CR410.	AA12	/13 (Crittog	rafia	1)

			_	
API	PE	ы	()	Α

Roma, 7 GIUGNO 2013.

COGNOME	MOME	MATRICOLA
COGNOME	NOME	MAIRICOLA

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.

FIRMA	1	2	3	4	5	6	7	8	9	10	

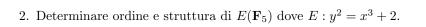
1. Si descrivano:

-b- L'algoritmo MCD-binario;

-c- L'algoritmo di Pollard per la fattorizzazione degli interi;

⁻a- L'algoritmo dei quadrati successivi;

-d-	L'algorimo di Pholig–Hellman per il calcolo dei logaritmi discreti;
-e-	Dopo aver descritto la nozione di algoritmo probabilistico di tipo Montecarlo, l'algoritmo di Miller–Rabin.



3. Dopo aver descritto quali sono i fattori irriducibili in
$$\mathbf{F}_p[x]$$
 di $x^{p^6} - x$ (p primo), nel caso in cui $p = 2$, li si elenchino tutti specificando quali tra questi sono primitivi.

4. Siano $n \in m$ interi tali che $m \equiv 3 \mod 4$, $m \equiv 2 \mod n$ e $n \equiv 1 \mod 8$. Si calcoli il simbolo di Jacobi $\left(\frac{(5m+n)^7}{m}\right)$.

5.	Dimostrare che se \mathbf{F}_q è un campo finito di caratteristica dispari, allor esiste sempre una curva ellittica su \mathbf{F}_q con dei punti razionali non ciclico.	gruppo
6.	Si descrivano i principali algoritmi di cifratura e decifratura.	