HOMEWORK 2 Due Feb 14 11:59PM on Gradescope.

Problem 1. (100 points.) Define the family of functions $F\colon \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ by

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

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}. For full credit avoid use of asymptotics.*

(Part A - 15 points.) Prove that F is a blockcipher according to the definition given in class.

(Part B - 15 points.) What is the running-time of a 2-query exhaustive key search adversary against F?

(Part C - 40 points.) Give the most efficient 2-query consistent key recovery adversary that you can with advantage 1 against F. Your answer should consist of the pseudocode for your proposed adversary followed by an analysis of its advantage (proving that it is 1) and resource usage (running-time and number of queries). *For full credit, your adversary should be significantly faster than exhaustive key search. Exhaustive key search gets no points.*

(Part D - 30 points.) Would you expect your adversary in Part C to recover the target key (rather than merely a consistent key)? Why or why not? *The right yes/no answer with missing or completely incorrect justification gets no points.*