15-859(I) Theoretical Foundations of Cryptography

Homework 5 **due: March 31, 2003**

Ground Rules. You may speak with other students about these problems, and you may use any source you can find, but you must reference any source you use in your write-up. Please hand in a computer-generated hard copy of your solutions at the beginning of class on the due date.

1. **Efficient Semantically Secure PKC from tOWP** Let P be a family of trapdoor one-way permutations, and let b_p be a hardcore-bit for $p \in P$. Associate with P the cryptosystem $S_P = (G, E, D)$ defined as follows:

   - $G(1^k)$: Choose $(p, p^{-1}) \leftarrow P_k$. $e = p$, $d = p^{-1}$.
   - $E(p, m = m_1, \ldots, m_\ell)$: Choose $r_1 \leftarrow U_k$. define $b_i = b_p(r_i)$, $r_{i+1} = p(r_i)$, $c_i = m_i \oplus b_i$. Output $c_1, c_2, \ldots, c_\ell, r_{\ell+1}$.
   - $D(p^{-1}, c_1, c_2, \ldots, c_\ell, r_{\ell+1})$: Let $r_i = p^{-1}(r_{i+1})$, $b_i = b_p(r_i)$, $1 \leq i \leq \ell$. Set $m_i = c_i \oplus b_i$, and output $m_1, m_2, \ldots, m_\ell$.

   Prove that S_P is polynomially secure if P is a trapdoor one-way permutation family. Notice that for an ℓ-bit plaintext, S_p has ciphertexts of length $\ell + k$, compared to $k\ell$ in the system described in class.

2. **Hybrid Semantically Secure PKC** Let $P = (G_P, E_P, D_P)$ be a semantically secure PKC for the message space $\{0,1\}^k$ and let $S = (G_S, E_S, D_S)$ be a IND-CPA-secure symmetric cryptosystem. Prove that the "hybrid encryption scheme" given by

   $$G_H(1^k) = G_P(1^k) \ ,$$

   $$E_H(e, m) = E_P(e, K) || E_S(K, m) : K \leftarrow G_S(1^k) \ ,$$

   $$D_H(d, c_1 || c_2) = D_S(D_P(d, c_1), c_2) \ ,$$

   is also polynomially secure.

3. **Polynomial and Semantic Security** Let $S = (G, E, D)$ be a PKC. Prove that if S is polynomially insecure, then S is also semantically insecure: that is, S is polynomially secure if it is semantically secure. Combined with the result in class, this gives us that polynomial security and semantic security are equivalent.