AITI Kenya Challenge Problem
Cracking the Caesar Cipher

Suppose you want to send a sensitive message over an insecure network connection. The Caesar cipher (named after Julius Caesar) is a simple encryption method you that works as follows:

1. Each English letter is assigned a numerical value. That is, 'A' = 0, 'B' = 1, 'C'=2, etc., until 'Z'=25. Treat lower-case the same as upper case, so 'a' = 'A' = 0. Let the period '.' = 26, comma ',' = 27, and space ' ' = 28.

2. Messages are encrypted using a key of equal length. Only someone who has the key will be able to decrypt and read the message. To all others, the message is unreadable. In the Caesar cipher, each letter of the message is encrypted by adding the message letter's value to a key letter's value modulo 29. That is $(m_i + k_i) \bmod 29 = c_i$, where m_i is the ith letter of the message, k_i is the ith letter of the key, and c_i is the ith letter of the ciphertext.

   For example, if the message is:
   "ONE IF BY LAND, TWO IF BY SEA."
   and the key is:
   "THE CELERY STALKS AT MIDNIGHT."
   then the encrypted message (ciphertext) is:
   "EUI,KJKFMXRWT,KALN ,ELJ,MTGUWX"

   Note that 'O' = 14 and 'T' = 19 and (14 + 19) mod 29 = 33 mod 29 = 4. That is the encoded value of 'E', which is the first letter of the ciphertext.

3. To decrypt the ciphertext, the receiver subtracts the key value modulo 29. That is $(c_i - k_i) \bmod 29 = m_i$. For technical reasons in Java, you may want to compute this as $(c_i + (29 - k_i)) \bmod 29 = m_i$, which is an equivalent value.

4. You intercept a series of seven-letter messages encrypted with the Caesar cipher. Fortunately, the sender has used the same key for each message. You know that the sender has a fondness for beer and football, so some of the messages may be related words. Using those facts, write a program to help you find the plaintext of all the following messages, as well as the key they were encrypted with:

   "C IKMHH"
   "CP,SQII"
   "OPXL.XI"
   "BMVRMJH"
   "NMVKPTU"
   "YMISIZM"
   "MZIEVTT"

EC.S01 Internet Technology in Local and Global Communities
Spring 2005-Summer 2005