Foundations of Cryptography

Homework Set No. 2

Date Due: Nov 29th 2006

1. 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. Show that if probabilistic one-way functions exist, then so do deterministic ones.

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?

3. Many-time probabilistic authentication: a) Suggest a definition to the k-time authentication problem b)Suggest a solution to the problem.

4. Suppose that in the many-time identification problem there is a bound on the number of sessions Eve can listen. suggest formulation of the problem and a solution.

5. Show, under reasonable assumptions (e.g. one-way functions exist) that there is a function f that is (i) one-way on its iterates (ii) Given x it is easy to x' such that $f(x) = f(x')$ and it is easy to invert f on x'.