



THE ENIGMA ENCRYPTION MACHINE.

ONE MORE JEWEL TO VISIT IN THE MUSEUM OF THE ARTILLERY ACADEMY IN SEGOVIA

THIS MONTH WE INCLUDE AN ARTICLE RECEIVED FROM THE MUSEUM OF THE ARTILLERY ACADEMY. IT HAS BEEN REVISED BY THE TEACHERS IN THE ENGLISH WING OF THE FOREIGN LANGUAGES DEPARTMENT (EGE), AND, ALTHOUGH IT IS NOT A TEST-LIKE COMPOSITION, IT CONTAINS GOOD EXAMPLES OF DESCRIPTIVE LANGUAGE AS WELL AS OF NARRATION IN THE PAST TENSE.

The Artillery Academy owns a copy of the Enigma encryption machine model K-293 that is on display for every visitor of the Military School in Segovia.

The invention of the first Enigma machine defined as model A is attributed to the German engineer Arthur Scherbius in 1918. However, **it would not be until** 1923 that the first of these machines would be released at the Chiffiermaschinen AG factory in Berlin, for initial commercial as well as military purposes.

This first model A machine, which was soon improved with model B, was apparently very similar to a typewriter at that time. **However**, the problems with printing on paper made it evolve towards the subsequent commercial models C, D and K.

In these models, paper printing was replaced with an alphabet panel whose letters would light up. **Therefore**, the operation was based on an electromechanical device, which, by pressing the keys as in a typewriter, operated electrical switches that caused the movement of some rotors. The electrical signal would follow a different path when the different keys were pressed. **Finally**, the electrical power after going through the encryption of the rotors, would illuminate the corresponding lamp of the alphabet located at the top.

While from the point of view of the operator its handling was very simple, in terms of encryption, it was a replacement algorithm that offered millions of unrepeatable codes. This complex system made the Germans think that this secret code was impossible to "break". **Then**, with the new need imposed by the war, the manufacturing of these machines was nationalized and its production had an exclusive military use.

In spite of the system complexity, the combination of several technical and human factors contributed to the breaking of the codes, which have proved really useful in our knowledge of the machine operation. The breaking of the codes began in Poland and was mainly carried out by mathematicians. They proposed a solution, but the German occupation of Poland made it impossible to develop these kinds of machines in their country. Finally, this solution was adopted by England where the machine reached its technical/scientific success.

Factors such as boredom, misuse and negligence on the German operators' side, and observation and intelligence on the allies' technicians, led to the amazing discovery of how to break the codes. Perhaps the most significant example of this fact is represented by a certain message: An operator pressed the "T" key repeatedly and, **since** they knew that a key would never reveal its own spelling, they suspected that the message was a test and discovered the code. Other examples were messages that were reiterated as greetings, congratulations, etc..., and provided a known sequence. **Although** the codes were broken, this fact was not revealed until long after the war ended.

As for the K-293 model that concerns us and how it came to Spain, at present there is no doubt: the first ten machines arrived in Spain in 1936. A second shipment with ten more, acquired by the Government of Burgos, arrived in January 1937, with the same model and the following serial numbers: from K-287 to K-294, as well as K-225 and K-226. **Consequently**, the displayed copy of the Enigma encryption machine K-293 at the Artillery Academy in Segovia must be included within these groups.

MORAL

Hard work and perseverance have their reward. It served well for the code-breakers, and it also applies today for studying languages. Work hard, and results will come.

"Our wishes come true through the work that we do"

Plautus, Persa, 1.629 (c.200 B.C.)

WATCH OUT

Use of different linkers

- However,
- Therefore,
- Finally,
- While (from the point of view...)
- Then,
- In spite of (the system complexity)
- Since (they knew...)
- Although
- Consequently...

