Foundations of Cryptography

Homework Set No. 3

Date Due: Dec 20th 2006

1. Let $\{D_n\}$ and $\{D'_n\}$ be two distributions that are (i) Computationally indistinguishable (ii) Polynomial time samplable. Suppose that $y_1, y_2, \ldots y_m$ are all sampled according to $\{D_n\}$ or all are sampled according to $\{D'_n\}$.
Prove: no probabilistic polynomial time machine can tell, given $y_1, y_2, \ldots y_m$, whether they were sampled from $\{D_n\}$ or $\{D'_n\}$.

2. Show that if pseudo-random generators exist, then one-way functions exist.

3. Suppose that the function g maps a given a seed into a sequence of blocks. Let $\ell(n)$ be the number of blocks a given a seed of length n is mapped to. If the input (seed) is random, then the output *passes the next-block unpredicatability* test: For any prefix $0 < i < \ell(n)$, for any probabilistic polynomial time adversary A that receives the first i blocks of $y = g(x)$ and tries to guess the next block y_{i+1}, for any polynomial $p(n)$ and sufficiently large n

$$|\Pr[A(y_1, y_2, \ldots, y_i) = y_{i+1}]| < 1/p(n)$$

Show how to convert a next-block unpredictable generator into a pseudo-random generator.

4. A function $S : \{0,1\}^* \times \{0,1\}^* \mapsto \{0,1\}^*$ is called a *pseudo-random synthesizer* if (i) it is polynomial time computable and (ii) For any m polynomial in n, if $\langle x_1, \ldots, x_m \rangle$ and $\langle y_1, \ldots, y_m \rangle$ are chosen uniformly at random from $\{0,1\}^n$, then the output of S on all the combinations of these assignments, $(S(x_i, y_j))_{i,j=1}^m$, is indistinguishable from a random $m \times m$ matrix with entries of size $|S(x_i, y_j)|$ to a polynomial-time observer.

1. Show how to construct a synthesizer from the Diffie-Hellman assumption.
2. Show how to constrict a synthesizer from trapdoor permutations.