



ANNUNCIO DI SEMINARIO

Martedì 27 Maggio, ore 16.30, aula XX

Le Macchine Crittografiche Enigma e O.M.I.Nistri

Antonio Fucci

Abstract

Le macchine crittografiche hanno rappresentato il primo esempio di sistemi elettromeccanici per la cifratura dell'informazione e la protezione dei dati. Il continuo avvicinarsi di miglioramenti nelle tecniche di attacco e di miglioramenti nel loro progetto ha rappresentato il seme per le moderne teorie della crittografia e della crittanalisi, ed ha inoltre fornito spunti fondamentali alla teoria dell'elaborazione automatica dei dati ed allo sviluppo dei primi elaboratori.

Il seminario ha lo scopo di illustrare la storia ed i principi di funzionamento di due macchine cifranti ben note: la tedesca macchina Enigma e l'italiana macchina O.M.I.Nistri, ormai rarissima. Saranno illustrate le parti che compongono la macchina: tastiera, scambiatori (rotori), visore, cablaggio dei rotori, riflettore, anello, spinette, orologio. Si illustreranno il cifrario ed il settaggio della macchina, e si eseguirà una prova di cifratura e decifratura di un messaggio in ambiente simulato. Saranno inoltre presentati due esemplari originali di tali macchine.

Antonio Fucci (I8000PU SWL) è dedito allo studio ed al collezionismo di apparati e radio militari storici. E' organizzatore di eventi, seminari e mostre espositive su apparati radio, sistemi radar e crittografici. E' consigliere della ARS (Amateur Radio Society) ed esperto di sistemi per telecomunicazioni militari, ECM, NAV e macchine cifranti.

Tutti gli interessati, ed in particolare gli studenti, sono invitati a partecipare