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. Dimostrare che è possibile calcolare dei coefficienti di Bezout per due interi positivi in tempo polinomiale e calcolarli nel caso di 65 e 23.

2. Descrivere l'algoritmo di divisione di Karatsuba analizzandone la complessità.

3. Calcolare il seguente simbolo di Jacobi senza fattorizzare: $\left(\frac{4531}{2317}\right)$.

4. Dimostrare che i numeri di Carmichael non hanno fattori quadratici.

5. Spiegare la nozione di algoritmo probabilistico di tipo Montecarlo e illustrare l'algoritmo di Miller Rabin per la primalità analizzandone la complessità.

6. Calcolare il reticolo dei sottocampi di $\mathbf{F}_{3^{12}}$ spiegando i risultati teorici utilizzati.

7. Dopo averne spiegato il funzionamento, dare un esempio di implementazione del crittosistema Massey–Omura su un campo con 31 elementi.

8. Descrivere in generale la nozione di Firma Digitale e spiegare in particolare il funzionamento dell'algoritmo DSS.

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 $\mathbf{F}_5$

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