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

Quiz 1

Professor Somesh Jha Oct 16, 2020 (Friday)

Instructions: Please follow the instructions given below.

- (Step 1): Write your name and student-id on the answer sheet.
- (Step 2): Make sure you number each of the sheets.
- If you do not follow the instructions given above, you will automatically lose *10 points*.

1. (20 points) Determine whether the following functions are negligible or not.
Part A (5 points) : $2^{-k\log(n)}$, where k is a positive integer
Part B (10 points) : $\frac{1}{n^{50}+n^3} - 2^{-\sqrt{n}}$
Part C (5 points) : $\frac{1}{2^{n^{\frac{1}{3}}}(n^3+n^7)}$

2. (25 points) Let s be a n-bit seed and $G(s)$ be a PRG such that output of G is $2n$-bits when given a n-bit seed (e.g. $l(n) = 2n$). Consider a function F defined as follows: $F(s) = s \cdot G(s)$ (recall that $\cdot$ denotes concatenation of two bit strings).. What is the expansion factor of F? Is F a PRG? Use the two-world argument to justify your answer.

3. (30 points) Let $S = \{r_1, \cdots, r_m$ be a set of m distinct n-bit strings (m is a constant with no dependence on n). Assume you pick a random n-bit string r and E is the event that $r \in S$. Prove that $P(E)$ is a negligible function of n. Assume that you repeat this experiment independently $p(n)$ ($p(n)$ is a polynomial in n). Can you upper bound the probability that in one of these trials the event happens? Is this probability negligible?
Hint: In the second part of the question the following inequality might be helpful.

$$P(E_1 \vee E_2 \vee \cdots \vee E_j) \leq \sum_{i=1}^{j} P(E_i)$$

In the equation given above $\vee$ is the "or" (this inequality is called the union bound).

4. (25 points) Describe the indistinguishability game where power of the adversary is restricted to probabilistic polynomial time (PPT) and is allowed the probability of winning the game "slightly" more than half? Clearly mark in the game where the two relaxations happen.