Crypto

Based on Chapter 2 of *Information Security (2nd Edition)* by Mark Stamp

1. Decrypt the following message that was encrypted using a simple substitution cipher. The plaintext has no spaces or punctuation. (warning: there may be the odd transmission error) Submit the plaintext answer and key, along with an explanation on how you solved the problem and all source code that you developed (use Java, C, or Python) to help you arrive at your answer. The cyphertext is as follows:

   PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWA
   XBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXQVXGTVJV
   WLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXPFHXZHVFAG
   FOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQH
   FOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJT
   QOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFL
   QHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZ
   QWGFLVWPTOFFA

   Note, that you will need to write your own code to decrypt the message. Using code or websites available on the Internet or other places to decrypt the message is not allowed. Instead, you should use a large English text corpus from, for example, Wikipedia and do a character frequency analysis on the data as was described in class. Your code should remove spaces, punctuation, and non-alphabetic characters and convert the remaining characters to upper case. Then, your code should do a character frequency analysis on the ciphertext. Explain what you did to recover the plaintext after the two frequency analyses. Submit your data and code along with the key and the recovered plaintext.

2. Implement the RC4 algorithm using the C programming language (submit your code along with your answers). Suppose the key consists of the following seven bytes: (0x1A, 0x2B, 0x3C, 0x4D, 0x5E, 0x6F, 0x77). For each of the following, give S in the form of a 16x16 array where each entry is in hex.

   a. List (in Hex) the permutation S and indices *i* and *j* after the initialization phase has completed
   b. List (in Hex) the permutation S and indices *i* and *j* after the first 100 bytes of keystream have been generated
   c. List (in Hex) the permutation S and indices *i* and *j* after the first 1000 bytes of keystream have been generated

Submission requirements:

1) There should be one file named README.txt explaining which file contains what part of the assignment (source code and data) and explaining the procedure to compile your code.

2) Every subsequent file should contain the name of part of assignment it covers, so for example, if the file contains the C code for question 1, name the file Q1.c and so on.

3) Create a .zip or a .tar.gz of all the files that you submit and upload a single .zip or .tar.gz on bblearn. The .zip or .tar.gz should be named as first letter of your first name and last name followed by the assignment number. So, for example, for assignment 1, if your name is Jane Doe, submit JDoe_hw1.zip or JDoe_hw1.tar.gz