Cognome: Nome: Matricola:

Elementi di Crittografia

Docente: Paolo D'Arco

Appello del 22 Febbraio 2022

1) **Riduzioni: metodologia.** Si descriva concisamente 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 **G** è un PRG, allora lo schema di cifratura che associa il cifrato

$$\mathbf{c} := G(\mathbf{s}) \otimes \mathbf{m} \qquad \text{al messaggio } \mathbf{m}$$

dove **s** è il seme scelto **uniformemente** a caso e $\otimes$ rappresenta l'operazione di or esclusivo, è uno schema di cifratura **EAV sicuro**.

2) **Segretezza Perfetta.** Si spieghi cosa si intende per schema di cifratura “perfettamente segreto”. Inoltre, si formalizzi la nozione, discutendo le tre forme equivalenti che sono state presentate a lezione.

3) **Funzioni pseudocasuali.** Si spieghi informalmente cos'è una funzione pseudocasuale e se ne fornisca la definizione formale. Inoltre, sia $F:\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ una funzione pseudocasuale e sia $G: :\{0,1\}^n \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ definita al modo seguente

$$G(k, x_1||x_2) = x_1 \,||\, F(k,x_2)$$

dove k, x_1 *e* x_2 sono stringhe di n bit. È G una funzione pseudocasuale?

E se F fosse one-way, risulterebbe anche G one-way?

4) Si spieghi in modo chiaro e conciso come funziona il test di Miller e Rabin e quali risultati della teoria dei numeri utilizza.

5) **Crittosistemi a chiave pubblica.** Si descriva la struttura degli schemi di cifratura DHIES ed ECIES: in particolare, se ne discutano la strategia di progettazione e 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. In particolare, si spieghi come la produzione efficiente di contraffazioni, implichi l'inversione efficiente della permutazione RSA.