Activitat de Criptografia

Taller Màquina Enigma: Com xifraven els nazis a la Segona Guerra Mundial

Objectius	Des d'una vesant lúdica, però rigorosa, es pretén introduir a l'estudiant en el funcionament de la Màquina Enigma i el xifrat/desxifrat real amb aquest mètode criptogràfic. També s'introduirà l'ambient històric en el qual se situa la Màquina en l'evolució de la Criptografia i el seu ús en la Segona Guerra Mundial.
Descripció	L'activitat té un format de taller ajudat amb una presentació amb transparències que permeten situar l'ús d'aquest mètode criptogràfic. S'utilitzarà un model físic que actua com una Màquina Enigma real de tres rotors. Es disposarà d'aparells per aproximadament dos alumnes o menys per màquina i s'aprendrà a xifrar i a desxifrar amb ella. També s'explicarà com han de fer els estudiants per construir una màquina per ells mateixos després del taller (seguint una versió moderna del model estàndard ja proposat per Alan Turing). Tot aquest coneixement es proporcionarà situant aquest mètode criptogràfic en la història de la Criptografia, l'ús que es va fer a la Segona Guerra Mundial així com la seva seguretat relacionant-la amb la dificultat matemàtica (combinatòria) per trencar el mètode.
Materials utilitzats	S'utilitzaran els models de Màquines Enigma proporcionades pel Grup d'Investigació de Matemàtica Aplicada la Criptografia de la UPC per xifrar i desxifrar. Aquests xifrats i desxifrats es faran en un ambient amè, d'experimentar i jugar amb les màquines. Els estudiants xifraran de la mateixa manera que es feia amb la màquina original i es parlarà de la dificultat matemàtica de trencar aquest mètode criptogràfic.
Bibliografia webgrafia	És preferible que els estudiants vinguin sense haver consultat cap bibliografia i sense haver preparat, però això sí, motivats per fer l'activitat. Durant el taller es donaran els links a Internet a on ampliar els coneixements.
	Alumnes de quart d'ESO, 1r. i 2n. de Batxillerat Grup màxim 40 alumnes, però preferible de menys de 30-20.
	Nom persona que imparteix taller: professor responsable Germán Sáez Moreno del Grup d'Investigació de Matemàtica Aplicada la Criptografia de la UPC (https://mak.upc.edu/ca/benvingut)

	Horari del taller: a convenir Durada: al voltant d'una hora