CS 171: Problem Set 2

Due Date: February 8th, 2024 at 8:59pm via Gradescope

1. Negligible/Non-negligible functions

Let $f, g : \mathbb{N} \to \mathbb{R}$ be negligible functions, let $p : \mathbb{N} \to \mathbb{R}$ be a polynomial such that $p(n) > 0$ for all $n \in \mathbb{N}$.

(a) Define $h : \mathbb{N} \to \mathbb{R}$ as $h(n) = f(n) + g(n)$. Prove that h is a negligible function.

(b) Define $h : \mathbb{N} \to \mathbb{R}$ as $h(n) = f(n) \cdot p(n)$. Prove that h is a negligible function.

For each function below, either prove that it is negligible or prove that it is non-negligible (all logarithms are base 2).

(c) $f(n) = n^{-100} + 2^{-n}$

(d) $f(n) = 1.01^{-n}$

(e) $f(n) = 2^{-(\log n)^2}$

(f) $f(n) = e^{-\log^3 n} + e^{-\log^2 n} + e^{-\log n}$

2. 2-time security?

An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is said to be 2-time perfectly secure if for any $(m_1, m_2) \in \mathcal{M} \times \mathcal{M}$ and $(m_1', m_2') \in \mathcal{M} \times \mathcal{M}$ such that $m_1 \neq m_2$ and $m_1' \neq m_2'$ and for any $c_1, c_2 \in \mathcal{C}$ the following holds:

$$\Pr[\mathsf{Enc}(K, m_1) = c_1 \wedge \mathsf{Enc}(K, m_2) = c_2] = \Pr[\mathsf{Enc}(K, m_1') = c_1 \wedge \mathsf{Enc}(K, m_2') = c_2].$$

Note that in the above definition the key K is the same for encrypting m_1, m_2 (resp. m_1', m_2'). Consider the following encryption scheme for the message space $\mathbb{Z}_{23}$.

- Gen: Sample two elements $a \xleftarrow{\$} \mathbb{Z}_{23}$ and $b \xleftarrow{\$} \mathbb{Z}_{23}$.
- $\mathsf{Enc}((a, b), m)$: Output $c = a \cdot m + b \mod 23$.
- $\mathsf{Dec}((a, b), c)$: Compute $m = (c - b) \cdot a^{-1} \mod 23$ if a is invertible. Otherwise, output error.

Show the following.

1. Prove that for any message $m \in \mathbb{Z}_{23}$,

$$\Pr[\mathsf{Dec}(K, \mathsf{Enc}(K, m)) = m] = \frac{22}{23}$$

2. Prove that this is 2-time secure.

3. Getting Adversarial

Alice the Frog is very excited to share her new encryption scheme with you. You are responsible for convincing her it is insecure. The objective of this question is to familiarize you with the security framework of computational indistinguishibility. Download the `zip` file at `eecs171.com/assets/homework/hw2.zip`. Fill in the `TODO`s and upload your completed `scheme2.py` and `adversary.py` to Gradescope. You are provided with 5 files:

- `scheme1.py` specifies Alice's encryption scheme. Do not change this code.
- `scheme2.py` is where you should write the decryption scheme corresponding to the encryption scheme in `scheme1.py`.
- `correctness.py` provides you with a basic sanity test to confirm that the decryption scheme you wrote successfully recovers a plaintext encrypted with Alice's encryption scheme. Typically, we require that correctness is enforced for every message, but here, we are only checking for random messages.
- `security.py` contains the computational indistinguishibility security game which invokes the adversary. Typically, we require that the adversary succeeds with probability only non-negligibly better than 1/2, but here, we are checking that the adversary succeeds with probability 1.
- `adversary.py` is where you will write the adversarial code which is invoked by `security.py` in the security game. As shown in the skeleton code, note that the adversary is called twice.

Note: When making your submission, highlight both files and compress them directly, rather than zipping a folder containing the files.