CS 601.442/642 – Modern Cryptography Instructors: Aditya Hegde and Harry Eldridge

Homework 2

Deadline: February 5; 2026, 11:59pm ET

Instructions

- The solutions must be submitted via Canvas.
- You must typeset your solutions. We suggest using LaTeX or Typst.

Problems

1. (50 points) For each function $g(\lambda)$ below, prove or disprove if $g(\lambda)$ is negligible.
   (a) (25 points) Let $f(\lambda) \in \omega(\log \lambda)$ and $g(\lambda) = 2^{-f(\lambda)}$.
   (b) (25 points)
   $$g(\lambda) = \begin{cases} \lambda^{-100} & \text{if } \lambda \text{ is even} \\ 2^{-\lambda} & \text{otherwise} \end{cases}.$$
2. (50 points) Recall that two ensembles $X = \{X_i\}_{i \in \mathbb{N}}$ and $Y = \{Y_i\}_{i \in \mathbb{N}}$ are computationally indistinguishable, denoted by $X \overset{c}{\approx} Y$, if for all non-uniform PPT adversaries $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that for all $\lambda \in \mathbb{N}$,
   $$\left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 1\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 1\right]\right| \leq \nu(\lambda),$$
   where the probability is over the choice of x, y and randomness of $\mathcal{A}$.
   (a) (25 points) Show that if $X \overset{c}{\approx} Y$ then for all non-uniform PPT adversaries $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that for all $\lambda \in \mathbb{N}$,
   $$\left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 0\right]\right| \leq \nu(\lambda),$$
   where the probability is over the choice of x, y and randomness of $\mathcal{A}$.
   (b) (25 points) Let $X \overset{c}{\approx} Y$. What is the maximum value of
   $$\left|\Pr_{x \leftarrow X_\lambda}\left[\mathcal{A}(1^\lambda, x) = 0\right] - \Pr_{y \leftarrow Y_\lambda}\left[\mathcal{A}(1^\lambda, y) = 1\right]\right|$$
   for any non-uniform PPT adversary $\mathcal{A}$?