Track B
INFA723 Homework 1

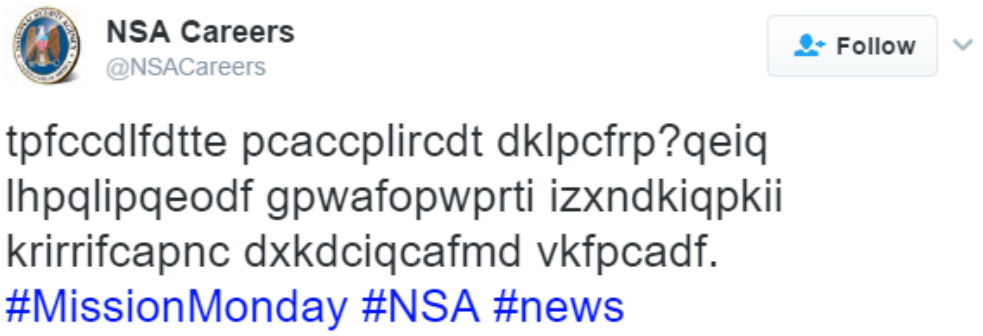
The homework assignment will be graded based on the following criteria:

- Accuracy: 1) the solution meets specific requirements in the problem description; 2) the solution produces correct results; 2) the procedures adopted in the solution are technically sound.
- Efficiency: efficiency will be one of the criteria when grading programing assignment. The solution should produce the desired results efficiently.
- Effort/neatness: the solution includes excellent effort, and all relate work is shown neatly and organized well.

Homework assignment feedback will be available through the DropBox folder on D2L.

NSA Careers posted three encrypted tweets in May 2014. The tweets are encrypted using the substitution technique we introduced in the class.

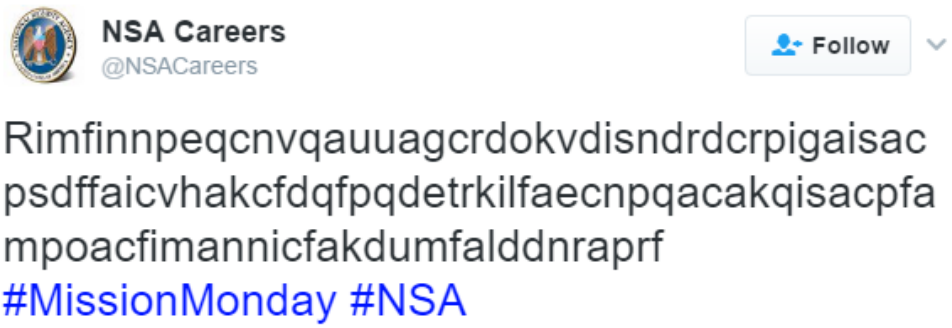
NSA Encrypted Tweet #1



url: https://twitter.com/nsacareers/status/463321993878994945?lang=en

Cipher text: tpfccdlfdtte pcaccplircdt dklpcfrp?qeiq lhpqlipqeodf gpwafopwprti izxndkiqpkii krirrifcapnc dxkdciqcafmd vkfpcadf.

NSA Encrypted Tweet #2



url: https://twitter.com/NSACareers/status/465839250328809472

Cipher text:
Rimfinnpeqcnvqauuagcrdokvdisndrdcrpigaisacpsdffaicvhakcfdqfpqdetrkilfaecnpqacakqisacpfampoacfim
annicfakdumfalddnraprf

NSA Encrytped Tweet #3

url: https://twitter.com/NSACareers/status/468399492640034816
Cipher text:
nbylcrhspclbyxrnmlbzevsmlchscrhrhnmbebfsvhcxmxxrmzencmfyvychclcmscgmyimkcncxmxrydsmnrhsby
emfmmefrhxrfdyrfczmtchmscgby

Pick up any encrypted tweet (only one) and answer the following questions:

1. (20 points) What is the plain text? (You can use any tools you have to decrypt the tweet.)
2. (80 points) Write a program (using a programming language at your choice) to decrypt the tweet. The program will read the encrypted tweet from a file, decrypt the tweet, and print the plaintext on the screen.
    a. Using tools is not allowed in this question.

b. Using a static hard coded substitution key, e.g., a key decrypted from a tool, is not allowed. You program needs to conduct cryptography analysis to find the key.

All the steps must be done using your own written program. **Using a hard-coded substitution key in the program is not a solution for the program (there will be no credit for such solutions).**

Note: For all the programming assignments, you can choose any operating systems to develop your code. A README.txt is required to submit any programming assignments. In the README.txt, you need to provide the following information:

1) How to compile your program?
2) How to run the program, e.g., usage of program?
3) What is the expected output when running the program?
4) Any descriptions which can help me understand, compile, run, and verify your answers. (FYI: I check every programming assignment turned in!)

Zip all you source code, project files, supporting files, and README.txt and submit the all-in-one zip file together to the D2L Dropbox.