Cognome: Nome: Matricola:

Elementi di Crittografia

Docenti: Paolo D'Arco e Barbara Masucci

Simulazione pre-appello

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, $f_{\mathbf{K}}(r) \odot \mathbf{m}$> 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) **HMAC.** Si spieghi in modo chiaro e conciso

- cos’è e quale problema risolve
- come funziona (anche un diagramma commentato va bene)
- perché è stato progettato in quel modo (paradigma di riferimento)
- perché si ritiene sicuro

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