Programming Assignment 1

Implement a toy symmetric cryptosystem based on the following method.

a. Keys are 16-bit randomly generated values.

b. Messages are randomly generated strings with an even number of characters. (Valid characters are upper and lower case letters, as well as spaces.) One can always add a blank at the end of an odd-length string.

c. The encryption of a message *M* of length *n* (in bytes) is given by

$$E_K(M) = M \oplus (K \| K \| K \cdots),$$

where the key *K* is repeated *n/2* times. "||" here is **String Concatenation Operator.**

d. The decryption algorithm for a ciphertext C is the same as the encryption algorithm:

$$D_K(C) = C \oplus (K \| K \| K \cdots).$$

Implement a brute-force decryption attack for this cryptosystem and test it on randomly generated English character message. Automate the process of detecting whether a decrypted message is English characters.

Graduate students task and bonus task for undergraduate students:

The randomly generated message has to be an English words message rather than English character message. That means you have to use English words dictionary in your program. Thus, the brute force will continue until find an English words message.

Instruction:

1. You should use Java programming language to do this assignment and follow the structure of the demo work.
2. Your work should be in one ".java" file named by "*CampusID*A1.java".
3. Your program should be runnable without any error or exception. Any program has errors or exceptions will receive 0 as grade.
4. A Copied program will receive 0 as grade.
5. Each step should finish in one specific method. Please refer to the "Assignment1Demo.java" file.
6. Please states clearly you are an undergraduate student of graduate student in the comments board when you submit your work and also in the first line of your program.

Deadline: Sunday, Feb. 11th, 11:59 pm
Late deadline: Thursday, Feb. 15th, 11:59 pm