Exercise 1: Formulate a definition of perfect binding for string commitment. In addition, prove that the hiding for bit commitment implies hiding for string commitment, as defined in class. (Hint: use a hybrid argument to prove that the first definition implies the second.)

Exercise 2: Consider an experiment in which the adversary outputs two vectors of plaintexts of length $t(n)$. Then, $t(n)$ independently chosen keys are used to encrypt the challenge ciphertext; the $i^{th}$ plaintext in the chosen vector is encrypted with the $i^{th}$ key. Formally define security for an eavesdropping adversary (use the indistinguishability formalization). Does security for a single encryption imply security under this definition? Prove or refute in both the private-key and public-key settings.

Exercise 3: Prove that the “Encrypt-then-MAC” paradigm yields a private-key encryption scheme that is secure under CCA2-attacks. (Describe the construction formally, and prove that it is secure. Start from a private-key encryption scheme that is CPA-secure and a MAC, and construct a new encryption scheme that is CCA2-secure.)

Exercise 4: Prove that any secure signature scheme can be transformed into one that uses a deterministic signing algorithm. Hint: use pseudorandom functions in order to carry out the transformation.