

Exercise (Trivial restriction to IND-CPA adversary). *Prove that that any adversary \mathcal{A} against IND-CPA games*

$$\begin{array}{cc}
 \mathcal{G}_0 & \mathcal{G}_1 \\
 \left[\begin{array}{l} (\text{sk}, \text{pk}) \leftarrow \text{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\text{pk}) \\ c \leftarrow \text{Enc}_{\text{pk}}(m_0) \\ \text{return } \mathcal{A}(c) \end{array} \right. & \left[\begin{array}{l} (\text{sk}, \text{pk}) \leftarrow \text{Gen} \\ (m_0, m_1) \leftarrow \mathcal{A}(\text{pk}) \\ c \leftarrow \text{Enc}_{\text{pk}}(m_1) \\ \text{return } \mathcal{A}(c) \end{array} \right.
 \end{array}$$

can be converted to a new adversary \mathcal{B} against IND-CPA games that always outputs two different challenge messages $m_0 \neq m_1$ so that the advantage remains the same and the computational overhead is constant.

Solution.

Hint: Decompose probability wrt condition $m_0 = m_1$