Cognome: Nome: Matricola:

Elementi di Crittografia

Docenti: Paolo D'Arco e Barbara Masucci

23 Giugno 2016

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

1) **Sicurezza Semantica.** Si dia la definizione di Sicurezza Semantica e Indistinguibilità.

   - Si dimostri la relazione di uguaglianza tra indistinguibilità e sicurezza semantica.

2) **Modalità operative.** Si spieghi in modo chiaro e conciso

   - Quali sono le principali modalità operative utilizzate (anche usando delle rappresentazioni)

3) **Funzioni HASH.** Si spieghi in modo chiaro e conciso::

- L’estensione di dominio di Merkle-Damgard
- Si dimostri la sicurezza dello schema.

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 EAV-sicuro.Si fornisca la motivazione dell'uguaglianza tra EAV e CPA sicurezza in crittografia asimmetrica. 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 EAV-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.