Homework 2
Introduction to Information Security (266-642)
Due Date: Feb 26, 2003 (Wednesday)

Note: You can talk to your classmates, instructor, and TA about the problems. However, unless stated otherwise, problems should be written up individually. University of Wisconsin rules for academic misconduct apply.
In the homework, "the Stallings book" refers to [2] and "the Handbook" refers to [1] (I have linked the Handbook to the class homepage. You can download it for free.)

Question 1 (OFB mode, 20 points): The following two questions are on the *output feedback mode* (*OFB*).
Part A: Prove that the encrypt and decrypt stages of the OFB mode work correctly, i.e., one obtains the plaintext after decryption. First, prove this for the first stage. After that, prove it in general for the i-th stage.

Part B: Explain the following quote from the book:

One advantage of the OFB method is that bit errors in transmission do not propagate.

Question 2 (Meet-in-the-Middle attack 20 points): Assume that Oscar has three pairs (P, C), (P_1, C_1), and (P_2, C_2) of plain and cipher texts. Explain the meet-in-the-middle attack on 2DES in this context. Also compute the probability that Oscar succeeds, i.e., he finds the correct key pair used in 2DES.

Question 3 (SDES 30 points):
Part A: Problem 3.2 from the Stallings book.

Part B: Problem 3.3 from the Stallings book.

Question 4 (DES 30 points):
Part A: Problem 3.12 from the Stallings book.

Part B: Problem 3.13 from the Stallings book.

References

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

[2] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 1998.