

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**

test di primalità

- dato un intero N a k bit, come scoprire se è un primo?
- posso provare a fattorizzarlo per **divisioni successive**: devo fare al più \sqrt{N} divisioni, quindi è in $\mathcal{O}(2^{k/2})$ – scopro se è primo, e trovo anche i fattori
- i test di primalità scoprono se N è primo; se non lo è **non scopriamo niente dei suoi fattori**
- fino al 2002 si conoscevano solo test di primalità polinomiali **probabilistici**, non **deterministici**

test deterministici e test probabilistici

- un test **deterministico** dà una risposta certa: N è primo o non lo è
- un test **probabilistico** \mathcal{T} consiste in una successione di test $\{\mathcal{T}_m\}_{m \in \mathbb{N}}$ e una successione che va a zero $\{\epsilon_m\}_{m \in \mathbb{N}}$ tale che,
 - se N **non** passa il test \mathcal{T}_m allora **non è primo**,
 - la probabilità che N superi i test $\mathcal{T}_1, \dots, \mathcal{T}_m$ e non sia primo è minore di ϵ_m
- i test di primalità probabilistici più usati sono quello di **Solovay-Strassen** (1977) e quello di **Miller-Rabin** (1980)

AKS

- fino al 2002 si conoscevano solo test di primalità polinomiali **probabilistici**, non **deterministici**
- nel 2002, M. Agrawal insieme a due suoi dottorandi, Kayal e Saxena, hanno trovato un algoritmo **polinomiale** per determinare la primalità
- inizialmente, in $\mathcal{O}(k^{12})$ – nel 2005, Lenstra e Pomerance lo portano a $\mathcal{O}(k^6)$
- **primes** è in **P**

idea per test

- per mostrare che un numero N non è primo si mostra che non si comporta come un primo
- si “cercano prove” del fatto che N non si comporta come un primo
- senza cercare i suoi fattori

PT di Fermat e test di Fermat

- il PTdF dice che, se p è un primo e $1 \leq a \leq p - 1$, allora $a^{p-1} \equiv 1 \pmod{p}$
- vogliamo scoprire se N è primo – se trovo $a \leq N - 1$ e $a^{N-1} \not\equiv 1 \pmod{N}$ sappiamo per certo che N non è primo – senza sapere niente sui suoi fattori
- questo è il **test di Fermat**
 - prendo $a < N$, calcolo (a, N) ; se $\neq 1$, N non è primo
 - se $(a, N) = 1$, calcolo $a^{N-1} -$ se $\not\equiv 1 \pmod{N}$ allora N non è primo
- per esempio, $2^{322} \equiv 157 \pmod{323}$; quindi 323 non è primo ($323 = 17 \cdot 19$)

pseudoprimi

- se però $a^{N-1} \equiv 1 \pmod{N}$ – non posso concludere che N è primo
- per esempio $2^{340} \equiv 1 \pmod{341}$, ma $341 = 11 \cdot 31$
- si dice che N è uno **pseudoprimo** in base a se N non è primo, $(a, N) = 1$ ma $a^{N-1} \equiv 1 \pmod{N}$. 341 è uno pseudoprimo in base 2.
- possiamo provare diversi valori per a : per esempio $3^{340} \not\equiv 1 \pmod{341}$ – quindi 341 non passa il test!

numeri di Carmichael

- non basta: esistono numeri N che sono **pseudoprimi** in base a **per ogni possibile base a** dove $1 \leq a < N$ e $(a, N) = 1$
- un tale N si dice **numero di Carmichael**
- per esempio, si può vedere che 561 è un ndC (è il più piccolo)
- il test di Fermat non va bene
- dà comunque un'idea di come può funzionare un test di primalità