Cognome: Nome: Matricola:

Elementi di Crittografia

Docente: Paolo D'Arco

Appello del 17 Febbraio 2021

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 il problema **DDH è difficile** nel gruppo G, allora lo scambio di chiavi Diffie-Hellman è **EAV-sicuro**.

2) **Segretezza Perfetta.** Si dimostri che in ogni schema di cifratura perfettamente segreto, l'insieme delle chiavi di cifratura deve avere cardinalità maggiore o uguale alla cardinalità dell'insieme dei messaggi. Inoltre, si spieghi perché il one-time pad risulta insicuro rispetto alla trasmissione di messaggi multipli, per qualsiasi nozione significativa di sicurezza rispetto a messaggi multipli.

3) **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, ordinati in base al peso di hamming delle rispettive rappresentazioni binarie, più quella di un ulteriore intero y_{m+1}, dato dalla somma mod 2^n di essi. Precisamente

$$G(x_1 \ldots x_m) = y_1 \ldots y_m y_{m+1}, \qquad \text{dove } y_{m+1} = \Sigma_i y_i \bmod 2^n$$

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

Nota: ricordo che il peso di hamming hw di una stringa binaria è il numero di uno della stringa, e.g., hw(100010101)=4

4) **Autenticazione.** Si descriva in modo chiaro e conciso lo schema di autenticazione HMAC e se ne discuta la sicurezza.

5) **Crittosistemi a chiave pubblica.** Si descriva il KEM che usa una funzione hash e la permutazione RSA. Inoltre, si provi che risulta CCA-sicuro nel random oracle model, assumendo che il problema RSA sia difficile.

6) **Schemi di identificazione.** Si descriva lo schema di identificazione di Schnorr e se ne discuta la sicurezza.

   Opzionale: se il verificatore **è onesto**, cioè esegue il protocollo scegliendo la challenge in accordo alla distribuzione uniforme, risulta lo schema, per questo caso, *a conoscenza zero*? Argomentare la risposta.