Cognome: Nome: Matricola:

Elementi di Crittografia

Docenti: Paolo D'Arco

Appello 9 Gennaio 2018

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

     $$\mathbf{c} := \langle r, f_{\mathbf{k}}(r) \odot \mathbf{m} \rangle \qquad \text{al messaggio } \mathbf{m}$$

     dove r e la chiave k sono scelti **uniformemente** a caso, è uno schema di cifratura **CPA sicuro**.

2) **Funzioni hash.** Si descriva la trasformata di Merkle-Damgard per estendere il dominio di una funzione di compressione e si provi che trovare efficientemente collisioni per la funzione estesa implica trovare efficientemente collisioni per la funzione di compressione sottostante.

3) **Primalità.** Si spieghi in modo chiaro e conciso

- come possono essere generati numeri primi casuali di n bit
- cosa ci assicura che riusciamo a trovarne con alta probabilità con un numero di tentativi polinomiale in n
- come funziona il test di Miller e Rabin e quali risultati della teoria dei numeri utilizza

4) **Funzioni one-way.** Si spieghi in modo chiaro e conciso

- cosa sono e come si definiscono
- perché sono sufficienti per realizzare tutta la “crittografia simmetrica”

5) **Gruppi ciclici e crittosistema El-Gamal.** In modo chiaro e conciso, si spieghi:
   - cos'è un gruppo ciclico
   - come sono definiti i problemi DL e DH (computazionale e decisionale) su tali gruppi
   - come funziona lo schema di cifratura di El-Gamal (discutendone la sicurezza).

6) **Schemi di firme digitali.** Si descriva il funzionamento dello schema di firme RSA-FDH e si fornisca uno sketch della prova di sicurezza.