HOMEWORK 3 Due Feb 28 4:59PM on Gradescope.

Note: In showing a function families below are not secure PRFs, exhaustive key search or birthday attacks are inefficient and do not get any points. To get points your adversaries must be *practical* (making at most a handful of queries and using minor additional resources).

Problem 1. (30 points.) Define the family of functions $F\colon \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ by $F(K, M) = \mathsf{AES}(M, K)$. Show that F is not a secure PRF. Make sure to follow the three steps outlined in class for this. State the advantage you conclude for your adversary. Additionally, analyze worst-case resource usage (number of queries and running-time — you do not need to count things like reading/writing input/output; if in doubt, ask). Here and on future assigments and exams I'd prefer you to give concrete running-time as a function of the bit-length of the input, but use T_{AES} for the worst-case time to compute AES or AES^{-1} as usual. Also I may not explicitly ask you for advantage and resource usage in the future; you just have to give it.

Problem 2. (70 points.) Let $G\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ 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 $G^{(r)}\colon \{0,1\}^k \times \{0,1\}^{2\ell} \to \{0,1\}^{2\ell}$ 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 - 30 points.) Show that $G^{(1)}$ is not a secure PRF. Follow the same guideline and give advantage and resource usage as above.

(Part B - 40 points.) Show that $G^{(2)}$ is not a secure PRF. Follow the same guideline and give advantage and resource usage as above.