

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. Dimostrare che se  $p$  è primo, allora  $x^5 \equiv 1 \pmod{p}$  ammette  $\gcd(p-1, 5)$  soluzioni. Determinare un valore di  $m$  tale che  $X^5 \equiv 1 \pmod{m}$  ammette esattamente 25 soluzioni modulo  $m$ .

2. Dopo aver spiegato il funzionamento dei sistemi crittografici che usano i logaritmi discreti, si illustri il funzionamento di ElGamal utilizzando come gruppo  $\mathbf{F}_{16}^*$ .

3. Descrivere l'algoritmo dei quadrati successivi in un qualsiasi monoide moltiplicativo discutendone la complessità.

4. Calcolare il simbolo di Legendre  $\left(\frac{97543}{21345}\right)$  utilizzando le proprietà dei simboli di Jacobi e giustificando ogni passaggio.

5. Dopo aver definito la nozione di pseudo primo forte, si illustri come utilizzarla per scrivere un test di primalità probabilistico.

6. Si determini la probabilità che un polinomio irriducibile su  $\mathbf{F}_7$  di grado 6 risulti primitivo.

7. Fornite un esempio di curva ellittica definita su un campo con 27 elementi per cui  $E(\mathbf{F}_{27})$  è ciclico.  
*sugg: cercare una curva ellittica su  $\mathbf{F}_3$  con un opportuno numero di elementi.*

8. Sia  $E : y^2 = x^3 + x$ , Dimostrare che se  $p \equiv 1 \pmod{4}$  allora il gruppo  $E(\mathbf{F}_p)$  non è ciclico. Determinare tale gruppo nel caso in cui  $p = 5$ .