	-	DI		- т			
А	Р	м	Η; Ι		٠.(	) A	

Roma, 3 SETTEMBRE 2014

<i>COGNOME</i>	<i>NOME</i>	MATRICOLA

Risolvere il massimo numero di esercizi accompagnando le risposte con spiegazioni chiare ed essenziali. Inserire le risposte negli spazi predisposti.  $NON\ SI\ ACCETTANO\ RISPOSTE\ SCRITTE\ SU\ ALTRI\ FOGLI.\ Scrivere\ il proprio\ nome\ anche\ nell'ultima\ pagina.\ 1\ Esercizio = 3\ punti.\ Tempo\ previsto:\ 2\ ore.\ Nessuna\ domanda\ durante\ la\ prima\ ora\ e\ durante\ gli\ ultimi\ 20\ minuti.$ 

FIRMA	1	2	3	4	5	6	7	8	9	10	

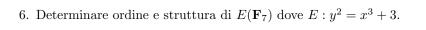
<sup>-</sup> Si descrivano:

-2- L'algoritmo per calcolare i simboli di Jacobi (senza fattorizzare);

-3- L'algoritmo Baby Steps Giant Steps per il calcolo dei logaritmi discreti;

<sup>-1-</sup> L'algoritmo dei quadrati successivi;

-4-	4- L'algorimo di Pholig–Hellma	n per il calcolo dei logar	itmi discreti;	
-5-	5- Dopo aver descritto la nozion	ne di algoritmo probabili	stico di tipo Montecarlo,	l'algoritmo di Miller–Rabin.



7. Dopo aver descritto quali sono i fattori irriducibili in  $\mathbf{F}_p[x]$  di  $x^{p^4} - x$  (p primo), nel caso in cui p = 2, li si elenchino tutti specificando quali tra questi sono primitivi.

8. 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  $\left(\frac{(5m+n)^7}{m}\right)$ .

9.	. Dimostrare che se $\mathbf{F}_q$ è un cam dei punti razionali non ciclico.	po finito di caratteristica	dispari, allora esiste ser	mpre una curva ellittica s	u $\mathbf{F}_q$ con gruppo
10.	. Si descrivano i principali algorit	zmi di cifratura e decifrat	ura.		