Hacettepe University Computer Engineering Department Information Security Lab.

Homework 1

Subject : Block Ciphers
Due Date : 02.11.2022
Language : Java
T.A. : Ali Baran TAŞDEMİR

Introduction:

You are expected to develop a simple encryption/decryption tool name *FileCipher*.

Requirements:

For the tool *FileCipher*, the requirements are listed below:

- The program must support four encryption modes (CBC, CFB, OFB, CTR) and two encryption algorithms (DES, 3DES). These modes must be implemented via Electronic Code Book (ECB) scheme. You can not use prebuild modes except ECB.[1]
- The program must be executed by command line arguments and print results on files.
- All encrypted and decrypted files should be placed in the folder where the original input file is located.
- Block size for DES and 3DES has been selected as 64.
- You must record all operations (encryption/decryption) and their execution time (in ms) in a log file. (named *run.log*)
- Don't modify the input file via the program.

Implementation Details

Arguments

The program must be executed by command line arguments. The arguments are listed below;

$FileCipher\ -e\ -i\ inputFile\ -o\ outFile\ algorithm\ mode\ key\_file$

- $-e$ or $-d$ denotes encryption and decryption. To encrypt input use $-e$, to decrypt the input use $-d$.
- $-i$ *inputFile* denotes the name/path of the input file.
- $-o$ *outFile* denotes the name/path of the output file.

[1] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

- *algorithm* denotes the name of the encryption/decryption algorithm, which can be DES or 3DES.
- *mode* denotes the mode of the encryption/decryption algorithm, which can be CBC, CFB, OFB, or CTR.
- *key_file* denotes the name/path of the file that contains the initialization vector, key, and nonce values.

Examples:

Encryption:

```
FileCipher −e −i inputfile.txt −o encrypted.txt DES CBC key.txt
FileCipher −e −i sample.txt −o secret.txt 3DES CTR key.txt
```

Decryption:

```
FileCipher −d −i encrypted.txt −o decrypted.txt DES CBC key.txt
FileCipher −d −i secret.txt −o solved.txt 3DES CTR key.txt
```

Key File

The key file must consist of Initialization Vector (IV), Key, and Nonce values. Each value must be separated by "-" in the file. The content of the key file;

IV - Key - Nonce

An example of the content of the key file:

key_example1.txt

```
9eRecAhatUvYduFYPYbU - 5YBuFATucUweceMY - 3YXysuZy6YG49YKasa1U
```

or;

simple_key.txt

```
write21Anything56For33IV2 - Also5For,The1Key97 - it2Is5ok7If0you5Keep7Secret
```

Log File

You must record all runs and their execution time in a log file. The execution time should be in milliseconds. And the log file should be named *run.log* and placed in the folder where the original input file is located. Each line in the log file must be recorded in the following format:

inputFile outFile encordec algorithm mode execution_time

An example of the content of the log file:

run.log

```
inputfile.txt encrypted.txt enc DES CBC 64
encrypted.txt decrypted.txt dec DES CBC 51
sample.txt secret.txt enc 3DES CTR 78
secret.txt solved.txt dec 3DES CTR 59
```

Your program should create *run.log* file if it does not exist in the working directory. Otherwise, the program should open the existing log file and append the new entry at the end of the file.

Notes:

1. You can use crypto API. But you can not use prebuild modes except ECB.
2. You must submit the homework in groups of two.
3. You should prepare a report that describes your approach to the problem with the details of your implementation. You must write down all group members' names and ids. Reports will be graded too.
4. You can ask your questions about the homework via Piazza. (`www.piazza.com/hacettepe.edu.tr/fall2022/bbm465`)
5. T.A. as himself has the 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. You must compile and test your code on Eclipse Platform for Windows before submission.
7. You will submit your work via the submission system.
   (`www.submit.cs.hacettepe.edu.tr`)
   The submission format is given below:
   → <student id.zip>
   → src /*.java
   → report.pdf

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.