Computer Science and Engineering, UCSD — Fall 09
CSE 207: Modern Cryptography — **Instructor:** Mihir Bellare
Problem Set 2 — October 5, 2008

Problem Set 2

Due: Monday October 12, 2009, in class.

Collaboration is *not* allowed on this problem set, meaning you must do it on your own. See the course information sheet for more information and details about rules.

Problem 1. [**20 points**] Define the family of functions $F\colon \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ by $F(K, M) = \mathsf{AES}(M, K)$. Assuming AES is a secure PRF, is F a secure PRF? If so, explain why. If not, present the best attack (with analysis) that you can.

Problem 2. [**60 points**] Let $F\colon \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^L$ be a family of functions where $l, L \geq 128$. Consider the game G of Fig. 1.

```
Game G

procedure Initialize
$K \xleftarrow{\$} \{0,1\}^k$ ; $b \xleftarrow{\$} \{0,1\}$

procedure LR($x_0, x_1$)
Ret $F(K, x_b)$

procedure Finalize($b'$)
Ret $(b = b')$
```

Figure 1: Game G for Problem 2.

We define

$$\mathbf{Adv}^{\mathrm{lr}}_{F}(B) \;=\; 2 \cdot \Pr\left[\mathrm{G}^{A} \Rightarrow \mathsf{true}\right] - 1\ .$$

Let $(x_0^1, x_1^1), \ldots, (x_0^q, x_1^q)$ be the queries that B makes to its oracle. (Each query is a pair of l-bit strings, and there are q queries in all.) We say that B is *legitimate* if $x_0^1, \ldots, x_0^q$ are all distinct, and also $x_1^1, \ldots, x_1^q$ are all distinct. We say that F is LR-secure if $\mathbf{Adv}^{\mathrm{lr}}_{F}(B)$ is "small" for every legitimate B of "practical" resources.

1. [**10 points**] Show that the legitimacy condition is necessary for LR-security to be "interesting" by showing that if F is a block cipher then there is an efficient, illegitimate B such that $\mathbf{Adv}^{\mathrm{lr}}_{F}(B) = 1$. Say how may queries B uses and what is its time-complexity.

2. [**25 points**] Let B be a legitimate lr-adversary that makes q oracle queries and has time-complexity t. Show that there exists a prf-adversary A, also making q oracle queries and

having time-complexity close to t, such that

$$\mathbf{Adv}_F^{\mathrm{lr}}(B) \;\leq\; 2 \cdot \mathbf{Adv}_F^{\mathrm{prf}}(A) \;.$$

State what is the time-complexity of A. Explain why this reduction shows that if F is a secure PRF then it is LR-secure.

3. [**25 points**] Is the converse true? Namely, if F is LR-secure, then is it a secure PRF? Answer YES or NO. If you say YES, justify this via a reduction, and, if NO, via a counter-example. (The latter means a particular family of functions F which you can prove is LR-secure but which you can show via an attack is not a PRF.)

We clarify that F above is a family of functions. It is not required to be a block cipher except in part **1.**