Foundations of Cryptography

Homework Set No. 2

Date Due: Nov 20th 2003

1. Show that if the subset sum assumption holds, then the subset sum function is one-way. (Note the definition of the assumption is the lecture slides).

2. Show that the hardest case of subset sum is when $n = m$ I.e. If there is any function g such that for $m = g(n)$ the $(n, g(n))$-subset sum assumption holds, then the (n, n)-subset sum assumption holds.

3. Show a function f such that

- If f is polynomial time invertible (on all instances), then $P = NP$.
- But f is *not* one-way.

4. Show that if strong one-way functions exist, then there exists a a function which is a weak one-way function but not a strong one.