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

Risolvere il massimo numero di esercizi fornendo spiegazioni chiare e sintetiche. it Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. 1 Eesrcizio = 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	9	TOT.

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

   a. E' vero che tutte le curve ellittiche sono non singolari?

   .....

   b. Fornire un esempio di una curva ellittica su un campo finito con gruppo dei punti razionali non ciclico.

   .....

   c. Determinare le radici primitive (i.e. generatori) in $\mathbf{F}_2[\alpha]$ dove $\alpha^4 = 1 + \alpha$.

   .....

   d. E' vero che in $\mathbf{F}_q[X]$ esistono polinomi irriducibili di ogni grado?

   .....

2. Dopo aver definito la nozione di polinomio primitivo, calcolare la probabilità che un polinomio irriducibile di grado 8 su $\mathbf{F}_7$ sia primitivo.

3. Dimostrare che un polinomio monico, riducibile e senza fattori quadratici di grado 5 in $\mathbf{F}_q[X]$ è un fattore di $X^{q^{12}} - X$.

4. Spiegare il funzionamento del Crittosistema ElGamal fornendo un esempio esplicito su un campo con 13 elementi.

5. Dopo averne spiegato il funzionamento, implementare uno scambio chiavi Diffie–Hellmann in un campo finito con 32 elementi.

6. Spiegare la rilevanza del metodo Baby-Steps-Giant-Steps nella teoria delle curve ellittiche su campi finiti.

7. Sia $E : y^2 = x^3 - x$. Determinare la struttura del gruppo $E(\mathbf{F}_7)$.

8. Supponiamo $\mathbf{F}_4 = \mathbf{F}_2[\xi], \xi^2 = 1 + \xi$. Determinare il numero di punti su un campo con 2^{100} elementi della curva ellittica su $\mathbf{F}_4$

$$E : y^2 + y = x^3 + \xi$$

9. Scrivere e dimostrare le formule per la duplicazione di un punto (finito) su un curva ellittica in un campo finito con caratteristica maggiore di 3.