How Cryptology Affect the Outcome of World War II

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

How Cryptology Affect the Outcome of World War II

Cryptology and information protection had been used for many years. In Ancient Warfare, Julius Caesar of the Roman Empire use the Caesar Cipher to protect his message to his general (1). Today, information protection has been widely using not only for military purposes and government but also in the private sector such as financial banking, data privacy, and daily communications. All Information is well protected these days. In my opinion, the most achievement that cryptology is the decoding of the Engima system that help the Allied win World War II.

# What is the Enigma System

Enigma System is an encryption communication machine that was designed by the Germans and Japan to help them protect their military’s information transformation.

## Why Enigma?

The fastest way to communicate is by using the signal that travels through the air. Communication transfer from point A to point B over the air was considered the most convenient and fastest way due to the flexibility in location (1). There was no cable to connect from Japan to Germany at that time, so I assume they use radio stations and towers to transfer information. Therefore, Enigma was designed.

## How do Enigma’s functionality and design

According to (1), Enigma resembles a typewriter and works in the following steps:

* Encoding:
  + Set the machine to the code of the device
  + Key in the letter of the message by letter
  + Each letter that lights up on the machine while typing will be sent out as part of the encrypted messages
* Decoding:
  + Press the key corresponding to the letters in the encrypted message.
  + The letter of the original message will light up on the Enigma machine

# The Bombe system

According to Chapple, M., & Seidl, D. (2023), the Bombe System was developed from the Ultra Project (led by British mathematicians Alan Turning). It was a very large, special purpose computer. Bombe's main duty is to break the Enigma code. After many years of development, the Bombe was able to decode the communications from the Enigma machine. Thus, the Allied war planners gained great insight into German Operations, and the entire German communication system fell into the Allied hands. Therefore, the development of Bombe is the turning point to winning the war and saving the lives of billions of people.

References

Chapple, M., & Seidl, D. (2023). Chapter 1: Information as a Military Asset. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 9–20). essay, Jones & Bartlett Learning. (1)