CS 430: Cyber Security

Cryptomatic (15 pts)

DUE: End of Day January 25th , 2019

The Jean-Tailléfer & Pierre-Wacozyk cryptosystem is defined as follows:

1. Keys are 16-bit values.
2. Messages are strings with an even number of characters. If the input string is odd, add a blank at the end of the string.
3. The encryption of a message M of length n (in bytes) is given by:

**Ek (M) = M  (K || K || …),**

where the key K is repeated n/2 times.

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

**Dk (M) = M  (K || K || …).**

**Your task:**

1. (5 points) Implement the cryptosystem above to encrypt and decrypt a file for a given key.
2. (5 points) Implement a brute-force decryption attack for this cryptosystem.
3. (5 points) Write a short and concise report (two pages maximum) on your brute force algorithm that explains how it decrypt the message with brute force. Don’t forget to include short examples to backup your claim. The idea of the report is to provide an overview of your algorithm and the program without having to go through the source code.

**Requirements & Deliverables:**

1. You are to work alone but you can discuss the problem with your classmates.
2. Your program must consist of a single JAVA file and a test text file is available at MUOnline.
3. **Use two characters for the key (instead of a long binary string of 0s and 1s)**.
4. The program must have a menu with three option (GUI/TUI):
   1. Enter the filename and key to encrypt
   2. Enter the filename and key to decrypt
   3. Enter the filename to brute force (print the key to the screen and the decrypted text to a file)
5. We will run your program so be sure to provide detailed instructions and to comment the code sufficiently. Source code(s) without proper comments will receive deductions up to 10 points. Remember, proper comments != over commenting.
6. Note: if you are using pure brute force with a large dictionary, it may take too long to decrypt without a key. Make sure that you write your program efficiently enough so that it should not take more than five minutes to crack a file.
7. Prof. Thompson claimed that he wrote the fastest brute force algorithm. Can you beat his time?\*