MATH 3540 **Name:** _____
Homework 2

Directions

1. Complete the following questions.

---

1. Consider the one-time pad over the message space of 6-bit strings, where Pr[M=001000] = 0.15 and Pr[M=110011] = 0.85. What is Pr[C=000000]?

2. An equivalent definition for the byte-wise XOR operator is given by the following: Suppose A and B sets then $A \bigoplus B = (\tilde{}A \cap B) \cup (A \cap \tilde{}B)$. Prove that XOR is associative: $(A \bigoplus B) \bigoplus C = A \bigoplus (B \bigoplus C)$ for all binary strings A,B, and C.

3. Prove or refute: Every encryption scheme for which the size of the key equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

4. Prove or refuse: the vigenere cipher is perfectly secrect when for all messages m in the message space and for all k in the key space we have $|m| = |k|$ and $|M| = |K|$.

5. Three ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key.

   (a) Suppose that the 10th byte of the first ciphertext is observed to be 0xB3 and the 10th byte of the second ciphertext is observed to be 0xE7. Let m1 (resp., m2) denote the 10th ASCII character in the first (resp., second) message. What can you conclude about m1, m2?

   (b) The 10th byte of the first ciphertext is observed to be 0x66, the 10th byte of the second ciphertext is observed to be 0x32, and the 10th byte of the third ciphertext is observed to be 0x23. Let m1 (resp., m2, m3) denote the 10th ASCII character in the first (resp., second, third) message. What can you conclude about m1, m2, and m3?