CS6500 - Network Security
Assignment 1: OpenSSL interface and performance analysis

Instructor: Krishna M. Sivalingam
Assigned on: *Aug. 13, 2017*
Due on: *Aug. 22, 2017, 11PM on Moodle*

The objective of this assignment is to understand and use the OpenSSL (`http://openssl.org` API, for invoking existing cryptographic algorithmic implementations.

1 Symmetric Encryption

The first part is to invoke the necessary symmetric cryptographic algorithms.

The following inputs are obtained from the command line:

`./myenc -o <oper> -a <alg> -m <mode> -k <keysize> -i <inpfile> -o <outfile>`

The possible choices for each command line argument are:

- Operation: Enc, Dec
- Algorithm: AES, DES, 3DES
- Mode: CBC, ECB, CTR
- Key size: depending on the algorithm one of 56, 112, 168, 128, 192

The objective is to obtain the relevant key from the user input passphrase and call the associated OpenSSL routines for encryption and decryption. The data from the input file is either encrypted or decrypted (based on the command line operation specified) and stored in the output file. Base64 encoding can also be used.

2 Performance evaluation

The performance metrics to be measured are: (i) Mean Block encryption time, (ii) Mean Block Decryption time, for each algorithm.

For DES, the parameters varied are: (i) filesize (10KB, 100KB), (ii) all three modes specified. For each filesize, report the average times across all blocks of the file.

For 3DES, the parameters varied are: (i) filesize (10KB, 100KB), (ii) all three modes specified; (iii) two choices for the keysize (112 and 168). For each filesize, report the average times across all blocks of the file.

For AES, the parameters varied are: (i) filesize (10KB, 100KB), (ii) all three modes specified; (iii) two choices for the keysize (128 and 192). For each filesize, report the average times across all blocks of the file.

The performance values are to be presented in Tabular form, one for each encryption algorithm. The table should also include the time required for a successful brute-force attack for each of the algorithms/keysize combinations, based on extrapolation of the average times obtained. Decide on a suitable table format. The report should specify the system configuration used (CPU, Memory, etc.).

3 What to Submit on IITM Moodle

A single tar.gz file with name ROLLNO-Lab1.tgz containing:

- Source files and Makefile
- PDF of the performance study report
- A README File that explains how to compile and run the program; whether your programs works correctly or whether there are any known bugs/errors in your program.

4 Grading

- Symmetric Encryption and Decryption: 60 points (20 per algorithm)
- Performance Study and Report: 30 points (10 per algorithm)
- Viva Voce Exam: 10 points

5 Policies

- This is an INDIVIDUAL assignment. Please refer to first day handout (on Moodle) regarding penalties for any form of academic dishonesty, plagiarism, etc. There should be no downloaded code.
- Plagiarism Checking Software will be used.
- The program must be written in OpenSSL C/C++ interface.
- Refer:

  `https://wiki.openssl.org/index.php/Libcrypto_API`
  `https://wiki.openssl.org/index.php/EVP_Symmetric_Encryption_and_Decryption`
  `https://www.feistyduck.com/library/openssl-cookbook/`
  `http://shop.oreilly.com/product/9780596002701.do`