Program 2: Hill Cipher

CPSC370: Introduction to Computer Cryptology

Due Wednesday, September 28, 2016 11:59PM

In this programming assignment, you are asked to write C/C++/Java codes to implement encryption/decryption functions for 3×3 Hill Cipher.

1 Details of the program

You need to do the following tasks:

1. Implement a function that computes the inverse of a 3×3 matrix mod 26 (Hint: you can use lookup table to find the multiplicative inverse mod 26).

x	1	3	5	7	9	11	15	17	19	21	23	25
inv(x)	1	9	21	15	3	19	7	23	11	5	17	25

2. Implement a function that computes the inverse of a 3×3 matrix (K) mod 26. Specifically, you need to compute the determinant and the cofactors for the construction of K^{-1}.

3. Implement encryption/decryption functions for 3×3 Hill Cipher (Hint: your encryption function should be general enough to hand any length of text. You should add one or two `xx` if it is not divisible by 3.

4. Using the following key

$$K = \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{vmatrix}.$$

   (a) Invoke your inverse function and print out the inverse of the above key K (mod 26).

   (b) Invoke your encryption function to print out the cipher text, given the above key and the plaintext of "`paymoremoney`".

   (c) Invoke your decryption function to print out the plaintext using the cipher text above.

5. Using the following key

$$K = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{vmatrix}.$$

   (a) Invoke your inverse function and print out the inverse of the above key K (mod 26).

   (b) Invoke your encryption function to print out the cipher text, given the above key and the plaintext of "`hillcipherisfuntome`".

   (c) Invoke your decryption function to print out the plaintext using the cipher text above.

2 Submission

1. **Electronic submission** (Due by Wednesday, September 28, 2016 11:59PM)

   (a) Make sure that your program is compilable

   (b) Zip both the source codes and output screenshots into a file. The file format is as follows: `FirstNameLastName_Program2.zip` (e.g., `DongshengChe_Program2.zip`)

   (c) Upload the zip file onto D2L Dropbox

2. **Hardcopy submission** (Due by Thursday, September 29, 2016 in class)

   Your hardcopy should include:

   - Grading sheet (top)
   - Source code (middle)
   - Output screenshots (bottom)