

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 = 3 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 | 10 |
|-------|---|---|---|---|---|---|---|---|---|----|
| | | | | | | | | | | |

1. Si descrivano:

-a- L'algoritmo dei quadrati successivi;

-b- L'algoritmo MCD-binario;

-c- L'algoritmo di Pollard per la fattorizzazione degli interi;

-d- L'algoritmo di Diffie-Hellman per il calcolo dei logaritmi discreti;

-e- Dopo aver descritto la nozione di algoritmo probabilistico di tipo Montecarlo, l'algoritmo di Miller-Rabin.

2. Determinare ordine e struttura di $E(\mathbf{F}_5)$ dove $E : y^2 = x^3 + 2$.

3. Dopo aver descritto quali sono i fattori irriducibili in $\mathbf{F}_p[x]$ di $x^{p^6} - x$ (p primo), nel caso in cui $p = 2$, li si elenchino tutti specificando quali tra questi sono primitivi.

4. Siano n e m interi tali che $m \equiv 3 \pmod{4}$, $m \equiv 2 \pmod{n}$ e $n \equiv 1 \pmod{8}$. Si calcoli il simbolo di Jacobi $\left(\frac{(5m+n)^7}{m}\right)$.

5. Dimostrare che se \mathbf{F}_q è un campo finito di caratteristica dispari, allora esiste sempre una curva ellittica su \mathbf{F}_q con gruppo dei punti razionali non ciclico.

6. Si descrivano i principali algoritmi di cifratura e decifratura.