1. We compare a PRG and a PRF.
   PRG has input seed and output string0.
   PRF has input key, string1 and output string2.
   Some of these variables must be uniformly random, some are pseudorandom, and some have no particular distribution.

   Which ones must be uniformly random?  
   Which ones are pseudorandom? 

2. What does CPA-security mean.

3. The adversary \(\mathcal{A}\) in the CPA experiment has oracle access to the encryption function. What does this mean?

4. In the CPA encryption experiment the adversary \(\mathcal{A}\) has access to an encryption oracle before and after selecting his challenge messages \(m_0, m_1\). When he asks the oracle for the ciphertext message, after he has selected the challenge messages \(m_0, m_1\): must he exclude these two messages from the one he asks the oracle to encrypt for him? Justify your answer.