There are two Gradescope submissions for this assignment, one PlayCrypt code and one short-answer. This PDF is being given out so that you can see what the problems look like in mathematical notation, but you do not need to submit a PDF anywhere.

We suggest that you start with this version. Work out a solution using pencil and paper. Move to implementation in PlayCrypt only after that.

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.

Note: This problem set is due after the midterm. We strongly suggest understanding the topics prior to the midterm.

**Problem 1 [10 points]** This question is about the MAC UF-CMA game, on slides 31-32 of “Message Authentication Codes.” The set $S$ in the game keeps track of all the queried messages $M$ and disallows any $M \in S$ from being a winning forgery in $\text{Finalize}(M^*, T^*)$. Suppose we change the game as follows. Instead of tracking messages $M$ in $S$ we instead track tags $T$. That is, if a query $\text{Tag}(M)$ produces tag $T$ then $S \leftarrow S \cup \{T\}$. Now $\text{Finalize}(M^*, T^*)$ returns $\text{true}$ if $T^* = T_K(M^*)$ but $\text{false}$ if $T^* \in S$.

Do you think that this change makes any difference to the UF-CMA game? Is it better or worse at capturing common applications of MACs? Submit your answer on the Gradescope assignment “Short Answer 4.” A few sentences is sufficient.
Problem 2 [50 points] Let \( E : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l \) be a block cipher and let \( T_E \) denote the time to compute \( E \) or \( E^{-1} \). Let \( D \) be the set of all strings whose length is a positive multiple of \( l \), meaning:
\[
D = \{ M \in \{0,1\}^* : |M| > 0 \text{ and } |M| \mod l = 0 \}.
\]
In the pseudocode below, \( M[1]M[2] \ldots M[n] \leftarrow M \) means we break \( M \) into \( l \)-bit blocks, with \( M[i] \) denoting the \( i \)-th block and \( n \) the number of blocks.

Define the hash function \( H_2 : \{0,1\}^k \times D \to \{0,1\}^l \) as follows:

\[
\text{Alg } H_2(K, M) \\
C[0] \leftarrow 0^n \\
\text{For } i = 1, \ldots, n \text{ do } W[i] \leftarrow E(K, C[i - 1] \oplus M[i]) ; C[i] \leftarrow E(K, W[i] \oplus M[i]) \\
\text{Return } C[n]
\]

Show that \( H_2 \) is not collision-resistant by presenting an \( O(T_E + l) \)-time adversary \( A_2 \) with \( \text{Adv}_c^{\text{cr}} H_2(A_2) = 1 \). Begin with the starter code posted on the course website, and submit your solution to this problem on the Gradescope assignment “Problem Set 4.”

---

Problem 3 [50 points] Let \( E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n \) be a block cipher with \( n \geq 4 \). Let
\[
D = \{ M \in \{0,1\}^* : 0 < |M| < n2^n \text{ and } |M| \mod n = 0 \}.
\]
Let \( T : \{0,1\}^k \times D \to \{0,1\}^n \) be defined as follows:

\[
\text{Alg } T_K(M) \\
M[1] \ldots M[m] \leftarrow M ; M[m + 1] \leftarrow \langle m \rangle ; C[0] \leftarrow 0^n \\
\text{For } i = 1, \ldots, m + 1 \text{ do } C[i] \leftarrow E_K(C[i - 1] \oplus M[i]) \\
T \leftarrow C[m + 1] ; \text{Return } T
\]

Above, \( M[1] \ldots M[m] \leftarrow M \) means we break \( M \) into \( n \)-bit blocks, and \( \langle m \rangle \) denotes the \( n \)-bit binary representation of the integer \( m \). (For example, if \( n = 8 \) and \( m = 2 \) then \( \langle m \rangle = 00000010 \).)

Show that \( T \) is an insecure message-authentication code by presenting an \( O(n) \)-time adversary \( A \), making at most 2 queries to its \text{Tag} oracle and one query to its \text{Verify} oracle, and achieving \( \text{Adv}^{\text{uf-cma}}_A(T) = 1 \). Begin with the starter code posted on the course website, and submit your solution to this problem on the Gradescope assignment “Problem Set 4.”