Homework 1

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. For the PlayCrypt question, even though this PDF says "pseudocode," you won't turn any pseudocode in — instead you'll submit your PlayCrypt code.

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 [100 points] Alice is a student taking ESC (Engineering and Science of Computers) 701. In class she learned that DES was a block cipher that was initially the standard block cipher everyone used, but became obsolete as the key size was too small to resist brute force attacks.

After some thought, she had an idea: what if she constructed a new block cipher built on top of DES with a key size larger than what DES uses? That way, this new block cipher would have the strong internal design of DES while also solving the problem of its small key size. The best of both worlds!

Her proposed DES improvement is described below, where F is the new block cipher and E is the internal block cipher used by F. For example, Alice can set E to DES.

Let $k, n \geq 4$ and let $E\colon\ \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Define $F\colon\ \{0,1\}^{k+n} \times \{0,1\}^n \to \{0,1\}^n$ 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 $K_2, M \in \{0,1\}^n$.

Bob looked at the construction Alice proposed, and felt there was something not quite right with it. Your task is to confirm Bob's suspicions and show that Alice's scheme can indeed be broken.

(a) **[50 points]** Present in pseudocode a 1-query adversary A_1 that has advantage $\mathbf{Adv}^{\mathrm{kr}}_F(A_1) = 1$ and running time $\mathcal{O}(T_E + k + n)$.

(b) **[50 points]** Present in pseudocode a 3-query adversary A_3 that has advantage $\mathbf{Adv}_F^{\mathrm{kr}}(A_3) = 1$ and running time $\mathcal{O}(2^k \cdot (T_E + k + n))$.

Begin with the starter code posted on the course website, and submit your solution to this problem on the Gradescope assignment "Problem Set 1."

Problem 2 **[10 points]** Suppose Bob wants to recover the **actual** key someone is using in Alice's block cipher with just a few chosen plaintexts. Look at the two different attacks you designed in the previous question — should Bob use the one in part a or part b? Explain your answer **in no more than 2 sentences**.

Submit your answer to the Gradescope assignment "Short Answer 1."
