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. Si descriva un algoritmo per calcolare in tempo polinomiale la parte intera di $m^{1/2}$ per ogni intero positivo m.

2. Supponiamo che $e = 5$ sia la chiave di cifratura di un crittosistema RSA con modulo $n = 53 \cdot 43$. Si calcoli la chiave d di decifratura.

3. Dimostrare che in $\mathbf{F}_p$ l'equazione $x^m \equiv 1 \bmod p$ ammette $\gcd(p-1, m)$ soluzioni. Quante ne ammette in $\mathbf{Z}/(101 \cdot 103)\mathbf{Z}$?

4. Definire il simbolo di Jacobi ed illustrare un algoritmo polinomiale per calcolarlo.

5. Spiegare il funzionamento dei protocolli crittografici incontrati nel corso.

6. Si determini la probabilità che un polinomio irriducibile su $\mathbf{F}_2$ di grado 8 risulti primitivo.

7. Determinare tutti i generatori di $\mathbf{F}_5[\tau], \tau^2 = 2$ e di ciascuno determinare il polinomio minimo.

8. Determinare la struttura del gruppo dei punti razionali di una curva ellittica definita su $\mathbf{F}_{101}$ sapendo che ha un punto P di ordine 41.

9. Siano $E_1 : y^2 = x^3+x+1$ e $E_2 : y^2 = x^3+x+4$ due curve definite su $\mathbf{F}_5$. Dopo aver verificato se sono ellittiche determinarne ka struttura della gruppo dei punti razionali su $\mathbf{F}_5$ e si $\mathbf{F}_{5^2}$.