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 = 3 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	10	
.....											

1. Si descriva un algoritmo per calcolare in tempo polinomiale la parte intera di $m^{1/5}$ per ogni intero positivo m.

2. Descrivere l'algoritmo di moltiplicazione di Karatsuba.

3. Dimostrare che se p è primo, allora $x^4 \equiv 1 \bmod p$ ammette $\gcd(p-1, 4)$ soluzioni. Determinare un velore di m tale che $X^4 \equiv 1 \bmod m$ ammette esattamente 32 soluzioni.

4. Calcolare il simbolo di Legendre $\left(\frac{97543}{21345}\right)$ utilizzando le propritetà dei simboli di Jacobi.

5. Si illustri l'algoritmo di Euclide esteso con particolare riguardo alle relazioni ricorsive per il calcolo dell'identità di Bezout. Lo si abblichi per calcolare l'identità di Bezout tra 54 e 98.

6. Si determini la probabilità che un polinomio irriducibile su $\mathbf{F}_5$ di grado 6 risulti primitivo.

7. Determinare i polinomi minimi e gli ordini degli elementi di $\mathbf{F}_{16}$.

8. Considerare una curva ellittica E definita su un campo con 2^{10} elementi. Supponiamo che $P \in E(\mathbf{F}_{2^{10}})$ abbia ordine 7 e che $Q \in E(\mathbf{F}_{2^{10}})$ abbia ordine 19. Se sappiamo che $E(\mathbf{F}_{2^{10}})$ non è ciclico, cosa possiamo dire della sua struttura?

9. Sia $E : y^2 = x^3 + x$, Dimostrare che se $p \equiv 1 \bmod 4$ allora il gruppo $E(\mathbf{F}_p)$ non è ciclico. Determinare tale gruppo nel caso in cui $p = 3$.

10. Spiegare il funzionamento di tutti i protocolli crittografici incontrati nel corso.