

# CRITTOGRAFIA

lezioni di lunedì

---

5 ottobre

ore 11:15

---

---

---

---



$$N = \sum_{i=0}^{\lfloor n/\log n \rfloor - 1} 2^i = \frac{2^{\lfloor n/\log n \rfloor - 1}}{2 - 1}$$

$$= 2^{\lfloor n/\log n \rfloor} - 1 < 2^n$$

$$S = 2^n$$

$T = \# \text{ seq. } \underline{\text{non}} \text{ concidi}$

$$T \leq N < S \Rightarrow T \leq S$$

$$\lim_{n \rightarrow \infty} \frac{T}{S} \leq \frac{2^{\lfloor n/\log n \rfloor} - 1}{2^n} \xrightarrow[2^n \rightarrow 0]{} 0$$

Generatori di numeri pseudocasuali basati su  
cifroni simmetrici.

- cifrario simmetrico
- chiave
- si sostituisce il messaggio ~~con~~ con un valore  
iniziale legato al generatore

ESEMPIO approvato dal FIPS

usa il DES

$r = \#$  bit delle parole prodotte ( $r = 64$ )

$s =$  seme ~~casuale~~ casuale di  $r$  bit

$m = \#$  parole da produrre

$k =$  chiave segreta del cifrario

Generatore ( $s, m$ ) // flusso di output di  $m+r$  bit

$d$  = rappresentazione in  $r$  bit di data e ora

$$y = G(d, k);$$

$$z = s$$

for ( $i = 1$ ;  $i \leq m$ ;  $i++$ ) {

$$x_i = G(y \oplus z, k);$$

$$z = G(y \oplus x_i, k);$$

comunicare  $x_i$  all'esterno;

}

# Algoritmi randomi

LAS VEGAS

- generano un risultato  
SICURAMENTE CORRETTO  
in un tempo  
PROBABILMENTE BREVE  
(QuickSort)

MONTE CARLO

- generano un risultato  
PROBABILMENTE CORRETTO  
in un tempo  
SICURAMENTE BREVE  
(test di primalità)

probabilità di errore

← →  
asimmetricamente  
piccole matematicamente  
misurabile

# Test di primalità (Miller, Robin, $\approx$ anni '80)

$N$  numero intero di  $n$  bit disponibili

$$N-1 = 2^w z$$

w  
poni

$z$  disponibile

w è ~~esso~~ l'esponente della potenza di 2 più grande che divide  $N-1$

$$N=17$$

$$N-1=16 = 2^4 \cdot 1$$

\*  $z=1$   
 $w=4$

$$N=21$$

$$N-1=20 = 2^2 \cdot 5$$

$z=5$   
 $w=2$

sì calcola  
in tempo  
polinomiale nel  
# di cifre di  $N$   
( $n = \log N$ )

$N$  $N-1$  $\frac{N-1}{2}$  $\frac{N-1}{4}$  $\vdots$  $\vdots$  $f = 1$ 

# divisioni per 2  $\leq \underline{\log N} = n$

$N$  sia un numero primo

sia  $2 \leq y \leq N-1$  intero arbitrario

$$N-1 = 2^{\omega} \cdot 2$$

$2$  disponi

$N$  primo  $\Rightarrow$

P1:  $\text{mcd}(N, y) = 1$

P2:  $y^{2^i} \pmod{N} = 1$

OR

$$\exists i, 0 \leq i \leq \omega-1 \text{ t.c.}$$

$$y^{2^i} \pmod{N} = -1$$

$$i \in [0, \omega-1]$$

$$y^{1((2^i) + 2)}$$

## Lemma 1 (Miller, Robin)

Se  $N$  è un numero composto, il numero di interi compresi tra  $2$  e  $N-1$  ~~che~~ che soddisfano entrambi i predicati  $P_1$  e  $P_2$  è minore di  $N/4$ .

prob. di  
scegliere  
un  
testimone  
che rende  
veri  $P_1$  e  $P_2$

$$\frac{N/4}{N-2} < \frac{1}{4}$$

N

y: scelto a caso in  $[2, N-1]$

- se uno dei due predicatori è falso  
 $\Rightarrow N$  è certamente composito

- se i predicatori sono entrambi veri  
 $\Rightarrow N$  è composto con probabilità  $< \frac{1}{4}$   
dunque  $N$  è primo con probabilità  $> \frac{3}{4}$

Iterando k volte:

la probabilità di errore  $< \left(\frac{1}{4}\right)^k$

$$k = 30$$

$$\left(\frac{1}{4}\right)^{30} \approx 10^{-18}$$

VERIFICA ( $N, y$ ) // Controlla la validità del certificato  $y$   
 ( $y$ : certificato del fatto che  $N$  sia composto)

```

if ( P1 == falso OR P2 == falso ) return 1 // N È CERTAMENTE
else return 0; // N È probabilmente primo
                (prob. errore < 1/4)
    
```

TEST MR ( $N, k$ )

---

```

for (i = 1; i ≤ k; i++) {
    - scegli a caso  $y \in [2, N-1]$ 
    - if ( VERIFICA ( $N, y$ ) == 1) return 0; // N È certamente
                                                COMPOSTO
    }
    return 1; // N È probabilmente primo
                (prob. errore <  $(\frac{1}{4})^k$ )
    
```

## VALUTAZIONE del PREDICATO P2

$$y^2 \bmod N = 1$$

OR

$$y^{2^i \cdot 2} \bmod N$$

esponente massimo per  $y^i$ :

$$i = \omega - 1$$

$$0 \leq i \leq \omega - 1$$

$$N-1 = 2^\omega \cdot z$$

$$2^{\omega-1} \cdot 2 = \frac{N-1}{2}$$

$$y^{\frac{N-1}{2}} \bmod N$$

al massimo voglio  
eseguire  $\log N$  ~~moltiplicazioni~~  
moltiplicazioni

# Algoritmo delle Quadriature successive (esponenti in base veloce)

$$x = y^z \bmod s$$

$x, z, s$  dello stesso ordine  
di grandezza

- 1 - si scomponne l'esponente  $z$  in una somma di potenze di 2

$$z = \sum_{i=0}^t k_i \cdot 2^i \quad k_i \in \{0, 1\}$$

ESEMPIO

$$2^{45} = 32 + 8 + 4 + 1$$

$$t = \lfloor \log_2 z \rfloor = \Theta(\log z)$$

2- si calcolano tutte le potenze

$$\begin{aligned}y^{2^i} \bmod s \\= \left( y^{2^{i-1}} \right)^2 \bmod s\end{aligned}$$

$$1 \leq i \leq t = \lceil \log_2 z \rceil$$

come quadrato delle potenze precedenti.

ESEMPIO  $x = g^{45} \bmod 11$

$$45 = \cancel{32} + \cancel{8} + 4 + 1$$

$$t = \lceil \log_2 45 \rceil = 5$$

$$y = 9$$

$$y^2 \bmod s = g^2 \bmod 11 = 4$$

$$y^4 \bmod s = (4)^2 \bmod 11 = 5$$

$$y^8 \bmod s = (5)^2 \bmod 11 = 3$$

$$y^{16} \bmod 11 = 3^2 \bmod 11 = 9$$

$$y^{32} \bmod 11 = 9^2 \bmod 11 = 4$$

$$3 - \text{calculation} \quad x = y^2 \pmod{5}$$

$$x = \prod_{i: k_i \neq 0} y^{2^i} \pmod{5}$$

$$\begin{aligned} y^2 \pmod{5} &= g^{65} \pmod{11} = g^{32+8+4+1} \pmod{\cancel{g^{65}}} \pmod{11} \\ &= (g^{32} \pmod{11})(g^8 \pmod{11}) \cdot (g^4 \pmod{11}) (g^1 \pmod{11}) \\ &\quad \text{mod } 11 \\ &= (4 * 3 * 5 * 9) \pmod{11} = \textcircled{1} \end{aligned}$$

Costo:

$$t = \Theta(\log_2 z) \text{ è quadratico}$$

si può t moltiplicazioni

$$\Theta(\log_2 z) \quad \text{quadratiche}$$

e

$$\Theta(\log z) \quad \text{moltiplicazioni}$$

ogni moltiplicazione ha  
un costo quadratico del più  
quadratico nel # di cifre



Alg. polinomiale nella dimensione dei  
dati