MTH6115 Cryptography Exercises 1

Hand in to BLUE BOX on SECOND FLOOR of math sci building before 4:30pm on Tuesday 20/1/09.

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.*

Q1 Decipher the following ciphertext which was sent to Caeser by one of his spies in the Roman senate.

ORJNE RGURV QRFBS ZNEPU

[10]

Q2 (a) Decipher the following ciphertext which was constructed using a substitution cipher, taking care to explain how you arrive at your solution.

```
MAXSK CGPIY AILNI GPTQI YXPHA XYINP LGHAX HALYU XGVXQ KTXMA XAIPF
NKCBA HIQKG BSKNL HMAXI PPNXM MXPLH HKBCJ MKSSL YXLGA XNZIG QJDIQ
QXHGL YKQIM SLGBX NMSLG IQQJS KCGPK GXQIM HYNXI MXPMH IZTIM MAXQL
YUXPL HIWCX CXSKN ZXPIA XIPKS AXNLG AXNZL GPXPB LGBHK DINPM HAXMA
IPKDL GLHMY IBXPM HIQQI HHAXM CFMLP LINJT KMHKS SLYXF CHHAX GMAXG
KPPXP NXIQL MLGBH AIHHA LMQXH HXNDI MHAXQ IMHMA XDKCQ PXVXN MXGPH
ALMMH IZTHA XQIMH MAXDK CQPXV XNQLY UBKKP MHIZT WCXCX MTCHG LYKQI
LGIPI JQKGB SCNJJ KCFKC BAHHA KCMIG PMIGP HAXGH AXSKQ QKDLG BDXXU
HAXTN LYXKS ZILQD XGHCT IBILG BKKPK GXZKN XKSQL SXMPC HLXMP LMYAI
NBXPS KNHAX VXNJQ IMHHL ZXIII
```

[40]

(b) Is the substitution cipher used in (a) an affine substitution? Justify your answer. [10]

Q3 (a) Write out a table of multiplicative inverses for the congruence classes modulo 11. [10]

(b) Write out a table of multiplicative inverses for those integers modulo 12 which have them. [10]

(c) Use Euclid's algorithm to find the multiplicative inverse of 35 modulo 288. [10]

(d) Determine the number of integers modulo 288 which have multiplicative inverses. [10]