Regió7
Barcelona

08/06/16

Prensa: Diaria
Tirada: 7.024 Ejemplares
Difusión: 5.686 Ejemplares

Cód: 103064339

Página: 8

Sección: LOCAL Valor: 1.068,00 € Área (cm2): 366,4 Ocupación: 38,3 % Documento: 1/1 Autor: GEMMA CAMPS | MANRESA Núm. Lectores: 36000

De tatuar els missatges al cap, a la màquina Enigma

Un taller del cicle «Temps de matemàtiques» ofereix un viatge en el temps pels diferents mètodes per xifrar i desxifrar missatges secrets

Crònica

GEMMA CAMPS | MANRESA

Montserrat Alsina, professora de la UPC i investigadora de les matemàtiques, va iniciar la sessió amb un senzill exercici per demostrar les dificultats de desxifrar en relació amb xifrar. Xifrar: el número resultant de multiplicar 3 per 5; desxifrar: trobar dos números que, multiplicats, donin 35. La primera operació és més ràpida, sobretot si, en el segon cas, en lloc de dos números que facin 35 demanem que facin 455.020.999, per exemple. Aquest sistema és el que utilitzen els bancs per evitar que els espiïn, va dir. Quan siguin realitat els ordinadors quàntics, però, n'hauran de trobar un altre.

Alsina va oferir el taller «Top secret» dins del cicle «Temps de matemàtiques», organitzat per l'Ateneu les Bases i la UPC a Manresa. Del rudimentari mètode de rapar el cap als esclaus, tatuar-los un missatge, deixar que els creixés el cabell de nou per tapar-lo i enviar-los al receptor, va passar a explicar el primer sistema una mica més sofisticat. El xifrat de Cèsar, del segle I aC, consistent a desplaçar les lletres de l'abecedari de manera que, movent-les tres llocs, en lloc de posar HOLA posaríem ELIX.

Per xifrar de manera més sistemàtica triant una clau diferent cada vegada es va fabricar un disc mecànic. No obstant això, descobrir la clau requeria massa temps i es va buscar un mètode més eficient per trobar-la, com l'anàlisi de freqüències, consistent a localitzar cada lletra depenent de la seva freqüència d'aparició en el missatge. A *Un manuscrit per desxifrar els missatges*, Abu Iusuf al-Kindi (s. IX) va utilitzar aquest sistema.

La introducció de la màquina Enigma, utilitzada pels nazis durant la Segona Guerra Mundial, va portar els assistents a veure un fragment de la pel·lícula que en parla. Alan Turing, que la va desxifrar, és considerat l'autor del primer ordinador de la història.

A l'inici del taller, Alsina va demanar als presents que fessin l'exercici d'imaginar què posarien en un maletí per fer d'espies si fossin al segle I. Les assistents més menudes van respondre que hi posarien un mòbil, i ella els va recordar la importància, malgrat la comoditat que suposen els avenços que han comportat les noves tecnologies, d'exercitar la capacitat de pensar i d'utilitzar la lògica.

De fet, va recordar que el llibre del Kama-Sutra (s. IV d. C) recomanava que les dones haurien d'estudiar 64 arts, incloent-hi l'art del vestir, de preparar perfums, de fer conjurs, de jugar a escacs i, com a art número 45, el de l'escriptura secreta. Per als més interessats en el tema va aportar un llibre, *L'art de la divulgació secreta*, i una pàgina web, *La cambra negra*, que segur que els agradaran.

G. C.

Montserrat Alsina en un moment del taller «Top secret», ahir, a la UPC

L'APUNT

I demà, «Una passejada per la història del nostre calendari»

La darrera sessió del cicle serà demà, a les 7 de la tarda, a l'auditori de l'Ateneu les Bases. Anton Aubanell, a qui Alsina va definir ahir com un comunicador extraordinari, explicarà el paper de les mates per adaptar l'any civil a l'any natural.