COGNOME .... *NOME* .... *MATRICOLA* ....

Risolvere gli esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. *Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.* Ogni esercizio vale 7.5 punti.

1. Mostrare che se a, b e c sono interi positivi con $a, b, c \leq p$ (p primo), allora è possibile calcolare $a^{(b^c)} \bmod p$ in $O(\log^3 p)$ operazioni bit. *(Sugg. Usare sia l'algoritmo delle potenze successive che il Piccolo Teorema di Fermat.)*

2. Supponiamo che Alice voglia mandare a Bernardo il messaggio

   MANDAMI I DENARI

   e che voglia farlo usando RSA.
   a. Qual'è un possibile valore per un modulo RSA se Alice vuole mandare il messaggio con pacchetti di 3 lettere e usando come esponente di cifratura $e = 3$?
   b. Si cifri il primo pacchetto del messaggio usando la risposta del punto a.
   c. Si decifri il messaggio cifrato $c =$ (MI0).

3. Si illustri l'algoritmo dei quadrati successivi calcolando $3^{26} \bmod 17$ (non usare il piccolo teorema di Fermat).

4. Alvaro ha deciso di pagare i debiti perchè ha vinto al Superenalotto. Alvaro deve una certa cifra x a molte persone e una cifra y a molte altre persone. Sapendo che se estingue il debito con 7 persone a cui deve x gli rimangono 6 milioni e se estingue il debito con 12 persone a cui deve y gli rimangono 2 milioni. Sapreste dire quale è la cifra minima che ha vinto Alvaro? e sapendo che ha vinto meno di 5 miliardi sapreste dire quale è la cifra massima? (P.S.: tutte le cifre e le vincite in questione sono multipli interi di un milione)

5. (Quickies): Scrivere solo la risposta delle seguenti domande:
   i. Quale è grosso modo la probabilitè che un numero a caso con 2000 cifre binarie sia primo?
   ii Se $p = 2q + 1$ è primo e q è un primo dispari, quanto vale $\varphi(\varphi(p))$?
   iii. Quale è il più piccolo esponente di cifratura è possibile scegliere se il modulo RSA è $n = pq$ con $p = 43$ e $q = 331$?

i.

ii.

iii.