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. Alice vuole spedire a Bernardo il messaggio SI usando l'algoritmo ElGamal con il campo F_{64}. Scelgono il polinomio primitivo $g(x) = x^6 + x + 1 \in \mathbf{F}_2[x]$ e realizzano il crittosistema lavorando con $\mathbf{F}_2[\alpha]$, $\alpha^6 = \alpha + 1$.
   i. Scegliere le chiavi pubbliche per Alice e Bernardo e calcolare le chiavi private.
   ii. Crittare il messaggio SI usando due pacchetti spiegando come associare alle lettere elementi di $\mathbf{F}[\alpha]$.
   iii. Scrivere la formula per la decifratura.
   . *Suggerimento: scegliere le chiavi private in modo che i calcoli risultino semplici.*

2. Si calcoli (se è possibile) il logaritmo discreto $\log_3(5)$ in $\mathbf{F}_{17}$ utilizzando l'algoritmo di Shanks.

3. Considerare l'equazionr su $\mathbf{F}_7$:

$$E : y^3 = x^3 + 3x$$

Dopo aver mostrato che E è una curva ellittica, determinare tutti gli elementi di $E(\mathbf{F}_7)$ e determinarne la struttura come gruppo abeliano (*cioé scrivere* $E(\mathbf{F}_7)$ *come prodotto di un numero opportuno di gruppi ciclici*).

---

4. Spiegare come funziona il crittosistema di Massey–Omura.
