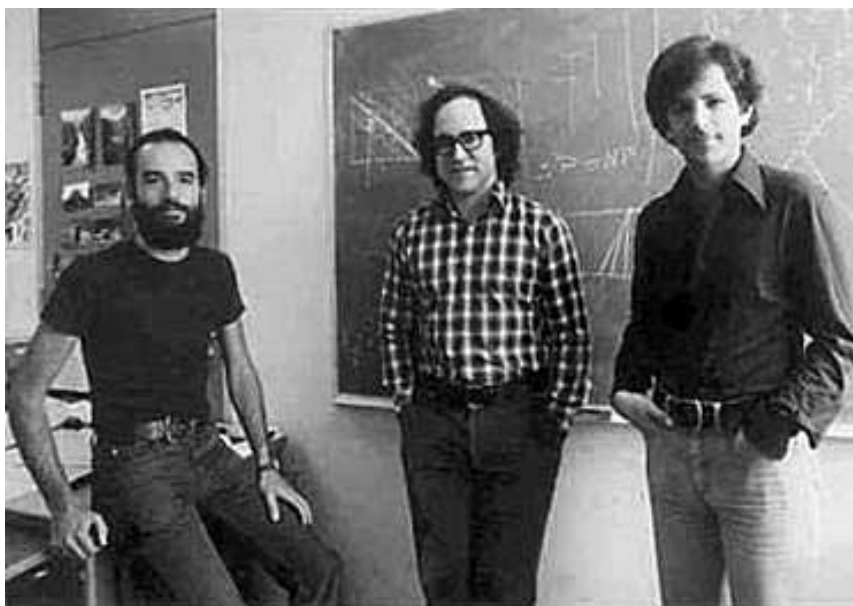


una possibile funzione unidirezionale

- moltiplicare due interi a n bit è **facile** (in $\mathcal{O}(n^2)$ con l'algoritmo usuale)
- trovare un primo a n bit, e verificare che è primo, è **facile** (vedremo poi)
- fattorizzare un numero a n bit è **difficile** ($2^{cn^{1/3}}$)
- si può costruire un crittosistema a chiave pubblica basato su questa osservazione?

il CS a chiave pubblica RSA - 1978



Shamir, Rivest, Adelman

crittosistema RSA

- Sia $N = pq$, p, q primi. Sia $\mathcal{P} = \mathcal{C} = \mathbb{Z}_N$.
- Lo spazio delle chiavi è

$$\mathcal{K} = \{(N, p, q, d, e) \mid de \equiv 1 \pmod{\phi(N)}\}.$$

- Se $k = (N, p, q, d, e)$ è una chiave, poniamo
- $e_k(x) = x^e \pmod{N}$
- N e e sono la **chiave pubblica**
- $d_k(y) = y^d \pmod{N}$
- p, q, d sono la **chiave privata**

cifratura e decifratura

$$e_k(x) = x^e \pmod{N}, \quad d_k(y) = y^d \pmod{N}$$

- verifichiamo che $d_k(e_k(x)) = x$
- $ed \equiv 1 \pmod{\phi(N)}$, quindi $ed = 1 + k\phi(N)$
- se $(x, N) = 1$, allora

$$\begin{aligned} (x^e)^d &= x^{1+k\phi(N)} \\ &= (x^{\phi(N)})^k x \\ \text{Eulero} &\equiv 1^k x \pmod{N} \\ &\equiv x \pmod{N} \end{aligned}$$

- se $x \notin U(\mathbb{Z}_N)$, vale il corollario già visto (N è il prodotto di due primi)

quindi la funzione di cifratura è **iniettiva**

implementazione dell'RSA

- Bob genera casualmente due primi “grandi”, p e q , con $p \neq q$
- calcola $N = p \cdot q$ e $\phi(N) = (p - 1) \cdot (q - 1) = pq - (p + q) + 1$
- genera (in maniera non necessariamente casuale) un esponente e con $1 < e < \phi(N)$, tale che $(e, \phi(N)) = 1$
- calcola $d = e^{-1} \pmod{\phi(N)}$
- la chiave pubblica è (N, e) , quella privata è (p, q, d)

un esempio

- Bob sceglie $p = 17$ e $q = 11$
- $N = 187$ e $\phi(N) = 16 \cdot 10 = 160 (= 2^5 \cdot 5)$
- Bob sceglie $e = 7$; allora $d = e^{-1} = 23 \pmod{160}$; pubblica la chiave $N = 187$ e $e = 7$
- Alice vuole cifrare il testo in chiaro 88 da mandare a Bob
- calcola $88^7 = 11 \pmod{187}$ e lo invia a Bob
- Bob riceve 11; per decifrare, calcola $11^{23} \pmod{187}$, e ritrova 88

Problemi facili (polinomiali)

- ① dato un intero N , vedere se è primo (vedremo poi)
- ② dati e e M , trovare (e, M) ; se è 1, calcolare l'inverso di e modulo M (alg. di Euclide – polinomiale)
- ③ calcolare la f.ne $x \rightarrow x^e \pmod{N}$ (alg. square & multiply – polinomiale)

Problemi difficili

- ④ dato un intero N , fattorizzarlo
- ⑤ dato un intero N , calcolare $\phi(N)$
- ⑥ dati N e e , trovare d tale che $(x^e)^d = x \pmod{N}$

Problemi facili

- ① dato un intero N , vedere se è primo (test di primalità)
- ② dati c e M , trovare (c, M) ; se è 1, calcolare l'inverso di c modulo M (alg. di Euclide – polinomiale)
- ③ calcolare la f.ne $x \rightarrow x^e \pmod{N}$ (square and multiply)

problemi “facili” - primalità

- ci sono **infiniti numeri primi** (Euclide)
- la dimostrazione è per assurdo (è la più celebre dimostrazione per assurdo): supponiamo ci siano solo un numero finito di primi, e siano questi p_1, p_2, \dots, p_k
- consideriamo il numero $p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$
- questo numero non è divisibile per nessuno dei p_1, p_2, \dots, p_k – e allora quali sono i suoi fattori primi?
- ci sono infiniti primi – quanti sono i numeri primi che precedono un dato intero x ?

teorema dei numeri primi

- $\pi(x)$ = numero di primi p con $p \leq x$
- esempio: $\pi(30) = 4 + 4 + 2 = 10$
- **teorema dei numeri primi:** $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1$
(quindi asintoticamente, $\pi(x) \approx \frac{x}{\log(x)}$)
- congetturato da Legendre, poi da Gauss (nel 1792 - a quindici anni!)
- dimostrato da Hadamard, de la Vallée Poussin verso fine 800 (importante contributo di Chebyshev \sim 1850)

x	10^3	10^6	10^9
$\pi(x)$	168	78.498	50.847.478
$[x/(\log x)]$	145	72.382	48.254.942
$[\pi(x)(\log x)/x]$	1,159...	1,084...	1,053...

teorema dei numeri primi - interpretazione probabilistica

- dato un intero positivo N , la probabilità che un numero $< N$ scelto a caso sia primo è $\pi(N)/N$
- per N molto grande $\approx 1/\log(N)$
- esempio: la probabilità che un numero casuale con al più 100 cifre decimali sia primo è $\approx 1/\log(10^{100}) \approx 1/230$
- possiamo scartare i numeri pari (che sono $1/2$) e i multipli di 3 (che sono $1/3$): possiamo scartare $2/3 = 1/2 + 1/6$. La probabilità di trovare un primo diventa $\approx 1/77$.
- se sappiamo controllare se un intero è primo, trovare primi grandi è facile