Cognome: Nome: Matricola:

Elementi di Crittografia

Docente: Paolo D'Arco

Appello del 1 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 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) **Funzioni pseudocasuali.** Si spieghi informalmente cos'è una funzione pseudocasuale e se ne fornisca la definizione formale. Inoltre, si analizzi la funzione con chiave

$$F(k, x) = k \oplus x^2$$

dove k ed x sono stringhe di n bit (e l'operazione di quadratura è mod 2^n), e si discuta l'eventuale pseudocasualità della funzione.

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.