MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

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

$\mathcal{G}_0$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)$
return $\mathcal{A}(c)$

$\mathcal{G}_1$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}$
$(m_0, m_1) \leftarrow \mathcal{A}(\mathsf{pk})$
$c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)$
return $\mathcal{A}(c)$

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 $m_0 = m_1$