UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Algebra

Alessandro D'Andrea

6. Crittografia RSA

Richiami

- $(\mathbb{Z}/n)^\times$ è un gruppo rispetto alla moltiplicazione
- Teorema di Eulero: se gli elementi invertibili in $\mathbb{Z}/n$ sono in totale $\varphi(n)$, allora $a^{\varphi(n)} \equiv 1 \mod n$ non appena $\mathrm{MCD}(a, n) = 1$.
- Oggi: **Come calcolare potenze modulo n sia di elementi invertibili che di elementi non invertibili**
- **Crittografia RSA**

Potenze modulo *n*

Supponiamo di voler calcolare 2^{1234} modulo 101. Strade possibili:

- Calcoliamo 2^{1234} e poi calcoliamo il resto nella divisione per 101
- Calcoliamo le potenze di 2 modulo 101 moltiplicando ogni precedente potenza per 2
- Utilizziamo in modo intelligente il Teorema di Eulero

Potenze, caso invertibile - I

La base 2 è invertibile modulo 101.

- Se MCD$(a, n) = 1$, allora $a^{\varphi(n)} \equiv 1 \mod n$.

Poiché 101 è primo, $\varphi(101) = 100$. Allora

$$2^{100} \equiv 1 \mod 101.$$

Quindi

$$2^{1234} = 2^{12 \cdot 100 + 34} = (2^{100})^{12} \cdot 2^{34} \equiv 1^{12} \cdot 2^{34} \equiv 2^{34} \mod 101.$$

Calcolare 2^{34} è più semplice, o quantomeno più rapido.

Potenze, caso invertibile - II

$$
\begin{aligned}
2^2 &= 4 \\
2^4 = (2^2)^2 &= 4^2 = 16 \\
2^8 = (2^4)^2 &= 16^2 = 256 \equiv 54 \mod 101 \\
2^{16} = (2^8)^2 &\equiv 54^2 = 2916 \equiv -13 \mod 101 \\
2^{32} = (2^{16})^2 &\equiv (-13)^2 = 169 \equiv 68 \mod 101
\end{aligned}
$$

$$
2^{34} = 2^{32} \cdot 2^2 \equiv 68 \cdot 4 = 272 \equiv 70 \mod 101
$$

In conclusione,

$$
2^{1234} \equiv 2^{34} \equiv 70 \mod 101.
$$

Potenze, caso non invertibile - I

Abbiamo imparato a calcolare rapidamente una potenza $\mod n$ quando la base è invertibile.

Calcoliamo 2^{1234} modulo 100. Problema: $\text{MCD}(2, 100) = 2 \neq 1$.

Il teorema cinese dei resti ci dice che possiamo calcolare un numero modulo 4 e modulo 25 e poi mettere insieme queste informazioni.

Sappiamo che $2^2 \equiv 0 \mod 4$, quindi ogni potenza successiva è 0.

Ora calcoliamo $2^{1234} \mod 25$.

Potenze, caso non invertibile - II

Per quanto riguarda $2^{1234} \mod 25$, abbiamo $\varphi(25) = 20$ e $\mathrm{MCD}(2, 25) = 1$. Poiché

$$1234 = 61 \cdot 20 + 14,$$

allora

$$2^{1234} \equiv 2^{14} \mod 25.$$

$$\begin{aligned} 2^2 &= 4 \\ 2^4 = (2^2)^2 &= 4^2 = 16 \\ 2^8 = (2^4)^2 &= 16^2 = 256 \equiv 6 \mod 25 \end{aligned}$$

$$2^{14} = 2^8 \cdot 2^4 \cdot 2^2 \equiv (6 \cdot 16) \cdot 4 = -16 \equiv 9 \mod 25$$

Potenze, caso non invertibile - III

$$\begin{cases} 2^{1234} \equiv 0 \mod 4 \\ 2^{1234} \equiv 9 \mod 25. \end{cases}$$

Risolviamo allora

$$\begin{cases} x \equiv 0 \mod 4 \\ x \equiv 9 \mod 25. \end{cases}$$

Abbiamo $x = 9 + 25t$. Sostituendo, $9 + 25t \equiv 0 \mod 4$, cioè

$$t \equiv -1 \mod 4.$$

Allora $t = -1 + 4s$, e sostituendo nuovamente, $x = 9 + 25(-1 + 4s)$, cioè

$$x \equiv -16 \equiv 84 \mod 100.$$

In conclusione, $2^{1234} \equiv 84 \mod 100$.

Potenze modulo $N = pq$

Se $N = pq$, dove $p < q$ sono primi, allora $\varphi(N) = (p-1)(q-1)$.

- Se MCD$(a, N) = 1$, allora $a^{\varphi(N)} \equiv 1 \mod N$.
  - $a^{\varphi(N)+1} \equiv a \mod N$;
  - $a^{k\varphi(N)+1} \equiv a \mod N$.
- Se MCD$(a, N) = p$, allora
  - $a^{q-1} \equiv 1 \mod q$
  - $a^q \equiv a \mod q$
  - $a^n \equiv 0 \mod p$ per ogni $n \geq 1$
  - $a^q = a^{(q-1)+1} \equiv a \mod pq = N$
  - $a^{h(q-1)+1} \equiv a \mod N$.
  - $a^{\varphi(N)+1} \equiv a \mod N$.
  - $a^{k\varphi(N)+1} \equiv a \mod N$.
- Se MCD$(a, N) = q$ oppure pq, succede la stessa cosa.

Le potenze di a modulo $N = pq$ si ripetono ogni $\varphi(N)$ esponenti, a prescindere dal valore di a.

Crittografia a chiave pubblica

Ho bisogno di ricevere messaggi sicuri.

- Rendo pubblica una chiave per codificare i messaggi che devono essermi inviati
- Tengo privata una chiave per decodificare i messaggi che ho ricevuto codificati
- **Codificare, se si è in possesso della chiave pubblica, deve essere una procedura rapida**
- **Decodificare, se si è in possesso della chiave privata, deve essere una procedura rapida**
- **Decodificare, se non si è in possesso della chiave privata, deve essere una procedura molto lenta**
- **Ricavare la chiave privata dalla chiave pubblica deve essere una procedura molto lenta**

Problema: trovare uno schema crittografico che abbia tutte queste proprietà.

Crittografia RSA - I

Lo schema crittografico RSA possiede (più o meno) tutte queste proprietà.

Messaggio in chiaro: $0 \leq m < N = pq$.

Chiave (pubblica) di codifica: $1 \leq d < \varphi(N)$, scelto in modo che $\overline{d}$ sia invertibile $\mod \varphi(N)$.

Codifica: $m \mapsto m^d \mod N$.

Un computer calcola rapidamente $m^d \mod N$.

Per decodificare devo estrarre la radice d.esima di m^d modulo N.

Crittografia RSA - II

Se d è invertibile modulo $\varphi(N)$, posso calcolare il suo inverso h con l'algoritmo euclideo e l'identità di Bézout.

Chiave (privata) di decodifica: $1 \leq h < \varphi(N)$, scelto in modo che $\overline{h}$ sia l'inverso di $\overline{d}$ in $\mod \varphi(N)$.

Se $dh \equiv 1 \mod \varphi(N)$, allora

$$(m^d)^h = m^{dh} = m^{1+k\varphi(N)} \equiv m \mod N.$$

Decodifica: $m \mapsto m^h \mod N$.

Un computer calcola rapidamente $m^h \mod N$.

Crittografia RSA - III

Chi ha prodotto le chiavi ha scelto due numeri primi p, q che conosce, e li ha moltiplicati ottenendo $N = pq$. I numeri p e q sono tenuti privati, mentre N viene reso pubblico.

Chi ha prodotto le chiavi può calcolare facilmente $\varphi(N) = \varphi(pq) = (p-1)(q-1) = N + 1 - (p+q)$.

Conoscere $\varphi(N)$ è equivalente a conoscere la fattorizzazione $N = pq$, perché da N e da $\varphi(N)$ si ricava la somma $p + q$.

Non sono note procedure rapide per fattorizzare un numero (grande). Sono invece note procedure rapide per trovare primi grandi.

Trovare due primi grandi e moltiplicarli è veloce. Fattorizzare il prodotto così ottenuto richiede molto tempo.

Crittografia RSA - IV

Nella pratica:

- Si producono due numeri primi p, q di 1024 cifre binarie, cioè circa 300 cifre decimali. (richiede secondi)
- Si calcola il prodotto $N = pq$ e si sceglie $1 < d < \varphi(N)$ in modo che $\overline{d}$ sia invertibile $\mod N$. (pressoché immediato)
- Si calcola l'inverso $\overline{h}$ di $\overline{d}$. Si ottiene $1 < h < \varphi(N)$. (pressoché immediato)
- Si rendono pubblici N, d. Si tiene privato h.
- Tutti possono codificare un messaggio utilizzando N, d. (frazioni di secondo)
- Tutti possono decodificare un messaggio **se conoscono** h. (frazioni di secondo)
- Conoscere h è (pressoché) equivalente a fattorizzare N. (Allo stato attuale: svariate decine di anni utilizzando una rete **molto grande** di sistemi dedicati?)

Anticipazioni

Fra qualche lezione, cercheremo di capire, qualitativamente, come trovare primi grandi.

Avremo bisogno di capire come funzionano le congruenze quadratiche.