Homework 25

Austin Frownfelter Matthew Bialecki

March 23, 2018

1 Problem 44

1.1 Part a

Assume there exists a function f that runs in polynomial time n^k for some $k > 0$.

Construct a g such that it takes as input $x' = (x, 0^{|x|^k})$ and runs f on input x. g will run f in time $\leq |x|^k$, which is run in time $\leq |x'|$

1.2 Part b

Proof by contrapositive.

Assume there exists an A such that A inverts f_u quickly, then there must exist an algorithm B that inverts f quickly by using A to guess the inverse of f. Thus, if f_u is not one-way, then there do not exist one-way functions f. Therefore, if there exist one-way functions, then f_u is one-way.

2 Problem 45

2.1 Part a

Proof by contrapositive.

If an algorithm can guess a bit of x with probability greater than $\frac{1}{2}$ + negligible, then it is not computationally secure. In addition, the algorithm would guess a bit of x where x is a string of random bits, such that the probability is greater than just guessing. Thus, if an algorithm is not computationally secure, it is not semantically secure. Therefore, if an algorithm is semantically secure, it is also computationally secure.

2.2 Part b

When B uses A($E_u(0^m)$), the result (an xor of 0's with random bits) is still random. B is still in the random distribution of X_n, which means A is not able to guess better than it. Thus, the result is semantically secure.

2.3 Part c

Since we may know the distribution of the mapping (to 0 or 1), we can guess what the message was. However, we do not know which message maps to which output. Thus, we can do no better than guessing with uniform probability.