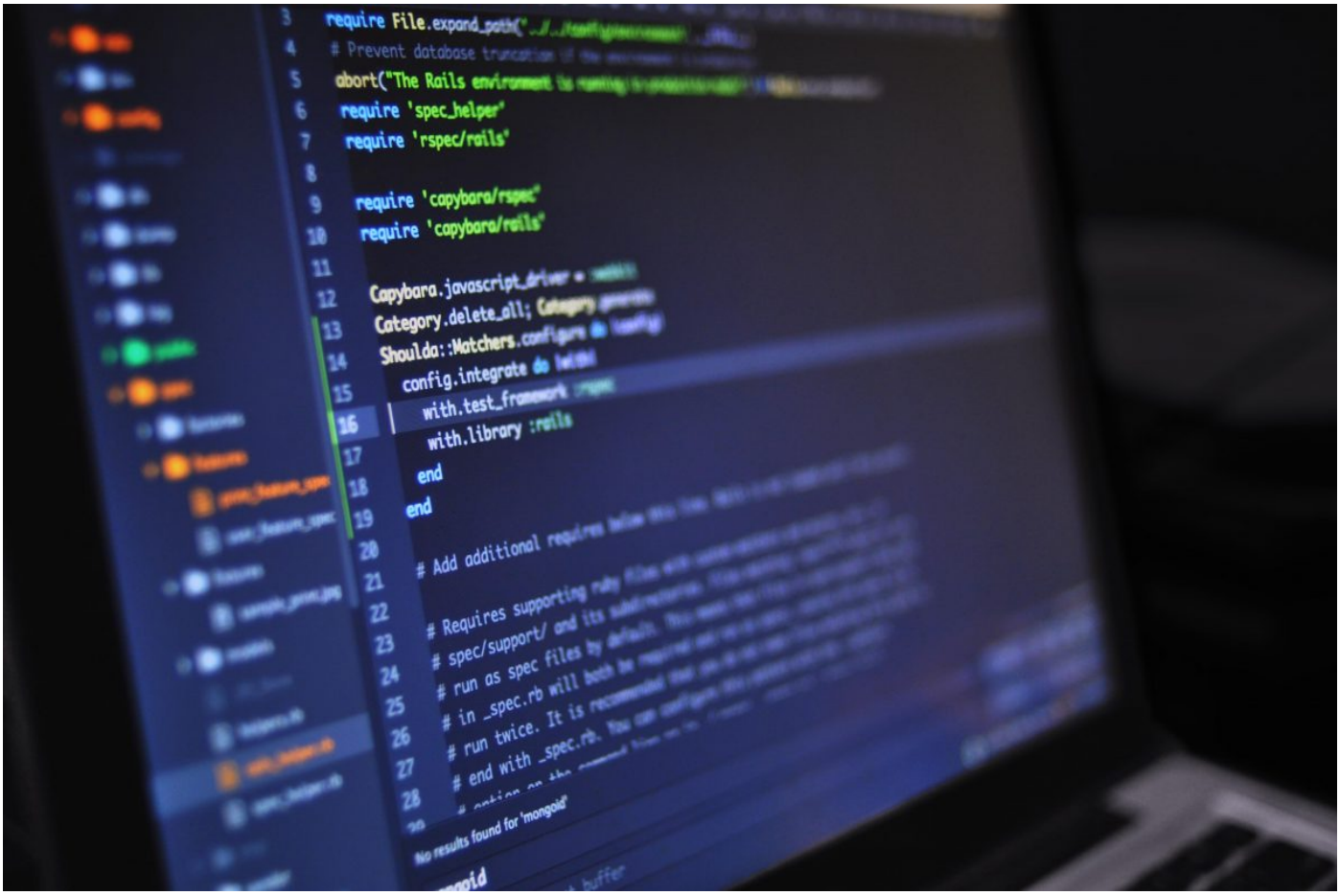
News



La crittografia: dal campo di battaglia al pin del bancomat

di Emanuele Bottazzi

*SECONDARIA DI 2° GRADO - **MATEMATICA, INFORMATICA***

CHE COS'È LA CRITTOGRAFIA?

Cara lettrice, caro lettore, ti presento Alice e Bob.

Alice e Bob hanno diversi problemi. Innanzitutto desiderano comunicare, ma non si possono vedere di persona. Di conseguenza sono costretti a scambiarsi messaggi con dei mezzi che non sono sicuri, come le e-mail. Inoltre temono che la loro nemica giurata, Eva, intercetti la loro corrispondenza per leggerla di nascosto. Di fronte a queste difficoltà, Alice e Bob hanno ideato dei metodi per comunicare in modo che nessuno riesca a capirli. In altre parole, hanno inventato la crittografia.

Rizzoli EDUCATION

News

LA CRITTOGRAFIA ANTICA

Secondo Plutarco, i primi Alice e Bob della storia dell'Occidente sono stati i generali spartani. La loro tecnica per inviare messaggi segreti si chiama scitala, ed è descritta nella Vita di Lisandro. Una delle Alice più famose della storia è Giulio Cesare. Questo imperatore ha ideato uno dei cifrari più longevi, che ancora oggi è ricordato con il suo nome.

LA CRITTOGRAFIA MODERNA

Fino alla seconda guerra mondiale gli Alice e Bob della storia sono stati condottieri, generali, monarchi e rivoluzionari. Chi sono invece gli Alice e Bob della nostra società? Sei tu, cara lettrice, quando prelievi con il bancomat. Sei tu, caro lettore, quando accedi all'area riservata di un sito internet con una password. Il pin del bancomat e le password dei servizi online sono le chiavi d'accesso ai nostri risparmi e ai nostri documenti personali: non devono cadere nelle mani di Eva! Di conseguenza, è fondamentale che la banca o i siti che visitiamo non li conoscano: in caso contrario, Eva potrebbe rubarli.

Quindi la banca Alice chiede a Bob di identificarsi mediante il suo codice segreto per autorizzarla alle operazioni, ma allo stesso tempo non può conoscere il suo pin. Per soddisfare queste richieste che a prima vista sembrano incompatibili, si utilizzano funzioni dell'aritmetica modulare facili da calcolare e difficili da invertire. Una di queste è l'elevamento al quadrato modulo un prodotto di primi, sulla quale si basa il protocollo di identificazione Fiat-Shamir.

PER APPROFONDIRE

- Alcuni cifrari antichi, inclusa la scitala e il cifrario di Cesare, sono descritti dal professor Pigola dell'Università dell'Insubria: www.dfm.uninsubria.it/pigola/stage2017/CrittografiaSimmetrica.pptx
- Il protocollo di identificazione Fiat-Shamir descritto dalla Carneige Mellon University: https://www.cs.cmu.edu/afs/cs/academic/class/15827-f98/www/Slides/lecture3/base.013.html
- Una versione didattica dei protocolli di identificazione a conoscenza zero è descritta sulla rivista Archimede https://riviste.mondadorieducation.it/archimede/wp-content/uploads/sites/2/2019/02/Bottazzi_Archimede_4_18.pdf

SCOPRI L'OPERA

CARTESIO

Trovi altri spunti interdisciplinari con le discipline dell'area STEAM (scienze, tecnologia, ingegneria, arte) nel corso Cartesio per il triennio dei licei umanistici, oltre a proposte per svolgere attività di Debate o di Webquest a partire da approfondimenti di storia della matematica.

Rizzoli EDUCATION

News

Scopri di più

Rizzoli EDUCATION