MATH 3540 **Name:** ____________________

Day 3

Directions

1. Complete the following questions.

1. Compute 1111 1010 $\bigoplus$ 1001 1101.

2. What is the result of encrypting the ASCII plaintext ”abc” using the byte-wise XOR shift cipher (where encryption is done using byte-wise XOR) and key 0x4B?

3. Consider the Vigenere cipher over the lowercase English alphabet, where the key can have length 1 or length 2, each with 50% probability. Say the distribution over plaintexts is Pr[M='aa'] = 0.3 and Pr[M='ab'] = 0.7.

   (a) What is Pr[C='bb']?

   (b) What is Pr[M='aa' ‖ C='bb']?

4. Prove that if a single character is encrypted, then the shift cipher is perfectly secret.