

PROYECTO ENIGMA

“Máquina Enigma, código resuelto”

Durante el próximo mes de Febrero se proyectará en el Museo Militar de Burgos sito en el “Palacio de Capitanía” el video “Proyecto Enigma”, una virtualización de la máquina Enigma donde se muestra el secreto de su funcionamiento así como su ingenioso interior con los rotores más famosos e imaginativos en la época.



**UNIVERSIDAD
DE BURGOS**

Todo ello gracias al convenio marco de colaboración entre el Ministerio de Defensa y la Universidad de Burgos, para el establecimiento de un marco general de cooperación en el campo académico, científico y cultural de interés común.

Fruto del trabajo final de grado comunicación audiovisual de la alumna Dña. Sara Martínez López de la Facultad de Humanidades y Comunicación, sobre el fondo ES18-129 del Museo Histórico Militar de Burgos, con las colaboraciones y asesoramiento del propio Museo; del experto investigador, escritor y apasionado en criptografía D. José Ramón Soler, Doctor Ingeniero Industrial y Licenciado en Informática, coordinado por el profesor D. Andrés Bustillo Iglesias, corriendo a cargo de D. Pablo Corbí Serna la locución del video y de D. Álvaro Aliste Rábano el apoyo a la realización técnica.

La máquina ENIGMA modelo K

Desde los comienzos de las máquinas de cifrado con rotores en 1915, por Hugo Alexander Koch, no es hasta 1923 cuando irrumpe la máquina de cifrado más enigmática, “Enigma” comercializándose con este nombre, desarrollada y patentada por la compañía Scherbius & Ritter.

La máquina Enigma K modelo comercial es una evolución de Enigma D, se usó en la guerra Civil Española. Esta Enigma K se comercializó con esta letra a partir del 1936, que era el descendiente destacado de la versión D (modelo A27).

En principio con su caja cerrada parece una humilde pero elegante caja de marquetería de unas dimensiones de 15x28x30 cm, como si fuera la caja donde nuestra abuela guardaba las bobinas e hilos de coser, pero una vez que la abrimos aparece nuestra sorpresa ¡Una máquina de escribir!, pero ahí no acaba nuestro asombro cuando vemos que es más que una simple máquina de escribir y leemos una chapita con la leyenda “K 296”... ¡tengo que descubrir este enigma!.

Ante mí tengo una máquina Enigma de la que tanto se ha hablado; ¡hasta ví la película “El código Enigma” sobre la vida e historia del genial matemático Alan Turing!



Una máquina que se compone fundamentalmente de: un teclado electromecánico de 26 caracteres, un panel luminoso de idéntico número bombillas que el teclado, rotores, reflector y en su versión militar disponía de un clavijero en el frontal.

La máquina Enigma K (modelo A27) consta de tres rotores o modificadores, cada uno de ellos con 26 caracteres que hace un total de 26^3 combinaciones posibles, es decir 17.576 posibilidades, pero esto no se detiene aquí, ya que estos discos son intercambiables, lo que indica que es $26^3 \times 6$ lo que incrementa sus opciones a 105.456, pero eso no es todo, ya que cada rotor tiene un anillo exterior para situar una letra de inicio y volvemos generar otras 26^3 posibilidades.

$$26^3 \times 26^3 \times 6 = 1.853.494.656 \text{ combinaciones posible}$$

Una cifra espectacular para esos años. Pero había máquinas Enigma de hasta 8 rotores y con clavijero, que permitían un número enorme de conexiones; eran las versiones militares de los Cuarteles Generales Nazis en la II Guerra Mundial. Hablamos de cifras en el entorno de 10^{28} ¡ 1.556.215.256.125.916.549.119.449.341 ! combinaciones posibles.



Nuestra máquina Enigma K-296 estaba asignada a la C.G. Sexta Región Militar, en el “Palacio de Capitanía” en la misma ubicación donde se encuentra en la actualidad expuesta.

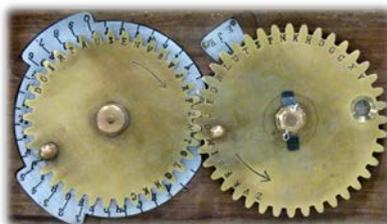
El fin de la máquina Enigma fue el fruto del trabajo ingente de muchos matemáticos e ingenieros, de los que destaca Alan Turing una mente muy brillante, padre de la computación y

precursor de la informática moderna: Sus aportaciones en el campo de la criptografía sirvieron para que la II Guerra Mundial terminara antes de lo esperado, gracias a la decodificación de los planes secretos de los nazis encriptados por su máquina Enigma. En 1937 publica el libro “Los números computables” donde abre los ojos a los límites teóricos de cualquier ordenador futuro.



Turing descifró el código 'Enigma', que la Alemania Nazi consideraba inexpugnable, con el trabajo de constante de la maquina llamada “Bomba de Turing”. Posteriormente diseñó y desarrolló Colossus, una de las primeras computadoras programables.

También podrán ver al lado de la máquina Enigma, el curioso y eficaz ingenio de “Clave Norte”



Museo Histórico Militar de Burgos



Biografía:

Revista de Historia y Cultura Militar

Boletín Enigma

<http://www.cryptomuseum.com>

José Ramón Soler “Spanish Enigma: A History of the Enigma in Spain” 2010