CS 435: Introduction to Cryptography **Fall 2016-17**

Homework 2

Professor Somesh Jha **Due:** October 9

1. Consider an encryption scheme, where the plaintext and ciphertext are n-bit strings. The key generation algorithm works as follows: generate a $\frac{n}{2}$-bit random string s (assume n is even) and the key is $k = s\|s$ (where $\|$ is concatenation). Encryption and decryption work exactly as one-time pad $c = m \oplus k$ and $m = c \oplus k$.

   a) Can this scheme be perfectly secret?

   b) What is the probability of an adversary winning the indistinguishability game?

2. Let f and g be negligible functions and p be any positive polynomial.

   a) Prove that the function $p(n) \cdot f(n)$ is a negligible function.

   b) Prove that $\frac{1}{\left(\frac{1}{f(n)}+\frac{1}{g(n)}\right)}$ is a negligible function.

3. Let G_0, G_1 be two different pseudorandom generators where $|G_0(s)| = |G_1(s)|$.

   Prove that no efficient distinguisher can detect wheter it is given a pseudorandom string output by G_0 or a pseudorandom string output by G_1.

   In other words, prove that, for any PPT algorithm D, there is a negligible function negl such that

$$\left|\Pr[D(G_0(s)) = 1] - \Pr[D(G_1(s)) = 1]\right| \leq \mathsf{negl}(n)$$

   where both probabilities are taken over uniform choice of $s \in \{0,1\}^n$ and the randomness of D.

   [**Hint**: Use triangle inequality "$|x + y| \leq |x| + |y|$ for any real numbers $x, y \in \mathbb{R}$".]

4. **(3.6)** Let G be a pseudorandom generator where $|G(s)| > 2|s|$. If G' is defined as follows, State and Justify whether they are necessarily pseudorandom generator or not?

   a) Define $G'(s) = G(s_1 \cdots s_{n/2})$, where $s = s_1 \cdots s_n$.

   b) Define $G'(s) = G(s||1^{|s|})$.

   c) Define $G'(s) = G(\overline{s})$, where $\overline{s}$ is the bitwise complement of s