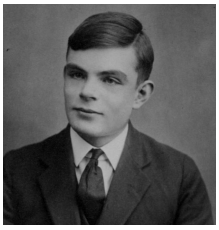
MATEMATICA E STORIA

Messaggi in codice



Durante la Seconda guerra mondiale, gli inglesi, con l'aiuto del matematico Alan Turing (1912-1954) e della macchina Colossus, sono riusciti a decifrare i messaggi in codice dei servizi segreti tedeschi.

Che cosa è la crittografia?

LA RISPOSTA

La **crittografia** (dal greco *kryptós*, «nascosto», e *gráphein*, «scrivere») è la scienza delle «scritture segrete» o «in codice».

La si usa per fare in modo che le informazioni comunicate non siano comprese da tutti, ma soltanto da coloro che conoscono il codice utilizzato in fase di scrittura e sono perciò in grado di decifrarlo.

Ipotizziamo che Alice voglia spedire un messaggio segreto a Bob. Dovrà prima trasformarlo mediante un algoritmo, una **funzione**, in un testo cifrato. Poi Bob, una volta ricevuto il messaggio, dovrà decifrarlo con la **funzione inversa** di quella usata da Alice per cifrarlo. Se Alice, per cifrare l'informazione, sostituisce mediante la funzione f ogni elemento x del suo testo con $f(x)$, allora Bob potrà decrittare il messaggio solo conoscendo l'inversa della funzione f. Perciò chiamiamo «chiave di crittazione» la funzione f usata per cifrare il testo, e la sua inversa **chiave di decrittazione.**

Il primo vero e proprio sistema per la cifratura, secondo il racconto scritto da Svetonio in *Vite dei Cesari*, fu usato da Giulio Cesare durante la guerra contro i Galli. Il **cifrario di Cesare** opera per traslazione. Se per esempio la traslazione è di tre lettere, ogni lettera del messaggio in chiaro viene sostituita da quella che occupa il terzo posto successivo nell'alfabeto: la A diventa D, la B diventa E e così via, finché la Z diventa C. Così facendo, il messaggio in chiaro *SERVONO RINFORZI* diventa il messaggio in codice: VHUBRQR UNQIRUCN.

A	B	C	…	Z
↓	↓	↓	↓	↓
D	E	F	…	C

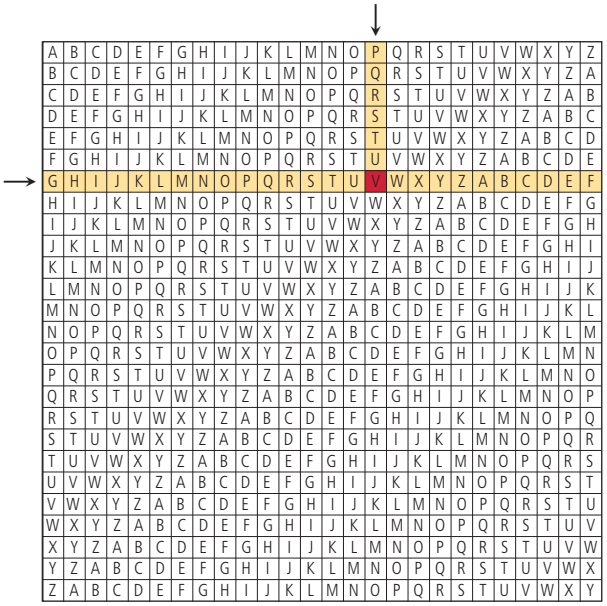
La chiave di decrittazione qui è il valore della traslazione. Si hanno quindi solo 26 cifrari distinti (perché 26 sono le lettere dell'alfabeto internazionale, quindi le possibilità di traslazione). Uno di questi cifrari è in realtà inutilizzabile perché banale: è l'identità che trasforma l'alfabeto in se stesso e quindi produce un messaggio cifrato identico a quello in chiaro.

ATTIVITÀ DI RICERCA

Il cifrario di Vigènere

Il cifrario pubblicato nel 1586 da Blaise de Vigènere è molto simile a quello di Cesare, ma introduce in più l'utilizzo di una parola chiave.

- Cerca in Internet come funziona questo cifrario e poi ottieni il messaggio cifrato corrispondente a «PROVA DI CIFRATURA» mediante la chiave «GAMBO».
- Prova poi a decrittare il seguente messaggio cifrato sapendo che la parola chiave è «DOMANI». Ricordati di usare l'alfabeto inglese.
  DHFAPKDFQ GYQ LFDIQCFWNIYQ JOXLV IOZM OEI VSETN



Copyright © 2016 Zanichelli editore S.p.A., Bologna
Questo file è una estensione online dei corsi di matematica di Massimo Bergamini, Graziella Barozzi e Anna Trifone