Problem 8): For a public key encryption scheme $\prod = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, we define **CPA** security according to the probability obtaining a secure result, as defined in the privacy experiment $\mathsf{PubK}^{\text{LR-cpa}}_{\mathcal{A},\prod}$. This experiment goes as follows

The LR-orcale experiment $\mathsf{PubK}^{\text{LR-cpa}}_{\mathcal{A},\prod}(n)$

1. *$\mathsf{Gen}(1^n)$ is run to obtain keys (pk, sk).*
2. *A uniform bit $b \in \{0, 1\}$ is chosen.*
3. *The adversary $\mathcal{A}$ is given input pk and oracle access to $\mathsf{LR}_{pk,b}(\cdot, \cdot)$.*
4. *The adversary $\mathcal{A}$ outputs a bit b'.*
5. *The adversary $\mathcal{A}$ is defined to be 1 if $b' = b$, and 0 otherwise. If $\mathsf{PubK}^{\text{LR-cpa}}_{\mathcal{A},\prod}(n) = 1$, we say that $\mathcal{A}$* **succeeds**.

Using this definition for the experiment $\mathsf{PubK}^{\text{LR-cpa}}_{\mathcal{A},\prod}$, we say that the encryption scheme $\prod$ is secure if the probability of $\mathcal{A}$ succeeding during $\mathsf{PubK}^{\text{LR-cpa}}_{\mathcal{A},\prod}$