CS655: Cryptography **Spring 2007**

Homework #1

Due date & time: 10:30am on January 23, 2007. Hand in at the beginning of class (preferred), or email to the instructor (ninghui@cs.purdue.edu) by the due time.

Late Policy: Late homework will not be accepted.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (10 pts) Prove that, if $g : \{0,1\}^n \longrightarrow \{0,1\}^{cn}$, where c is an integer greater than 1, is a (t, ϵ)-PRNG, then g is also a $(t', \epsilon/(1 - 2^{-n(c-1)})$-one-way function for some t' close to t.

Problem 2 (10 pts) We say that a symmetric cipher has the ciphertext-uniform property if and only if for any probabilistic distribution of the plaintext, the distribution of the ciphertext is uniform over the ciphertext space.

a Prove that any cipher that has the ciphertext-uniform property also has perfect secrecy.

b Is ciphertext-uniform necessary for perfect secrecy? If your answer is yes, give a proof. If your answer is no, give a counter example.