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	9	TOT.
.....										

1. Illustrare un algoritmo per determinare se un polinomio a coeffcienti su un campo finito è irriducibile.

2. Calcolare la probabilità che un polinomio monico di grado 6 su $\mathbf{F}_2$ sia irriducibile e la probabilità un polinomio irriducibile grado 6 su $\mathbf{F}_2$ sia primitivo. Si dia un esempio di un polinomio primitivo di grado 6 su $\mathbf{F}_2$.

3. Dare un esempio di implementazione dello scambio delle chivi di Diffie Hellmann su un campo con 49 elementi.

4. Utilizzare il metodo Baby Step Giant Step per calcolare il logaritmo discreto $\log_3 5$ dove $5 \in \mathbf{Z}/29\mathbf{Z}$.

5. Illustrare il funzionamento dell'algoritmo Pohlig Hellmann per il calcolo dei logaritmi discreti analizzandone la complessità.

6. Spiegare il funzionamento del Crittosistema El Gamal fornendo un esempio esplicito su un campo con 8 elementi.

7. Dimostrare che se $\mathbf{F}_q$ è un campo finito che ammette esclusivamente un sottocampo proprio, allora $q = p^l$ dove p e l sono numeri primi.

8. Determinare le radici primitive di un campo con 2^7 elementi.

9. 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 $\mathbf{F}_5$

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