CRITTOGRAFIA 2016/17 – Appello del 10 febbraio 2017

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" (se esiste) 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 [6 punti]

Dato un intero *n* **definire** la funzione di Eulero $\Phi(n)$, **indicare** se è noto un algoritmo efficiente per calcolarla e **spiegare** in termini matematici quale implicazione avrebbe questo algoritmo sui cifrari DES e RSA e sui protocolli di firma.

Esercizio 3 – Firma digitale [12 punti]

Sia *S* la somma delle sei cifre decimali del proprio numero di matricola. Si ponga $M = S + 20$.
Si convertano le cifre di *M* in binario su 4 bit, se ne calcoli lo EXOR bit a bit e si riconverta il valore ottenuto in un numero decimale *H* che sarà usato come hash di *M*.

Per due utenti Alice e Bob di un sistema RSA si considerino i seguenti insiemi di parametri.

Alice: $p = 5$, $q = 11$, $e = 7$, $d = 23$.
Bob: $p = 7$, $q = 13$, $e = 5$, $d = 29$.

Alice deve spedire a Bob il messaggio *M* cifrato e firmato in hash, impiegando le chiavi RSA e la funzione hash di cui sopra.

1. **Eseguire** esplicitamente tutte le operazioni aritmetiche eseguite da Alice e Bob nella trasmissione e verifica del messaggio M e della firma.
2. **Spiegare** per quale motivo si impiega una funzione hash per la firma.