# 1ST MIDTERM, CS/ECE/MATH 435, MARCH 9, 2012

Nigel Boston

Answer all four questions below. Show your working. Full credit will not be given for just the answer without any justification. Make sure you answer each part of each question.

1. Are the following statements true or false? No justification is needed for your answers to this question.

(a) Hill ciphers acting on blocks of length two have perfect secrecy.

(b) When choosing a password, high entropy is desirable.

2. (a) Give the formal definition of cryptosystem.

(b) Give two examples of cryptosystem, one monoalphabetic, one polyalphabetic, showing how the definition in (a) fits in each case.

(c) Define the three kinds of attack on cryptosystems.

3. A message encrypted by an affine cipher reads: JHATAYJABIK.

(a) Use frequency analysis to guess the decryption of at least two of the above letters.

(b) Find the decryption and encryption functions.

(c) Decrypt the message.

4. The following message, encrypted by a Vigenere cipher, is received: GLCF DLCY YMLY OXQL YYEZ DLCL YYEZ QIRY YML

(a) Explain Kasiski's method and what it tells us about the above message.

(b) Given that the keyword is KEYS, decrypt the message.

(c) Why is frequency analysis misleading when trying to decrypt a Vigenere ciphertext? Use the above message to illustrate.

(d) The index of coincidence of the encrypted message is 0.109. What is the reason behind it being so high?

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX