Foundations of Cryptography

Homework Set No. 5

Date Due: Jan 28th 2007

1. Consider the following construction of a pseudo-random function on a *very* large domain, from one on large domain. Let $F_S : \{0,1\}^n \mapsto \{0,1\}^m$ be a pseudo-random function, and let H be a family of universal hash functions $h : \{0,1\}^{n'} \mapsto \{0,1\}^n$ such that $\Pr_{h \in_R H}[h(x) = h(x')] \leq \epsilon$ for every $x \neq x'$. Construct $F'_S : \{0,1\}^{n'} \mapsto \{0,1\}^m$ by having $F'_{S,h}(x) = F_S(h(x))$. What can you say about the quality of the family F'?

2. **Encrypting the secret key.** A key-dependent chosen-plaintext attack is a generalization of chosen-plaintext attack, in which the attacker is also allowed to provide a polynomial-time computable function g and to receive an encryption of the message $m = g(sk)$, where sk is the secret key.

   (a) Give an example of an encryption scheme which is semantically secure against a chosen-plaintext attack but is *totally insecure* (i.e., allows retrieving the secret key) when given an encryption of the secret key. Either public-key or shared-key schemes are valid.

   (b) Length preserving encryption: Show that *any* length preserving encryption scheme is totally insecure against an adaptive key-dependent chosen plain-text attack. I.e., show that by adaptively choosing functions g_i, an attacker can retrieve the secret key.

3. **Combiner for public-key encryption schemes.** Given two candidate public-key encryption schemes, E_1 and E_2, construct a third scheme that is semantically secure against a chosen-plaintext attack if and only if at least one of E_1 and E_2 is semantically secure against a chosen-plaintext attack.

4. Given a family of pseudo-random permutations on domains D which are powers of 2, suggest a family of pseudo-random permutation on any domain size.