Presentación de la máquina ENIGMA

Martes, 26 de octubre del 2010, a las 13 horas

Lugar: Museu de la Ciència i de la Tècnica de Catalunya. Rambla d'Ègara, 270. TERRASSA

EL ENIGMA Y LA ENCRIPTACIÓN DE MENSAJES DURANTE LA GUERRA

La encriptación de mensajes

La encriptación de mensajes es la técnica que altera las representaciones lingüísticas de un mensaje a fin de ocultar su significado. A lo largo de la historia, se han ideado diferentes sistemas de encriptación más sencillos: tintas invisibles que reaccionan con el calor o elementos químicos, escritura invertida, sistemas de substitución de letras, símbolos, etc.

En tiempos de guerra, la encriptación es un arma clave, ya que permite la comunicación de información entre los componentes de un mismo bando con la seguridad de no ser descubiertos por el adversario. Una tarea primordial de los diferentes bandos será, pues, la de conseguir sistemas de encriptación de alta seguridad y, por otro lado, desencriptadores capaces de desentrañar los mensajes aparentemente indescifrables.

El Enigma, un arma clave en la encriptación de mensajes durante la II Guerra Mundial

La máquina Enigma fue creada en 1923 por el ingeniero alemán Arthur Scherbius, basándose en una patente holandesa previa.

En su inicio, la máquina fue utilizada sobre todo en el envío de mensajes encriptados dentro del contexto comercial e industrial, pero pronto se aplicó al contexto militar, convirtiéndose en una de las máquinas protagonistas de la encriptación en la II Guerra Mundial.

Utilizada por el bando nazi y sus aliados, el Enigma era capaz de establecer mensajes con más de 456.976 combinaciones en cada una de las 24 posibles posiciones de sus rotores, convirtiéndose en un verdadero quebradero de cabeza para el bando contrario.

Las máquinas enigma en España, como la que podemos ver hoy, fueron utilizadas para encriptar mensajes en transacciones comerciales, industriales y militares, durante la Guerra Civil y la posguerra.

La decodificación de un mensaje *Enigma* se precisaba una máquina de iguales características con los rotores orientados en la misma posición. Pero si no se podía saber la posición de los rotores ni el código utilizado, no había otra manera de descifrar el mensaje que realizar una gran cantidad de cálculos para encontrar, poco a poco, los patrones establecidos y descifrar el código de encriptación.

Para realizar éste gran número de cálculos el ejército inglés creó el centro militar de Bletchley Park, en el cual un gran ordenador, el Colossus, era capaz de realizar cálculos fiables a alta velocidad y descifrar los más de mil mensajes *Enigma* que interceptaban día a día al ejército alemán. Así pues podemos afirmar que la decodificación de mensajes Enigma así como la de otras máquinas decodificadoras fue uno de los catalizadores de la creación de los primeros ordenadores.

FITXA TÈCNICA ENIGMA:

Máquina de encriptación ENIGMA

Marca: Enigma Chiffiermaschinen AG.

Modelo: modelo D

Número de serie: K 358

Año: primera mitad siglo XX

Inventor: Hugo Alexander Koch

Procedencia: Instituto de Historia y Cultura Militar – MINISTERIO DE DEFENSA

DEPÓSITO: EJÉRCITO DE TIERRA ESPAÑOL (INSTITUTO DE HISTORIA Y CULTURA MILITAR – MINISTERIO DE DEFENSA).

Exposición del 26 de octubre del 2010 al 10 de octubre del 2011 · www.mnactec.cat