Foundations of Cryptography

Homework Set No. 1

Date Due: Nov 13th 2003

1. If $f : \{0,1\}^n \mapsto \{0,1\}^n$ is one-to-one as well as a one-way function then it is a called a *one-way permutation.* In what complexity class does the problem of inverting one-way permutations reside?

Recall that we showed that the problem of of inverting one-way functions is in NP.

2. If $f : \{0,1\}^n \mapsto \{0,1\}^n$ is a one-way function, is f_L where $f_L(x)$ consists of the first half of the bits of $f(x)$ necessarily a one-way function?

3. If f is a one way function is $g(x) = f(f(x))$ necessarily a one-way function?