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. Bob ha votato per GORE alle elezioni americane. Vuole mandare il suo voto per posta elettronica e insieme al voto (GORE) manda la sua firma digitale. Considerando che la sua chiave pubblica RSA è $(e, n) = (5, 1121)$ e la sua chiave privata è $(d, n) = (209, 1121)$. Quale è la sua firma? (*Osservazione: Sia il voto che la firma consistono in due pacchetti!*)

2. Alice e Bernardo comunicano con il Crittosistema di Rabin. Bernardo sceglie come chiave pubblica $(r, n) = (20, 23 \cdot 19)$. Scrivere le funzioni di cifratura e di decifratura e decifrare il messaggio 21 sapendo che Alice cifra solo messaggi dispari corrispondenti a numeri divisibili per 3.

3. Spiegare che cosa è un algoritmo Las Vegas con probabilità di successo δ.

---

4. Fattorizzare 3233 usando il fatto che $\{1, 3232, 794, 2439)\}$ sono le radici quadrate di 1 in $\mathbf{Z}/3233\mathbf{Z}$.

---

5. (Quickies): Scrivere solo la risposta delle seguenti domande:
   i. Se Bernardo ha chiave pubblica $(5, 23 \cdot 29)$. Quali dei seguenti sono autentici (hanno la firma RSA di Bernardo) e quali sono falsi? (SI,129) (BO,310) (MA,190) (TO,495) (CU,9)
   (N.B. Le lettere sono numeri in base 22 cioè A= 1, $\cdots$ Z= 21)
   ii Sapendo che n è privo di fattori quadratici e che l'equazione $x^3 \equiv 1 \bmod n$ ha più di 28 soluzioni, cosa possiamo dire sul numero dei fattori primi di n?
   iii. Quante soluzioni ha $x^3 \equiv 1 \pmod{5 \cdot 7 \cdot 13 \cdot 19}$?
   iv. Trovare dei valori primi di p, q e r in modo che $x^3 \equiv 1 \pmod{pqr}$ abbia un'unica soluzione.

---

i.
ii.

iii.

iv.