Exercise 1  
(12 points) 

1. Give the definitions of DL, CDH, DDH.
2.Give the definition of IND-CPA.
3. Give the definition of LR.
4. Develop \((a + b)^2 = \ldots\)

**Solution:**

1. Let \(G = (\langle g \rangle, *)\) be any finite cyclic group of prime order.
   
   Idea: it is hard for any adversary to produce \(x\) if he only knows \(g^x\).
   
   For any adversary \(A\),
   \[\text{Adv}^{DL}(A) = \Pr\left[ A(g^x) \rightarrow x \mid x, y \overset{R}{\leftarrow} [1, q]\right]\]
   is negligible.

2. For any adversary \(A\),
   \[\text{Adv}^{CDH}(A) = \Pr\left[ A(g^x, g^y) \rightarrow g^{xy} \mid x, y \overset{R}{\leftarrow} [1, q]\right]\]
   is negligible.

3. For any adversary \(A\),
   the advantage of \(A\)
   \[\text{Adv}^{DDH}(A) = \Pr\left[ A(g^x, g^y, g^z) \rightarrow 1 \mid x, y \overset{R}{\leftarrow} [1, q]\right] \]
   
   \[\text{Adv}^{DDH}(A) = \Pr\left[ A(g^x, g^y, g^z) \rightarrow 1 \mid x, y, r \overset{R}{\leftarrow} [1, q]\right] \]
   is negligible.

   This means that an adversary cannot extract a single bit of information on \(g^{xy}\) from \(g^x\) and \(g^y\).
4. Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $\text{IND}_{\text{CPA}}^b(\mathcal{A})$ be the following algorithm:

- Generate $(pk, sk) \overset{R}{\leftarrow} \mathcal{K}(\eta)$.
- $(s, m_0, m_1) \overset{R}{\leftarrow} \mathcal{A}_1(\eta, pk)$
- $b' \overset{R}{\leftarrow} \mathcal{A}_2(\eta, pk, s, \mathcal{E}(pk, m_b))$
- return $b'$.

Then, we define the advantage against the IND-CPA game by:

$$\text{Adv}_{\text{IND}_{\text{CPA}}}^b(\eta) = \Pr[b' \overset{R}{\leftarrow} \text{IND}_{\text{CPA}}^b(\mathcal{A}) : b' = 1] - \Pr[b' \overset{R}{\leftarrow} \text{IND}_{\text{CPA}}^0(\mathcal{A}) : b' = 1]$$

5. $LR(m_l, m_r, b) = \begin{cases} m_l & \text{if } b = 1 \\ m_r & \text{if } b = 0 \end{cases}$

Exercise 2

(6 points)

Prove that any deterministic symmetric encryption scheme is IND-CPA insecure.

Solution: Adversary can easily distinguish encryptions of different plaintexts from encryptions of identical plaintexts

- Adversary $A(E_k(LR(-, -), b))$
- Let $X, Y$ be distinct strings in plaintext space
- $C_1 \leftarrow E_k(LR(X, Y, b))$
- $C_2 \leftarrow E_k(LR(Y, Y, b))$
- If $C_1 = C_2$ then return 1 else return 0

The IND-CPA advantage of $A$ is 1

$$\Pr[\text{Exp}_{SE}^{\text{IND}-\text{CPA}-0}(A) = 1] = 0 - \Pr[\text{Exp}_{SE}^{\text{IND}-\text{CPA}-1}(A) = 1] = 1$$

Exercise 3

(12 points)

We define Square Diffie-Hellman (SCDH) by: On input $g, g^x$, and output: $g^{x^2}$.

Prove that SCDH $\iff$ CDH with two reductions:

1. SCDH $\Rightarrow$ CDH.
2. SCDH $\Leftarrow$ CDH.
Solution:

- **SCDH ⇐ CDH.**
  Given an adversary $A$ who can break CDH (On input $g, g^x, g^y$, computing $g^{xy}$). Then $A$ can break SCDH given $g, g^x, g^y$ as input of CDH.

- **SCDH ⇒ CDH.** Given an adversary $A$ who can break SCDH (On input $g, g^x$, computing $g^{x^2}$). Then $A$ can break CDH by the following way:
  Given $g, g^x, g^y$, can we compute $g^{xy}$. With $g^x$ and $g^y$ we get $\alpha_1 = g^{x^2}$ and $\alpha_2 = g^{y^2}$ using SCDH. Knowing $g^x$ and $g^y$ we can give to $A g^{x+y}$ to obtain $\beta = g^{(x+y)^2}$.
  We can obtain $g^{2xy}$ dividing $\beta$ by the product of $\alpha_1$ and $\alpha_2$. 