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 $\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}$. This experiment goes as follows

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

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* $\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}(n) = 1$, *we say that* $\mathcal{A}$ **succeeds**.

Using this definition for the experiment $\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}$, we say that the encryption scheme $\prod$ is secure if the probability of $\mathcal{A}$ succeeding, $\Pr\left[\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}(n) = 1\right]$ satisfies the condition

$$\Pr\left[\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}\ (n) \tag{8.1}$$

where $\mathsf{negl}\ (n)$ is a function/value which is negligible on the order of n.

In detail, what we are seeking is indistinguishability of multiple encryptions. That is to say, if we have the plain-text of two different messages (*denote them* m_1 *and* m_2), which we encrypt using a public key (*denote it* pk), then an adversary $\mathcal{A}$ having access to the cipher-text of both messages ***and*** the public key should not be able to distinguish the cipher-text of the messages under any circumstances. Using pk, the encryption algorithm (*denoted* Enc_{pk}) generates cipher-text from messages m_1 and m_2. We use

$$\mathsf{Enc}_{pk}(m_1) \qquad \underline{\textbf{and}} \qquad \mathsf{Enc}_{pk}(m_2)$$

to denote the cipher-text generated for these messages, respectively.

We denote both the information (pk, $\mathsf{Enc}_{pk}(m_1)$, & $\mathsf{Enc}_{pk}(m_2)$) available/provided to the adversary $\mathcal{A}$ by

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) \tag{8.2}$$

furthermore, we also use this notating to represent the outcome of running PubK on $\mathcal{A}$. When $\mathcal{A}$ succeeds, then the expression in 8.2 yields the result

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) = 1 \tag{8.3}$$

The expression in 8.2 yields

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) = 0 \tag{8.4}$$

otherwise.

Since **CPA** security requires security over multiple encryptions using the same public key, we will formally define this security using ***two*** pairs of messages that are all being encrypted using the same public key. We denote the first pair of messages by $m_{1,0}$ and $m_{2,0}$. Similarly, the second pair of messages are denoted by $m_{1,1}$ and $m_{2,1}$. We now use the same notation as in 8.2 with these message pairs (*and their associated public key* ph) to represent the attack by $\mathcal{A}$. This gives

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right), \tag{8.2 a}$$

for the first message pair; and

$$\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right), \tag{8.2 b}$$

for the second message pair.

Before proceeding, we point out that we can equivalently use the expression from 8.3 in place of the $\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}(n) = 1$ term from 8.1. More clearly, we may formally write this equivalence as

$$\mathsf{PubK}^{\mathsf{LR\text{-}cpa}}_{\mathcal{A},\prod}(n) = 1 \qquad \longleftrightarrow \qquad \mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_1\right), \mathsf{Enc}_{pk}\left(m_2\right)\right) = 1$$

This allows us to write a version of 8.1 for both and . For the first message pair (*represented in*), this gives the result

$$\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right) = 1\right] \leq \frac{1}{2} + \mathsf{negl}_0\left(n\right), \tag{8.3}$$

where negl_0 represents the negligible function required to satisfy this expression as applied to this message pair (*we are making allowances in case the results in and use different* negl *functions*). Writing our expression for the second message pair In a similar fashion yields

$$\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right) = 1\right] \leq \frac{1}{2} + \mathsf{negl}_1\left(n\right) \tag{8.4}$$

where negl_1 represents the negligible function required to satisfy this expression as applied to this message pair just as before (*we will see later that any difference between these* negl *functions is inconsequential; however differentiating between the* negl *functions used in either case is required for mathematical rigor*).

To continue the equation in 8.4 is subtracted from the equation in 8.3, after which the result *difference* will be simplified, thereby allowing us to obtain the following expressions for the initial and then the simplified results

$$\Big\{\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right)=1\right]- \\ -\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right)=1\right]\Big\} \leq \left(\frac{1}{2}+\mathsf{negl}_0\left(n\right)\right)-\left(\frac{1}{2}+\mathsf{negl}_1 0\left(n\right)\right)$$

$$\Big\{\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right)=1\right]- \\ -\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right)=1\right]\Big\} \leq \mathsf{negl}_0\left(n\right)-\mathsf{negl}_1\left(n\right)$$

Taking the absolute value of this simplified expression allows us to obtain the result

$$\Big|\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right)=1\right]- \\ -\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right)=1\right]\Big| \leq \left|\mathsf{negl}_0\left(n\right)-\mathsf{negl}_1\left(n\right)\right| \tag{8.5}$$

Considering the right-hand-side of 8.5, we see that $\left|\mathsf{negl}_0\left(n\right)-\mathsf{negl}_1\left(n\right)\right|$ also negligible itself. Therefore, we may define another negligible function, of order n, that satisfies the relation

$$\left|\mathsf{negl}_0\left(n\right)-\mathsf{negl}_1\left(n\right)\right| = \mathsf{negl}\left(n\right),$$

where negl is another negligible function, of order n. Applying this to the expression in 8.5, we obtain the final result

$$\Big|\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,0}\right), \mathsf{Enc}_{pk}\left(m_{2,0}\right)\right)=1\right]- \\ -\Pr\left[\mathcal{A}\left(pk, \mathsf{Enc}_{pk}\left(m_{1,1}\right), \mathsf{Enc}_{pk}\left(m_{2,1}\right)\right)=1\right]\Big| \leq \mathsf{negl}\left(n\right) \tag{8.6}$$

which provides a formal definition for **CPA** security. In simple terms, the expression in 8.6 formally describes the requirement that a **CPA** secure encryption scheme be ***non-deterministic***. That is to say, the expression in 8.6 mathematical quantifies the requirement that the cipher-text generated by any **CPA** secure encryption scheme be indistinguishable for any arbitrary pair of messages. It is the arbitrary nature of the messages that give rise to the requirement for non-determinism because the result in 8.6 must hold when the messages are ***identical***. The only way for identical messages to be indistinguishably enciphered is for the encryption scheme used to encipher them to allow, with some non-zero probably, every possible message in the message space $\mathcal{M}$ to encrypted into any cipher-text in the cipher-text space, $\mathcal{C}$.

Now, we will define **CCA** security, again, in terms of an indistinguishability experiment. We will continue to denote the encryption scheme in question as $\prod = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$; however, we will denote the experiment by $\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\prod}$. We describe *this* experiment as follows

The CCA indistinguishability experiment $\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\prod}(n)$

1. $\mathsf{Gen}(1^n)$ *is run to obtain keys* (pk, sk).
2. *The adversary* $\mathcal{A}$ *is given* pk *and access to a* <u>*decryption*</u> *oracle*, $\mathsf{Dec}_{sk}(\cdot)$. *The adversary,* $\mathcal{A}$*, outputs a pair of messages,* m_0, m_1*, which have the same length.* (*The messages must must in the message space,* $\mathcal{M}$*, that is associated with* pk.)
3. *A uniform bit* $b \in \{0, 1\}$ *is chosen, and then a cipher-text* $c \leftarrow \mathsf{Enc}_{pk}(m_b)$ *is computed and given to* $\mathcal{A}$.
4. *The adversary* $\mathcal{A}$ *continues to interact with the decryption oracle, but* <u>*may not*</u> *request a decryption of* c *itself. Finally,* $\mathcal{A}$ *outputs a bit* b'.
5. *The output of the experiment is defined to be* 1 *if* $b' = b$ (*the adversary* $\mathcal{A}$ ***succeeds***), *and* 0 *otherwise.*

Similar to how we arrived at the expression in 8.1, this definition of $\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\prod}$ can be used to show that the encryption scheme $\prod$ is secure by requiring that the probability of $\mathcal{A}$ succeeding, $\Pr\left[\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\prod}(n) = 1\right]$ satisfiy the condition

$$\Pr\left[\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}\ (n) \tag{8.7}$$

Unfortunately, without serious modification, public key cryptograph is ***NOT*** secure under the **CCA** paradigm.