CS 435: Introduction to Cryptography **Spring 2020**

Homework 2

Professor Somesh Jha **Due:** Feb 26 (Midnight)

1. Exercise 2.4 from the textbook.
2. Prove Theorem 2.9 using definition II (equation (2.1) in the textbook).
3. Consider a scheme OTP$'$ = $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where $\mathcal{K} = \{0,1\}^{\ell}$, $\mathcal{M} = \{0,1\}^{2\ell}$ and $\mathcal{C} = \{0,1\}^{2\ell}$. Gen generates a random ℓ-bit string as a key, $\mathsf{Enc}_k(m) = kk^R \oplus m$ (where k^R is the reverse of ℓ-bit string k) and $\mathsf{Dec}_k(c) = kk^R \oplus c$.

   Does the scheme work? Prove using definition III (indistinguishability game) that this scheme is not perfectly secret.
4. Let $f(n)$ be a negligible function and k a positive integer. Prove the following:
   (a) $f(\sqrt{n})$ is negligible.
   (b) $f(\frac{n}{k})$ is negligible.
   (c) $f(n^{1/k})$ is negligible.