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	9	TOT.
.....										

-1- Determinare una stima per il numero di operazioni bit necessarie a moltiplicare due interi minori di m^2.

-2- Calcolare il seguente simbolo di Jacobi $\left(\frac{3258}{9839}\right)$.

-3- Dato il numero binario n $= (10001011101)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive (Non passare a base 10 e non usare la calcolatrice!)

-4- Carlo scopre il valore di $\varphi(n)$ dove n è il modulo RSA che Alice e Bernardo stanno usando per comunicare. Come può usare questa informazione per decifrare i messaggi?

-5- Spiegare il funzionamento del test di primalità di Solovay–Strassen introducendo le nozioni necessarie.

-6- Dopo aver calcolato il numero di polinomi irriducibili di grado 6 su $\mathbf{F}_2$, si dimostri che il polinomio $X^6 + X + 1$ è irriducibile e si verifichi se è primitivo.

-7- Si fornisca un esempio del funzionamento del crittosistema ElGamal su un campo finito con 49 elementi *suggerimento: Usare il polinomio* $x^2 + 1$

-8- Enunciare l'algoritmo ρ di Pollard spiegandone il funzionamento.

-9- Dopo aver verificato che si tratta di una curva ellittica, determinare (giustificando la risposta) l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su $\mathbf{F}_7$

$$y^2 = x^3 - x + 1.$$