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	TOT	
.....										

1. Determinare il numero di elementi del campo di spezzamento di
$(T^{2^{45}} + 30T^{2^{40}} + 27T^{2^{27}})(T^{2^5} + 21T^{2^4} + 31)(T^{24} + 20T^{15} + 9T^{16} + 7)(T^3 + 2T + 1) \in \mathbf{F}_2[T]$

2. Dopo aver spiegato il funzionamento del crittosistema RSA, dimostrare che se Carlo conosce il modulo RSA n e il valore $\varphi(n)$, allora può agevolmente trovare i fattori primi di n.

3. Descrivere in dettagli l'Algoritmo di Pholig Hallmann per il calcolo dei logaritmi discreti.

4. Siano n e m interi tali che $n \equiv 6 \bmod 20m$ e $m \equiv 7 \bmod 24$. Calcolare il simbolo di Jacobi $\left(\frac{m}{n}\right)$ giustificando ogno passaggio.

5. Enunciare e dimostrare il criterio di caratterizzazione (criterio di Korselt) per i numeri di Carmichael.

6. Si determini la probabilità che un polinomio irriducibile su $\mathbf{F}_3$ di grado minore usuale a 5 risulti primitivo.

7. Dimostrare che una curva ellittica definita su un campo di caratteristica due ha al più un punto di ordine due.

8. Determinare l'ordine della curve ellittica $y^2 = x^3 + 2x + 1$ su $\mathbf{F}_{25}$. Cosa è possibile affermare sulla struttura di $E(\mathbf{F}_{25})$?