Foundations of Cryptography

Homework Set No. 9

Date Due: Januray 22nd 2004

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.