Foundations of Cryptography

Homework Set No. 3

Date Due: Nov 27th 2003

1. Show that if probabilistic one-way functions exist on then so do deterministic ones. Probabilistic one-way functions are functions that are hard to invert and there exists a probabilistic machine operating in polynomial time that on any input computes the function correctly with probability at least 2/3.

What happens if the latter probability of success is $1/poly(n)$?

2. Suppose that $N = P \cdot Q$. Show how to use a routine that given N and y can find x such that $x^2 = y \bmod N$ in order to factor. What happens to the probability of success and running time?