# 6.5610 Recitation 4 Practice Problems

Katherine Zhao

March 1, 2024

# Practice Problems

Let $\mu : \mathbb{N} \to \mathbb{R}$ be a negligible function, and let $p$ be a polynomial such that $p(k) \geq 0$ for all $k > 0$. State whether the following functions are negligible:

# Practice Problems

Let $\mu : \mathbb{N} \to \mathbb{R}$ be a negligible function, and let $p$ be a polynomial such that $p(k) \geq 0$ for all $k > 0$. State whether the following functions are negligible:

- $c\mu(k)$ where $c > 0$ is a constant

# Practice Problems

Let $\mu : \mathbb{N} \to \mathbb{R}$ be a negligible function, and let $p$ be a polynomial such that $p(k) \geq 0$ for all $k > 0$. State whether the following functions are negligible:

- $c\mu(k)$ where $c > 0$ is a constant
- $\mu(p(k))$

# Practice Problems

Let $F$ be a PRF. Which of the following schemes are CPA secure encryption schemes?

# Practice Problems

Let $F$ be a PRF. Which of the following schemes are CPA secure encryption schemes?

- $\text{Enc}(k, (m_1, m_2)) = (r_1, r_2, F(k, r_1) \oplus m_1, F(k, r_2) \oplus m_2)$ where $r_1, r_2$ are random

# Practice Problems

Let $F$ be a PRF. Which of the following schemes are CPA secure encryption schemes?

- $\text{Enc}(k, (m_1, m_2)) = (r_1, r_2, F(k, r_1) \oplus m_1, F(k, r_2) \oplus m_2)$ where $r_1, r_2$ are random
- $\text{Enc}(k, m) = (r, F(k, m) \oplus r)$

# Practice Problems

Give a PIR scheme where we have $O(N)$ bits for request and $O(\lambda)$ bits for response.