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- Dato il numero binario $n = (100110100101)_2$, calcolare $[\sqrt{n}]$ usando lalgoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)

-2- Descrivere l'algoritmo dei quadrati successivi in un monoide moltiplicativo e descriverne la complessità.

-3- Definire il simbolo di Jacobi, elencarne le proprietà e descrivere in algoritmo per calcolarlo in tempo polinomiale.

-4- Descrivere il gruppo delle basi euleriane modulo un intero dispari m. Dopo aver verificato che è un gruppo, dimostrare che se m è composto, allora il gruppo è un sottogruppo proprio del gruppo degli invertibili modulo m.

-5- Descrivere il funzionamento di un sistema crittografico in cui RSA viene usato contemporaneamente per cifrare e per firmare (in modo digitale) il testo.

-6- Determinare il numero di elementi del campo di spezzamento su $\mathbf{F_2}$ del polinomio $(x^8 + x^4 + 1)(x^{128} + x)(x^5 + x + 1)$.

-7- Dopo averne spiegato il funzionamento, dare un esempio di implementazione del sistema di scambio delle chiavi alla Diffie-Hellman su un campo con 16 elementi.

-8- In $\mathbf{F}_{31}$ calcolare i seguenti logaritmi discreti: $\log_3(11)$ e $\log_{17}(11)$.

-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 $\mathbf{F}_7$

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