COSC-466: Homework 2

Problem 1. (40 points.) This problem constucts a silly blockcipher out of AES and asks you to cryptanalyze it. This is meant to get you comfortable with the definitions and how physical key length is different from effective key length.

Define the family of functions $F\colon \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ by

$$\begin{array}{l}\textbf{Algorithm } F_{K_1\|K_2}(x_1\|x_2)\text{:}\\ \quad \text{Return } \mathsf{AES}^{-1}(K_1, x_1 \oplus x_2)\|\mathsf{AES}(K_2, \overline{x_2})\end{array}$$

for all $K_1, K_2, x_1, x_2 \in \{0,1\}^{128}$. Here '$\|$' denotes string concatenation, '$\oplus$' denotes bit-wise exclusive-or, and $\overline{x}$ denotes the bit-wise complement of a string x. Let T_{AES} denote the time for one computation of AES or AES^{-1}. Below, running-times are worst case and should be functions of T_{AES}. Do not use asymptotic (big-oh) notation, and assume one query takes unit time.

(Part A - 5 points.) Prove that F is a blockcipher. Grading guidline: Must use definition of blockcipher given in class. No partial credit.

(Part B - 5 points.) What is the running-time of a 4-query exhaustive key search adversary against F? Grading guideline: Must use definition of q-query exhaustive key search adversary given in class. No partial credit.

(Part C - 30 points.) Give the most efficient 4-query key recovery adversary that you can with advantage 1 against F. Concisely state your proposed adversary in pseudocode and formally analyze both its advantage and resource usage. Grading guidline: 25 points for pseudocode of adversary. Must be faster than a 4-query exhaustive key search adversary to get any credit. Adversary must run in time $c \cdot T_{\mathsf{AES}} \cdot 2^{128}$ for $c \leq 10$ for full credit, otherwise half credit. 5 points for resource analysis — here and below please count running-time and number of queries.

Problem 2. (20 points.) This problem shows you that switching the key and the input to a secure PRF renders it insecure.

Define the family of functions $F\colon \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ by $F(K,M) = \mathsf{AES}(M,K)$. Show that F is not a secure PRF. Again, concisely state your proposed adversary in pseudocode and formally analyze its advantage and resource usage. Grading guideline: 15 points for pseudocode of adversary. *Here and in remaining problems, generic attacks such as exhaustive key search or birthday attack get no credit.* Adversary must have advantage about advantage $1 - 2^{-128}$, make at most 3 queries, and have running time at most $3 \cdot T_{\mathsf{AES}}$ for full credit. Otherwise half credit.

Problem 3. (40 points.) Recall that the construction of DES uses 16 "Feistel rounds." In addition to (intuitively) providing confusion and diffiusion, a salient feature of this approach is that it yields *invertibility*. One may ask if we can formally analyze this technique. Below you are asked to show

that a very small number of Feistel rounds (1 or 2) does *not* result in a secure PRF, regardless of what one assumes about the round function (denoted G below). A seminal result from the 1980's called the Luby-Rackoff Theorem shows 3 rounds *is* enough if the round function is itself a PRF. Since then it has also been shown that more rounds increase the number of queries required to break the construction. This lends some insight into why the designers of DES were really smart!

Let $G\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ be a family of functions (it is arbitrary but given, meaning known to the adversary) and let $r \geq 1$ be an integer. The *r-round Feistel cipher associated to G* is the family of functions $G^{(r)}\colon \{0,1\}^k \times \{0,1\}^{2\ell} \to \{0,1\}^{2\ell}$ defined as follows for any key $K \in \{0,1\}^k$ and input $x \in \{0,1\}^{2\ell}$:

Algorithm $G^{(r)}(K,x)$:
  Parse x as $L_0 \| R_0$ where $|L_0| = |R_0| = \ell$
  For $i = 1$ to r do:
    $L_i \leftarrow R_{i-1}$; $R_i \leftarrow G(K, R_{i-1}) \oplus L_{i-1}$
  Return $L_r \| R_r$

(Part A - 10 points.) Show that $G^{(1)}$ is not a secure PRF. As usual, concisely state your proposed adversary in pseudocode and formally analyze its advantage and resource usage. Grading guideline: 8 points for pseudocode of adversary. Here and in Part B, adversary must have advantage about $1 - 2^{-\ell}$, make at most 3 queries, and do minor additional computation for full credit, otherwise half credit. 2 points for resource analysis.

(Part B - 30 points.) Show that $G^{(2)}$ is not a secure PRF. As usual, concisely state your proposed adversary in pseudocode and formally analyze its advantage and resource usage. Grading guideline: Grading guideline: 25 points for pseudocode of adversary. 5 points for reseource analysis.

Optional Challenge Problem. (100 extra credit points.)

(70 points.) Suppose we model a blockcipher $E\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ (e.g., let $E = \mathsf{AES}$ and $k, \ell = 128$) as a truly random function for *every* key, that is, that for *every* $K \in \{0,1\}^k$, $E_K(\cdot)$ is an independent random function from the set of all functions from $\{0,1\}^\ell$ to $\{0,1\}^\ell$. In this model, give the best lower-bound you can on the probability that a q-query exhaustive key search adversary outputs the *target* key (rather than merely a consistent key) as a function of q, k, ℓ. Grading guidline: Must make non-trivial progress to receive any points. Points awarded at instructor's discretion.

(30 points.) The above model is is known as the *ideal cipher model*. How does modeling a blockcipher this way differ from assuming it's a secure PRF? Grading guideline: Must accurately compare models. Points awarded at instructor's discretion.