MTH6115 Cryptography

Assignment 2 For handing in on 31st January 2011

Your solutions to Questions 1 (a), 5 and 7 should be handed in to the ORANGE box on the GROUND floor by 3:30 pm on Monday 31st January 2011.

Remember: *The work you hand in should be your OWN work. If you work in groups make sure you YOURSELF understand the answers that have been obtained, and write up your answers YOURSELF. I take a dim view of copied answers, and will penalise them severely when I detect them.*

1 Solve the following affine substitution ciphers:

(a) RNRERMW RERZRER WMRERNR; and

(b) QXNUX MTFQFJJ TUMHW HJMUT STGAGTS TUMJH WHMUT JJFQFTM XUNXQ.

(Hint: The correct spacing for these is R NRE R MWRE R ZRERW MRERNR and QXN UXMT F QFJJTUM H WHJM ..., but try the ciphers without this knowledge first.)

2 Alice has (mis-)encrypted a piece of text using the affine map $\theta_{4,1} : x \mapsto 4x + 1$ (applied to the standard English alphabet). She sent the following to Bob.

```
HZRRB TTTNF RVDRT JFFFH VTFDB THJRJ BBXBP RDRRV DFVZH ZDZHF
BJHJD RRHBL RJZHH RFZDR RLHVR DRLHT TDBHR HXXRB VRNHV VHJDT
ZTNRJ HJDRR HBZXR VVBZR VRBJR TJZRN DVHBZ HZ
```

Attempt to help Bob to uncover the original message. Did you succeed? If not, how far did you get, and what was the sticking point?

3 Let V_m denote a Vigenère cipher (with keyword) of length m on the alphabet $\mathscr{A}$ of size n. (Note that a V_d is also a V_m if $d \mid m$.)

(a) Prove that the composition of a V_4 and a V_6 is a Vigenère cipher, and determine the least m such that this composition is guaranteed to be a V_m.

(b) With m as in the previous part, how many V_m's are there?

(c) How distinct ciphers can be obtained by composing a V_4 and V_6? (I shall call this the *number of keys* of such a cipher, though arguably 'number of keys' could refer to a different concept.)

Repeat the question with V_a and V_b in place of V_4 and V_6, for arbitrary $a, b \geqslant 1$.

4 Calculate $\phi(n)$ for $n = 120$, 121, 122, 123, 124, 125, 126, 127 and 128.

5 Prove that $\mathrm{Aff}_1(\mathbb{Z}_n)$ [also known as $\mathrm{AGL}_1(\mathbb{Z}_n)$] is non-abelian whenever $n \geqslant 3$.

6 Decrypt the following Vigenère cipher.

```
VPTXYZESQY SNPNDENLOX HVZVTBWLPR BGSVKZUICL RXNQHOPRPO JHKVRICNVR
OBWHXZUIEO VRUMIOEKEW CAEZPAPSPF HBWLPVVBTY WFHBWLECRP PIIKKBWHWS
GMCBWVFBDA IJVBNWINTQ ILVJCVSJSD RCILVBGGQV EIFAPUHZPW IOIICXESMT
CBXVRJKVKV PMKVVHPCQN IOICGBILVJ KVIOIVPOAP WYCTEOESGB DDMEIBDPXJ
UPDYXEGAHH RUEWWLVVPK TPXYCAQLGF OMLPHVNGZU SNPICKMJQN ILRLUMSPRM
KAJHPRTBHZ LFTBEHRXTI BZEIGXGVFR DTNZPZIPIS CRPVDFMEIE WLRZVKDTIJ
VWSLGIAXIP RXEQEOIIUJ JAMDUCGLCF WEXSPTQXTH RPYINALVTM PYITKXWLVJ
VPPAEIGUJJ LDQZTIEUNG PMJVEBTKFP UCROPRPOJH KVIIBLWKJI CALVXQVLRV
TMRPTYGZ
```

Hint: No trigram occurs 4 or more times, and only BWL, ILV, IOI and LVJ occur 3 times in the ciphertext.

7 The following problem is taken from Chin Chiu Shao's book *Su Shu Chiu Chang* (Nine Sections of Mathematics), written in 1247. A ko is a unit of volume. [By modern standards, this question is not well posed. You have to make various reasonable assumptions in answering it. You should state what assumptions you have made.]

> Three thieves, A, B and C, entered a rice shop and stole three vessels filled to the brim with rice but whose exact capacity was not known. When the thieves were caught and the vessels recovered, it was found that all that was left in Vessels X, Y and Z were 1 ko, 14 ko and 1 ko respectively. The captured thieves confessed that they did not know the exact quantities they had stolen. But A said that he had used a horse ladle (capacity 19 ko) and taken the rice from X. B confessed to using his wooden shoe (capacity 17 ko) to take the rice from vessel Y. C admitted that he had used a bowl (capacity 12 ko) to help himself from the rice from vessel Z. What was the total amount of rice stolen?