MTH6115 Cryptography Exercises 2

Hand in to BLUE BOX on SECOND FLOOR of math sci building before 4:30pm on Friday 30/1/09.
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 Let x, y be positive integers with $x \geq y$.
(a) Prove that if we divide x by y to get a remainder r with $0 \leq r < y$ then $r < x/2$. Deduce that Euclid's algorithm requires at most $\lfloor \log_2 x + \log_2 y \rfloor$ divisions to find $\gcd(x, y)$. [10]
(b) Describe an algorithm which uses at most $\lfloor \sqrt{x} \rfloor$ divisions to either find a proper factor of x or else deduce that x is prime. [10]
(c) Suppose that x and y are both of size approximately 10^{20} and that each division takes 0.01 seconds (independently of the numbers used in the division). How long will the algorithms given in (a) and (b) take in a worst case? [10]

Q2 The following ciphertext was enciphered using an affine substitution cipher.

```
GWNQZ ADGTR BILZT WGWBM NENNO WBOKE BIIEJ GGWNA NQNAN NWBDT
ZMNOZ GGWND NHROK RONLZ TWGWB MNENN ORJGD ZKNGW NERSE JGBTB
ZOWNW BDLBK NGWNK NHZDZ ROBTB ZODGJ DBGGW NNOKR QGWNK BVPNK
ZKOGK NQNOK GWNLP NIINO RJTWZ HBOGE NHAZG ZHBIR QGWNA NQNAN
NEJGZ HBOEN HAZGZ HBIRQ LVKNQ NOKNA DORGK NQNOK ZOTZG PNIIG
WNVPN ANURR AYYYY
```

(a) Find the affine permutation $\theta_{b,c}$ which deciphers it and use it to determine the plain text. [25]
(b) Construct the affine permutation $\theta_{s,t}$ which was used to encrypt the plain text. [10]

Q3 Decipher the following ciphertext which was constructed using a Vigenère cipher, taking care to explain how you arrive at your solution.

```
KLHSS BJLDM IGFRH SVLCP LRRWC CLUSQ KOQFA ZYIUV XKVCI FYQUM
XWVRD XKVCI FYQUK UVEWI IVFPY VEQUK UVEWZ RQVVV KVHEK WYXRW
MJYXE RGNWS UKLHN MQNIK RZHUS QVXKR XLEEO FXRWK DDIVK LLJWH
RWREE QUMKR ZHKLH LXPFW WIIJR VGWSU KLHGP DPIUJ JRIXK RXLKW
HVQHU XRSII ISPNL HIILN EVJXD EHLEK DEIYV RWWYO XEPVW YEHHI
PDEHV TSUVH DEHGV WHIZH UXRZX WFSNL WVFQH KMPVX RXIWZ RWFSX
IWWZH HRJWV VWYIJ FEOZX ZRWDU MIWMF LPWGI UZSGS YWNIZ VEWYI
UVHWY EWRRG KLHEM QKLHC EVKXZ VRWPQ LEYWV WRWXK VJLIW WYEOW
AHTEP VMQKS WYIJR PHRRG XSWRF LKSII LBKLP RFRLX RLVVV PYVWT
```

Hint: search for trigrams beginning with the letter K. [35]