**COMP 483/MATH 450 Homework 1**

**Due Wednesday, January 11**

The following are paper-and-pencil problems. Please do not use a computer when doing these problems. Calculators are okay. Show your work on all problems. You may submit your work on Moodle or on paper.

1. Problems 2.14, 2.15, 2.18, 2.20 from your textbook, with the following changes:
	1. In problem 2.14 (a), change the message to be encrypted to be “meet at five” instead of the longer message given in the text.
	2. If you aren’t familiar with matrix multiplication and inversion, please see me or go to the MPC to figure it out.
	3. In problem 2.18 (a), change the plaintext to be encrypted to be “sendcashquick” instead of the plaintext “sendmoremoney”.
2. **Instructions for this problem:** Make an attempt to break this cipher by hand. DO NOT spend hours and hours of your time on it! Turn in work that shows a sincere effort. If you do the optional programming problem, attempt to break the cipher with your program.

The following text has been encoded using an affine cipher. Attempt to break the cipher and find the encryption key. Show all your work, including guesses, errors, and dead ends. (This includes a frequency table if you make one, or part of one.) You do not need to finish deciphering the message if you are sure of your key. We will use “a” = 01 for this affine cipher.

QBVDL WXTEQ GXOKT NGZJQ GKXST RQLYR XJYGJ NALRX OTQLS LRKJQ FJYGJ NGXLK

QLYUZ GJSXQ GXSLQ XNQXL VXKOJ DVJNN BTKJZ BKPXU LYUNZ XLQXU JYQGX NTYQG

XKXQJ KXULK QJNQN LQBYL OLKKX SJYQG XNGLU XRSBN XOFUL YDSXU GJNSX DNVTY

RGXUG JNLEE SXLYU ESLYY XUQGX NSLTD GQXKB AVBKX JYYBR XYQNQ GXKXZ LNYBS

LRPBA VLQXK JLSOB FNGLE EXYXU LSBYD XWXKF SJQQS XZGJS XQGXF RLVXQ BMXXK

OTQKX VLJYX UQBZG JQXZL NG

Hint: to find the key, you may want to look at the ciphertext letters corresponding

 to the plaintext letters that are early in the alphabet, such as *a* and *e*.

1. There are at least two ways in practice to decrypt a “3x + 2” affine cipher: table lookup and subtract 2 and “divide” by 3 (mod 26). Give advantages and disadvantages of each from an implementation point of view. Extend your answer to a general “ax + b” affine cipher.