1 Introduction to Cryptography: HW 2

1. Bellare-Rogaway Book: Problem 3.2

2. Bellare-Rogaway Book: Problem 3.5
(Hint: Let $X_1, \ldots, X_n$ be n independent 0-1 random variables such that $Pr(X_i = 1) = p$ then $Pr(X_1 \oplus X_2 \oplus \ldots \oplus X_n = 1) = \frac{1}{2}\left[1 - (1-2p)^n\right]$)

3. Bellare-Rogaway Book: Problem 3.6

4. Suppose sequence of plaintext blocks $M_1, M_2, \ldots, M_n$ are encrypted using a block cipher to produce ciphertext blocks $C_1, C_2, \ldots, C_n$. Suppose that one of the cipher text blocks (say C_i) sent incorrectly. Show that the number of plaintext blocks that will be decrypted incorrectly is equal to one for ECB mode; and equal to two in CBC mode.

5. Prove that one time pad encryption discussed in the class is perfectly secure.