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?

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

Problemi facili (polinomiali)

1. dato un intero N, vedere se è primo
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 $x \to x^e \pmod N$
   (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 $(x^e)^d = x \pmod N$

- Se Eve riesce a fattorizzare $N = pq$, ottiene le info private di Bob
- dunque violare l'RSA non può essere più difficile che fattorizzare
- conoscere la fattorizzazione $\iff$ calcolare $\phi(N)$:
  - $\Rightarrow$ ovvio
  - $\Leftarrow$ conoscere N $(= pq)$ e
    $\phi(N)$ $(= (p-1)(q-1) = N - (p+q) + 1)$ vuol dire conoscere la somma $(N - \phi(N) + 1)$ e il prodotto (N) di p,q – quindi conoscere p e q
- se Eve risolve 6, dati N e e, trova d tale che
  $(x^e)^d = x \pmod N$
- (Miller) ho buone probabilità di riuscire a fattorizzare N (vedremo poi)
- i problemi difficili sono tra loro equivalenti

i problemi 4,5 e 6 sono quindi equivalenti: ma questo non prova che la sicurezza di RSA è equivalente alla fattorizzazione – c'è la possibilità di trovare la radice e-sima in qualche altro modo...

RSA e fattorizzazione

- risolvere uno dei tre "problemi difficili" è computazionalmente equivalente a fattorizzare N
- questo non basta a dire che per violare bisogna fattorizzare N
- si potrebbe riuscire a decrittare senza calcolare l'esponente d

l'equivalenza si ha con il

RSA problem: dati e e N, calcolare le radici e-sime modulo N

non si sa se l'RSA problem è equivalente alla fattorizzazione

RSA problem e fattorizzazione

RSA problem: dati e e N, calcolare le radici e-sime modulo N

- se si sa fattorizzare N, si può risolvere l'RSA problem
- c'è un algoritmo polinomiale che calcola radici e-sime modulo p se $(e, p-1) = 1$
- è facile vedere (teorema cinese dei resti) che calcolare la radice e-sima di x mod p e mod q $\Rightarrow$ calcolare la radice e-sima di x mod $N = pq$
- per provare l'equivalenza basta provare una riduzione del tipo
  - algoritmo efficiente per il calcolo relle radici e-sime mod N $\Rightarrow$ algoritmo efficiente per fattorizzare N
- trovare questa riduzione è probabilmente il più importante problema aperto della PKC
- una tale riduzione esiste per $e = 2$ - radici quadrate. Questo si usa nel CS di Rabin

RSA – funzione trapdoor unidirezionale

- una trapdoor (botola) one-way function è una funzione unidirezionale che diventa facile da invertire, se si conosce un'informazione supplementare
- la nostra lo è: abbiamo visto che si può invertire la f.ne $f_e : x \to x^e \pmod N$ usando la funzione $f_d : y \to y^d \pmod N$, se $ed \equiv 1 \pmod{\phi(N)}$
- l' informazione supplementare è l'esponente d – difficile da ricavare dalle informazioni pubbliche

fattorizzazione

- la difficoltà di fattorizzare interi grandi non va comunque sopravvalutata
- nel 77, Rivest, Shamir e Adelman hanno proposto una sfida nella rubrica di Martin Gardner su *Scientific American*
- bisognava decifrare un testo cifrato con l'RSA-129 – con chiave pubblica $e = 9007$ e

```
N = 114381625757888867669235779976146
        612010218296721242362562561842935 7
        069352457338978305971235639587050 5
        898907514759929002687954354 1
```

- Rivest stimava che per fattorizzare N ci sarebbero voluti 40 quadrillioni di anni (1 quadrillione $=10^{15}$)
- il testo è stato decrittato nel 1994, da un team coordinato da Derek Atkins, Michael Graff, Arjen Lenstra, Paul Leyland usando il calcolo distribuito – il calcolo è durato sei mesi, ha coinvolto 1600 macchine
- il testo in chiaro era

  the magic words are squeamish ossifrage

- questo successo è dovuto essenzialmente al miglioramento degli algoritmi di fattorizzazione