Cybersecurity
Homework Assignment 1

COSC 3371
2019 Fall

Please solve the following problems by completing the attached Java source file (`HW1.java`). For each problem, replace the code **between** `// BEGIN SOLUTION` and `// END SOLUTION` with your solution (please do not modify other parts of the code). The submission uploaded to Blackboard should include the completed Java source file. Please make sure that you use only standard libraries and that the uploaded source file can be compiled and executed without errors and unhandled exceptions.

In each problem, your goal is to recover a plaintext from a given ciphertext.

Problem 1 (3 points): Substitution Cipher

Agent James Vond,

One of our secret agents, Agent 006, has recently gone missing in the Caribbean. At the time of his disappearance, he was investigating a reclusive billionaire, Dr. On. We do not have any information that would connect Dr. On to criminal activities, but our agent was quite insistent on the investigation. This was the last message that we received from our agent:

"ROYQWH KQXXJYQ: N LQGNQAQ HDJH FO. VW NX J KQKLQO VZ J XQMOQH MONKQ VOYJWNSJHNVW MJGGQF U.D.J.W.H.V.K., IDVXQ YVJG NX HVHJG IVOGF FVKNWJHNVW. HDQNO UGJW NX HV JMBRNOQ J XRUQOIQJUVW JWF HV DVGF HDQ IVOGF OJWXVK. N ZQJO HDJH IQ FV WVH DJAQ KRMD HNKQ LQZVOQ HDQT XRMMQQF.

N DJAQ OQMQWHGT NWHQOMQUHQF JW QWMOTUHQF KQXXJYQ (JHHJMDKQWH MNUDQO2.HCH) HDJH IJX XQWH LT FO. VW HV VWQ VZ DNX MVWXUNOJHVOX, HDQ NWZJKVRX KO. LGVIZNQGF. N KJWJYQF HV FNXMVAQO HDJH HDQ KQXXJYQ IJX QWMOTUHQF RXNWY HDQ PJMEJG MNUDQO (XQQ XVROMQ MVFQ), LRH N IJX WVH JLGQ FNXMVAQO HDQ XQMOQH EQT, JWF HDQ MNUDQO XQQKX HV LQ RWLOQJEJLGQ. N JK JZOJNF HDJH FQMOTUHNWY HDNX KQXXJYQ NX HDQ VWGT IJT HV XHVU FO. VW'X VOYJWNSJHNVW.

UGQJXQ XQWF OQNWZVOMQKQWHX NKKQFNJHQGT! N HONQF HV JMH MJRHNVRXGT, LRH N DJAQ J ZQQGNWY HDJH FO. VW'X DQWMDKQW JOQ VWHV KQ. N FVW'H EWVI DVI GVWY N DJAQ LQZVOQ HDQT FNXMVAQO KT OQJG NFQWHNHT JWF KT XQMOQH DNFNWY UGJ" [sudden end of transmission]

We believe that the message was encrypted using a substitution cipher, but we do not have the key to decrypt it. Agent Vond, we task you with decrypting the message and finishing the investigation. Since Agent 006 disappeared without a trace under such suspicious circumstances, it is imperative that you discover what happened as soon as possible.

Sincerely,
M

The ciphertext was encrypted using a substitution cipher, and the plaintext is an English-language message. Note that whitespaces and punctuations are not encrypted.

- Compute and print the frequency of each letter (from `A` to `Z`) in the ciphertext (1.5 points).
- Decrypt the ciphertext and print the plaintext (1.5 points). You can manually identify which plain letter is substituted for which cipher letter by comparing the computed frequencies with the following typical frequencies:

```
E: 0.108
T: 0.075
A: 0.067
O: 0.058
I: 0.055
N: 0.051
R: 0.047
S: 0.047
H: 0.037
D: 0.034
C: 0.032
M: 0.027
L: 0.025
P: 0.016
Y: 0.016
G: 0.015
U: 0.014
W: 0.013
B: 0.013
F: 0.011
V: 0.008
K: 0.004
Z: 0.002
J: 0.001
Q: 0.001
X: 0.001
```

Problem 2 (1.5 points): Brute Force

Once you have decrypted Agent 006's message, you realize that the fate of the world is at stake. Unfortunately, the design of the Jackal cipher is rather confusing, and there is no time to analyze it given the urgency of the situation.

Notice that the number of possible keys is very low for the Jackal cipher, and assume that the plaintext is an English-language message. Can you find the correct key and decrypt the ciphertext? Hint: You do not need to understand the cipher or its implementation to find the key.

Problem 3 (1.5 points): "One-Time" Pad

After decrypting the message, you immediately fly to Hawaii and prepare to intercept the exchange. With the element of surprise on your side, you easily defeat the agents of P.H.A.N.T.O.M. You expect to retrieve the secret plans from them; unfortunately, all you find is a USB drive with a single encrypted file.

You have everything that you need for decrypting `cipher3.txt`: the cipher algorithm ("one-time" pad with repeating key) as well as the secret key. Hint: the binary XOR operation in Java can be performed using the ^ operator (e.g., `byte xor = (byte)(byte1 ^ byte2);`).