Cognome ..... *Nome* ..... *Matricola* .....

Risolvere il massimo numero di esercizi fornendo spiegazioni chiare e sintetiche. *Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.* 1 Esercizio = 4 punti. Tempo previsto: 2 ore. Nessuna domanda durante le prima ora e durante gli ultimi 20 minuti.

1	2	3	4	5	6	7	8	9	TOT.

1. Rispondere alle seguenti domande con una giustificazione di 1 riga:

   a. E' possibile calcolare i simboli di Jacobi senza fattorizzare?

   .....

   b. I simboli di Jacobi hanno applicazioni in crittografia?

   .....

   c. E' possibile implementare RSA con un esponente di cifratura pari? perchè?

   .....

   d. Dare un esempio di curva ellittica $E/\mathbf{F}_p$ in cui $\#E(\mathbf{F}_p)$ è dispari.

   .....

2. Spiegare il funzionamento del crittosistema RSA.

3. Definire la nozione di pseudo primo di Miller Rabin e dimostrare che 91 è pseudo primo di Miller Rabin in base 10 e in base 22.

4. Calcolare il simbolo di Jacobi $\left(\frac{m}{n}\right)$ sapendo che $n \equiv 7 \bmod 4m$ e che $m \equiv 3 \bmod 28$.

5. Dopo aver definito la nozione di numero di Carmichael, si enunci e dimostri il criterio di Korselt.

6. Sia $E : y^2 = x^3 + Ax + B$ una curva ellittica su un campo $\mathbf{F}_p$ di caratteristica maggiore di 3. Dimostrare che se $P = (\alpha, \beta) \in E(\mathbf{F}_p)$ è un punto di ordine tre, allora α è una radice del polinomio:

$$\Psi_3(X) = 3X^4 + 6AX^2 + 12BX - A^2$$

7. Sapendo che una curva ellittica E su $\mathbf{F}_{101}$ ha un punto di ordine 50, cosa possiamo dire su $\#E(\mathbf{F}_{101})$?

8. Si determini $\#E(\mathbf{F}_{5^{20}})$ quando $E : y^2 = x^3 + 2x - 3$.

9. Si dimostri la legge di reciprocità quadratica.