

## Problem Set 3

**Due:** Thursday January 31, 2008, in class.

See course information section (on course web page) for instructions and rules on working on problem sets and turning them in.

---

**Problem 1. [60 points]** Let  $\mathcal{K}$  be the key-generation algorithm that returns a random 128-bit string as the key  $K$ . Let  $\mathcal{E}$  be the following encryption algorithm, based on the block cipher AES:

```
algorithm  $\mathcal{E}_K(M)$ 
  if  $|M| \neq 64$  then return  $\perp$  // Only encrypts 64 bit messages
   $R \xleftarrow{\$} \{0, 1\}^{64}$ 
   $C \leftarrow \text{AES}_K(R||M)$ 
  return  $C$ 
```

Above, “ $x||y$ ” denotes the concatenation of strings  $x$  and  $y$ , and  $x \xleftarrow{\$} \{0, 1\}^{64}$  is the operation of picking a random 64 bit string and calling it  $x$ .

1. [10 points] Specify a decryption algorithm  $\mathcal{D}$  such that  $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  is a symmetric encryption scheme providing correct decryption.
  2. [40 points] Give the best attack you can on this scheme. Your attack should take the form of an ind-cpa adversary  $A$  that makes  $q$  oracle queries and has  $O(q)$  running time, and you should specify  $\text{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)$  as a function of  $q$ . Indicate roughly for what value of  $q$  the advantage is at least  $1/2$ . (The better the attack, meaning the smaller the value of  $q$  for which this is true, the more points you get.)
  3. [10 points] As a result of your attack, do you consider the scheme to be secure or insecure? Discuss.
-