Task 1 — Public-Key Encryption

Let $PKE = (Kg, Enc, Dec)$ be a public-key encryption scheme with message space $M = \{0, 1\}$, i.e., $PKE$ can only encrypt one-bit messages. We want to use $PKE$ to encrypt longer messages – say $\ell$-bit long. To this end, we consider the construction $\overline{PKE} = (\overline{Kg}, \overline{Enc}, \overline{Dec})$ which encrypts $\ell$-bit messages bit-by-bit using $PKE$. More precisely, it behaves as follows. (Here, $M[i]$ denotes the $i$-th bit of a string $M$ and $v[i]$ the $i$-th component of a vector $v$.)

**Procedure $\overline{Kg}$:**

\[
\text{For } i = 1 \text{ to } \ell \text{ do } (SK_i, PK_i) \leftarrow Kg
\]

\[
PK \leftarrow [PK_1, \ldots, PK_n]
\]

\[
SK \leftarrow [SK_1, \ldots, SK_n]
\]

\[
\text{Return } (PK, SK)
\]

**Procedure $\overline{Enc}_{PK}(M)$:** // $M \in \{0, 1\}^{\ell}$

\[
\text{For } i = 1 \text{ to } \ell \text{ do } C[i] \leftarrow Enc_{PK_i}(M[i])
\]

\[
\text{Return } C
\]

**Procedure $\overline{Dec}_{SK}(C)$:**

\[
\text{For } i = 1 \text{ to } \ell \text{ do } M[i] \leftarrow Dec_{SK_i}(C[i])
\]

\[
\text{Return } M[1] \| \ldots \| M[\ell]
\]

In particular, ciphertexts $C$ for $\overline{PKE}$ are $\ell$-dimensional vectors whose components are ciphertexts for $PKE$.

a) [5 pts] Prove that $\overline{PKE}$ is not IND-CCA secure.

**Hint:** Give a concrete attack breaking IND-CCA-security.

b) [15 pts] Assume that $PKE$ is IND-CPA secure. Prove that $\overline{PKE}$ is also IND-CPA secure.

**Hint:** Proceed as follows:

- Formally describe a sequence of games $G_0, G_1, \ldots, G_\ell$ where the adversary $A$ asks a single query $(M_0, M_1)$ to the LR$_b$ oracle, for $M_0, M_1 \in \{0, 1\}^\ell$. For this query, Game $G_i$ returns $C$ such that

  \[
  C[j] \leftarrow Enc_{PK_i}(M_0[j])
  \]

  for all $i < j \leq \ell$, and

  \[
  C[j] \leftarrow Enc_{PK_i}(M_1[j])
  \]

  for all $1 \leq j \leq i$.

- Prove that $Adv_{\overline{PKE}}^{\text{ind-cca}}(A) = \Pr[G_0 \Rightarrow 1] - \Pr[G_\ell \Rightarrow 1]$.

- For all $1 \leq i \leq \ell$, prove that there exists an adversary $B_i$ such that

  \[
  Adv_{\overline{PKE}}^{\text{ind-cca}}(B_i) = \Pr[G_{i-1} \Rightarrow 1] - \Pr[G_i \Rightarrow 1].
  \]

- Conclude IND-CPA security of $\overline{PKE}$ from the above.