STUDENT ID: 159-26-5358
STUDENT NAME: Zaphod Beeblebrox

Problem 1.
Your friend shows you an algorithm INV that can invert a given function f in PPT, but only for those f(x) where the first 20 high-order bits of x are all 1's. However, if the first 20 bits are not all 1's, you assume that for any PPT adversary A, the probability that A inverts F becomes negligible as the length of the input increases. Could f be a one-way function? (Prove your answer). If not, is there a way to use f as a building block to build a one-way function? If so, show how to do it and prove your answer; if not, show a counterexample.

Problem 2.
Let $f(*)$ be any one-way function. Define $f_k(*)$ to be the function that applies f sequentially k times. For any k, give an example of a function f, such that $f_k(x)$ is a one-way function, but $f_{k+1}(x)$ is not a one-way function.

[**Hint:** you can assume that g is a one-way permutation, and construct $f_k(*)$ using g.]

Problem 3.
Explain the similarities and the differences between ZK proofs and ZK arguments, and give formal definitions for both.

Problem 4. Let $f(x_1, \dots, x_n)$ be a multivariate polynomial over a finite field $\mathbb{F}$ of the total degree d. In the **sumcheck protocol**, a prover $\mathcal{P}$ claims that $\mathbf{S = \Sigma_{x \in \{0,1\}^n} f(x)}$ equals to some value **S***.

1. Outline the steps of the sumcheck protocol between the prover and verifier.
2. Explain how the verifier's final check ensures soundness.
3. Why is it crucial that f has low total degree? What goes wrong if f has degree $> d$?

Problem 5. Consider a zero-knowledge proof for the statement: "A given graph G is 3-colorable." Would this protocol be *perfect*, *statistical*, or *computational* zero-knowledge? Briefly justify your answer.

Problem 6. Consider a secure pseudo-random generator (PRG) G that maps n-bit seed s to $2n$-bit output $G(s)$. Define $LH(*)$ to be a function that takes as an input $2n$ bits, and outputs the first half of its input bits. Define $RH(*)$ similarly (for the right half). Define:

$$F(s) = G(LH(G(s))G(RH(G(s))$$

1. What is the output length of F?
2. If G is a secure PRG, is F a secure PRG? Either show a counter-example or prove it.