Exercise 1

Suppose we are given a cryptosystem (G, E, D). Assume an adversary develops an algorithm Alg running in time T that can take a ciphertext $E_K(x)$ for an m-bit plaintext x and compute the first bit of x. Describe an adversary that plays the game in the CPA security definition and uses Alg to try to distinguish the real and ideal case. Which advantage can you obtain by asking a single query to the oracle? In terms of the parameters (t, q, μ, ε), which parameter values does your adversary obtain? How would your result change if Alg cannot compute the first bit with certainty but can only guess it with probability $p > 1/2$?

Solution: Define the adversary A, who sends any plaintext x to the oracle, and keeps track of the first bit sent, b. It takes $E_K(x)$ and uses Alg to recover the first bit b' back. If the first bit returned by Alg matches: $b' = b$, then A will return real, and if it does not, it will return ideal. Using more queries would increase the chance of A confirming the suspicion of being in an ideal game, but a single query is all that needs to be considered in the question.

Now we compute the probabilities in order to find the advantage:

$$P(\text{Output "real"} \mid \text{ideal}) = P(b' = b \mid \text{ideal}).$$

$$P(\text{Output "real"} \mid \text{real}) = P(b' = b \mid \text{real}).$$

If the ideal oracle is in play, there is a 1 in 2 chance that it will flip the first bit from the real oracle (Assuming ciphertext distribution is uniform). If this happens, the adversary will immediately know the ideal oracle is in play. So $P(b' = b \mid \text{ideal}) = 0.5$

On the other hand, if the real oracle is in play, the adversary will have no reason to ever suspect the ideal oracle is in play, since the real oracle will always have the correct first bit when the adversary uses Alg. So we have $P(b' = b \mid \text{real}) = 1$.

All this to tell us the advantage:

$$Adv_A(O_{\text{real}}, O_{\text{ideal}}) = \left|\frac{1}{2} - 1\right| = \frac{1}{2}.$$

Through this attack we have the parameters:

$$\begin{aligned} t &= T \\ q &= 1 \\ \mu &= m \\ \varepsilon &= \frac{1}{2}. \end{aligned}$$

Since we are limited to 1 query, and all the parameters are given by Alg.

Now, if Alg guesses the first bit correctly with some probability $p > \frac{1}{2}$, then the probability $P(b' = b \mid \text{ideal}) = \frac{1}{2}$ by the same assumption of uniform plaintexts.

In the real case, the probability $P(b' = b \mid \text{real}) = p$, the probability of Alg returning the correct first bit. So we now have:

$$Adv_A(O_{\text{real}}, O_{\text{ideal}}) = \left|p - \frac{1}{2}\right| = p - \frac{1}{2}.$$

So our advantage is $\varepsilon = p - \frac{1}{2}$, and the other parameters remain unchanged.