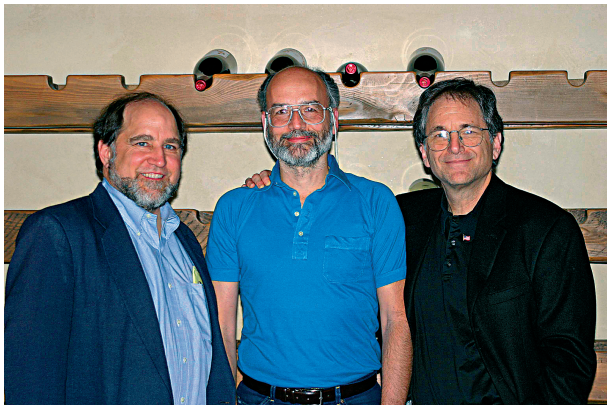
I codici segreti e la crittografia

A tutti è noto il problema della sicurezza nell'uso dei codici bancari, nelle trasmissioni di informazioni via Internet, nei pagamenti online, nell'invio e ricezione di e-mail e così via.
Se si cercano informazioni più dettagliate a questo riguardo, si scopre che quasi tutto si basa sulla trasmissione di codici numerici che, se vengono scoperti, consentono di accedere a informazioni riservate, quali conti correnti bancari, carte di credito, codici di identificazione dei computer e così via.
Per evitare che dati personali o segreti possano venire scoperti, si codificano queste informazioni in modo tale che solo chi trasmette il messaggio e chi lo riceve siano in grado di comprendene il significato; in altre parole si usa la **crittografia**.
Semplificando un po' la procedura, la codifica di un'informazione avviene in questo modo. Il messaggio viene dapprima scomposto in varie parti mediante una chiave segreta, normalmente costituita da un numero di molte cifre, ottenuto come prodotto di due numeri primi molto grandi; chi riceve il messaggio codificato, conoscendo la chiave, lo ricompone e lo interpreta.
Uno dei metodi di costruzione della chiave è detto *RSA* dal nome dei suoi autori, Ron Rivest, Adi Shamir e Leonard Adleman *(nella foto)*, che lo inventarono nel 1978.



Per scoprire come funziona questo metodo dobbiamo prima chiarire l'uso dell'operatore **mod**; dati due numeri interi a e b la scrittura

$$a \bmod b$$

indica il resto della divisione intera di a con b. Per esempio:

$27 \bmod 5 = 2$ perché $27 : 5$ ha come resto 2

$76 \bmod 8 = 4$ perché $76 : 8$ ha come resto 4

Ciò detto, l'RSA funziona in questo modo.

1. Si scelgono due numeri primi a e b grandi
2. si sceglie un numero c che sia minore del prodotto ab e tale che il prodotto $(a-1)(b-1)$ ed il numero c stesso siano primi fra loro (non è necessario che c sia primo)

Una prima osservazione che possiamo fare a questo punto è che i numeri $a-1$ e $b-1$ sono pari e che quindi il loro prodotto $(a-1)(b-1)$ è anch'esso pari; quindi c deve essere dispari altrimenti non sarebbe primo con $(a-1)(b-1)$.

3. Si calcola il numero d in modo che $(dc-1)$ sia divisibile per $(a-1)(b-1)$
4. indicato con k il numero intero da crittare (il testo in chiaro) si calcola $k^c \bmod (ab)$, cioè il resto della divisione di k^c per il prodotto ab.

Il numero ottenuto (il testo in codice), che indichiamo con m è la traduzione in codice di k.

5. Il ricevente, che riceve il numero m, deve a questo punto decrittarlo, cioè deve risalire a k; per farlo si esegue questo calcolo:
   $m^d \bmod ab$
   Questo sistema è detto a chiave pubblica perché i numeri ab e c sono resi pubblici, mentre il numero d è la chiave privata. Vediamo un esempio calcolando il codice crittato del numero 15. Sceglieremo due numeri primi a e b non troppo grandi per non complicare il calcolo; ricorda però che, nelle situazioni reali, questi numeri sono scelti apposta molto grandi in modo che anche un computer veloce impieghi un tempo infinito (relativamente ai tempi di una decodifica) a scomporre il prodotto ab.

1. Poniamo
   $a = 11$ e $b = 23 \quad \rightarrow \quad ab = 11 \cdot 23 = 253$
2. Calcoliamo $(a-1)(b-1) = 10 \cdot 22 = 220$ e

scegliamo il numero $c < 253$ che sia primo con 220, per esempio $c = 21$; infatti
$M.C.D.(220, 21) = 1$.

I numeri 253 e 21 costituiscono la chiave pubblica.

Osserva che però non sono noti i numeri a e b e quindi nemmeno il numero 220.

3. Calcoliamo un numero d in modo che $(dc - 1)$ cioè $(21d - 1)$ sia divisibile per 220, vale a dire che $21d - 1$ deve essere un multiplo di 220 :

$21d - 1 = h \cdot 220$

Se hai imparato a risolvere le equazioni numeriche alla scuola media sai che questa relazione è equivalente alle seguenti:

$$21d = h \cdot 220 + 1 \qquad \rightarrow \qquad d = \frac{220h + 1}{21}$$

e si deve trovare un valore di h in modo che d sia intero. Procediamo per tentativi:

$h = 1 \qquad d = \frac{221}{21}$

$h = 2 \qquad d = 21$

Il successivo valore di h che dà un d intero è 23 ed in questo caso $d = \frac{220 \cdot 23 + 1}{21} = 241$

Poniamo $d = 241$ che è quindi la chiave privata che solo l'autore del messaggio ed il ricevente devono conoscere.

4. Calcoliamo

$k^c \bmod (ab)$: $\quad 15^{21} \bmod 253 = 158$

Abbiamo quindi trovato che $m = 158$.

Il testo in codice è 158 ed è il messaggio che viene trasmesso.

5. Il ricevente, che conosce il valore di d è il solo che può decodificare il codice con la formula $m^d \bmod ab$:

$158^{241} \bmod 253 = 15$

Il messaggio decrittato è 15.

In questo esempio abbiamo crittato e decrittato un numero; per la traduzione in codice di un messaggio linguistico si deve prima convertire il messaggio in una serie di numeri. I metodi possono essere diversi:

- si può convenire che ogni lettera del messaggio, compresi gli spazi fra una parola e l'altra, corrispondano ad un numero che potrebbe essere quello del codice ASCII (puoi trovare la tabella dei codici ASCII in un qualsiasi testo di informatica);
- si può costruire un vocabolario di un certo numero di parole base a cui associare un numero;
- si può scegliere un libro qualsiasi, in possesso sia della persona che trasmette che di quella che riceve il messaggio, e indicare il numero di pagina, il numero di riga e il numero d'ordine nella riga di una parola, e così via.

Due ragazzi provano a scambiarsi messaggi usando il metodo *RSA*; per evitare calcoli esageratamente laboriosi, usano numeri primi abbastanza piccoli e, visto che hanno entrambi lo stesso vocabolario della lingua italiana, convengono di far corrispondere ad ogni parola del codice il numero che si ottiene accostando il numero di pagina in cui si trova la parola con il numero d'ordine della parola in quella pagina (sempre composto da due cifre); per esempio, se la parola *casa* si trova a pagina 328 ed è la sesta parola di quella pagina, il numero che la identifica è 32806. Per tutto ciò che non esiste sul vocabolario useranno la tabella dei codici ASCII.
Aiutali a codificare i seguenti messaggi (metti i verbi all'infinito per semplificare la traduzione).

a. Domani compito di matematica. Studiamo insieme?

b. Sei invitato alla mia festa sabato sera.
(Suggerimento: il testo da codificare potrebbe essere: "Invitato mia festa sabato sera")

c. Luca è davvero simpatico, ma la sua ragazza è una smorfiosa.
(Suggerimento: il testo potrebbe essere: "Luca davvero simpatico, sua ragazza smorfiosa")

d. La nuova ragazza arrivata in classe è davvero carina.

e. Hai sentito l'ultimo pezzo di Ligabue? Davvero fantastico.