



Presentació de la màquina ENIGMA

Dimarts, 26 d'octubre del 2010, a les 13 hores

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

L'ENIGMA I L'ENCRIPCIÓ DE MISSATGES DURANT LA GUERRA

L'encriptació de missatges

L'encriptació de missatges és la tècnica que altera les representacions lingüístiques d'un missatge per tal d'ocultar-ne el seu significat.

Al llarg de la història s'han ideat diferents sistemes d'encriptació més o menys senzills: tintes invisibles que reaccionen amb l'escalfor o elements químics, escriptura invertida, sistemes de substitució de lletres, símbols, etc.

En temps de guerra, l'encriptació és una arma clau, ja que permet la comunicació d'informació entre els components d'un mateix bàndol amb la seguretat de no ser descoberts per l'adversari. Una tasca primordial dels diferents bàndols serà, doncs, la d'aconseguir sistemes d'encriptació d'alta seguretat i, d'altra banda, descriptadors capaços de treure l'entrellat dels missatges aparentment indesxifrables.

L'enigma, una arma clau en l'encriptació de missatges durant la II Guerra Mundial

La màquina encriptadora Enigma fou creada al 1923 per l'enginyer alemany Arthur Scherbius, basant-se en una patent holandesa prèvia. Primerament fou utilitzada en l'enviament de missatges dins del context comercial i industrial però ben aviat es va aplicar al context militar esdevenint una de les màquines protagonistes de l'encriptació en la II Guerra Mundial.

L'Enigma, utilitzat pel bàndol nazi i els seus aliats, era capaç d'establir missatges amb més de 456.976 combinacions en cada una de les 24 possibles posicions dels seus rotors, esdevenint un veritable maldecap per al bàndol contrari.

Les màquines enigma a l'estat espanyol, com la que podem observar, foren utilitzades per encriptar missatges en transaccions comercials, industrials i militars, durant la Guerra Civil i la Post-Guerra.

La decodificació d'un missatge enigma requeria d'una màquina d'iguals característiques amb els rotors orientats en la mateixa posició. Però si no es podia saber la posició dels rotors ni el codi utilitzat, s'havia de realitzar una gran quantitat de càlculs per trobar els patrons establerts i desxifrar el codi d'encriptació.

Per realitzar aquest gran nombre de càlculs l'exèrcit anglès va crear del centre militar de Bletchley Park, on un gran ordinador, el Colossus, era capaç de fer càlculs fiables a alta velocitat i desxifrar més de mil missatges enigma que interceptaven dia a dia a l'exèrcit alemany. Així doncs podem afirmar que la descriptació de missatges Enigma així com d'altres codificadors fou un dels catalitzadors de la creació dels primers ordinadors.

C

El president del Consell Rector del Museu de la Ciència i de la Tècnica de Catalunya

es complau a convidar-vos a l'exposició de la màquina

ENIGMA:

UNA MÀQUINA CLAU EN LA CODIFICACIÓ DE MISSATGES

La presentació tindrà lloc dimarts 26 d'octubre, a les 13 hores, al Museu de la Ciència i de la Tècnica de Catalunya (mNACTEC). Rambla d'Ègara, 270. Terrassa

Terrassa, octubre del 2010

Generalitat de Catalunya
Departament de Cultura
i Mitjans de Comunicació

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
DIRECCIÓN GENERAL DE RELACIONES INSTITUCIONALES

FITXA TÈCNICA ENIGMA:

Màquina d'encriptació ENIGMA

Marca: Enigma Chiffiermaschinen AG.

Model: model D

Número de sèrie: K 358

Any: primera meitat segle XX

Inventor: Hugo Alexander Koch

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

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

Exposició del 26 d'octubre del 2010 al 10 d'octubre del 2011 · www.mnactec.cat