Exercise 1
Prove that

\[
\text{ADV}^{\text{IND-XXX}}_{\text{S}, \text{A}}(\eta) = Pr[b' \xleftarrow{R} \text{IND}^{1}(A) : b' = 1] - Pr[b' \xleftarrow{R} \text{IND}^{0}(A) : b' = 1]
= 2Pr[b' \xleftarrow{R} \text{IND}^{b}(A) : b' = b] - 1
\]

Exercise 2
Prove that the encryption algorithm of an IND-XXX scheme must probabilistic, if it is stateless.

Exercise 3
Prove that \( DDH \leq CDH \leq DL \)

Exercise 4
Prove that under CDH assumption El-Gamal is OW-CPA.

Exercise 5
Prove that under DDH assumption El-Gamal is IND-CPA.