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

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

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

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

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

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

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