*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. Scrivere il proprio nome anche nell'ultima pagina.* Ogni esercizio vale 3 punti.

1. Quale è la probabilità che un polinomio irriducibile $f$ di grado 8 su $\mathbf{F}_7$ risulti primitivo?

2. Spiegare il metodo di fattorizzazione $p - 1$.

3. Fissare una radice primitiva di $\mathbf{F}_{5^2}$ ed utilizzarla per simulare un scambio chiavi alla Diffie–Hellmann

4. Fattorizzare $f(x) = (x^{10} + 3x^5 + 1)(x^2 + 2)(x^2 + 1)$ su $\mathbf{F}_5$ e dopo averne fissato un campo di spezzamento $\mathbf{F}$, si scrivano tutte le radici di $f(x)$ in $\mathbf{F}$.

5. Spiegare il funzionamento del crittosistema Massey–Omura sul gruppo dei punti razionali di una curva ellittica.

6. Dopo aver verificato che si tratta di una curva ellittica, determinare (giustificando la risposta) l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_7$

$$y^2 = x^3 - x + 5.$$

7. Spiegare l'algoritmo di Berlekamp.

8. Spiegare il significato delle seguenti funzioni di Pari:
ispseudoprimes($n$); znprimroot($n$); znstar($n$); znorder($x$); ffinit($p, n, x$).

9. Implementare in pari il crittosistema di El Gamal.

10. Dato un gruppo ciclico $G$, sia $g$ un suo generatore e $p$ un primo tale che $p^4 \| \#G$. Supponiamo che $X$ denoti il logaritmo discreto di $\alpha \in G$. Si scriva uno pseudo codice per calcolare $X \bmod p^4$.

| NOME E COGNOME | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | TOTALE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ..... | | | | | | | | | | | |