MATH 3540 **Name:** ______________________
Day 4

Directions

1. Complete the following questions.

1. Prove that XOR is commutative.

2. What is the resulting ciphertext of encrypting the message 0xAF C0 4D using the one-time pad and key 0xC9 2B 39.

3. You observe three ciphertexts all resulting from encryption of ASCII plaintexts containing English letters and spaces only, using the one-time pad and the same key. The 10th byte of the first ciphertext is 0xA8, the 10th byte of the second ciphertext is 0xED, and the 10th byte of the third ciphertext is 0xBD. What is the 10th ASCII character of the third plaintext?

4. Which of the following are true for obtaining perfect secrecy using the one-time pad, assuming the message space contains messages all of some fixed length?

   (a) The key must be as least as long as the messages in the message space.

   (b) The all-0 key must be avoided, since when the all-0 key is used the ciphertext is equal to the message being encrypted.

   (c) The key should be chosen uniformly.