Foundations of Cryptography

Homework Set No. 10

Date Due: January 29th 2004

1. 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. Bonus: Can you think of simple examples of block generators?