Homework 2

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 $F : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ be a function family. Bob claims that they can distinguish between F and a truly random function in the PRF game. In particular, Bob chooses $m \in \mathcal{M}$, queries $c_1 \leftarrow \mathbf{Fn}(m)$; $c_2 \leftarrow \mathbf{Fn}(m)$. If $c_1 = c_2$ then Bob decides that they are interacting with F (outputs 1) and if $c_1 \neq c_2$ then Bob decides that they are interacting with a truly random function (outputs 0).

Alice disagrees with Bob; she thinks that *for all* function families F, this attack strategy will have advantage 0 in the PRF game.

Do you agree with Bob, Alice, or neither? Submit your answer as **no more than two sentences** on the Gradescope assignment "Short Answer 2."

Problem 2 [100 points] Let G: $\{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a family of functions and let $r \geq 1$ be an integer. The *r-round Feistel cipher associated to G* is the family of functions $G^{(r)}$: $\{0,1\}^k \times \{0,1\}^{2l} \to \{0,1\}^{2l}$, defined as follows for any key $K \in \{0,1\}^k$ and input $x \in \{0,1\}^{2l}$:

Alg $G^{(r)}(K, x)$
$L_0 \| R_0 \leftarrow x$
For $i = 1, \ldots, r$ do
    $L_i \leftarrow R_{i-1}$; $R_i \leftarrow G(K, R_{i-1}) \oplus L_{i-1}$
Return $L_r \| R_r$

In the first line, we are parsing x as $x = L_0 \| R_0$ with $|L_0| = |R_0| = l$, meaning L_0 is the first l bits of x and R_0 is the rest.

The Feistel construction with many rounds was historically a common way to turn a non-invertible function family G into a block cipher $G^{(r)}$. (For example, DES was constructed this way.) In this problem, you'll show that if the number of rounds r is too small, the result won't be secure, regardless of G:

1. **[40 points]** Show that $G^{(1)}$ is not a secure PRF by presenting an $\mathcal{O}(k+l)$-time adversary A making one query to its **Fn** oracle and achieving $\mathbf{Adv}^{\text{prf}}_{G^{(1)}}(A) = 1 - 2^{-l}$.

2. **[60 points]** Show that $G^{(2)}$ is not a secure PRF by presenting an $\mathcal{O}(k+l)$-time adversary A making two queries to its **Fn** oracle and achieving $\mathbf{Adv}^{\text{prf}}_{G^{(2)}}(A) = 1 - 2^{-l}$.

Begin with the starter code posted on the course website, and submit your solution to this problem on the Gradescope assignment "Problem Set 2."
