Problem Set 3

Due: Monday October 19, 2009, in class.

Collaboration is allowed on this problem set. See the course information sheet for collaboration rules.

Problem 1. [100 points] Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and let algorithm $\mathcal{K}$ return $K \stackrel{\$}{\leftarrow} \{0,1\}^k$. Assume messages to be encrypted have length $\ell < n$. Let $\mathcal{E}$ be the following encryption algorithm:

algorithm $\mathcal{E}_K(M)$
  if $|M| \neq \ell$ then return $\perp$ // Only encrypts ℓ-bit messages
  $R \stackrel{\$}{\leftarrow} \{0,1\}^{n-\ell}$
  $C \leftarrow E_K(R \,\|\, M)$
  return C

Above, "$x \,\|\, y$" denotes the concatenation of strings x and y.

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. Given an even number q, your attack should take the form of an ind-cpa adversary A that makes q oracle queries and has running time around that for $O(q)$ applications of E. Specify $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A)$ as a function of q, n, ℓ. Letting $n = 128$, make a table showing, for values $\ell = 1, 16, 32, 64, 96$, the smallest value of q for which the advantage is at least $1/4$. (The better the attack, the more points you get.) For the analysis, you may find Lemma A.1 below useful.

3. [**40 points**] Give a reduction of the IND-CPA security of $\mathcal{SE}$ to the PRF security of E. This means you must state a theorem that upper bounds the ind-cpa advantage of a given ind-cpa adversary A as a function of the prf-advantage of a constructed prf-adversary B and (possibly) n, ℓ and the number q of LR-queries made by A. This is analogous to results we have seen in class for CTRC and CBC\$ encryption. Prove your theorem using a game sequence. The better the theorem (meaning the quantitative relationship) the more points you get.

4. [**10 points**] As a result of the above, do you consider the scheme to be secure or insecure? Discuss this for $E = \mathsf{AES}$ and $\ell = 1, 16, 32, 64, 96$.

A Generalized birthday lemma

Let N, r be positive integers and let S be a set of size N. Suppose we pick $y_1, \ldots, y_r$ at random from S and also pick $z_1, \ldots, z_r$ at random from S. Let $D(N, r)$ be the probability that there exist i, j such that $y_i = z_j$.

Lemma A.1 Let N, r be positive integers. Then

$$D(N, r) \;\geq\; \frac{C(N, 2r)}{2} \; .$$
