Assignment 3  
Computer Science 349  
Spring 2004  
Due: Start of class on Thursday, February 19, 2004

**Reading:** Singh, Chapter 4; Stinson, Sections 1.2.3 – 1.2.5, 1.3

**Remark.** Several of these exercises may be time consuming. Exercise 3.2 in particular may require either considerable counting/calculation, or (and this is to be preferred) it will require writing a relatively simple computer program to do the counting for you. In either case you should start the assignment early in order to avoid the usual last minute tangles.

**Exercise 3.1.** Turing’s probable word attack, as described in Chapter 4 of Singh searches for directed cycles connecting plaintext and ciphertext as illustrated in Figure 3.1.

![Figure 3.1](image_url)  

However, Turing strengthened his attack by using the fact that the Enigma cipher is involutory. To understand how, consider the plaintext/ciphertext pair

\[
\text{ob er kom m a n d o d er we h r ma c h t}^{1}
\]

\[
\text{Z M G E R F E W M L K M T A W X T S W V U I N Z}
\]

A directed graph is constructed whose vertices consist of alphabetic characters and whose arcs (directed edges) are of the form \((x, e_K(x))\), where \(x\) is a plaintext letter and \(e_K(x)\) is its corresponding ciphertext letter. For example, since the plaintext letter o corresponds to the ciphertext letter Z, \((O, Z)\) is an arc of the directed graph. Complete this construction for the given example. List the cycles likely to be used by Turing’s BOMBEs in the involutory case? What cycles could be used in if the cipher had been noninvolutory? Briefly justify your answer.

**Exercise 3.2.** (Stinson 1.21b) The ciphertext shown in Figure 3.2 is obtain from the plaintext using a Vigenère Cipher. Give a clearly written description of the steps you follow to decrypt the message. This should include all statistical analysis and computation you performed. The plaintext is take from “The Diary of Samuel

---

1 The Wehrmacht loved their titles (and so did the cryptanalysts at Bletchley Park).
Marchbanks,” by Robertson Davies., Clarke Irwin, 1947. (Hint. A simple computer program will surely help here. Finding the keyword length and producing a table similar to Table 1.4 in the Stinson text is worth nearly full credit even if you don’t figure out what the text says.)

Figure 3.2. Ciphertext obtained using a Vigenère Cipher

Exercise 3.3. (Stinson 1.26) We describe a special case of a Permutation Cipher. Let $m$, $n$ be positive integers. Write out the plaintext, by rows, in $m \times n$ rectangles. Then form the ciphertext by taking the columns of these rectangles. For example, if $m = 4$, $n = 3$, then we would encrypt the plaintext “cryptography” by forming the following rectangle:

```
cryp
togr
aphy
```

The ciphertext would be “CTAROPYGHPRY”

a. Describe how Bob would decrypt a ciphertext string (given values for $m$ and $n$).

b. Decrypt the following ciphertext, which was obtained by using this method of encryption:

```
MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW
```