CRYPTOLOGY PROBLEMS

1. Suppose you have found a message encoded by the caesar.vbp program. Modify the program so that it would ***decode*** the message.

2. A particularly simple type of substitution code is known as a Caesar code, after Julius Caesar who supposedly used it. In terms of our program, the '***translation***'string is in normal alphabetical order, but it is shifted to the left by any arbitrary number of letters. The letters that are pushed out of the front end of '***translation***' are added to the back. For example if we shifted '***translation***' by four letters, it would be:

   translation = "efghijklmnopqrstuvwxyzabcd"

   With this '***translation***' every letter in the original english message is replaced by the letter four letters after it in the alphabet (four letters after z is d). Since the shift can be any number from 1 to 25 characters, there are 25 different Caesar codes.

   Suppose you have a coded message that was encoded with one of the Caesar codes, but of course, you don't know which one. Write a program that will decode the message by systematically trying all 25 Caesar codes.

   Try your program on the following message:

   jvunyhabshapvuz fvb jhu hwwsf av aol jph mvy h qvi