Homework 4

Due Date: March 6, 2002 **100 Points**

1. (*40 points*) The purpose of this problem is to show the unbreakability of the one-time pad. Suppose we are using a Vigenère scheme with 27 characters in which the 27th charater is the space character, but with a one-time key that is as long as the message. In what follows, we represent a space by an underscore "_". Given the ciphertest
`ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS`
find one key that yeilds the following plaintext:
`MR_MUSTARD_WITH_THE_CANDLESTICK_IN_THE_HALL`
and a second key that yeilds the following plaintext:
`MISS_SCARLET_WITH_THE_KNIFE_IN_THE_LIBRARY_`
[from Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd edition, Prentice-Hall, ©1999; problem 2.2]
2. (*30 points*) Consider the RSA scheme with $p = 17$ and $q = 43$. Alice chooses her public key to be $e = 29$.
   a. Find Alice's private key.
   b. Bob wants to send Alice the message "HI", which he encodes as 190. What is the ciphertext of that message?
   c. Please show how Alice deciphers the message.
   d. (*extra credit*) "HI" is encoded as 190. Given that the cipher will transmit *only* capital letters, please show why "HI" is encoded as the numbr 190. What would "LO" be encoded as?
3. (*30 points*) Chapter 12, exercise 9. Please remember to show your work.