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

Exercise (IND-CPA security ⇒ randomised encryption). *Upper bound the probability that a t-time adversary $\mathcal{A}$ can win the game*

$$\begin{array}{l}\mathcal{G}_0\\ \left[\begin{array}{l}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\ m \leftarrow \mathcal{A}(\mathsf{pk})\\ \textbf{\textit{return}}\ \mathsf{Enc}_{\mathsf{pk}}(m) = \mathsf{Enc}_{\mathsf{pk}}(m)\end{array}\right.\end{array}$$

under the assumption that the cryptosystem is (t,ε)-IND-CPA secure. What restrictions this result puts on the minimal size of the randomness space used for encrypting a message?

Solution. Hint: Given an adversary $\mathcal{A}$ construct an adversary $\mathcal{B}$ against IND-CPA games

$$\begin{array}{l}\mathcal{Q}_0\\ \left[\begin{array}{l}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\ (m_0,m_1) \leftarrow \mathcal{B}(\mathsf{pk})\\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)\\ \textbf{return}\ \mathcal{A}(c)\end{array}\right.\end{array}\qquad\qquad\begin{array}{l}\mathcal{Q}_1\\ \left[\begin{array}{l}(\mathsf{sk},\mathsf{pk}) \leftarrow \mathsf{Gen}\\ (m_0,m_1) \leftarrow \mathcal{B}(\mathsf{pk})\\ c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)\\ \textbf{return}\ \mathcal{A}(c)\end{array}\right.\end{array}$$

where $\mathcal{B}$ does a collision based decryption.