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- Determinare una stima per il numero di operazioni bit necessarie a moltiplicare due matrici $n \times n$ i cui coefficienti sono minori di e^n.

-2- Descrivere un algoritmo per calcolare i massimo comun divisore di due interi e descriverne la complessità.

-3- Calcolare il numero di soluzioni della seguente equazione

$$x^5 + x^2 + x + 1 \bmod 2 \cdot 3 \cdot 5.$$

-4- Mostrare che se n è un modulo RSA, ed è noto il valore di $\varphi(n)$ allora è possibile fattorizzare n in tempo polinomiale.

-5- Spiegare il funzionamento del test di primalità di Miller Rabin introducendo le nozioni necessarie.

-6- Calcolare la probabilità che un polinomio irriducibile di grado 11 su $\mathbf{F}_7$ risulti primitivo. Dare un esempio di polinomio irriducibile e non primitivo.

-7- Simulare uno scambio delle chiavi alla Diffie–Hellmann in un campo finito con 49 elementi *suggerimento: Usare il polinomio* $x^2 + 1$

-8- Enunciare l'algoritmo Pohlig–Hellmann per calcolare i logaritmi discreti in un gruppo ciclico finito dimostrandone la validità.

-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 $\mathbf{F}_7$

$$y^2 = x^3 + x + 1.$$