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 $n = (101101110101)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)

2. Illustrare il metodo di moltiplicazione di due numeri binari n e m mostrando che per eseguirla sono necessarie tante somme quanti sono gli 1 nell'espansione di m.

3. Trovare un valore di n intero per cui la congruenza $X^3 \equiv 1 \bmod n$ ha esattamente 9 soluzioni modulo n?

4. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. $b = 2^5 + 2^3 + 2^2 + 1$, quante moltiplicazioni in $\mathbf{Z}/m\mathbf{Z}$ sono necessarie per calcolare $2^b \bmod m$?

5. Spiegare il funzionamento dell'algoritmo binario per il calcolo del massimo comun divisore e se ne analizzi la complessità.

6. Calcolare la probabilità d'errore di un iterazione del test di primalità Solovay Strassen

7. Dimostrare che 6601 è un numero di Carmichael.

8. Calcololare il seguente simbolo di Jacobi senza fattorizzare: $\left(\frac{727}{325}\right)$.

9. Spiegare nei dettagli il funzionamento del crittosistema RSA e si dia un esempio di una sua implementazione.