

IMPERATORI, FRANCESCANI E SPIE

Piergiorgio Odifreddi

Gennaio 1996

Oltre ad essere uno degli strumenti di tortura preferiti dai professori di matematica delle scuole, i numeri primi (che sono quelli che non si possono dividere per nessun altro numero diverso da essi stessi, a parte ovviamente 1) hanno anche inaspettate applicazioni. Una recente concerne la *crittografia*, cioè la codifica di messaggi in modo da renderli difficili da leggere a chi non ne posseda la chiave.

Un metodo di codifica antico è quello chiamato *cesareo* perchè usato, secondo *Le vite dei Cesari* di Svetonio, dagli imperatori romani. Cesare Augusto scriveva i suoi messaggi sostituendo ogni lettera con quella seguente nell'alfabeto, di modo che ad esempio CESARE diventava DFTBSF. Giulio Cesare, leggermente più sofisticato, sostituiva ogni lettera con quella che la segue tre posti più in là nell'alfabeto, così che questa volta CESARE diventava FHVDUH.

Un po' più complicati sono i metodi che sostituiscono ciascuna lettera con un'altra, in ordine sparso ma fisso (ci sono miliardi di modi di farlo). Esempi famosi si trovano nei racconti *Lo scarabeo d'oro* di Edgar Allan Poe, e *Le avventure dei ballerini* di Arthur Conan Doyle.

Tutti questi metodi a sostituzione fissa non sono però molto difficili da decodificare. Oggi si conoscono infatti le frequenze precise di occorrenza di ciascuna lettera (in italiano la più frequente è la 'a', la meno frequente la 'q'), oltre che di particolari sequenze di lettere (ad esempio le doppie, o le 'ch'), nelle lingue comuni: una semplice analisi statistica permette quindi di decodificare un testo sufficientemente lungo in modo quasi automatico.

Un esempio straordinario di testo cifrato che invece non si è mai riusciti a decodificare è il cosiddetto *manoscritto di Voynich*, che si fa risalire a Ruggero Bacone (1220–1292), francescano e mago. Il manoscritto entrò in

possesso dell'imperatore Rodolfo II di Boemia nel 1666, languì per decenni nel collegio gesuita di Mondragone a Frascati, e fu infine acquistato dal polacco Wilfried Voynich nel 1912. Le sue 232 pagine sono scritte in un alfabeto di 21 lettere dall'apparenza mediorientale, e illustrate con centinaia di figure di donnine nude, piante inesistenti e animali fantastici. Che il manoscritto non sia una bufala è provato dal fatto che le sue lettere hanno una frequenza statistica non casuale (che sarebbe stato impossibile riprodurre a mano secoli fa), anche se diversa da quella delle lingue indoeuropee (e simile invece a quelle polinesiane). Ma i tentativi sia dei più famosi decrittatori militari, che ebbero invece successo coi messaggi tedeschi e giapponesi nelle due guerre mondiali, che dei computer sono stati finora frustrati.

Il metodo di codifica più usato oggi è basato sul fatto che è facile dividere un numero per un altro, ma è difficile scomporlo in fattori primi: facile qui significa che lo si può anche fare a mano, difficile che per numeri sufficientemente grandi neppure un computer lo può fare in un tempo ragionevole. Ad esempio, il numero 249.310.081 è prodotto di due numeri primi, ma anche un computer ci metterebbe un po' a scoprire quali; se invece si sa che uno dei due è 11.927, ottenere l'altro si può fare velocemente (per la cronaca, esso è 20.903).

Se poi si tratta di numeri più grandi, la cosa può diventare facilmente intrattabile. Ad esempio, nel 1977 due ricercatori moltiplicarono fra loro due primi di una sessantina di cifre ciascuno, e sfidarono il mondo matematico a trovare la decomposizione del loro prodotto, di 129 cifre: la risposta fu trovata nel 1993, dopo un anno di 'lavoro' che richiese la coordinazione, attraverso *Internet*, di 600 computer sparsi per il mondo. Si pensa che la fattorizzazione di numeri di 250 cifre possa richiedere qualcosa come milioni di anni.

L'idea per la crittografia è quindi quella di tradurre anzitutto i messaggi in numeri, associando ad ogni lettera un numero di due cifre e ad ogni parola la sequenza dei numeri corrispondenti: si ottiene così una codifica che sarebbe facile decodificare con l'analisi statistica. Ma poi si moltiplica il numero ottenuto per un primo molto grande, ottenendo un numero enorme: chi conosce la chiave, cioè il numero per cui si è moltiplicato, può facilmente decodificare il messaggio, ma chi non la conosce non può farlo in tempo ragionevole neppure con un computer.

Tempi duri per le spie, dunque, ma non impossibili: se la matematica non funziona più, continueranno comunque a funzionare sesso e denaro.