CRITTOGRAFIA 2017/18 – Appello del 20 giugno 2018

Nome:

Cognome:

Matricola:

Esercizio 1 – Crittografia ellittica [12 punti]

1. **Descrivere** l'algoritmo di Koblitz per trasformare un messaggio *m,* codificato come numero intero, in un punto di una curva ellittica prima $E_p(a,b)$.
2. **Spiegare** cosa si intende per "logaritmo discreto" di un punto *R* in base *P*.
3. **Descrivere** un algoritmo di scambio di messaggi cifrati e **spiegare** perché può ritenersi sicuro.

Esercizio 2 – Complessità in algebra [8 punti]

Dato un intero *n*

- **definire** la funzione di Eulero $\Phi(n)$
- **indicare** se è noto un algoritmo efficiente per calcolarla
- **dimostrare** che dato un intero *n* prodotto di due numeri primi, il calcolo della funzione di Eulero $\Phi(n)$ e la fattorizzazione di *n* sono problemi computazionalmente equivalenti.

Esercizio 3 - Cifrari perfetti [10 punti]

1. **Definire** i cifrari perfetti e spiegare a parole il significato di tale definizione.
2. **Dimostrare** che il cifrario *One-Time Pad* è un cifrario perfetto.
3. Nel cifrario *One-Time Pad* si sostituisca l'operatore XOR con NAND (AND negato). **Spiegare** se il protocollo funziona con le stesse proprietà del cifrario originale.