Solution of Exercisesheet 9

Exercise 9-1

Exercise 9-2

Exercise 9-3

(a) **To show:** Prove that regular CPA security implies λ-CPA security.
We do this by a reduction. We assume there is an efficient adversary $\mathcal{A}$ against the λ-CPA-security of Π. From this we construct our adversary $\mathcal{B}$ against the CPA-security of Π.

(b) **To show:** Prove that λ-CPA security implies normal CPA security
We do this by a reduction. We assume there is an efficient adversary $\mathcal{A}$ against the CPA-security of Π. From this we construct our adversary $\mathcal{B}$ against the λ-CPA-security of Π which invokes $\mathcal{A}$. $\mathcal{B}$ has to provide an encryption oracle for $\mathcal{A}$ To do this he forwards any message m $\mathcal{A}$ sends to his oracle to his own oracle and recieves the ciphertextvector C_b. He then forwards only the first ciphertext c_1 to $\mathcal{A}$.
$\mathcal{A}$ eventually outputs two messages $(\widetilde{m_0}, \widetilde{m_1})$, which $\mathcal{B}$ forwards to his challenger. From the recieved ciphertextvector C_b he again forwards only the first ciphertext to $\mathcal{A}$. Then $\mathcal{B}$ outputs the same bit b like $\mathcal{A}$ does.

Exercise 9-4