Homework Assignment #1B

Note

This assignment is due 2:20PM Tuesday, October 18, 2011. Please write or type your answers on A4 (or similar size) paper. Put your completed homework on the instructor's desk before the class starts. For late submissions, please drop them in Yih-Kuen Tsay's mail box on the first floor of Management Building II. 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 (5th edition): 5.1 (10 points), 5.4 (20 points), 5.6 (10 points), 6.4 (10 points), 6.7 (10 points), 6.11 (10 points), 6.12 (10 points).

2. Consider pseudorandom number generation based on block ciphers and assume AES-128 is used as the encryption algorithm. Prove that the period of the bit stream with the CTR mode of operation is 128×2^{128} bits long. (10 points)

3. Consider again pseudorandom number generation using AES-128. What is the expected period of the bit stream with the OFB mode of operation? Please justify your answer. (10 points)