Problem Set 1

Due: Tuesday January 24, 2017, in class.

By $a\|b$ we denote the concatenation of strings $a, b \in \{0,1\}^*$. (For example $010\|01 = 01001$.) The time to compute a blockcipher E, denoted T_E, is the time to compute E or E^{-1}. All times are worst case.

Problem 1 [60 points] Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Define $F\colon \{0,1\}^{k+n} \times \{0,1\}^n \to \{0,1\}^n$ as follows:

Alg $F(K_1\|K_2, M)$
$C \leftarrow E(K_1, M \oplus K_2)$
Return C

Above, $K_1 \in \{0,1\}^k$ and $K_2, M \in \{0,1\}^n$.

(a) [**8 points**] Is F a blockcipher? Answer YES or NO and prove your answer correct.

(b) [**8 points**] How much time is taken by a 3-query exhaustive key search attack on F? Your answer should be a function of T_E, k, n.

(c) [**18 points**] Present in pseudocode a 1-query adversary A_1 that has advantage $\mathbf{Adv}^{\mathrm{kr}}_F(A_1) = 1$ and running time $\mathcal{O}(T_E + k + n)$.

(d) [**26 points**] Present in pseudocode a 3-query adversary A_3 that has advantage $\mathbf{Adv}^{\mathrm{kr}}_F(A_3) = 1$ and running time $\mathcal{O}(2^k \cdot (T_E + k + n))$.

Problem 2 [40 points] Let $E_1\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ and $E_2\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be blockciphers. Define $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ by

Alg $E(K, M)$
$C_1 \leftarrow E_1(K, M)$; $C_2 \leftarrow E_2(K, C_1)$
Return C_2

Above, $K \in \{0,1\}^k$ and $M \in \{0,1\}^n$.

(a) [**10 points**] Prove that E is a blockcipher.

(b) [**30 points**] Let blockcipher $E_1\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be given. Specify in pseudocode the following:

- A blockcipher $E_2\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ —of your choice, allowed to depend on E_1— and its inverse $E_2^{-1}\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ such that the time to compute E_2 is $\mathcal{O}(T_{E_1} + k + n)$.

- A 1-query adversary A having running time $\mathcal{O}(T_{E_1} + k + n)$ and achieving advantage $\mathbf{Adv}_E^{\mathrm{kr}}(A) = 1$ against E, where E is defined as above based on the given E_1 and your E_2.
