

Homework 2

Due: Wednesday, October 13 at 9PM.

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 following problems correspond to two separate Gradescope assignments. Problem 1 is called **Homework 2** on Gradescope. This should be a write-up of your solution to Problem 1; this may be either a PDF compiled from L^AT_EX or a PDF scan of handwritten work. Please name your submission `hw2.pdf`. The second Gradescope assignment is called **PlayCrypt 2**. This is for submitting your completed Python code for Problem 2. Do not change the file name from `hw2.py`.

Problem 2 on this PDF complements the PlayCrypt homework problem, which can be found on the course website at <https://cseweb.ucsd.edu/classes/fa21/cse107-a/hw2.py>. You do not need to turn in a written answer for this problem and need only 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.

Problem 1 [10 points] Define the family of functions $F : \{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ by $F(K, M) = \text{AES}(M, K)$. Show that F is not a secure PRF by presenting in pseudocode an adversary A such that

- $\text{Adv}_F^{\text{prf}}(A) = 1 - 2^{-128}$
- A makes at most 2 queries to its **Fn** oracle
- A is very efficient.

You must prove that your A has the above properties. Note that $\text{AES}(M, K)$ denotes encrypting with key M and message K .

Problem 2 [10 points] Let $k, n \geq 4$ and let $E: \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a blockcipher. Define $F: \{0, 1\}^{k+n} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ 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 $\mathbf{Adv}_F^{\text{kr}}(A_1) = 1$ and running time $\mathcal{O}(T_E + k + n)$.
- (b) [5 points] Present in pseudocode a 3-query adversary A_3 that has advantage $\mathbf{Adv}_F^{\text{kr}}(A_3) = 1$ and running time $\mathcal{O}(2^k \cdot (T_E + k + n))$.

Problem 3 [0 points] Is there any feedback you would like to give us? Are there particular topics you would like to see in discussion sections? Include any comments in your `hw2.pdf` submission.
