CS 120/CSCI E-177: Introduction to Cryptography

Problem Set 6

Assigned: Nov. 9, 2006 Due: FRI Nov. 17, 2006 (1:10 PM)

Justify all of your answers. See the syllabus for collaboration and lateness policies. You can submit by email to `ciocan@eecs` (please include source files) or by hardcopy Carol Harlow in MD 343.

Problem 1. (Separating Passive and Active Security) In class, we saw that every encryption scheme that satisfies indistinguishability under chosen plaintext attack also satisfies multiple-message indistinguishability. In this problem, you'll see that the converse is false. Let $\{f_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\{0,1\}^n}$ be a family of pseudorandom functions (for security parameter n). Consider a probabilistic encryption scheme over message space $\{0,1\}^n$ where

$$E_k(m) = \begin{cases} (r, f_k(r) \oplus m, f_k(0^n)) & \text{if } m \neq f_k(0^n) \\ (r, f_k(r) \oplus m, k) & \text{if } m = f_k(0^n) \end{cases}$$

where $r \xleftarrow{R} \{0,1\}^n$ is chosen randomly for each encryption. Prove that this encryption scheme satisfies multiple-message indistinguishability, but is insecure against chosen-plaintext attack.

Problem 2. (Secure Identification) Consider the setting where a user needs to log on to a server, and the user and server share a secret key $k \xleftarrow{R} \{0,1\}^n$ that was selected when the user's account was first created. To avoid having to remember k, the user stores it on a PDA or smartcard, which can also perform computations for the user.

The traditional way for the user to identify herself to the server is by sending k to the server, which can then verify that it received the correct key. However, an adversary listening in on the communication would learn k and could later impersonate the user.

Using pseudorandom functions, design a protocol for identification that does not have this difficulty. That is, even after watching the user identify herself many times, a polynomial-time adversary should not be able to successfully impersonate the user (except with negligible probability). Justify the security of your scheme using the definition of pseudorandom functions.

Problem 3. (Modes of Operation) Recall that block ciphers (like AES or DES) are used for encryption via various *modes of operation*. Certain modes of operation are insecure regardless of the properties of the underlying block cipher.

1. Although in Output Feedback (OFB) Mode the initial value IV (denoted c_0 in the lecture notes) is transmitted in the clear, it must still be chosen at random. Explain why OFB with a deterministic choice of IV does not satisfy indistinguishability under chosen-plaintext attack.
2. Consider a Cipher Block Chaining (CBC) variant in which a random initial value $c_0 = IV$ is chosen (and sent in the clear) but instead of computing each ciphertext block as $c_{i+1} = F_k(c_i \oplus m_{i+1})$, the encryption rule is $c_{i+1} = c_i \oplus F_k(m_{i+1})$. Show that this variant does not satisfy indistinguishability under chosen-plaintext attack.

Problem 4. (Attacks on Round-Reduced AES) In this problem, you will show that AES with a very small number of rounds is insecure. The high-level structure of AES as described in class should suffice for this problem; in particular, the solution does not require an understanding of arithmetic over finite fields. You may find it helpful to read the attacks on round-reduced substitution-permutation networks in KL §5.1. (Note that these attacks refer to the structure shown in Figure 5.1, not 5.2, and that AES does not exactly fit this structure.)

1. Show that 1-round AES is not (a concrete-security version of) a family of pseudorandom permutations.

2. Show that using 1-round AES in Counter (CTR) Mode results in an encryption scheme that is not secure against chosen-plaintext attack.

3. Show that 2-round AES is not a family of pseudorandom permutations. (Hint: show how to construct two inputs for which the outputs disagree at most one column.)

4. Extra credit: Show that 3-round AES is not a family of pseudorandom permutations. (Hint: A distinguishing advantage of $\approx 1/2^8$ should be considered 'nonnegligible'.)