Crittografia - Logaritmo discreto

Davide Patrizi

24 aprile 2011

0.1 Obbiettivo

Studiare **baby step giant step** e **pollard kangaroo** per la risoluzione del logaritmo discreto.

0.2 Strumenti

- linguaggio di programmazione: **Racket** (http://racket-lang.org/)
- linguaggio per la creazione dei grafici: **R** (http://www.r-project.org/)

0.3 Valori di riferimento

0.3.1 Primi

I numeri primi (p) presi in considerazione sono:

- 200087
- 2000303
- 20000159
- 200000447
- 2000000579
- 20000000687
- 200000000423
- 20000000000567
- 2000000000000447 (solo per il pollard kangaroo)

0.3.2 Grafico

Ordinate

Sulle ordinate è stato inserito il valore del logaritmo del numero primo p.

Ascisse

Sulle ascisse è stato preso in considerazione il logaritmo del valore real della primitiva time-apply del linguaggio Racket, il numero reale in millesecondi richiesti per il risultato.

0.4 Grafici

0.4.1 Nota

Durante l'esecuzione del **baby step giant step** il pc è tornato un errore con messaggio "Racket virtual machine has run out of memory; aborting".

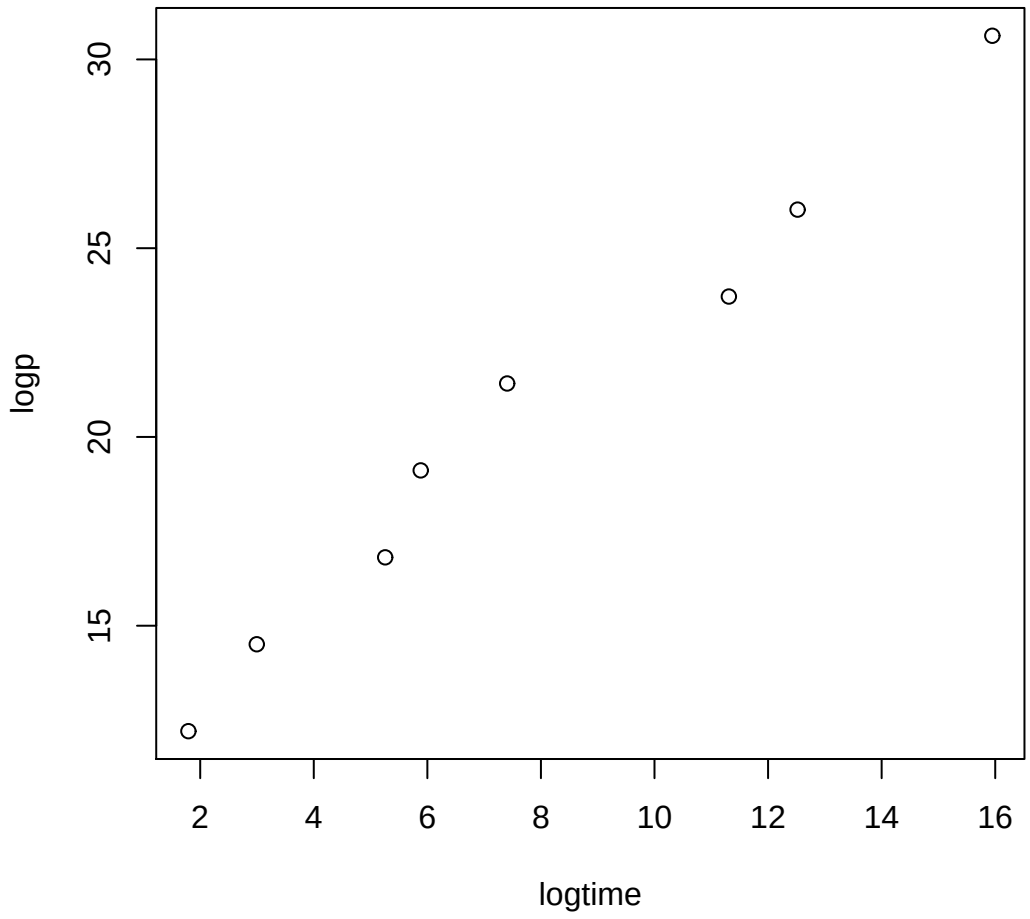

Figura 1: andamento baby step giant step

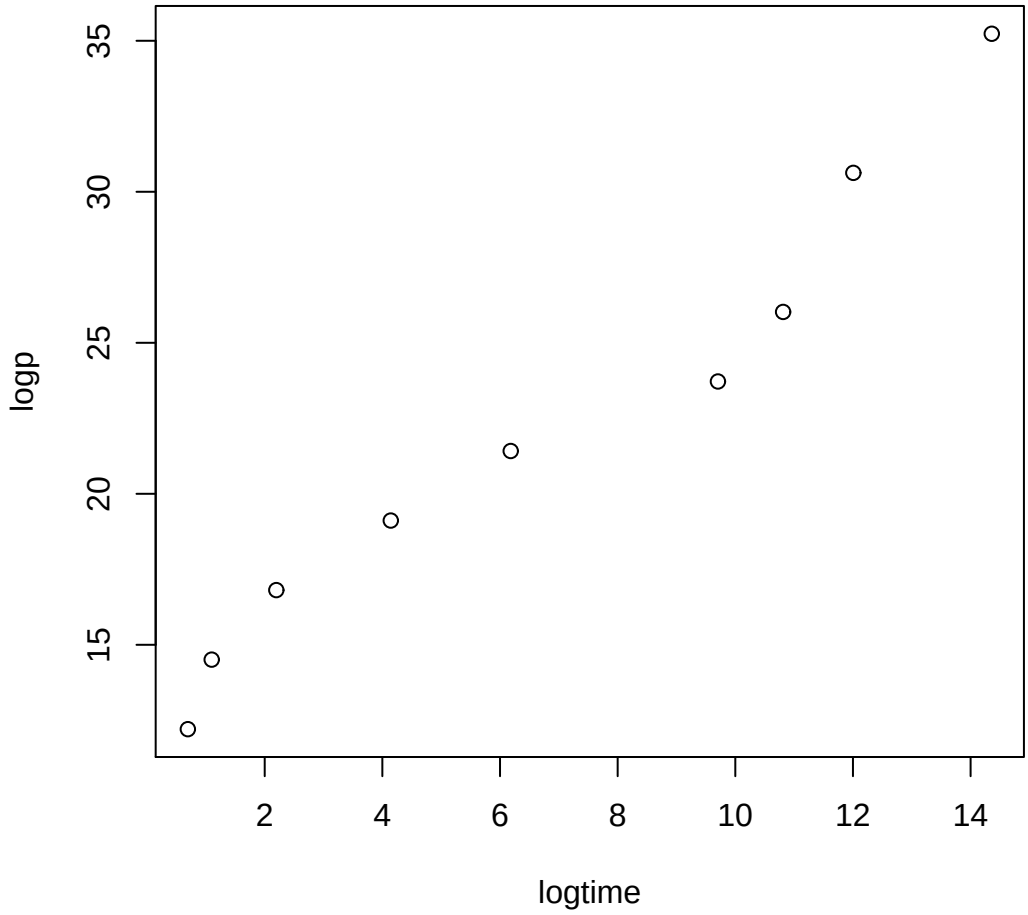

Figura 2: andamento pollard kangaroo