Homework 1

Problems for 7 th edition textbook:

- Page 27: P-1.4, a, b, c (10pt)
- Page 96: P-3.7 (10pt), P-3.8 (Note: Both ciphertext and plaintext are on page 78) (10pt)
- Page 98: P-3.19 (10pt), P-3.22 (Hint: Lay the message out in a matrix n letters across, n is the largest integer value) (10pt)

Problems for 6 th edition textbook:

- Page 26: P-1.4, a, b, c (10pt)
- Page 57: P-2.7 (10pt), P-2.8 (Note: Both ciphertext and plaintext are on page 38) (10pt)
- Page 59: P-2.19 (10pt)
- (Hint: Lay the message out in a matrix n letters across, n is the largest integer value) (10pt) In one of Dorothy Sayers's mysteries, Lord Peter is confronted with the message shown in Figure 3.10. He also discovers the key to the message, which is a sequence of integers:

7876565434321123434565678878765654 34321123434565678788787656544332112 34

1. Decrypt the message. Hint: What is the largest integer value?
2. If the algorithm is known but not the key, how secure is the scheme?
3. If the key is known but not the algorithm, how secure is the scheme?

> I thought to see the fairies in the fields, but I saw only the evil elephants with their black backs. Woe! how that sight awed me! The elves danced all around and about while I heard voices calling clearly. Ah! how I tried to see—throw off the ugly cloud—but no blind eye of a mortal was permitted to spy them. So then came minstrels, having gold trumpets, harps and drums. These played very loudly beside me, breaking that spell. So the dream vanished, whereat I thanked Heaven. I shed many tears before the thin moon rose up, frail and faint as a sickle of straw. Now though the Enchanter gnash his teeth vainly, yet shall he return as the Spring returns. Oh, wretched man! Hell gapes, Erebus now lies open. The mouths of Death wait on thy end.

Figure 3.10 A Puzzle for Lord Peter

Submission:

- Your homework could be typeset or handwritten, but must be saved as a .pdf file
- Submit your file onto Cougar Course following the due date below.

Due date and time:

This homework assignment will be due 5:00pm, June 10th (Wednesday).