Homework 3

There are two Gradescope submissions for this assigment, 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.

Problem 1 [10 points] Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme. Recall that we defined perfect security in the "Classical Encryption" slides. If $\mathcal{SE}$ is perfectly secure, is it necessarily true that $\mathcal{SE}$ is IND-CPA-secure? If $\mathcal{SE}$ is IND-CPA-secure, is it necessarily true that $\mathcal{SE}$ is perfectly secure?

Submit your answer on the Gradescope assignment "Short Answer 3." 1-2 sentences for each direction is sufficient.

Problem 2 [100 points] Let $k, n \geq 4$ be integers and let E: $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let T_E be the time to compute E or E^{-1}. Let $\mathcal{K}$ be the key-generation algorithm that returns a random k-bit string as the key K. Let $\mathcal{E}$ be the following encryption algorithm:

Alg $\mathcal{E}_K(M)$
$M[1] \dots M[m] \leftarrow M$
$R \xleftarrow{\$} \{0,1\}^n$; $C[0] \leftarrow R$
for $i = 1, \dots, m$ do
  $W[i] \leftarrow (R + i) \bmod 2^n$; $C[i] \leftarrow E_K(M[i] \oplus W[i])$
$C \leftarrow C[0]C[1] \dots C[m]$
return C

Above $W[i] \leftarrow (R+i) \bmod 2^n$ means we regard R as an integer, add i to it, take the result modulo 2^n, view this as an n-bit string, and assign it to $W[i]$. (For example if $n = 4$ and $R = 1110$ and $i = 3$ then $W[i] = 0001$.)

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 $M = 01101011$ then $M[1] = 0110$ and $M[2] = 1011$ and $m = 2$.)

1. **[20 points]** Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme satisfying the correct decryption condition. The running time of $\mathcal{D}$ should be $\mathcal{O}(m \cdot (T_E + n))$ when the ciphertext is $m + 1$ blocks long.

2. **[80 points]** Show that this scheme is not IND-CPA secure by presenting an $\mathcal{O}(T_E + k + n)$-time adversary A making one query to its **LR** oracle and achieving $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 1$.

Begin with the starter code posted on the course website, and submit your solution to this problem on the Gradescope assignment "Problem Set 3."
