Queen Mary
University of London

MTH6115 Cryptography

Assignment 1 For handing in on 24th January 2011

Your solutions to Question 3 should be handed in to the ORANGE box on the GROUND floor by 3:30 pm on Monday 24th 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 The following have been encrypted using (possibly different) Caesar shifts, with the standard 26 letter English alphabet. Firstly, a Latin phrase you will have seen often:

```
KLJBZ LA ABAHTLU.
```

And a quotation from René Descartes (Latin version):

```
MYQSDY OBQY CEW.
```

Decrypt them.

2 The Hawai‘ian alphabet has just 13 letters, which are ordered and numbered as follows. (The numbering is modulo 13.)

Letter	A	E	I	O	U	H	K	L	M	N	P	W	?
Number	0	1	2	3	4	5	6	7	8	9	10	11	12

The letters A, E, I, O, U are vowels and the rest are consonants, and I have used ? rather than ‘ for the ‘okina (glottal stop). In Hawai‘ian, each consonant must be followed by a vowel, and no word can end in a consonant. (Consecutive vowels are allowed.) How many Caesar shifts, affine substitution ciphers and substitution ciphers are available for the Hawai‘ian alphabet? The following is a piece of Hawai‘ian that has been encrypted using an affine substitution cipher. (Any macrons on the vowels have been ignored.)

K?U LN HNWAN HM ONENUHU INI?N M LN HNWAN M KN IML?P?KU M ONENUHU
NPN?. HMWAWM HUN U LNPN HUN NU LN IML?P?KU A LN UKMN ONENUHUWMN,
LN OMHMLAWA PMWAKALUN U OMHULA HUN NU U KN IML?P?KU M ONENUHU.

Decrypt it, assuming that the spaces above correspond to spaces in the original text. There are two possible answers if (like me) you know no Hawai‘ian.

3 Solve the following substitution cipher. Your solution should include an explanation of the method you use. Remember that despite cipher solving being an art form, you are writing a piece of Mathematics, and should state very carefully what you are assuming, and what you are deducing. You will lose marks if the marker thinks you are making dodgy 'deductions'. The end result should be rendered in good English.

OSMFM ZMXNW PEXVO MLGVF POEMH MZIXN MIXLI NSPMA MJMXO EPXOS
MGPXM IFOEI XLIFN SPOMN OYFMO SPEQM FPVLS IQQMX MLDSM XOSMU
PXZDM XOJIL IXLPO PEOSV YZSOO SIOOS PEDIE NIYEM LBWIF EMXPN
QVPEV XPXZO SPEMF IMXNV JQIEE MLIOP JMVGZ FMIOE VNPIH QVHPO
PNIHI XLMAM XMNVX VJPNN SIXZM LMEQP OMOSM BHVVL ESMLI XLDIF
GIFMO SMFMZ MXNWD IEIHE VIQMF PVLVG ZFMIO FMGPX MJMXO IXLNY
HOYFI HINSP MAMJM XOESI QPXZI XLIHO MFPXZ OSMEV NPMOI HEOFY
NOYFM VGBFP OIPXI EIDSV HMVXM VGOSM ZFMIO MEOQI OFVXE VGOSM
IFOEI XLIFN SPOMN OYFMD IEOSM QFPXN MFMZM XOSPJ EMHGS MMJBI
FUMLV XJIXW QFVTM NOEPX NHYLP XZOSM NVEOH WBYPH LPXZI XLFMG
YFBPE SPXZV GOSMB MIYOP GYHIX LMCVO PNBFP ZSOVX QIAPH PVXOS
MKYMM XVGBF POIPX GVFJV EOVGO SMFMZ MXNWD IENSI FHVOO M

Is the substitution used above an affine substitution cipher? Justify your answer.

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

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

(c) Write out a table of inverses for the nonzero integers modulo 19.

(d) Write out a table of inverses for those integers modulo 38 which have them.

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

(f) Use Euclid's algorithm to find the inverse of 17 modulo 251.

(g) Determine the number of integers modulo 480 which have multiplicative inverses.