Homework 2

1. Prove that the following modes of operation are CPA secure when used with a pseudorandom permutation:
    a. Counter Mode
    b. CBC
2. Solve the following exercises from chapter 3 of out textbook (first edition)
    a. 3.9
    b. 3.11
    c. 3.15
    d. 3.16
    e. 3.22
3. Encrypt the King James Bible using:
    a. AES in CBC mode of operation
    b. AES in Counter Mode of Operation
    c. DES in CBC Mode of Operation
    d. DES in Counter Mode of Operation
    e. 3DES in CBC Mode of Operation
    f. 3DES in Counter Mode of Operation

    You can use a cryptographic library for implementing AES, DES and 3DES and the modes of operation. For each of the six scenarios here specified, provide your code (copy and paste into a PDF file) and the times for encryption and decryption. For which of these modes of operation can you improve the running times by exploiting parallelization?