Cognome ..... *Nome* ..... *Matricola* .....

Risolvere il massimo numero di esercizi fornendo spiegazioni chiare e sintetiche. *Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.* 1 Esercizio = 4 punti. Tempo previsto: 2 ore. Nessuna domanda durante le prima ora e durante gli ultimi 20 minuti.

1	2	3	4	5	6	7	8	TOTALE

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:

   a. Lo scambio chiavi Diffie Hellmann è definito solo ne gruppo ciclico $\mathbf{F}_{p^n}^*$?

   .....

   b. E' vero che esistono campi finiti non isomorfi in cui i rispettivi gruppi moltiplicativi hanno lo stesso numero di generatori?

   .....

   c. Se $f, g \in \mathbf{F}_p[x]$ hanno lo stesso grado, è vero che le il campo di spezzamento di f contiene le radici di g?

   .....

   d. Scrivere tutti i polinomi irriducibili in $\mathbf{F}_2[x]$ di grado minore uguale a 4.

   .....

2. Dopo aver scritto le formule ricorsive per il calcolo dell'identità di Bezout tra due interi, si calcoli quella per $(1345, 9875)$. In seguito si calcoli il massimo comun divisore $(1345, 9875)$ utilizzando l'algoritmo binario.

3. Dopo aver dimostrato che 3 è una radice primitiva modulo 31, calcolare il logaritmo discreto $\log_3 2 \in \mathbf{Z}/30\mathbf{Z}$ utilizzando l'Algoritmo Baby Steps Giant Steps.

4. Spiegare il funzionamento di alcuni sistemi crittografici che basano la propria sicurezza sul problema del logaritmo discreto.

5. Determinare tutti gli interi X nell'intervallo $[-200, 10]$ tali che $\begin{cases} X \equiv 2 \bmod 4 \\ X \equiv 4 \bmod 5 \\ 3X \equiv 4 \bmod 7. \end{cases}$

6. Fornire un esempio esplicito di campo finito con 32 elementi e tra i suoi elementi si determini una radice primitiva.

7. Determinare il grado su $\mathbf{F}_{13}$ del campo di spezzamento del polinomio

$$(T^{13^8} - 27T^{13^5} + 26T^{13^4})(T^2 + 13T + 27)(T^3 + 14)(T^{13^8} + 25T^{13}) \in \mathbf{F}_{13}[T].$$

8. Dopo aver spiegato brevemente l'algoritmo dei quadrati successivi, calcolare $\alpha^{1047} \in \mathbf{F}_7[\alpha], \alpha^3 = \alpha - 2$.