Queen Mary
University of London

MAS 335 Cryptography

Assignment 1 For handing in on 24 January 2008

Your solutions to these questions should be handed in to the RED box on the SECOND floor by 3.30pm on Thursday.

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 This question has been encrypted. Decrypt it, and then answer it.

Sip uly ch jlcmih ch u zilycah wiohnls uhx uff sipl gucf cm vycha lyux vs nby jlcmih aoulxm. Qbun gynbix iz wlsjnialujbs il mnyauhialujbs gcabn sip omy ni myhx u mywlyn gymmuay ni sipl fuqsyl, uhx qbs?

2 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.]

> 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?

PTO

3 Solve the following substitution cipher. Your solution should include an explanation of the method you use.

```
TEYTQ BQEQB AXDBF MGJTM IVGYG GXETG PTBXD GQBLG BLLGL AJBIO
ITZGM IVGTG GXQMG NIJGV EOXGJ IYOGQ AKJGS EGXDN IXION TBTYI
TGPAX QMGTQ IQBTQ BDTAK QMGOI XUEIU GETGP IOQMA EUMKJ GSEGX
DNIXI ONTBT ZITKB JTQPG VGOAF GPYNI JIYDJ NFQAU JIFMG JTBXQ
MGQGX QMDGX QEJNT EYTQB QEQBA XDBFM GJTDA XQBXE GPQAY GETGP
EXQBO SEBQG JGDGX QONTB LAXTB XUMBX QMGDA PGYAA RQGOO TQMGP
JILIQ BDTQA JNAKM AZQMG YJGIR BXUYN GOBCI YGQMT DJNFQ IXION
TQTAK QMGDB FMGJE TGPYN LIJNS EGGXA KTDAQ TOGPQ AMGJQ JBIOI
XPGHG DEQBA XIFFI JGXQO NLIJN IXPMG JDAXT FBJIQ AJTQM AEUMQ
QMGBJ DBFMG JZITT GDEJG
```

4 (a) Write out a table of inverses for the integers modulo 13.

(b) Write out a table of inverses for those integers modulo 26 which have them.

(c) Prove that b has an inverse modulo k if and only if b and k are coprime (i.e. $\gcd(b,k) = 1$).

(d) Use Euclid's algorithm to find the inverse of 19 modulo 257.