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. E' vero che l'algoritmo Pohlig–Hellman si applica a qualsiasi gruppo finito ciclico?

   .....

   b. Quale è la probabilità che dati $(x_1, \ldots, x_{100}) \in (\mathbf{Z}/500\mathbf{Z}^{100})$ ci siano $i \neq j$ tali che $x_i = x_j$?

   .....

   c. Che differenza c'è tra polinomi irriducibili e polinomi primitivi?

   .....

   d. E' vero che in $\mathbf{F}_p[X]$ due polinomi di grado 30 si moltiplicano in $O(\log^2 p)$ operazioni bit?

   .....

2. Descrivere due algoritmi per il calcolo del massimo comun divisore di interi, determinarne la complessità e sfruttarli per calcolare con entrambi MCD$(75, 42)$.

3. Dopo aver definito i simboli di Jacobi e di Legendre dimostrare che se p e q sono numeri primi tali che $q \equiv 5 \bmod 4p$ e $p \equiv 2 \bmod 5$, allora il simbolo di Legendre $\left(\frac{p}{q}\right) = -1$.

4. Mostrare che se n è un modulo RSA di cui si conosce il valore di $\varphi(n)$, allora è possibile determinare efficientemente i fattori primi di n. Come si può utilizzare questa informazione per decifrare messaggi cifrati con RSA?

5. Descritto l'algoritmo di Miller Rabin per verificare la primalità di un intero, stimarne la probabilità d'errore quando è applicato con 10 iterazioni su interi con 1000 cifre decimali.

6. Descrivere brevemente tutti gli algoritmi crittografici che basano la propria sicurezza sul problema del logaritmo discreto.

7. Determinare tutti i sottocampi di $\mathbf{F}_{7^{50}}$ che contengono un sottocampo con 49 elementi.

8. Supponiamo $\mathbf{F}_4 = \mathbf{F}_2[\xi], \xi^2 = 1 + \xi$. Determinare il numero di punti su un campo con 2^{12} elementi della curva ellittica su $\mathbf{F}_4$

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

9. Descrivere il gruppo $E(\mathbf{F}_5)$ dove E è la curva ellittica definita da $y^2 = x^3 - x$.