Homework 2

Due: Thursday, April 14 at 12PM (noon).

You may discuss the problems in general terms in a group of size at most three. You are expected to write up your solutions yourself. Please credit your collaborators on your submission. You may use your course notes and slides to solve these problems. As usual our convention is that the running time of an adversary does not include the time taken by game procedures to compute responses to adversary queries.

The Gradescope assignment is called `HW2`. Please submit your completed Python code. Do not change the file name from `hw2.py`.

All problems on this PDF complement the PlayCrypt homework problem, which can be found on the course website at `https://cseweb.ucsd.edu/classes/sp22/cse107-a/resources/hw2/hw2.py`. You only need to turn in your Python solution to `PlayCrypt 2` on Gradescope. This version is being given out so that you can see what the problem looks like in mathematical notation. We suggest that you start with this version. Work out a solution using pencil and paper. Move to implementation in PlayCrypt only after that.

Detailed PlayCrypt instructions are included on a pinned Piazza note.

Extra information, such as who you collaborated with, must be put inside the `hw2.py` file that you submit.

Problem 1 [10 points] Let $k = 128$, $n = 8$ and let E: $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Define the family of functions $F : \{0,1\}^{128} \times \{0,1\}^8 \to \{0,1\}^8$ by $F(K, M) = E(K, M)$. Show that F is not a secure PRF by presenting in pseudocode an adversary A_{50} such that

- $\mathbf{Adv}^{\mathrm{prf}}_F(A_{50}) \approx 1$
- A_{50} makes at most 50 queries to its **Fn** oracle
- A_{50} is very efficient.

Problem 2 [10 points] Let $k, n \geq 4$ and 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) **[5 points]** Present in pseudocode a 1-query adversary A_1 that has advantage $\mathbf{Adv}^{\mathrm{kr}}_F(A_1) = 1$ and running time $\mathcal{O}(T_E + k + n)$.

(b) **[5 points]** Present in pseudocode a 3-query adversary A_3 that has advantage $\mathbf{Adv}^{\mathrm{kr}}_F(A_3) = 1$ and running time $\mathcal{O}(2^k \cdot (T_E + k + n))$.
