CR1 AA02/03 (Crittografia a chiave pubblica) ESAME SCRITTO Roma, 19 Settembre 2003.

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.

1. Dimostrare che il numero di operazioni bit necessarie a moltiplicare due interi con al più k cifre binarie è $O(k^2)$ spiegando tutti i passaggi.

2. Dati due numeri primi distinti p e q, si spieghi come risolvere il seguente sistema di equazioni di congruenze

$$\begin{cases} x^3 \equiv 1 \bmod p \\ x^4 \equiv 1 \bmod q \end{cases}$$

fornendo un esempio in cui il sistema ammette 12 soluzioni.

3. Supponiamo che n sia una chiave RSA e che sia noto il valore di $\varphi(n)$. Descrivere un algoritmo con complessità quadratica per fattorizzare n.

4. Si dimostri che se m è un intero dispari composto, allora esiste sempre un base $a \in U(\mathbf{Z}/m\mathbf{Z})$ rispetto a cui m non è pseudo primo di Eulero. Quale è l'applicazione di questa proprietà nei test di primalità?

5. Enunciare un algoritmo per calcolare il simbolo di Jacobi di due interi con tempo di esecuzione polinomiale.

6. Descrivere in dettaglio il crittosistema El-Gamal facendo un esempio nel caso del gruppo moltiplicativo di un campo finito.

7. Simulare uno scambio delle chiavi alla Diffie–Hellmann in un campo finito con 32 elementi

8. Dimostrare che $x^{p^h} - x + 1$ non ammette mai radici in un campo finito con $\mathbf{F}_{p^h}$ elementi. E' sempre irriducibile?

9. Calcolare la probabilità che un polinomio irriducibile di grado 6 su $\mathbf{F}_{11}$ risulti primitivo. Dare un esempio di polinomio irriducibile e non primitivo.

10. Enunciare l'algoritmo Pohlig–Hellmann per calcolare i logaritmi discreti in un gruppo ciclico finito dimostrandone la validità.

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

12. Enunciare le formule per la duplicazione di un punto razionale su una curva ellittica e spiegare come si ottengono.

NOME E COGNOME	1	2	3	4	5	6	7	8	9	10	11	12	TOT.
.....													