CR1 AA02/03 (Crittografia a chiave pubblica) ESAME SCRITTO Roma, 23 Luglio 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. Definire la nozione di operazione bit tipo sottrazione e mostrare che ogni sottrazione tra interi con al più k bit, può essere effettuata in meno di k operazioni bit.

2. Mostrare che se n è un modulo RSA, ed è noto il valore di $\varphi(n)$ allora è possibile fattorizzare n in tempo polinomiale.

3. Stimare il numero di operazioni bit necessarie a calcolare $[\sqrt{2^n \bmod 5^n}]$.

4. Spiegare il funzionamento del test di primalità di Solovay Strassen introducendo le nozioni necessarie.

5. Calcolare il seguente simbolo di Jacobi senza fattorizzare $\left(\frac{325893}{983832}\right)$.

6. Realizzare il campo $\mathbf{F}_{25}$ e calcolarne tutte le radici primitive.

7. Spiegare il funzionamento del sistema di scambio chiavi alla Diffie–Hellmann in un gruppo abeliano spiegando il collegamento con il problema del dei logaritmi discreti.

8. Mostrare che $x^2 + x + 1$ è irriducibile su $\mathbf{F}_p$ se e solo se $p \equiv 2 \bmod 3$.

9. Calcolare la probabilità che un polinomio (non necessariamente monico) grado 12 su $\mathbf{F}_7$ risulti monico e irricucibile.

10. Dopo aver descritto il crittosistema ElGamal su $\mathbf{F}_p$, se ne illustri il funzionamento con un esempio con $p = 31$.

11. Dopo aver dimostrato che è una curva ellittica si $\mathbf{F}_7$, calcolare la struttura del gruppo dei punti razionali di $y^2 = x^3 + x + 1$.

12. Descrivere l'algoritmo *Pohlig Hellman* per calcolare logaritmi discreti in un gruppo abeliano ciclico.

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