

CSE 651 Homework 3

Due: **Friday, April 23** by class time (10:30 am)

Midterm Exam 1: Monday, April 26

Scope: up to RC4 inclusively

Open books/notes

Calculators allowed

1. Do Problem 6.4 of Stallings. (Interpret part b as follows: After encrypting the entire message, you find an error in the first block of the message. You correct the error and re-encrypt P_1 . How many other blocks do you need to re-encrypt? (You don't need to answer the second question of part b, "What is the effect at the receiver?")
2. Do Problem 6.8 on the 5th edition (6.5 on the 4th) of Stallings. If a bit transmission error occurs in a ciphertext character in 8-bit CFB mode, how far does the error propagate (i.e., how many plaintext characters are likely to be recovered incorrectly)? (Assume DES is used.)
3. Consider Problem 6.11 on the 5th edition (6.8 on the 4th) of Stallings. Assume that P_N is 1-byte long. The first $N - 2$ blocks are encrypted as in the CBC mode. P_{N-1} and P_N are encrypted as follows.

$$Y_{N-1} = E_K(C_{N-2} \oplus P_{N-1})$$

$$C_N = \text{leftmost-byte}(Y_{N-1})$$

$$C_{N-1} = E_K(Y_{N-1} \oplus (P_N \parallel 000\dots 0))$$

Show how to decrypt C_{N-1} and C_N .

4. Do Problem 7.8 on the 5th edition (6.10 on the 4th edition) of Stallings. (Hint: for what values of $T[0..255]$, will it hold $i = j$ in the loop of Initial Permutation so that $S[i]$ ends up swapping with itself? Determine the value of $T[0]$, then $T[1]$, $T[2]$, and so on.)