1. (70 points) Suppose that we have a good PRF $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$. We want to build a good PRF $F : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^{2n}$. (Note that here the output length of $F$ is twice that of $E$.)

   a) (30 points) Bob suggests the following construction: $F_K(X) = E_K(X) \parallel E_K(\overline{X})$, where $\overline{X}$ is the complement of $X$. (For example $011 = 100$, and $1001 = 0110$.) Give an efficient PRF attack on Bob’s construction and analyze its advantage. Your attack should use just two queries.

   b) (40 points) Alice suggests the following construction. To compute $F_K(X)$, we first internally compute $Y \leftarrow E_K(X)$, and then output $E_K(Y) \parallel E_K(\overline{Y})$, where $\overline{Y}$ is the complement of $Y$ as defined in part (a).

   For a parameter $q$, give an attack on the PRF security of $F$ using at most $q$ queries that achieves advantage $\Omega(q^2)/2^n$. Analyze the advantage of your attack.

2 (40 points) Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a blockcipher. Let $F_{K_1,K_2}(x) = E_{K_1}(x \oplus K_2)$. Give a key-recovery attack on $F$ and analyze its advantage. The attack should use $O(2^k)$ number of queries and time, but only $O(1)$ space.

   **Note:** This is a key-recovery attack, meaning that you are always in the Real world. Don’t get confused with a PRF attack where you are either in the Real world or a Random world.

3 (40 points) Let $E : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a good PRF. Break the PRF security of $F_K(X) = E_K(X) \parallel E_K(E_K(X))$ and analyze the advantage of your attack.