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	TOT.
....										

1. Dato il numero binario $n = (101010110)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)

2. Determinare una stima per il numero di operazioni bit necessarie per calcolare $[\sqrt{a}]^{b^a} \bmod b$ dove $b \leq a^a$.

3. Trovare le soluzioni $X \in \mathbf{Z}$ della congruenza $X^3 \equiv 1 \bmod 91$?

4. Mostrare che se $f(X) = aX^2 + bX + c \in \mathbf{Z}/k\mathbf{Z}[X]$, le moltiplicazioni nell'anello quoziente $\mathbf{Z}/k\mathbf{Z}[x]/(f(X))$ si possono calcolare in $O(\log^2 k)$ operazioni bit. Vale la stessa conclusione se $\deg f > 2$?

5. Si illustri il funzionamento dell'algoritmo di Stein (algoritmo binario) per calcolare il massimo comune divisore di 72 e 90.

6. Supponiamo $a, m \in \mathbf{Z}$, e $(a, m) = 1$. Dimostrare che l'inverso moltiplicativo $a^* (\bmod m)$ è una potenza di a. Spiegare perchè se m ha al più due fattori primi allora conoscere tale potenza è computazionalmente equivalente a fattorizzare m.

7. Dopo aver enunciato il criterio di Korselt per i numeri di Carmichael lo si applichi per mostrare che $2821 = 7 \times 13 \times 31$ è un numero di Carmichael.

8. Quale la probabilit che un numero minore di 100 coprimo con 14 risulti primo?

9. Calcolare la successione di Miller Rabin di 3 modulo 49.

10. Spiegare nei dettagli il funzionamento del crittosistema RSA.