Cognome: Nome: Matricola:

Elementi di Crittografia

Docenti: Paolo D'Arco e Barbara Masucci

14 Settembre 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) **Cifratura autenticata.** Si spieghi in modo chiaro e conciso

- cos'è e perché è utile
- come si formalizza tale nozione
- con quale approccio generico può essere ottenuta
- che relazione sussiste con la nozione di "schema di cifratura CCA-sicuro"

3) **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.

4) **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

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.

6) **Schemi di identificazione.** Si spieghi in modo chiaro e coinciso che cosa si intende per schema di identificazione in un sistema interattivo. Si fornisca l'esempio di uno schema interattivo in tre round. Inoltre si spieghi lo schema di identificazione di Schnoor.