Answer each of the following to the best of your ability. This homework should be turned in on paper in class. You need to write explanations in complete sentences. The quality of your work counts for 10% of your grade.

1. For each of the following pairs of numbers decide if they are legitimate keys for an affine cipher using a modulus of 26 (so for just the characters a-z). If they are, find the deciphering keys. If they are not, explain why.

   (a) Multiplier $m = 9$ and Shift $s = 7$

   (b) Multiplier $m = 12$ and Shift $s = -5$

   (c) Multiplier $m = 13$ and Shift $s = 18$

   (d) Multiplier $m = 5$ and Shift $s = 12$

   (e) Multiplier $m = 8$ and Shift $s = -2$

   (f) Multiplier $m = -5$ and Shift $s = 3$

2. For each of the pairs of numbers in exercise 1, decide if they are legitimate keys for an affine cipher using a modulus of 36 (so for the characters a-z and digits 0-9). If they are, find the deciphering keys. If they are not, explain why.

3. Decrypt the following message that was encipher using an affine cipher. When done you need to give the multiplicative and shift keys for the cipher.

```
RHJIG ZEZML JFOZY FKHJF OZMUJ HCFMV RUZMH YHREZ RUKFM JHIRF
UEZVZ IHSYZ HURJH YHUOJ RUZMH YRNUF PIGZN RUVXF KZUVY HUOHU
ORBTF IZIGZ KRVGI XGRXI FMRDH YKMFJ JHMHI GFUIF PHIZM YFFRU
FMOZM DHIZV FMRDH YSRJE ZMLPZ YYHDB THRUI ZOIFF PRIGJ HIIZM
XJHIG ZJHIR DHYRT UOZMX IHUOZ BTHIR FUXSF IGIGZ XRJQY ZHUOB
THOMH IRDHY HSFTI SRUFJ RHYIG ZFMZJ RJIZZ JRUVP RIGHY FIFUZ
PXPRI GJHUL DGZZM KTYKH DIXHS FTIIG ZXBTH MZFKI GZGLQ FIZUT
XZ
```

4. Decrypt the following message that was enciphered using an arbitrary monoalphabetic cipher. When done you need to give the complete ciphertext alphabet.

```
W'J AKED RPPC QH WMHKREQX QMC CWBBKEKMHWQX
IQXILXLT; W FMPZ HOK TIWKMHWBWI MQJKT PB UKWMRT
QMWJQXILXPLT: WM TOPEH, WM JQHHKET AKRKHQUXK,
QMWJQX, QMC JWMKEQX, W QJ HOK AKED JPCKX PB Q
JPCKEM JQNPE-RWMKEQX.
```

5. The following message was enciphered using a Hill's cipher with a two by two matrix and a modulus of 26. Assuming this is a weather report, and so starts with the words weather report, use a known plaintext attack to decrypt the message and find the enciphering key.

```
SERMR PWZZI BWCDB WMHRC LYQWD NOJKU FNKIW JJRFP
YWYGS SNQRM RIQGB DXRPJ GDQYZ OWMDT CTQNW MHPRZ
PRRIU CZFJT HVHIP HRIMH RKQWH TPGGW QCORB JZOBM
VXFNB HGDRP YOCRR IAKCM CAXB
```