Homework 2

Due March 26

1. In case of modes operations, every mode requires the use of the initial vector(IV). IV should be new every time it encrypts the blocks of a file. In real life, how can we get the IV? List at least three possible ways of getting the IVs.

2. Consider the CBC mode. What if there is a communication error on one block of the ciphertext during transmission? Which impact does the error have on the following blocks of the ciphertext? Is it serious enough for us to consider?

3. Alice's RSA public key is (N,e) = (33,3) and her private key is d=7.

(a) If Bob encrypts the message M=19 for Alice, what is the ciphertext C?

(b) Show that Alice can decrypt C to obtain M.

(note: when you do exponential computation, use the fast exponential algorithm, i.e., square-and-multiply algorithm, not your calculator.)