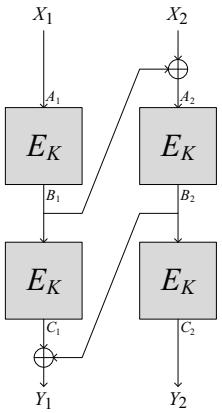
ECS 227 — Modern Cryptography — Spring 2010

Phillip Rogaway

Out: Thursday, 24 April 2010.
Due: Monday, 3 May 2010

5. Refer again to problem 4. Several students provided the following elegant construction to turn an n-bit blockcipher into a $2n$-bit one:



A. Does this construction provide a secure PRP if E is a secure PRP? Either prove that it does, using a game-playing proof, or prove that it does not.

B. Consider the same construction but using different and indpendent keys for all four of the underlying blockciphers. Does this construction yield a secure PRP if E is a secure PRP? Either prove that it does, using a game-playing proof, or prove that it does not.

6. 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*:

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

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 Π 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 (ind) sense.