the ENIGMA ciphers.



© Crown. Reproduced with kind permission, Director, GCHQ.

Once the German messages were decrypted, the British began supplying the Office of Strategic Services (OSS, precursor to CIA) with extensive information about foreign military, espionage, and sabotage activities. The most sensitive intelligence came from ULTRA—the code name applied to all intel coming from Bletchley Park, including the intercepts of German military messages sent with the ENIGMA machine. Because of the volume of the traffic and the overriding need for compartmentalization, the British insisted that the OSS set up a separate, extra-secure component to handle the material.

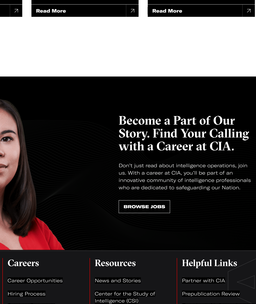


© Crown. Reproduced with kind permission, Director, GCHQ.

On March 1, 1943, OSS Director William J. Donovan created the Counterintelligence Division in the Secret Intelligence Branch—the first centralized, national-level counterintelligence office in US intelligence history and the predecessor of CIA's Counterintelligence Staff and Counterintelligence Center.

The Demise and Recognition of Alan Turing

Turing's work at Bletchley Park was vital in ending the war. General Dwight D. Eisenhower told the British intelligence chief in July 1945 that ULTRA, "saved thousands of British and American lives and, in no small way, contributed to the speed with which the enemy was routed and eventually agreed to surrender."



Nevertheless, Turing would spend the majority of his career focused on what would eventually become modern day computing. He was posted to serve with the US Navy's Cryptanalytic Section for several months in 1943, where he met and discussed mathematical models of communication and computation with Claude Shannon (the father of information theory). To this day, our communications networks are built on top of Shannon's ideas, while our computing devices, processors, and chips are built upon Turing's ideas. Turing's contribution to modern computing was so significant that the prestigious A.M. Turing Award—sometimes known as the "Nobel Prize" of Computer Science—is named after him.

In 1952, Turing was convicted of acts of "gross indecency" after he admitted to a sexual relationship with a young Manchester man who lived with him for a brief period in England. Turing was able to avoid jail time, but he lost his security clearances and was required to undergo "chemical sterilization" through hormone therapy. In 2013, more than 60 years after his conviction, Turing was granted a rare formal pardon by Queen Elizabeth II.

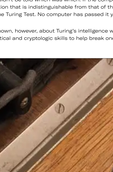
Turing died tragically in 1954 from cyanide poisoning. His death was officially declared a suicide, although some people believe it was an accident from a chemistry experiment. It wasn't until the 1970s that the story of ENIGMA was declassified and Turing could be recognized for his significant contributions to modern computer science, the world of cryptography, and the defeat of the Axis powers in WWII.

Tags:

Related Stories

Who First Cracked the ENIGMA Cipher?

Read More



The Intrepid Life of Sir William Stephenson

Read More

The Mapmaker's Craft: A History of Cartography at CIA

Read More

Become a Part of Our Story. Find Your Calling with a Career at CIA.

Don't just read about intelligence operations, join us. With a career at CIA, you'll be part of an innovative community of intelligence professionals who are dedicated to safeguarding our Nation.

BROWSE JOBS