Vigenere Cipher

Due date: May 4, 2016

You are to write code that will encode and decode a message encrypted using a Vigenere Cipher. You can do this as a single application with a choice to encode or decode, or you can implement two programs, with quite a bit of shared code.

The Vigenere Cipher is a symmetric cryptographic method based on the Caesar Cipher. Although not terribly secure, it is a significant improvement over the Caesar Cipher without much more effort. As a symmetric method, there is a key that must be shared between the sender and receiver. In this case, the key is actually a string of letters.

We will encrypt only the alphabetic characters in the message. Any blank space or punctuation will not be encrypted. The first letter of the message will be encrypted using a Caesar cipher with the first letter of the key. The second letter of the message is encrypted using the second letter of the key, and so on. You are almost certain to reach the end of the key before the end of the message, so we wrap around to the first letter of the key when we reach the end. Or you can imagine concatenating copies of the key to itself until you exceed the length of the message, but that would be a wasteful technique for implementation.

In the Caesar cipher, the encoding is done with a shift value. For example, with a shift of 1, then the letter 'A' would be encoded as a 'B', 'B' would be encoded as 'C', etc., up to 'Z' being encoded as 'A'. This shift value of one can be characterized as a 'B' shift. A shift of two could be called a 'C' shift, etc. Clearly there are only 26 distinct shifts, and one of those is an identify shift (the 0 or 'A' shift).

So, here are the 26 possible Caesar ciphers associated with the 26 letters of the alphabet:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP

RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

So, for example assume the message to be encoded is 'HELP ME', and the key is 'PEN'. The letter H in the message will be encoded using the row starting with 'P' (the first letter in the key). This gives us a 'W'. Then we encode the letter 'E' from the message with the second letter, also 'E' from the key. This gives us an 'I'. Then the 'L' gets encoded with the 'N', giving a 'Y'.

Now we are out of letters in the key, so we start over and the next letter in the message, 'P' gets encoded with the first letter from the key, also 'P'. Skipping the space, we eventually get the cipher text: 'WIYE QR'. Note that we just copied the space to the cipher and didn't skip a letter in the key. We had 6 letters in the message 'HELP ME' and used the letters from the key repeated as needed, giving us 'PENPEN'.

Submit your code on blackboard.