

## Homework Assignment #1B

### Note

This assignment is due 2:10PM Tuesday, November 1, 2016. Please write or type your answers on A4 (or similar size) paper. Drop your homework by the due time in Yih-Kuen Tsay's mail box on the first floor of Management Building 2. Late submission will be penalized by 20% for each working day overdue. You may discuss the problems with others, but copying answers is strictly forbidden.

### Problems

1. Solve the following exercise problems in Stallings' book (6th edition, international): 5.2 (10 points; for {02} instead of {01}), 5.4 (20 points; the key for the initial AddRoundKey equals the input key), 5.6 (10 points), 6.4 (10 points), 6.8 (10 points; consider the CFB mode with  $b = 128$  and  $s = 8$ ), 6.12 (10 points), 7.1 (10 points), 7.2 (10 points).
2. Consider pseudorandom number generation based on block ciphers and assume AES-128 is used as the encryption algorithm. What is the expected period of the bit stream with the OFB mode of operation? Please justify your answer. (10 points)