Cognome: Nome: Matricola:

Elementi di Crittografia

Docenti: Paolo D'Arco e Barbara Masucci

12 Luglio 2016

Non è ammesso alcun materiale per consultazione. Buon lavoro! ☺

1) **Riduzioni: metodologia.** Si descriva la struttura generale di una riduzione di sicurezza, evidenziando le motivazioni alla base dell'approccio e le proprietà che soddisfa. Inoltre, come caso d'esempio, si dimostri che:

   - se F è una funzione pseudocasuale, allora lo schema di cifratura che associa il cifrato **c** := < r, $f_K(r) \odot \mathbf{m}$> al messaggio **m**, (dove r e la chiave k sono scelti uniformemente a caso) è uno schema di cifratura CPA sicuro.

2) **MAC.** Si spieghi in modo chiaro e conciso

- cos'è
- come si prova la sicurezza di un Message Autenthication Code;
- come si costruisce uno schema MAC sicuro.

3) **Applicazioni di funzioni HASH.** Si spieghi in modo chiaro e conciso il funzionamento di:

- Schema commitment
- L'autenticazione mediante Merkle-Tree

4) **Gruppi ciclici.** Si spieghi in modo chiaro e conciso

- Cosa sono;
- Come sono definiti i problemi DL e DH(Computazionale e decisionale)
- Perché sono importanti igruppi di ordine primo in crittografia.

5) **Crittosistemi a chiave pubblica.** Si spieghi in modo chiaro e coinciso che cosa si intende per crittosistema a chiave pubblica CPA-sicuro. Inoltre si fornisca un esempio di crittosistema che soddisfa tale definizione. In particolare si descriva il funzionameno del crittosistema scelto e si fornisca uno sketch della prova di CPA-sicurezza. Si spieghi in modo chiaro e conciso

6) **Schemi di firme digitali.** Si spieghi in modo chiaro e coinciso che cosa si intende per schema di firme digitali sicuro rispetto ad un adaptive chosen message attack. Inoltre si fornisca la definizione di schema di firme RSA-FDH. In particolare si fornisca uno sketch della prova di sicurezza.