CR1 AA02/03 (Crittografia a chiave pubblica) ESAME SCRITTO Roma, 13 Giugno 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. Determinare una stima per il numero di operazioni bit necessarie a moltiplicare due matrici $n \times n$ i cui coefficienti sono minori di e^n.

2. Calcolare il numero di soluzioni della seguente equazione
$$x^5 + x^2 + x + 1 \bmod 2 \cdot 3 \cdot 5.$$

3. Dopo aver enunciato le proprietà dei numeri di Carmichael, dimostrare che 75361 è un numero di Carmichael.

4. Spiegare il funzionamento del test di primalità di Miller Rabin introducendo le nozioni necessarie.

5. Calcolare il seguente simbolo di Jacobi senza fattorizzare $\left(\frac{33331}{44447}\right)$.

6. Descrivere in dettaglio il crittosistema Massey Omura 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 49 elementi *suggerimento: Usare il polinomio* $x^2 + 1$

8. Dimostrare che $x^p + a$ è riducibile in ogni campo finito $\mathbf{F}_p$.

9. Calcolare la probabilità che un polinomio irriducibile di grado 11 su $\mathbf{F}_7$ risulti primitivo. Dare un esempio di polinomio irriducibile e non primitivo.

10. Su $\mathbf{F}_{31}$ calcolare i seguenti logaritmi discreti: $\log_3(11)$ e $\log_{17}(11)$.

11. Dopo aver dimostrato che è una curva ellittica si $\mathbf{F}_7$, calcolare la struttura del gruppo dei punti razionali di $y^7 = x^3 + x + 3$.

12. Descrivere l'algoritmo *Baby steps - Giant steps* (Shanks) per calcolare il numero dei punti razionali del gruppo dei punti razionali di una curva ellittica definita su in campo finito.

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