# LAB 1

## OpenSSL interface and performance analysis

Name: Ravindra kumar Roll No: CS21M050

**Question 1**:
Code provided in the zip file.

**Question 2**:

PERFORMANCE STUDY:

Encryption:

| ENCRYPTION | | | | | |
|---|---|---|---|---|---|
| Algo | Mode | Key size (in bits) | Average time per block for 10KB files (in ns) (A) | Average time per block for 1MB files (in ns) (B) | Mean Block Encryption time (in ns) (Average(A+B)) |
| 3DES | ECB | 168 | 348.3985936 | 321.4172157 | 337.340257325 |
| 3DES | CBC | 168 | 349.5134375 | 330.0317825 | |
| AES | ECB | 128 | 61.4601562 | 27.0429809 | 49.56406215 |
| AES | CBC | 128 | 74.4684374 | 35.2846741 | |
| AES | ECB | 192 | 71.2387275 | 28.5464676 | 54.9633837 |
| AES | CBC | 192 | 81.5053163 | 38.5630234 | |
| AES | ECB | 256 | 65.8618749 | 25.2377121 | 54.88741535 |
| AES | CBC | 256 | 83.5135937 | 44.9364807 | |

Decryption:

| DECRYPTION | | | | | | |
|---|---|---|---|---|---|---|
| Algo | Mode | Key size (in bits) | Average time per block for 10KB files (in ns) (A) | Average time per block for 1MB files (in ns) (B) | Mean Block Decryption time (in ns) (Average(A+B)) | Brute force attack time (Extrapolated) |
| 3DES | ECB | 168 | 309.1524858 | 315.7510671 | 313.294403425 | $2^{167}$*313.294403425 ns = $1.858468934\times10^{36}$ years |
| 3DES | CBC | 168 | 311.900355 | 316.3737058 | | |
| AES | ECB | 128 | 43.8840911 | 24.9215931 | 39.155834225 | $2^{127}$ * 39.155834225 ns = $211.251267581\times10^{21}$ years |
| AES | CBC | 128 | 51.6083568 | 36.2092959 | | |
| AES | ECB | 192 | 54.3741477 | 25.0453904 | 42.863402175 | $2^{191}$*42.863402175 ns = $4.265885594\times10^{42}$ years |
| AES | CBC | 192 | 61.7310676 | 30.303003 | | |
| AES | ECB | 256 | 56.2877841 | 26.9004329 | 42.599667225 | $2^{255}$ * 42.599667225 ns = $78.207516311\times10^{60}$ years |
| AES | CBC | 256 | 61.7842185 | 25.4262334 | | |

Hardware configuration of the system:
Brand: HP
Model: 15-BS164TU
Ram: 8GB DDR4 (2400 MHz)
Processor: Intel Core i5 8th Gen 8250U- Quadcore
Speed 1.6 GHz Turbo Boost Upto 3.4 GHz
Cache 6 MB
Hard disk: 1TB HDD (5400 RPM)

OS: Ubuntu 18.04 (64 bit)

**Question 3**:

FILE: l1-inp1.txt
Time required is(in millisec): 91.399884

FILE: input/l1-inp2.txt
Time required is(in millisec): 76.407224

FILE: l1-inp3.txt
Time required is(in millisec): 79.764578

FILE: l1-inp4.txt
Time required is(in millisec): 79.152201

FILE: l1-inp5.txt
Time required is(in millisec): 76.337308