Cognome: Nome: Matricola:

Elementi di Crittografia

Docente: Paolo D'Arco

Preappello del 22 Dicembre 2020

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 **DDH è difficile** nel gruppo G, allora lo schema di cifratura di El Gamal è 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.

Opzionale: la presentazione della prova sotto forma di riduzione formale vale un bonus in fase di correzione.

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

   - come funziona il test di Miller e Rabin e quali risultati della teoria dei numeri utilizza

4) **Generatori pseudocasuali.** Si fornisca la definizione di generatore pseudocasuale. Inoltre, si consideri il seguente generatore

$$G: \{0,1\}^{nm} \text{----------} > \{0,1\}^{n(m+1)}$$

Il generatore interpreta la stringa di input come la rappresentazione di **m** interi di **n** bit e dà in output la rappresentazione degli stessi **m** interi più quella di un ulteriore intero y, dato dalla somma mod 2^n di essi. Precisamente

$$G(x_1 \ldots x_m) = x_1 \ldots x_m y, \quad \text{dove } y = \Sigma_i x_i \bmod 2^n$$

È G un generatore pseudocasuale? Si supporti la risposta con un argomento rigoroso.

5) **Collision-resistance.** La teoria dei numeri permette di realizzare funzioni hash collision-resistant. Si descriva la costruzione su gruppi ciclici presentata a lezione e si dimostri che, se il problema DL è difficile relativamente al generatore di gruppi prescelto, allora la costruzione risulta resistente a collisioni.

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.