Cog	nome:	Nome:	Matricola:

## Elementi di Crittografia

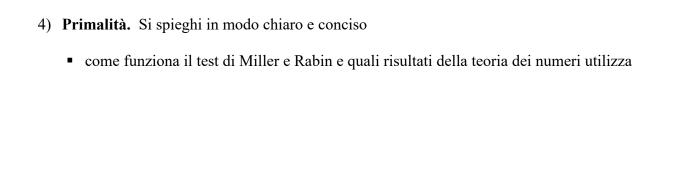
Docente: Paolo D'Arco

Appello del 16 Marzo 2021

- 1) **Riduzioni: metodologia.** Si descriva concisamente la **struttura generale** di una riduzione di sicurezza e si dimostri che:
  - se G è un PRG, allora lo schema di cifratura  $\mathbf{c}=G(\mathbf{s})\oplus\mathbf{m}$ , con  $\mathbf{s}$  scelto uniformemente a caso  $\mathbf{e}\oplus\mathbf{a}$  denotare l'operazione di xor bit a bit, è **EAV-sicuro**.

2) **Segretezza Computazionale.** Si spieghi perché è necessario, nella formulazione della nozione, rilassare le assunzioni utilizzate per la segretezza perfetta – avversari di *potere illimitato* e probabilità di *errore zero* – considerando, invece, avversari *ppt* e ammettendo probabilità di errore *trascurabili*. Inoltre, si diano le definizioni di schema di cifratura simmetrico CPA-sicuro e CCA-sicuro, rispettivamente.

3)	<b>Funzioni Pseudocasuali.</b> Si spieghi cosa sono informalmente e se ne fornisca una definizione formale. Inoltre, si consideri la funzione $F(\mathbf{k},\mathbf{x})=\mathbf{x}^2\oplus\mathbf{k}$ , dove $\mathbf{k}$ , $\mathbf{x}$ e $F(\mathbf{k},\mathbf{x})$ sono stringhe di n bit e $\mathbf{x}^2=\mathbf{x}^2$ mod $2^n$ . Rappresenta F una funzione pseudocasuale?



5)	Crittosistemi a chiave pubblica. Si dimostri che se il problema DDH è difficile nel gruppo G, allora la sahama di cifratura di El Gamal à CPA sigura. Inaltra si spiaghi coma costruira un KEM
	allora lo schema di cifratura di El Gamal è CPA-sicuro. Inoltre, si spieghi come costruire un KEM CCA-sicuro, nel random oracle model, usando le idee dello schema di El Gamal.

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

Opzionale: guardando lo schema come un sistema di prova, in cui il provatore dà prova della propria identità, se il verificatore è onesto, cioè esegue il protocollo scegliendo la challenge r in accordo alla distribuzione uniforme, risulta lo schema, per questo caso, a conoscenza zero? Argomentare la risposta.