Hacettepe University
Department of Computer Engineering
BBM465 Information Security Laboratory
Experiment 1

Subject:	Block Cipher
Language:	Java / C++
Due Date:	4/11/2019 - 23:59

1 Experiment

You are expected to develop a simple file encryption/decryption tool. The requirements are below:

- The program must support three encryption modes (CBC, OFB, CTR) and two encryption algorithms (AES, DES). However, these modes must be based on Electronic Code Book (ECB) scheme. In other words, you can not directly employ prebuilt CBC,OFB and CTR modes. Instead, you need to implement these modes via ECB mode by hand.

- The program must be executed as follows:
  Encryption:
  FileCipher −e −i infile −o outfile algorithm mode key_file
  Example:
  ```
  FileCipher -e -i textfile.txt -o coded.txt AES CBC mykeyfile.txt
  ```
  Decryption:
  FileCipher −d −i infile −o outfile algorithm mode key_file
  Example:
  ```
  FileCipher -d -i coded.txt -o plain.txt AES CBC mykeyfile.txt
  ```
  Explanations of these parameters as follows:

    * $-e$ or $-d$ specifies whether the program will do encryption or decryption
    * $-i\ infile$ specifies the name of the input file
    * $-o\ outfile$ specifies the name of the output file
    * *algorithm* specifies the encryption/decryption algorithm, which can be AES or DES
    * *mode* specifies the mode of the encryption/decryption algorithm, which can be CBC, OFB or CTR.
    * *key_file* contain the initialization vector and key values used for encryption/decryption operation

- All encrypted and decrypted files should be placed in the folder where the original input file is located.

- The key file must be consist of Initialization Vector, Key and Nonce value as follows:
  $IV - K - Nonce$

- Block size for DES has been selected as 64 while 128 has been preferred for AES.

- You must record all encryption/decryption operations and their execution times to the file named *run.log* as in the following format:
  infile outfile enc/dec algorithm mode exec_time

  Example run.log content

  ```
  inputfile.txt coded.txt enc AES OFB 134
  coded.txt inputfile.txt dec AES OFB 78
  sample.txt enc.txt enc DES CBC 66
  enc.txt original.txt dec DES CBC 45
  ```

  Execution time should be given in milliseconds. Your program should create *run.log* file if it does not exist in the working directory of the program. Otherwise, the program should open the existing file and append the log entry to the end of the file.

- You should not modify the original file.

2 Notes

1. In Java, you can use standard crypto API. In C++, you can use crypto++ API.

2. You should prepare a report involving your approach and details of the implementation you have coded. You must write down the names and ids of your teammates in the report in order to be evaluated correctly.

3. You can ask questions about the experiment via Piazza group (`piazza.com/hacettepe.edu.tr/fall2019/bbm465`).

4. Late submission will not be accepted!

5. T.A. as himself has right to partially change this document. However, the modifications will be announced in the Piazza system. In case, it is your obligation to check the Piazza course page periodically.

6. For Java, you must compile and test your code on Eclipse Platform for Windows before submission. For C++ based implementations, you should compile your code in Ubuntu 16.04 or 18.04

7. You are going to submit your experiment to online submission system: `www.submit.cs.hacettepe.edu.tr`

   The submission format is given below:
   <Group id>.zip
   −[java | cpp]/
   −−*.[java | cpp]
   −[report.pdf]

3 Policy

All work on assignments must be done with your own group unless stated otherwise. You are encouraged to discuss with your classmates about the given assignments, but these discussions should be carried out in an abstract way. That is, discussions related to a particular solution to a specific problem (either in actual code or in the pseudocode) will not be tolerated. In short, turning in someone elses work(from internet), in whole or in part, as your own will be considered as a violation of academic integrity. Please note that the former condition also holds for the material found on the web as everything on the web has been written by someone else.