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

Risolvere il massimo numero di 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.* 1 Esercizio = 4 punti. Tempo previsto: 2 ore. Nessuna domanda durante la prima ora e durante gli ultimi 20 minuti.

FIRMA	1	2	3	4	5	6	7	8	TOT	
.....										

1. Dimostrare che ogni elemento di $\mathbf{F}_{p^\alpha}$ ammette esattamente una radice p–esima. Calcolare la radice quadrata di $\alpha \in \mathbf{F}_2[\alpha], \alpha^5 = \alpha^2 + 1$ assumendo che $X^5 + X^2 + 1$ è irriducibile su $\mathbf{F}_2$.

2. Dopo aver spiegato il funzionamento dei sistemi crittografici che usano i logaritmi discreti, si illustri il funzionamento dello scambio chiavi Diffie Hellmann utilizzando come gruppo $\mathbf{F}_{16}^*$.

3. Descrivere in dettagli l'Algoritmo Baby Steps Giant Steps per il calcolo dei logaritmi discreti.

4. Siano n e m interi tali che $5 \not| m$, $5n \equiv 3 \bmod 8m$ e $m \equiv 13 \bmod 60$. Calcolare il simbolo di Jacobi $\left(\frac{m}{n}\right)$ giustificando ogni passaggio.

5. Dato un intero dispari $m \in \mathbf{N}$, Dimostrare che l'insieme $\mathcal{B}(m) = \{a \in (\mathbf{Z}/m\mathbf{Z}^*) : a^{(m-1)/2} \equiv \left(\frac{a}{m}\right) \bmod m\}$ è un sottogruppo di $\mathbf{Z}/m\mathbf{Z}^*$. Determinare la cardinalità di tale sottogruppo nel caso in cui $m = p$ è primo e nel caso in cui $m = 21$.

6. Determinare i polinomi minimi e gli ordini degli elementi di $\mathbf{F}_9$. Scrivere la fattorizzazione in irriducibili di $X^9 - X \in \mathbf{F}_3[X]$ e specificare quali dei fattori risultano primitivi.

7. Fornite un esempio di curva ellittica definita su un campo con 25 elementi per cui $E(\mathbf{F}_{25})$ è ciclico.
sugg: cercare una curva ellettica su $\mathbf{F}_5$ *con un opportuno numero di elementi.*

8. Sia $E : y^2 = x^3 - 5x + 8$ e siano $P = (10, 7), Q = (3, 11) \in E(\mathbf{F}_{101})$. Calcolare $2P$ e $P + Q$. Sapendo che il punto $R = (1, 2) \in E(\mathbf{F}_{101})$ ha ordine 31, cosa possiamo dire della struttura di $E(\mathbf{F}_{101})$?