# ECS 227 — Modern Cryptography — Winter 2009

*Phillip Rogaway*

Out: Wednesday, 11 February 2009.
Due: Friday, 23 February 2009.

**5.** *(Increasing the output length of a PRF.)* Suppose you are given a PRF $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. Construct from it a PRF $G : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^{2n}$. Formalize and prove that $F$ being a good PRF implies that $G$ will be.

**6.** *(A stronger notion of encryption-scheme security)* Consider the following notion of security for a symmetric encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, which we might call *indistinguishability from random bits*:

$$\mathbf{Adv}^{\mathrm{ind\$}}_{\Pi}(A) \;=\; \Pr[A^{\mathcal{E}_K(\cdot)} \Rightarrow 1] - \Pr[A^{\$^{|\cdot|}} \Rightarrow 1]$$

where $K$ is sampled from $\mathcal{K}$ and the second oracle, asked a query $X$, computes $Y \xleftarrow{\$} \mathcal{E}_K(X)$ and returns $|Y|$ uniform random bits. (Assume of $\Pi$ that $|\mathcal{E}_K(X)|$ depends only on $|X|$.) Formalize and prove that security in the ind\$-sense implies security in the real-or-random sense.