CR410 AA12	/13 (Crittografia	a chiave	pubblica)	
01010 11112	/ IU (Cirougiana	a ciliave	pubblica	

٨	PP	DT.	$\Gamma \cap$	\sim

Roma, 10 Febbraio 2014.

Coanome	Nome	Matricos	la
· ·	nero di esercizi fornendo spiegazioni chia		
NON SI ACCETTANO	RISPOSTE SCRITTE SU ALTRI FOG	LI. 1 Esercizio = 4 punti.	Tempo previsto: 2 ore. Nessuna
domanda durante le prim	na ora e durante gli ultimi 20 minuti.		
	1 2 3 4 5 6	7 8 9 TOT	

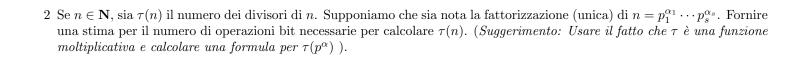
1	2	3	4	5	6	7	8	9	TOT.

 $1.\,$ Rispondere alle seguenti domande che forniscono una giustificazione di 1riga:

a. E' vero che se E è una curva ellittica definita su \mathbf{F}_{2^n} , allora non ha mai un equazione della forma $y^2 = x^3 + ax + b$?
b. E' vero che se tutti i fattori primi di $n-1$ sono più piccoli di $\log n$, allora è possibile determinare un fattore non banale di n in modo rapido? come?

c. E' vero che se $p>3$, il polinomio $X^2+2\in \mathbf{F}_p$ è irriducibile per alcuni valori di p ma non tutti?

d. E' vero che esistono modi per moltiplicare interi con complessità inferiore a quella quadratica?



3. Siano m, n interi tali che $m \equiv 3 \mod 4$, che $m \equiv 2 \mod n$ e che $n \equiv 1 \mod 8$. Si calcoli il seguente simbolo di Jacobi: $\left(\frac{(11m+n)^7}{m}\right)$.

4. Illustrare l'algoritmo dei quadrati successivi in un gruppo analizzandone la complessità. Considerare la curva ellittica $E: y^2 = x^3 - x$. Illustrare l'algoritmo appena descritto calcolando [5](1,0) dove $(1,0) \in E(\mathbf{F}_7)$.

5. Si dia la definizione di pseudo primo forte in base 2 $2^{2^{\beta}} \equiv -1 \bmod n \text{ per qualche } \beta < \alpha.$	e si mostri che se $n=2^{\alpha}+1$ è pseudo primo forte in base 2, allora
6. Fissare una radice primitiva di ${f F}_{2^4}$ ed utilizzarla per	simulare un scambio chiavi alla Diffie–Hellmann.
7. Dopo aver definito la nozione di polinomio primitivo s	u un campo finito, si calcoli la probabilità che un polinomio irriducibile
f di grado 8 su \mathbf{F}_5 risulti primitivo?.	

8. Fattorizzare $f(x) = (x^{12} + 5x^2 + 1)(x^2 + x + 2)(x^{10} + x^2 + 1)$ su \mathbf{F}_2 e determinare il numero di elementi del campo di spezzamento di f.

9. Dopo aver verificato che si tratta di una curva ellittica, determinare (giustificando la risposta) l'ordine e la struttura del gruppo dei punti razionali della curva ellittica su \mathbf{F}_7

$$y^2 = x^3 - x + 5.$$

.