Exercise 8.4

Task

An alternative definition to the one we give here for CPA security of public-key schemes goes as follows: from security parameter k the oracle generates a key pair (p_k, s_k) and gives the public key to the adversary A. The adversary chooses two plaintexts m_0, m_1 of the same length and sends them to the oracle. The oracle chooses a random bit b and sends $E_{pk}(m_b)$ to the adversary. Finally, the adversary outputs a bit b'. Let $p_A(k)$ be the probability that $b = b'$. We say the cryptosystem is secure if for all polynomial time adversaries it holds that $|\frac{1}{2} - p_A(k)|$ is negligible. The goal is to show that a cryptosystem is secure according to this definition if and only if it is secure according to the one from Definition 8.3. This is done by showing that if there is an adversary that breaks Definition 8.3, you can construct an adversary that breaks the alternative definition, and vice versa. For the first part, you are given A, who breaks Definition 8.3, and you must construct A' who uses A as subroutine, and breaks the alternative definition. Consider the following algorithm for A':

1. Get p_k from the oracle and give it to A.
2. A outputs a message m. A' now chooses a random message r of the same length as m, sets $(m_0, m_1) = (m, r)$ and sends the pair to the oracle.
3. The oracle returns a ciphertext $y = E_{pk}(m_b)$ for random bit b. Then A' gives y to A, who outputs a guess `real` or `ideal`.
4. If A said `real`, output $b' = 0$, else output $b' = 1$ (this makes sense because the m that A chose is the first message in the pair, and output `real` means that A thinks y contains m.) Now, show that if A has advantage ϵ, then $|\frac{1}{2} - pA'(k)| = \frac{\epsilon}{2}$.

You can start by using the fact that
$P[b = b'] = P[b = b'|b = 0] \times P[b = 0] + P[b = b'|b = 1] \times P[b = 1] = \frac{1}{2}(P[b = b'|b = 0] + P[b = b'|b = 1])$

Solution

Finish the case A → A'

Let's start by showing that $|\frac{1}{2} - pA'(k)| = \frac{\epsilon}{2}$ using $P[b = b']$.

$$P[b = b'] = P[b = b'|b = 0] \times P[b = 0] + P[b = b'|b = 1] \times P[b = 1] = \frac{1}{2}(P[b = b'|b = 0] + P[b = b'|b = 1]) =$$

$$\frac{1}{2}(P[b = b'|b = 0] + (1 - P[b \neq b'|b = 1])) = \frac{1}{2}(1 - P[b = b'|b = 0] - P[b \neq b'|b = 1]) = \frac{1}{2}(1 + \epsilon) = \frac{1}{2} + \frac{\epsilon}{2}$$

Now when we substitute in $|\frac{1}{2} - pA'(k)|$ we get $|\frac{1}{2} - \frac{1}{2} + \frac{\epsilon}{2}| = \epsilon$ and we're done.

A ← A'

For the second part we have to show that having access to A' we can construct A. The algorithm will be very similar:

1. The Oracle generates a private and public key (sk, pk) and gives the public key pk to A
2. A gives pk to A'
3. A' generates two messages - m_0, m_1 and gives them to A
4. A generates random bit $b \in 0, 1$
5. A sends m_b to the Oracle
6. The Oracle returns c_b = either $E(m_b)$ or $E(r)$ where r is a random message - real vs ideal world
7. We pass c_b to A', which outputs b'
8. If $b = b'$ we output that the oracle has used the `real` world, else, we say it's used the `ideal` world

$$Adv_A = |P[real|real] - P[real|ideal]| = |\frac{1}{2} + \epsilon - \frac{1}{2}| = \epsilon$$

Which shows that A' has the same advantage as A.