Homework 3

Due: Thursday, April 21 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.

This complements the PlayCrypt version of this problem set. You need turn in only the latter, on
Gradescope. This version is being given out so that you can see what the problems look like in
mathematical notation. Do not rename your homework file from hw3.py.

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.

Problem 1 [10 points] Let \( k, n \geq 8 \) be integers and let \( E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n \) be a block cipher. Let \( T_E \) be the time to compute \( E \). Let \( K \) be the key-generation algorithm that returns a random \( k \)-bit string as the key \( K \). Let \( E \) be the following encryption algorithm:

\[
\begin{align*}
\text{Alg } E_K(M) \\
M[1] \ldots M[m] &\leftarrow M \\
C[0] &\leftarrow \{0,1\}^n; \\
\text{count} &\leftarrow \text{int}(E(K, C[0])) \\
\text{for } i = 0, \ldots, m - 1 \text{ do} \\
\quad P[i] &\leftarrow \text{bin}(\text{count} + i \mod 2^n) \\
\quad A[i] &\leftarrow P[i] \oplus M[i + 1] \\
\quad B[i] &\leftarrow E(K, A[i]) \\
\quad C[i + 1] &\leftarrow B[i] \oplus P[i] \\
C &\leftarrow C[0]C[1] \ldots C[m] \\
\text{return } C 
\end{align*}
\]

Here, \( \text{int()} \) changes binary string (bytes) into integer and \( \text{bin()} \) changes integer to bytes string
(binary). The message space is the set of all strings whose length is a positive multiple of \( n \),
meaning these are the allowed messages. The first line above indicates that \( M \) is broken into \( n \)-bit blocks, with \( M[i] \) denoting the \( i \)-th block and \( m \) the number of blocks. (For example if \( n = 4 \) and \( M = \text{01101011} \) then \( M[1] = \text{0110} \) and \( M[2] = \text{1011} \) and \( m = 2 \).) The ciphertext \( C \) is \((m + 1)n\) bits long, with each \( C[i] \) being \( n \) bits for \( i = 0, \ldots, m \).
1. **[3 points]** Specify decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme satisfying the correct decryption condition of Slide 3. If the input ciphertext has length $(m + 1)n$ then the running time of $\mathcal{D}$ should be $O(m \cdot (T_E + n))$.

2. **[7 points]** Show that this scheme is not IND-CPA secure by presenting a $O(T_E + n)$-time adversary $A$ making one query to its LR oracle and achieving $\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) \geq 0.9$.

---

**Problem 2 [10 points]** Let $E: \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$ 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 $\ell$.

1. **[4 points]** Define the hash function $H_1: \{0, 1\}^k \times D \rightarrow \{0, 1\}^\ell$ via the CBC construction, as follows:

   \begin{align*}
   \text{Alg } H_1(K, M) \\
   C[0] \leftarrow 0^\ell \\
   \text{For } i = 1, \ldots, n \text{ do} \\
   \quad C[i] \leftarrow E(K, C[i - 1] \oplus M[i]) \\
   \text{Return } C[n]
   \end{align*}

   Show that $H_1$ is not collision-resistant by presenting an $O(T_E + \ell)$ time adversary $A_1$ with $\text{Adv}_{H_1}^{\text{cr}}(A_1) = 1$.

2. **[6 points]** Define the hash function $H_2: \{0, 1\}^k \times D \rightarrow \{0, 1\}^\ell$ as follows:

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

   Show that $H_2$ is not collision-resistant by presenting an $O(T_E + \ell)$ time adversary $A_2$ with $\text{Adv}_{H_2}^{\text{cr}}(A_2) = 1$. 