CR410 AA14/15 (Crittografia a chiave pubblica) ESAME DI FINE SEMESTRE Roma, 27 Maggio, 2015.

Cognome ..... *Nome* ..... *Matricola* .....

Risolvere il massimo numero di esercizi fornendo spiegazioni chiare e sintetiche. *Inserire le risposte negli spazi predisposti. NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI.* 1 Esercizio = 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 con una giustificazione di 1 riga:

   a. E' vero che se n è dispari, i fattori irriducibili di $x^{3^n} - x$ hanno tutti grado dispari?

   .....

   b. E' vero che non è possibile utilizzare le curve ellittiche su campi finiti per lo scambio chiavi Diffie – Hellman?

   .....

   c. Quale è la probabilità che un polinomio irriducibile di grado 5 su $\mathbf{F}_5$ risulti primitivo?

   .....

   d. E' vero che non esistono curve ellittiche su $\mathbf{F}_{11^2}$ tali che $E(\mathbf{F}_{11^2}) \cong \mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}/42\mathbf{Z}$?

   .....

2. Dopo aver spiegato brevemente il funzionamento del crittosistema RSA, si decifri il testo cifrato $\mathcal{C} = 25$ sapendo che la chiave pubblica $(7, 143)$.

3. Spiegare il funzionamento del test di primalità di Miller – Rabin.

4. Spiegare il funzionamento del crittosistema Goldwasser – Micali.

5. Dopo aver definito la nozione di numero di Carmichael ed averne richiamato le principali proprietà, dimostrare che 6601 è Carmichael.

6. Sia $E : y^2 + \alpha y = x^3$ una curva ellittica sul campo $\mathbf{F}_8 = \mathbf{F}_2[\alpha], \alpha^3 = \alpha + 1$. Determinare $\#E(\mathbf{F}_2[\alpha])$ e $\#E(\mathbf{F}_{2^6})$. E' possibile dire nulla sulla struttura di tali gruppi?

7. Determinare la struttura del gruppo dei punti razionali di una curva ellittica E su $\mathbf{F}_{53^2}$ sapendo che contiene un punto di ordine 392 e che ammette un unico punto di ordine 2.

8. Si consideri la curva ellittica $E : y^2 = x^3 + x + 1$ e si calcoli $\#E(\mathbf{F}_{3^{100}})$.

9. Dimostrare che una curva definita su un campo con caratteristica 3 ammette al più due punti di ordine tre.
suggerimento: *Studiare l'equazione* $2P = -P$ *per l'equazione di Weierstrass* $y^2 = x^3 + ax^2 + bx + c$.