Problem 1. (40 points.) Define the family of functions $F: \{0, 1\}^{256} \times \{0, 1\}^{256} \rightarrow \{0, 1\}^{256}$ by

Algorithm $F_{K_1\|K_2}(x_1\|x_2)$:
Return $AES^{-1}(K_1, x_1 \oplus x_2)\|AES(K_2, \overline{x_2})$

for all $K_1, K_2, x_1, x_2 \in \{0, 1\}^{128}$. Here ‘$\|$’ denotes string concatenation, ‘$\oplus$’ denotes bit-wise exclusive-or, and $\overline{x}$ denotes the bit-wise complement of a string $x$. Let $T_{AES}$ denote the time for one computation of $AES$ or $AES^{-1}$. Below, running-times are worst case and should be functions of $T_{AES}$.

(Part A - 5 points.) Prove that $F$ is a blockcipher.

(Part B - 5 points.) What is the running-time of a 4-query exhaustive key search adversary against $F$?

(Part C - 30 points.) Give the most efficient 4-query key recovery adversary that you can with advantage 1 against $F$. Concisely state your proposed adversary in pseudocode and formally analyze both its advantage and resource usage.

Problem 2. (20 points.) Define the family of functions $F: \{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ by $F(K, M) = AES(M, K)$. Show that $F$ is not a secure PRF. Again, concisely state your proposed adversary in pseudocode and formally analyze its advantage and resource usage.

Problem 3. (40 points.) Let $G: \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ be a family of functions (it is arbitrary but given, meaning known to the adversary) and let $r \geq 1$ be an integer. The $r$-round Feistel cipher associated to $G$ is the family of functions $G^{(r)}: \{0, 1\}^k \times \{0, 1\}^{2\ell} \rightarrow \{0, 1\}^{2\ell}$ defined as follows for any key $K \in \{0, 1\}^k$ and input $x \in \{0, 1\}^{2\ell}$:

Algorithm $G^{(r)}(K, x)$:
Parse $x$ as $L_0\|R_0$ where $|L_0| = |R_0| = \ell$
For $i = 1$ to $r$ do:
$L_i \leftarrow R_{i-1}$; $R_i \leftarrow G(K, R_{i-1}) \oplus L_{i-1}$
Return $L_r\|R_r$

(Part A - 10 points.) Show that $G^{(1)}$ is not a secure PRF. As usual, concisely state your proposed adversary in pseudocode and formally analyze its advantage and resource usage.

(Part B - 30 points.) Show that $G^{(2)}$ is not a secure PRF. As usual, concisely state your proposed adversary in pseudocode and formally analyze its advantage and resource usage.
Optional Challenge Problem. (100 extra credit points.)

(70 points.) Suppose we model a blockcipher $E : \{0,1\}^k \times \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ (e.g., let $E = AES$ and $k, \ell = 128$) as a truly random function for every key, that is, that for every $K \in \{0,1\}^k$, $E_K(\cdot)$ is an independent random function from the set of all functions from $\{0,1\}^\ell$ to $\{0,1\}^\ell$. In this model, give the best lower-bound you can on the probability that a $q$-query exhaustive key search adversary outputs the target key (rather than merely a consistent key) as a function of $q, k, \ell$.

(30 points.) The above model is known as the *ideal cipher model*. How does modeling a blockcipher this way differ from assuming it’s a secure PRF?