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 $n = (1111110101)_2$, 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 $[\sqrt{k^k \bmod T}]$ dove $T \leq k^3$.

3. Trovare un valore di n intero per cui la congruenza $X^6 \equiv 1 \bmod n$ ha esattamente 36 soluzioni modulo n?

4. Mostrare che le moltiplicazioni nellanello quoziente $\mathbf{Z}/6\mathbf{Z}[x]/(x^d)$ si possono calcolare in $O(d^2)$ operazioni bit mentre le addizioni in $O(d)$ operazioni bit.

5. Dopo aver spiegato il funzionamento dell'algoritmo di Euclide per il calcolo dell'identità di Bezout tra due interi, lo si applichi per calcolare l'identità di Bezout tra 27 e 63.

6. Fornire una stima per probabilità che un intero composto $n \leq 10^{50}$ privo di fattori primi minori di 101 sia dichiarato primo da 10 iterazioni del test di Miller Rabin

7. Dopo aver definito la nozione di numeri di Carmichael ed averne elencato alcune delle proprietà findamentali, si dimostri che 8911 è un numero di Carmichael.

8. Calcololare il seguente simbolo di Jacobi senza fattorizzare: $\left(\frac{232}{919}\right)$.

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