Homework Assignment #1B

Note

This assignment is due 2:10PM Tuesday, October 16, 2012. 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 (5th edition): 4.17 (10 points), 5.1 (10 points), 5.2 (10 points), 5.4 (20 points), 5.6 (10 points), 6.4 (10 points), 6.7 (10 points).

2. Create a table similar to Table 4.10(b) (in Stallings' book) for $GF(2^4)$ with $m(x) = x^4 + x + 1$. (10 points)

3. 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)