Exercise 1
(5 points) Give the Bayes formula and the definition of expectation.

Exercise 2
(10 points)
1. Give the definition of NM-CPA NM-CCA1 and NM-CCA2.
2. Justify unformally the implication relations between these three notions.

Exercise 3
(15 points) “Modifying El-Gamal”. We propose a modified version of El-Gamal encryption scheme. Consider the following scheme, where \( g_1, g_2 \) are two randomly-chosen generators in \( G \) a cyclic group:

\[
\begin{align*}
\text{KeyGen}(1^k): \\
x, y &\leftarrow Z_q; \\
h &= g_1^x g_2^y; \\
PK &= \langle g_1, g_2, h \rangle; \\
SK &= \langle x, y \rangle; \\
\text{output } (PK, SK);
\end{align*}
\]

\[
\begin{align*}
\text{E}(PK, m): \\
r &\leftarrow Z_q; \\
\text{output } \langle g_1^r, g_2^r, h^r \ast m \rangle;
\end{align*}
\]

\[
\begin{align*}
\text{D}(SK, u, v, e): \\
\text{output } \frac{e}{u^x v^y};
\end{align*}
\]

1. Correctness: Assuming an honest execution of the protocol, prove that \( \frac{e}{u^x v^y} = m \)
2. Prove that the modified scheme is semantically (IND-CPA) secure under the DDH assumption (Only the reduction as in exercises session).

Recall: DDH is given \((g, g^u, g^v, \alpha)\) guess whether \(\alpha\) is \(g^{uv}\) or \(g^r\) where \(r\) is a random value.

Hint: one can take \(g_1 = g\) and \(g_2 = g^u\).