Problem Set 3

Due: Monday February 9, 2009, 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. [50 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.

function $\mathcal{E}_K(M)$
  $R \xleftarrow{\$} \{0,1\}^{128}$
  $C[0] \leftarrow R$
  for $i = 1, \ldots, n$ **do**
    $R[i] \leftarrow (R + i) \bmod 2^{128}$
    $C[i] \leftarrow \mathsf{AES}_K(M[i] \oplus R[i])$
  $C \leftarrow C[0]C[1] \ldots C[n]$
  return C

Above $R[i] \leftarrow (R + i) \bmod 2^{128}$ means we regard R as an interger, add i to it, take the result modulo 2^{128}, view this as a 128-bit string, and assign it to $R[i]$. The message space is the set of all strings whose length is a positive multiple of 128, and, as usual $M[i]$ denotes the i-th (128-bit) block of a message M and n denotes the number of blocks.

1. **[10 points]** Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme.

2. **[40 points]** Show that this scheme is insecure by presenting a practical adversary A such that $\mathbf{Adv}^{\text{ind-cpa}}_{cpa}(\mathcal{SE})(A)$ is high. State the value of the advantage achieved by your adversary and the number of oracle queries it makes.

Problem 2. [25 points] A nuclear plant transmits 2^{35} ciphertexts to a monitoring station. Each ciphertext encrypts, under a key shared between the parties, a voltage measurement that is either HIGH or LOW. (Each of these values is encoded in binary for the encryption.) Consider the following choices of encryption scheme:

1. **[15 points]** DES in CBC\$ mode

2. [**15 points**] 2DES in CBC$ mode

3. [**15 points**] AES in ECB mode

For each choice, discuss possible threats and indicate to what extent they impact security. Highlight differences in the security provided by the schemes and what types of guarantees are available. Ultimately indicate for each choice whether it is secure or not. Strive to concisely provide only relevant information; you lose points otherwise.
