# Homework 2
# Introduction to Information Security (266-642)
# Due Date: March 6, 2006 (Monday)

**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 (15 points):** Problem 3.2 from the Stallings book.

**Question 4 (15 points):** Suppose Triple DES is performed by choosing two keys $K_1, K_2$ and computing $E_{K_1}(E_{K_2}(E_{K_2}(m)))$ (note that the order of the keys has been modified from the usual two-key version in Triple DES). Show how to attack this modified version with a meet-in-the-middle attack.

**Question 5 (Block ciphers 30 points):**
**Part A:** Problem 3.13 from the Stallings book.

**Part B:** Problem 3.15 from the Stallings book.

**Question 6 (DES 15 points) [Extra credit]:** Find a key $K$ such that $DES_K(\cdot) = DES_K^{-1}(\cdot)$. Such a key is sometimes called a *weak* key. How many weak keys can you find? Why do you think they are called weak?

## 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, 2006.