

Cognome Nome Matricola

Risolvere il massimo numero di esercizi fornendo spiegazioni chiare e sintetiche. it 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 la prima ora e durante gli ultimi 20 minuti.

1	2	3	4	5	6	7	8	9	TOT.

1. Rispondere alle seguenti domande che forniscono una giustificazione di 1 riga:

a. E' vero che se E è una curva ellittica definita su \mathbf{F}_3 , allora si può agevolmente calcolare $E(\mathbf{F}_{3^{100}})$?

.....

b. E' vero che se $p - 1$ ha soltanto fattori piccoli allora i logaritmi discreti in \mathbf{F}_p si calcolano efficientemente?

.....

c. Quanti sono i polinomi primitivi di grado minore di 5 in $\mathbf{F}_2[X]$?

.....

d. E' vero che in $\mathbf{F}_7[X]$ due polinomi di grado n si moltiplicano in $O(n^3)$ operazioni bit?

.....

2. Dopo aver descritto e dimostrato l'algoritmo per determinare i coefficienti di Bezout di due interi, lo si applichi per calcolarli nel caso in cui i due interi sono 130 e 78.

3. Dopo aver definito il simbolo di Legendre dimostrare che il numero di elementi in \mathbf{F}_p^* che hanno simbolo di Legendre pari a 1 è $(p-1)/2$.

4. Spiegare in tutti i dettagli il funzionamento del crittosistema RSA e in particolare spiegare le accortezze necessarie per scegliere le chiavi

8. Supponiamo $\mathbf{F}_8 = \mathbf{F}_2[\xi], \xi^3 = 1 + \xi$. Determinare il numero di punti di $E(\mathbf{F}_8)$ dove

$$E : y^2 + \xi y = x^3 + \xi$$

9. Supponiamo che E sia una curva ellittica definita su \mathbf{F}_{25} , che $P \in E(\mathbf{F}_{25})$ sia un punto di ordine 7 e che E abbia almeno due punti di ordine 2. Calcolare $\#E(\mathbf{F}_{25})$.