Problem 1: Random oracle model

Write down the definition of IND-CPA security in the random oracle model (for symmetric encryption schemes).

Solution. This can be specified textually or as a picture:

**Definition 1 (IND-CPA in the random oracle model)** An encryption scheme $(KG, E, D)$ consisting of a key-generation algorithm $KG$, an encryption algorithm $E$, and a decryption algorithm $D$ is IND-CPA in the random oracle model if for any polynomial-time algorithm $A$ there is a negligible function $\mu$, such that for all $\eta \in \mathbb{N}$ we have that

$$\left| \Pr[b' = b : H \xleftarrow{\$} \text{Fun}_M \to \mathbb{N}, k \xleftarrow{\$} KG^H(1^\eta), b \xleftarrow{\$} \{0, 1\}, (m_0, m_1) \xleftarrow{\$} A^{H,E^H(k, \cdot)}(1^\eta), c \xleftarrow{\$} E^H(k, m_b), b' \xleftarrow{\$} A^{H,E^H(k, \cdot)}(1^\eta, c)] - \frac{1}{2} \right| \leq \mu(\eta).$$

(Here we quantify only over algorithms $A$ that output $(m_0, m_1)$ with $|m_0| = |m_1|$.)

**Definition 2 (IND-CPA in the random oracle model)** An encryption scheme $(KG, E, D)$ is IND-CPA in the random oracle model if for any polynomial-time algorithm $A$ there is a negligible function $\mu$, such that for all $\eta \in \mathbb{N}$ we have that $|\Pr[b' = b] - \frac{1}{2}| \leq \mu(\eta)$ in the game in Figure 1.

(Here we quantify only over algorithms $A$ that output $(m_0, m_1)$ with $|m_0| = |m_1|$.)