Dal Codice di Cesare agli Acquisti On-line
Come la crittografia ci ha cambiato la vita

Mauro Orlandini

INAF/IASF Bologna

La crittografia (ovvero *"scrittura nascosta"*) è diventata oggigiorno uno strumento fondamentale: ad esempio permette tutte le transazioni telematiche sicure, senza le quali l'attuale sistema economico non potrebbe funzionare.

Se c'è qualcuno che "nasconde" informazioni ci sarà sempre qualche altro che cercherà di "svelarle". Per questo "gioco" si sono mobilitati i maggiori pensatori del tempo, sono stati sviluppati apparati tecnologici e matematici formidabili, e sono state perse battaglie, guerre e migliaia di vite umane.

Verranno descritti come i sistemi crittografici si sono evoluti nel tempo: dalla *mlecchita-vikalpa*, l'arte della scrittura in codice, descritta nel *Kāmasūtra* (IV sec A.C.), alla cifratura di Cesare (I sec A.C.), primo esempio di cifratura per trasposizione, fino alle moderne tecniche di cifratura polialfabetiche per trasposizione: cifratura di Vigenère (XVI sec) e di Vernam (XX sec).

Nel nostro *excursus* incontreremo personaggi famosi, come Maria Stuarda, la cui condanna a morte fu determinata dalla decifrazione della sua corrispondenza con i congiurati per deporre ed uccidere Elisabetta I.

Lo sviluppo dell'informatica (da parte di Alan Turing) fu guidata dalla necessità di decrittare i messaggi cifrati dai Tedeschi durante la Seconda Guerra Mondiale con la famosa macchina ENIGMA, alla cui base di funzionamento vi sono i dischi cifranti ideati da Leon Battista Alberti nel XV secolo.

Parleremo della maggiore rivoluzione nella crittografia, avvenuta negli anni 70 del XX secolo, ad opera di Duffie and Hellman: la separazione della chiave per cifrare il messaggio (detta chiave pubblica) da quella per decifrarlo (detta chiave privata), alla base del sistema *RSA* utilizzato, ad esempio, per gli acquisti online e da *WhatsApp*.

Infine verrà brevemente descritta la nuova frontiera: la crittografia quantistica, diventata realtà con il lancio nel 2016 del satellite Cinese *Micius*.