CS 601.442/642 – Modern Cryptography	Instructor: Abhishek Jain

Homework 1

Deadline: September 24; 2017, 11:59 PM

1 Negligible and Noticeable Functions

1. (5 Points) Prove that $2^{-\omega(\log(n))}$ is a negligible function.
2. (10 Points) If f and g are both negligible functions, then prove or disprove that f/g is a noticeable function. (Note: for disproving a claim, it suffices to show an example.)
3. (10 Points) In cryptography, the security of a system (adversary's probability of breaking the system) is expressed in terms of a *security parameter*. The length of the input of a cryptographic algorithm is also a function of the security parameter.

   Let f be a strong one-way function and let n be the security parameter that determines the length of the inputs to f. Consider a simple adversary A that tries to invert f by guessing exactly once. Is the probability that A inverts f, negligible in n, when:

   (a) $f : \{0,1\}^{\log(n)} \to \{0,1\}^n$

   (b) $f : \{0,1\}^n \to \{0,1\}^n$

   Explain your answer.

2 One-Way Functions

1. Let $f : \{0,1\}^n \to \{0,1\}^n$ be any one-way function. Prove (via reduction) or disprove (by building an efficient inverter) each of the following statements.

   (a) (10 Points) Let $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be s.t. for every $x_1||x_2 \in \{0,1\}^{2n}$, $|x_1| = |x_2|$, $f'(x_1||x_2) = f(x_1)||x_2$. Then f' is also a one-way function.

   (b) (10 Points) Let $f' : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be s.t. for every $x_1||x_2 \in \{0,1\}^{2n}$, $|x_1| = |x_2|$, $f'(x_1||x_2) = f(x_1) \oplus x_2$. Then f' is also a one-way function.

2. For any one-way functions f_1 and f_2 with the same domains and codomains, define:

$$f(x_1||x_2) = f_1(x_1) \oplus f_2(x_2)$$

   (a) (10 Points) Let $g : \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Define $f_1(x_1||x_2) = g(x_1)||(x_1 \oplus x_2)||0^{2n}$ and $f_2(x_1||x_2) = (x_1 \oplus x_2)||g(x_1)||0^{2n}$. It can be proven that f_1 and f_2 are also one-way functions.

   Given the above description of one-way functions f_1 and f_2, prove that f (as defined above) is also a one-way function.

   (b) (15 Points) Construct f_1 and f_2 such that if they are one-way functions, then f (as defined above) is also a one-way function.