CS3235 Tutorial for week 4
(Sept 1-Sept 5, 2003)

29th August 2003

1. Calculate the gcd of 231 and 1071. Show all working.

2. Use Fermat's theorem to show the inverse of $a = 6$ and $a = 7$ in the integers modulo 35521. Describe exactly how you did this.

3. **Question 7, Chapter 1 in textbook:** For each of the following statements, give an example in which the statement is true:

a. Prevention is more important than detection and recovery.

b. Detection is more important than prevention and recovery.

c. Recovery is more important than prevention and detection.

4. The following sentence is encrypted using a monoalphabetic substitution cipher. What this means is that an ordinary English sentence has been encrypted by changing each letter to some other letter.

(a) Decrypt the sentence:

```
BJSB NZCC SZKI D TBGTGCDHI LZVB HG HBI LZWVH VHJAIYH
NBG IFDZCV HBZV HG BZF
```

(b) Describe the technique you used to decrypt it.

You may find that the decrypt tool at `https://www-appn.comp.nus.edu.sg/~cs3235/mono.cgi` may be useful. It measures the frequency of letters in the sentence. (You figure out how to use it)

5. The following sentence is encrypted using a monoalphabetic substitution cipher.

(a) Decrypt the sentence:

```
MLTVXPQOI MXP NOCOMC OJMOIIQEO VOGILPXW DIO LB X COW
OVYLPO AK WLLSQPZ XC CYO PDTAOGI NQXWON. QB CYLIO PD
TAOGI AOWLPZ CL VOLVWO PLC GOWXCON CL, LG QPELWEON Q
P, CYO MLTVXPK I ADIQPOII, CYO MLTVXPK TXK QPEOICQZX
CO BDGCYOG CL NOCOGTQPO QB CYO OTVWLKOO QI DIQPZ CYO
VYLPO BLG CLL TDMY VOGILPXW ADIQPOII. IQTQWXGWK, HQC
Y OWOMCGLPQM TXQW, CYO MLTVXPK MXP PLCO CYO LDCZLQPZ
XNNGOIIOI, XPN BGLT CYLIO NOCOGTQPO QB CYO OTVWLKOO
QI DIQPZ OTXQW BLG VOGILPXW ADIQPOII. CYOIO TOCYLNI
XGO CKVQMXWWK MDTAOGILTO XPN GOFDQGO QPEOICQZXCQLP,
IL CYOK COPN PLC CL AO DION DPWOII VYLPO MXWWI LG OT
XQW QI IOEOGWK XBBOMCQPZ CYO ADNZOC LB CYO LGZXPQUXC
QLP LG CYO VGLNDMCQEQCK LB CYO OTVWLKOOI
```

(b) In some ways this is easier to decrypt than the sentence in Question 4. Why?