Scuola universitaria professionale
della Svizzera italiana
SUPSI

Matematicando*film*

Come proteggere le informazioni?

Grazie alla teoria dei numeri possiamo fare ogni giorno operazioni sicure

Il problema di Alice e Bob

Alice vuole mandare un messaggio a Bob, in modo che lui sia l'unico a leggerlo. Per evitare che qualunque persona diversa da Bob intercetti il messaggio e riesca a leggere il contenuto, Alice *cifra* il messaggio e Bob lo *decifra*, tornando così al testo originale, in modo da poterlo leggere.

Il cifrario di Cesare

Ogni lettera viene sostituita con la lettera che si trova un certo numero di posizioni dopo nell'alfabeto.

Provate a decifrare questo messaggio:
DYH FHVDUH

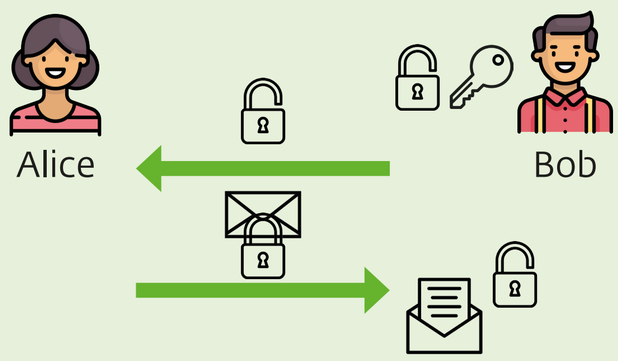
Per la risposta: www.matematicando.supsi.ch

Cifrare e decifrare: come?

Dall'antichità a oggi sono stati creati metodi di cifratura sempre più complessi: il fine è rendere i messaggi sempre più difficili da decifrare, nel caso in cui il nemico riesca a intercettarli. Tutti questi metodi hanno una caratteristica comune: per cifrare e decifrare il messaggio viene utilizzata la stessa chiave, che dev'essere nota ad Alice e Bob. Questi sistemi sono detti *simmetrici* o *a chiave privata*: prevedono che Alice e Bob abbiano un modo sicuro per scambiarsi la chiave, prima di poter iniziare a comunicare senza essere intercettati. Negli anni '70 del secolo scorso alcuni ricercatori cambiarono prospettiva: al posto di concentrarsi su come rendere sicuro lo scambio della chiave, iniziarono a pensare a come modificare l'intero sistema di cifratura.

Nacque così la cifratura *asimmetrica*: un sistema per cui mittente e destinatario possono usare due chiavi diverse per cifrare e decifrare il messaggio. In questo modo Alice e Bob non devono più scambiarsi la chiave!

Immaginiamo che Alice e Bob si stiano scambiando un messaggio nascondendolo in una cassetta di sicurezza.
Con la *cifratura asimmetrica*, Bob manda il suo lucchetto aperto ad Alice. Alice chiude la cassetta utilizzando il lucchetto di Bob e spedisce la cassetta; Bob la apre usando la propria chiave e legge il messaggio.
Il lucchetto rappresenta la *chiave pubblica* di Bob, mentre la chiave che apre il lucchetto è l'informazione che Bob deve tenere solo per sé, cioè la sua *chiave privata*.



Il contributo della matematica

Nella vita di tutti i giorni ci scambiamo messaggi attraverso sistemi elettronici che comunicano per mezzo di sequenze di numeri. La cifratura a chiave pubblica usa complesse operazioni matematiche basate sulle proprietà dei numeri, in particolare dei numeri primi.
Il principio è quello per cui dati due numeri primi anche molto grandi è possibile ottenere velocemente il loro prodotto, mentre non è banale il viceversa, cioè trovare i due numeri primi che moltiplicati tra loro danno un certo risultato.

La scomposizione in fattori primi

Bob sceglie due numeri primi (p e q), li tiene segreti, li moltiplica e comunica ad Alice il risultato (N). Alice usa N per cifrare il messaggio e Bob usa p e q per decifrarlo.
Immaginate che la chiave pubblica di Bob sia $N = 799'567$.
Riuscite a trovare p e q, cioè la sua chiave privata?

Per la risposta: www.matematicando.supsi.ch

Fonti
Singh, S. (2001). *Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a Internet*. BUR.
Icone realizzate da Freepik e Vectors Market, scaricate da www.flaticon.com