# Quiz/Attendance 3F

Total: [ ]

[ ] [ ]

**Firstname Lastname** **ID#**

Complete the narrative, filling in the blanks. Bracketed words are hints, not part of the narrative.

1. A pseudorandom generator (PRG) is a function $G\colon \{0,1\}^\ell \to \{0,1\}^L$ with $L > \ell$. We want $G(S)$ to *look* uniformly random when $S$ *is* uniformly random. To quantify this, we defined the *advantage* of an adversary $\mathcal{A}$ in attacking $G$ as the real number

$$\mathrm{Adv}^{\mathrm{prg}}_G(\mathcal{A}) \quad = \quad \Pr[S \xleftarrow{\$} \{0,1\}^\ell : \mathcal{A}(G(S)) \Rightarrow 1] - \Pr[R \xleftarrow{\$} \{0,1\}^L : \mathcal{A}(R) \Rightarrow 1] \,.$$

Here the symbol "⇒" means [or: is read] [ ].

An advantage of 0 would mean that $\mathcal{A}$ is doing [ ] at attacking $G$, while an advantage of 1 would mean that $\mathcal{A}$ is doing [ ] at attacking $G$. In general, the higher an adversary's advantage the [ ] it is doing.

2. In class we gave a *construction* to convert a PRG $g\colon \{0,1\}^\ell \to \{0,1\}^{\ell+1}$ to a PRG $G\colon \{0,1\}^\ell \to \{0,1\}^L$. Computing $G$ once required computing $g$ [ ] times.

3. To prove our construction sound, we gave a *reduction*. It quantifies the extent to which $g$'s security implies $G$'s. The reduction transformed an adversary $\mathcal{B}$ for attacking [ ] into an adversary $\mathcal{A}$ for attacking [ ].

We showed that if [ ] [a number] is large then [ ] [a number] is large, too.