

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
.....										

- Si descrivano:

-1- L'algoritmo di Euclide (per l'identità di Bezout) e suo il tempo di esecuzione. ;

-2- Gli algoritmi per la moltiplicazione degli interi a la loro complessità;

-3- L'algoritmo Baby Steps Giant Steps per il calcolo dell'ordine di una curva ellittica su un campo finito;

-4- L'algoritmo di Diffie-Hellman per il calcolo dei logaritmi discreti;

-5- Le varie definizioni di pseudo primi e le loro principali proprietà.

6. Determinare ordine e struttura di $E(\mathbf{F}_7)$ dove $E : y^2 = x^3 - 1$.

7. Dopo aver descritto quali sono i fattori irriducibili in $\mathbf{F}_p[x]$ di $x^{11^6} - x$ (p primo), si determini il numero di tali fattori che sono primitivi.

8. Dopo aver fornito la definizione di numero di Carmichael, si enuncino e dimostrino le principali proprietà dei numeri di Carmichael fornendone esempi.

9. Dimostrare che su \mathbf{F}_q , q dispari, c'è sempre una curva ellittica con gruppo dei punti razionali non ciclico.

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