

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 Eesrcizio = 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 che forniscono una giustificazione di 1 riga:

a. Determinate due fattori propri di 1000000000000000000040000000000000000003?

.....

b. È vero che $X^{97} - X + 3$ non ha radici modulo 97?

.....

c. Quanti sono i polinomi primitivi di grado 7 su \mathbf{F}_7 ?

.....

d. Perché, se $M = p \cdot q$ è un modulo RSA, l'esponente di cifratura e deve essere scelto in modo tale che $\gcd(e, \varphi(M)) = 1$?

.....

2. Descrivere due algoritmi per il calcolo del massimo comun divisore di interi, determinarne la complessità e sfruttarli per calcolare con entrambi $\text{MCD}(36, 63)$.

3. Determinare una stima per il numero di operazioni bit necessarie a moltiplicare due matrici $n^2 \times n^2$ i cui coefficienti sono minori di 2^n .

4. Calcolare il seguente simbolo di Jacobi senza fattorizzare $\left(\frac{325893}{983832}\right)$.

5. Si illustri il funzionamento del metodo di fattorizzazione ρ di Pollard.

6. Dopo aver descritto il crittosistema ElGamal su \mathbf{F}_p , se ne illustri il funzionamento con un esempio con $p = 29$.

7. Realizzare il campo \mathbf{F}_{25} e determinare l'ordine di tutti i suoi elementi.

8. Data una curva ellittica E , definita su \mathbf{F}_p , si spieghi il metodo per calcolare l'ordine del gruppo $E(\mathbf{F}_{p^{100}})$.

9. Dopo aver dimostrato che è una curva ellittica su \mathbf{F}_7 , calcolare la struttura del gruppo dei punti razionali di $y^2 = x^3 + x + 1$.