1. (5 points) In the definition of strong one-way functions, for any adversary $A$, we defined the following inversion probability to be small:

$$\Pr \left[ x \leftarrow \{0, 1\}^n, y \leftarrow f(x) : f(A(1^n, y)) = y \right]$$

What if we used the following alternate definition instead?

$$\Pr \left[ x \leftarrow \{0, 1\}^n, y \leftarrow f(x) : f(A(y)) = y \right]$$

Provide a function that satisfies this definition trivially but can be easily inverted.

2. (5 + 5 points) Formally define negligible and not-negligible functions.

3. (5 + 10 points) Assuming “Hardness of Factorization problem,” construct a weak one-way function $f$. Provide the construction of $f$ and the proof that an adversary that breaks $f$ can be used to solve the factorization problem.

4. (5 + 15 points) Given a weak one-way function $f$, construct a strong one-way function $g$. Provide the construction for $g$ and its security proof.

5. (Extra Credit Problem) Define a function $f^*$ such that, if there exists a one-way function, then $f^*$ is a one-way function.

6. (Extra Credit Problem) Read and outline the following:
   (a) Definition of “Distributionally one-way functions,”
   (b) Definition of “Uniform Generation Problem for NP,” and
   (c) The difference between these two problems.