**Turing vs Enigma**

In this part of the presentation, we are going to spoke about the role which played Alan Turing during de Second World War. I will introduce the historic context. Then Charles will explain the functioning of the Enigma machine. Finally, I’ll describe the functioning of the “bombe”.

**Historic context**

When the Second World War bursts, Turing is in charge in the Office of British deciphering. He is installed to Bletchley Park, a little village not very far from london, to break the codes used by the German navy. And he has manages to make it. Without this major discovery, England would have eventually capitulated suffocated by the German blockade. According to certain historians, his ideas allowed to shorten the war of 2 years.

But Alan Turing wasn’t alone. It’s an entire army which worked in Bletchley Park to decipher Enigma. Hundreds of messages were intercepted every day. They were illegible and piled up on desks. Nevertheless, English had an exact replica of the machine enigma. But Enigma is far too complicated. Having the machine is not enough. It’s impossible to break enigma with a pen and a sheet of paper. I let Charles explain you why.

**Principle of the bombe**

The bomb is a machine finalized by Alan Turing to decipher enigma. It is designed to look for the configuration of the rotors of the enigma machine. Each Bombe consists of 3 rows. A row counts 12 times 3 rotors. 3 rotors represent the mechanism of a machine Enigma. A rotor correspond to an enigma rotor, and contain 26 letter. The rotor will turn and check every possibilities until one is found.

Due to the enormous number of possibilities that enigma can create, finding the key to decipher the code using a modern computer with a simple algorithm (I mean test every possibilities one by one) could take one year! With an old machine which can check one thousand configurations by second, it would take 5 billion years to finish! So, how did they break the code?

In fact, Enigma isn’t perfect. One of his weakness is that one letter can’t be transformed in any other letter except itself. It means that a “A” can’t be transformed into a “A”. It seems ridiculous, but for a letter which is often repeated in a language like the “E” in French, a lot of configurations can be ignored (MONTRER UNE PHRASE SUR LE TRANSPARENT). It’s the first step to break Enigma. The second weakness was the discipline of the German. They lose the war because of a weather report and a polite phrase. I exaggerate a little when I say that. Actually, their problem was that every morning at six o’clock, they send a weather report packaging the word “Wetterbericht” (which means weather report) and finishing all the time by a wonderful “heil hitler”.

The cryptographists decided to find a place in the text where every letter is different from the real word. Remember that one letter can’t become itself. So, you took the word, and find a place where each letters are different. After that, they check every possibilities, but highly restricted by the place that can occupy the previous found words. Finally, they were able to find the solutions in about 20 minutes. We are far away of the 5 billions years!

**Voc utile**

**Decipher: décrypter**