Math 3207 Assignment 2, early February 2016

Please show all working and reasoning to get full marks for any question. Hand in your rough working as well so I can see how you investigated and reached your final results. You can use Maple at any point and can email me any worksheets you created.

You are reminded that plagiarism is a serious offense and when it is detected you will be punished. Feel free to discuss the questions in general with myself and your colleagues but the work attempted must be yours alone. A maximum of $20 - p_y$ marks can be received for this assignment if you hand your work in y days after the deadline, where p_y is the y^{th} prime number.

1. Explain using algebra why any digraph ending in A using the standard alphabet ordering will necessarily end in the same letter no matter what multiplier is used for affine encoding, but this will not happen for any other letters. Find how many digraphs map to themselves under affine encoding with a general multiplier a and shift b and under what conditions a matrix encoding can have a digraph which maps to itself. Give a non-trivial matrix M which has this property and find all digraphs such that M maps the digraph to itself. [6]

2. You have received the segment of text selected in class. Given that it is a palindrome (a sequence of letters that reads the same backwards as forwards) encoded using the affine digraph method:

   (a) Determine the affine multiplier using the fact that it is a palindrome of odd length and the given second letter of the plain text. [3]

   (b) Using what "JA" encodes to, find the affine shift and thus the decoding parameters. Manually apply them to find the first 6 letters of your text. If part (a) defeats you, let me know and I can supply what "ME" encodes to and then you can proceed, having lost some marks. [6]

3. Let the last 3 digits of your registration number be r, s and t. Find the solution of $x \equiv r \pmod{14}$, $x \equiv s \pmod{15}$ and $x \equiv t \pmod{17}$ using the Chinese Remainder Theorem. Give examples which show all the essentially different ways that the CRT can have different types of solutions modulo mn if m and n are not relatively prime. [5]

```
L "cjsrxsnr,rcsfr,joz" JA -> " df"

O "qapmxaqbqaimbaqd"  JA -> "al"

O "erxvk.ovcr. " JA -> "tv"

N "wvridwgnqweitvhp" JA -> "m."

E "yzpxxsdspxxzvk" JA -> "re"

A "qscageiars i" JA -> "hs"

I "nucv.wqwvvzubb" JA -> "lw"

A "utdtdsbeyevsutdtix" JA -> "yt"

A "xzipfzwzop,zbh" JA -> "dz"

O ",cbnmpmpjnqcwm" JA -> "ba"
```