

NETWORK SECURITY LAB 2 REPORT

**NAME: TRAN THI THOA
ID: S1242006**

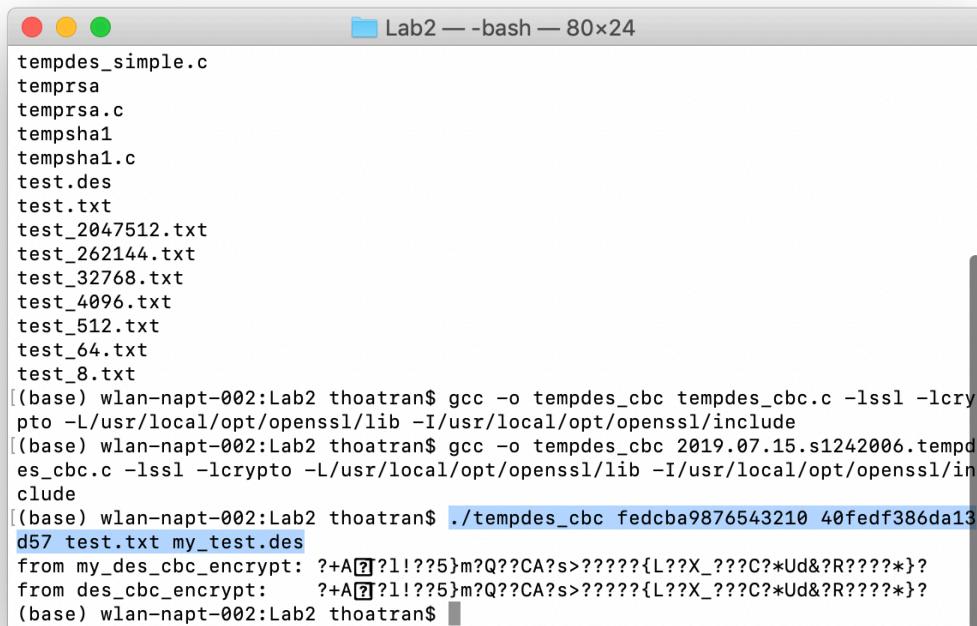
Problem 1: DES encryption/ decryption

The implementation of the tool to encrypt and decrypt files using DES in mode CBC is in the file “2019.07.15.s1242006.tempdes_cbc.c”

To compile and run the file, run the following command lines (on Mac OS):

```
gcc -o tempdes_cbc 2019.07.15.s1242006.tempdes_cbc.c -lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include  
./tempdes_cbc fedcba9876543210 40fedf386da13d57 test.txt my_test.des
```

The result will be:



```
tempdes_simple.c  
temprsa  
temprsa.c  
tempsha1  
tempsha1.c  
test.des  
test.txt  
test_2047512.txt  
test_262144.txt  
test_32768.txt  
test_4096.txt  
test_512.txt  
test_64.txt  
test_8.txt  
[(base) wlan-napt-002:Lab2 thoatran$ gcc -o tempdes_cbc tempdes_cbc.c -lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include  
[(base) wlan-napt-002:Lab2 thoatran$ gcc -o tempdes_cbc 2019.07.15.s1242006.tempdes_cbc.c -lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include  
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes_cbc fedcba9876543210 40fedf386da13d57 test.txt my_test.des  
from my_des_cbc_encrypt: ?+A[?]!??5}m?Q??CA?s>?????{L??X_??C?*Ud&?R????*}?  
from des_cbc_encrypt: ?+A[?]!??5}m?Q??CA?s>?????{L??X_??C?*Ud&?R????*}?  
(base) wlan-napt-002:Lab2 thoatran$
```

We can see that the encrypted texts by using built-in function `des_cbc_encrypt` and my DES-CBC function are the same.

Then, to see file `test.des`, run the following command line:

```
less test.des
```

The output will be:



```
?+A[?]!<E7><CF>^N5]^Zm<E2>Q<C0><FE>CA<9B>s><B5><92><EF><F3><B5><E6>{L<FF><AF>XESC<DE>_<EA><E0>^\<A9>^H<B7>@<E2>*Ud&<95>R^G<BB>^Z<DD>^F<E4><EE>*>}<ED>  
test.des (END)
```

Then, to see the file my_test.des, run the following command line:

```
less my_test.des
```

The output will be:



```
?+A[2]<D5>^N1|<E7><CF>^N5)^Zm<E2>0<C0><FE>CA<9B>s><B5><92><EF><F3><B5><E6>{L<FF>
<AF>XESC<DE>|<EA><E0>^<A9>^H<B7>C<E2>*Ud&<95>R^G<BB>^Z<DD>^F<E4><EE>*><ED>
my_test.des [END]
```

Therefore, we can see that these 2 files are the same , we can conclude that the built-in function des_cbc_encrypt and my DES-CBC encrypt function are similar .

Problem 2: Benchmark DES, RSA and SHA-1

(*) DES encryption/decryption

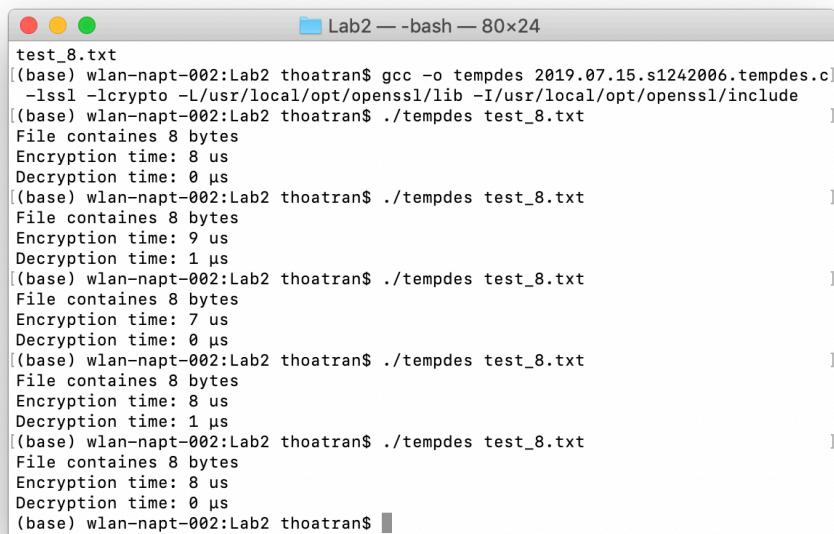
The implement code is In the file 2019.07.15.s1242006.tempdes.c

To compile and run the file, run the following command lines:

```
gcc -o tempdes 2019.07.15.s1242006.tempdes.c -lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include  
./tempdes [input_file]
```

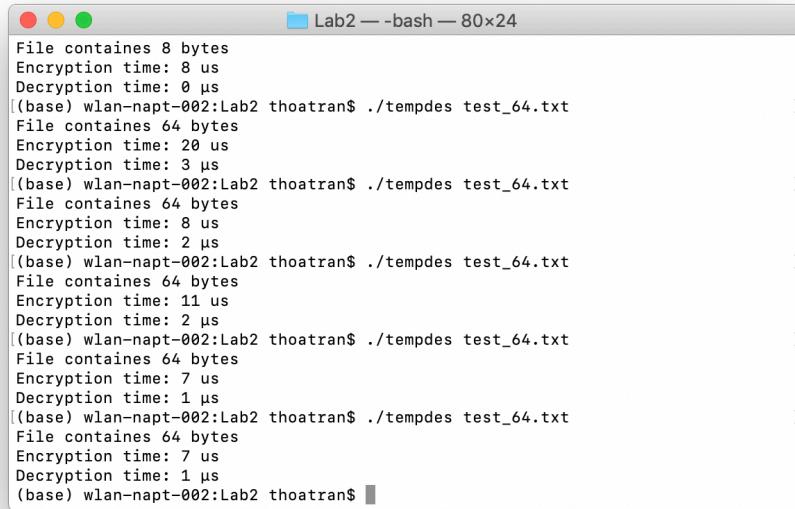
With the input file here is test_8.txt, test_64.txt, test_512.txt,... ,respectively.

+) For the test_8.txt, we have the output:



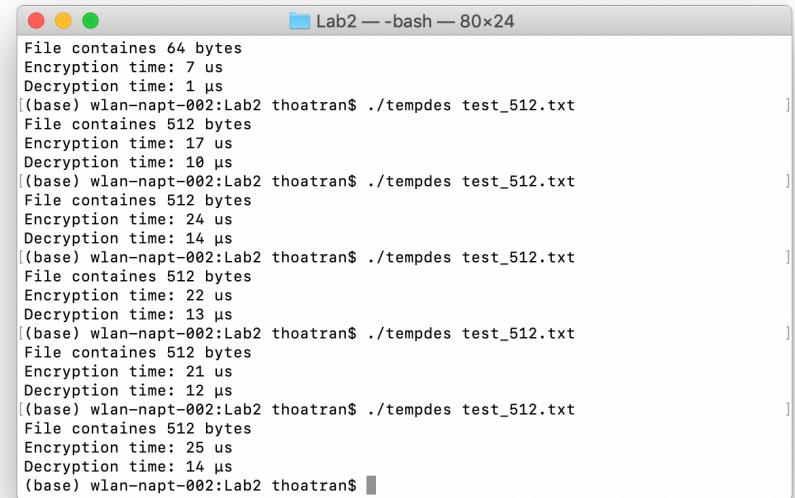
```
test_8.txt
[(base) wlan-napt-002:Lab2 thoatran$ gcc -o tempdes 2019.07.15.s1242006.tempdes.c
 -lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include
 [(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_8.txt
 File contains 8 bytes
 Encryption time: 8 us
 Decryption time: 0 µs
 [(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_8.txt
 File contains 8 bytes
 Encryption time: 9 us
 Decryption time: 1 µs
 [(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_8.txt
 File contains 8 bytes
 Encryption time: 7 us
 Decryption time: 0 µs
 [(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_8.txt
 File contains 8 bytes
 Encryption time: 8 us
 Decryption time: 1 µs
 [(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_8.txt
 File contains 8 bytes
 Encryption time: 8 us
 Decryption time: 0 µs
 (base) wlan-napt-002:Lab2 thoatran$ ]
```

+) For the file test_64, we have the output:



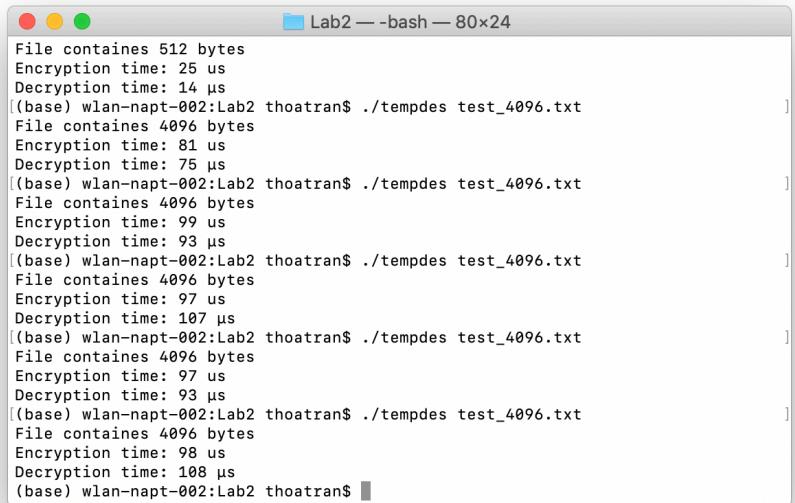
```
File contains 8 bytes
Encryption time: 8 us
Decryption time: 0 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_64.txt]
File contains 64 bytes
Encryption time: 20 us
Decryption time: 3 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_64.txt]
File contains 64 bytes
Encryption time: 8 us
Decryption time: 2 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_64.txt]
File contains 64 bytes
Encryption time: 11 us
Decryption time: 2 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_64.txt]
File contains 64 bytes
Encryption time: 7 us
Decryption time: 1 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_64.txt]
File contains 64 bytes
Encryption time: 7 us
Decryption time: 1 µs
[(base) wlan-napt-002:Lab2 thoatran$]
```

+) For the file test_512.txt, we have the output:



```
File contains 64 bytes
Encryption time: 7 us
Decryption time: 1 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_512.txt]
File contains 512 bytes
Encryption time: 17 us
Decryption time: 10 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_512.txt]
File contains 512 bytes
Encryption time: 24 us
Decryption time: 14 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_512.txt]
File contains 512 bytes
Encryption time: 22 us
Decryption time: 13 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_512.txt]
File contains 512 bytes
Encryption time: 21 us
Decryption time: 12 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_512.txt]
File contains 512 bytes
Encryption time: 25 us
Decryption time: 14 µs
[(base) wlan-napt-002:Lab2 thoatran$]
```

+) For the file test_4096.txt, the output will be:



```
File contains 512 bytes
Encryption time: 25 us
Decryption time: 14 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_4096.txt]
File contains 4096 bytes
Encryption time: 81 us
Decryption time: 75 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_4096.txt]
File contains 4096 bytes
Encryption time: 99 us
Decryption time: 93 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_4096.txt]
File contains 4096 bytes
Encryption time: 97 us
Decryption time: 107 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_4096.txt]
File contains 4096 bytes
Encryption time: 97 us
Decryption time: 93 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_4096.txt]
File contains 4096 bytes
Encryption time: 98 us
Decryption time: 108 µs
[(base) wlan-napt-002:Lab2 thoatran$]
```

+) For the file test_32768.txt, the output will be:

```
Lab2 — bash — 80x24
File contains 4096 bytes
Encryption time: 98 us
Decryption time: 108 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_32768.txt]
File contains 32768 bytes
Encryption time: 536 us
Decryption time: 484 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_32768.txt]
File contains 32768 bytes
Encryption time: 488 us
Decryption time: 441 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_32768.txt]
File contains 32768 bytes
Encryption time: 566 us
Decryption time: 555 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_32768.txt]
File contains 32768 bytes
Encryption time: 713 us
Decryption time: 689 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_32768.txt]
File contains 32768 bytes
Encryption time: 560 us
Decryption time: 552 us
(base) wlan-napt-002:Lab2 thoatran$
```

+) For the file test_262144.txt, the output will be:

```
Lab2 — bash — 80x24
File contains 32768 bytes
Encryption time: 560 us
Decryption time: 552 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_262144.txt]
File contains 262144 bytes
Encryption time: 7144 us
Decryption time: 3932 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_262144.txt]
File contains 262144 bytes
Encryption time: 4572 us
Decryption time: 3460 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_262144.txt]
File contains 262144 bytes
Encryption time: 5368 us
Decryption time: 3689 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_262144.txt]
File contains 262144 bytes
Encryption time: 4058 us
Decryption time: 3555 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_262144.txt]
File contains 262144 bytes
Encryption time: 3956 us
Decryption time: 3622 us
(base) wlan-napt-002:Lab2 thoatran$
```

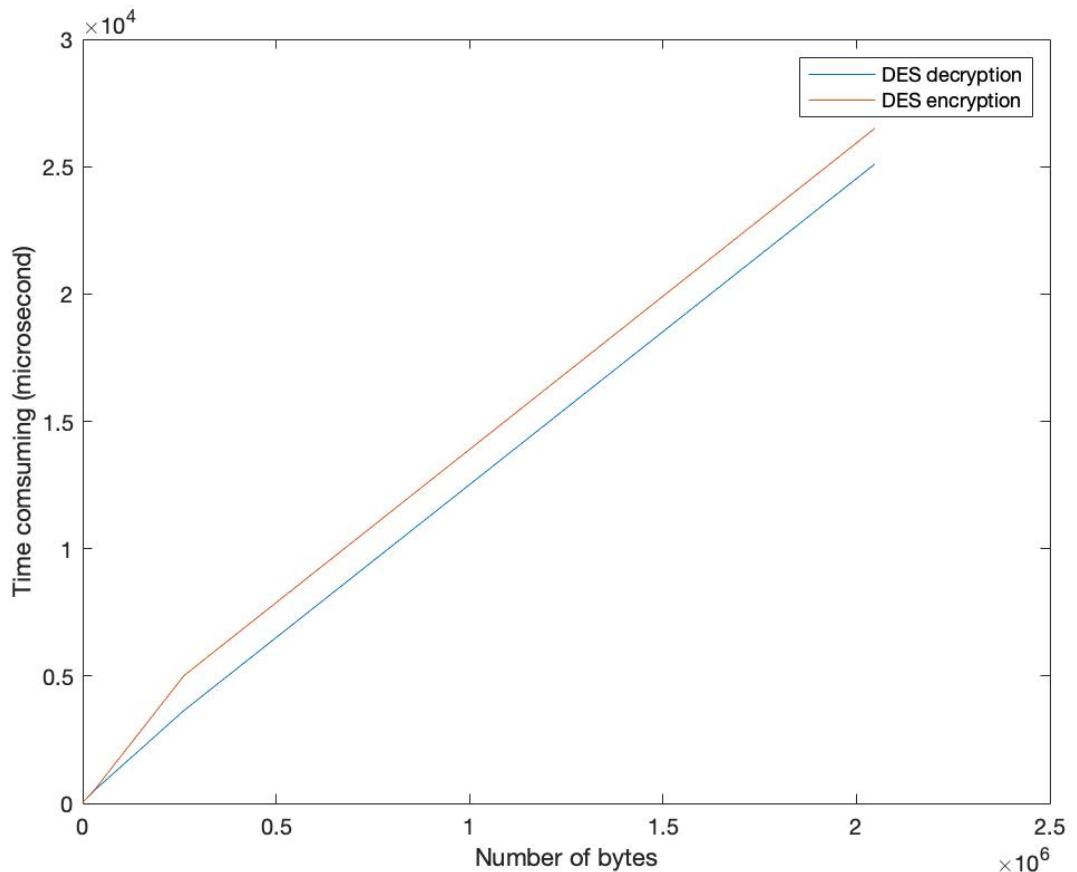
+) For the file test_2047512.txt, the output will be:

```
Lab2 — bash — 80x24
File contains 262144 bytes
Encryption time: 3956 us
Decryption time: 3622 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_2047512.txt]
File contains 2047512 bytes
Encryption time: 29798 us
Decryption time: 24584 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_2047512.txt]
File contains 2047512 bytes
Encryption time: 25556 us
Decryption time: 24885 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_2047512.txt]
File contains 2047512 bytes
Encryption time: 25558 us
Decryption time: 25135 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_2047512.txt]
File contains 2047512 bytes
Encryption time: 25741 us
Decryption time: 25489 us
[(base) wlan-napt-002:Lab2 thoatran$ ./tempdes test_2047512.txt]
File contains 2047512 bytes
Encryption time: 25847 us
Decryption time: 25408 us
(base) wlan-napt-002:Lab2 thoatran$
```

From the above results, we get the average time consuming of DES encryption/decryption (μs)

Number of bytes	8	64	512	4096	32768	262144	2047512
DES encryption.	8	10.6	21.8	94.4	572.6	5019.6	26500
DES decryption.	0.4	1.8	12.6	95.2	544.2	3651.6	25100.2

Therefore, we get the graph showing the relation between number of bytes and the time consuming for DES encryption/decryption:



(*) RSA encryption/decryption

The implement code is In the file 2019.07.15.s1242006.temprsa.c

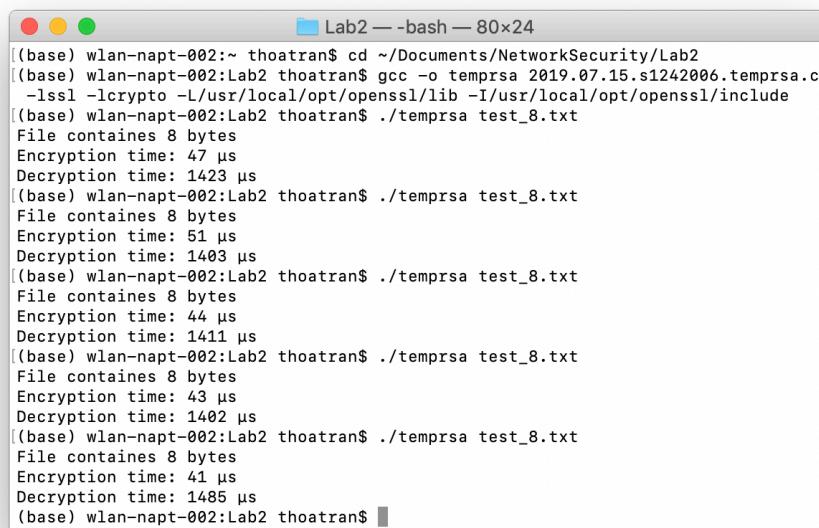
To compile and run the file, run the following command lines:

```
gcc -o tempras 2019.07.15.s1242006.temprsa.c -lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include
```

```
./temprsa [input_file]
```

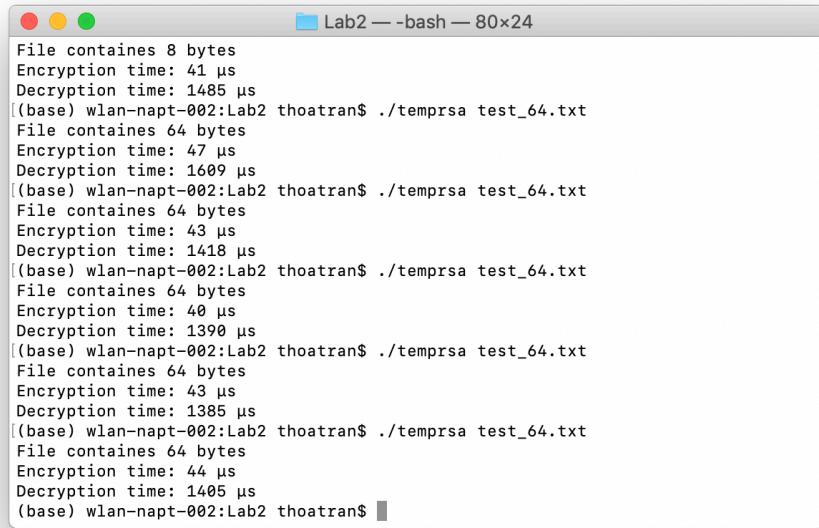
With the input file here is test_8.txt, test_64.txt, test_512.txt,... ,respectively.

+) For the file test_8.txt



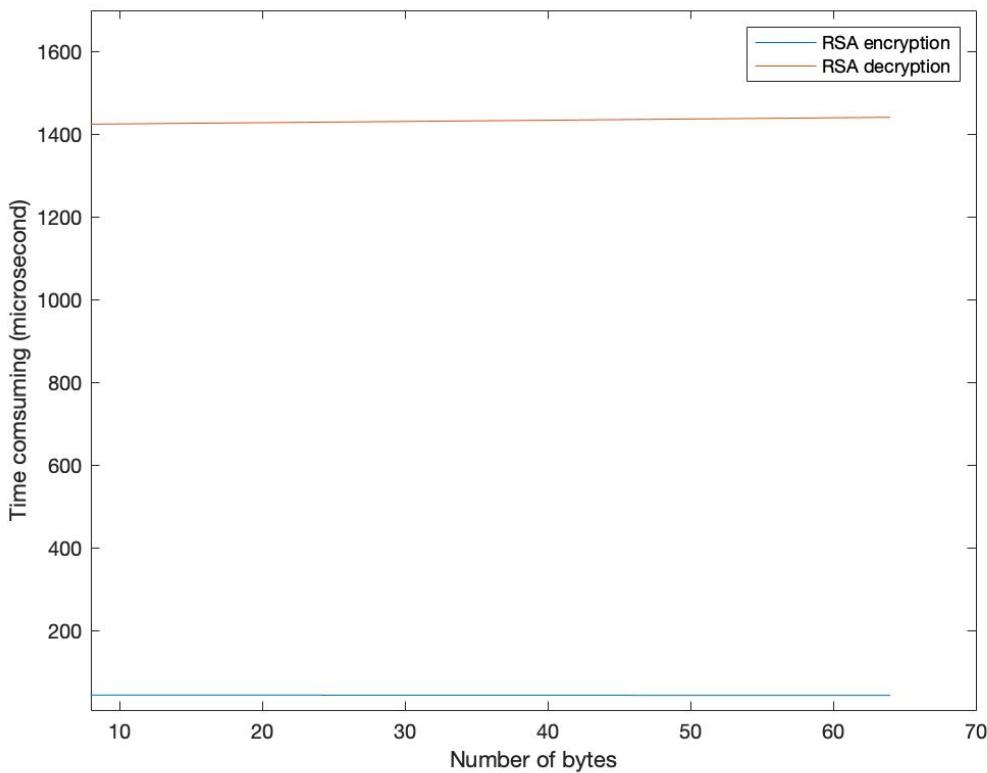
```
(base) wlan-napt-002:~ thoatran$ cd ~/Documents/NetworkSecurity/Lab2
(base) wlan-napt-002:Lab2 thoatran$ gcc -o tempras 2019.07.15.s1242006.temprsa.c
-lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_8.txt
File contains 8 bytes
Encryption time: 47 µs
Decryption time: 1423 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_8.txt
File contains 8 bytes
Encryption time: 51 µs
Decryption time: 1403 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_8.txt
File contains 8 bytes
Encryption time: 44 µs
Decryption time: 1411 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_8.txt
File contains 8 bytes
Encryption time: 43 µs
Decryption time: 1402 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_8.txt
File contains 8 bytes
Encryption time: 41 µs
Decryption time: 1485 µs
(base) wlan-napt-002:Lab2 thoatran$
```

+) For the file test_64.txt



```
File contains 8 bytes
Encryption time: 41 µs
Decryption time: 1485 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_64.txt
File contains 64 bytes
Encryption time: 47 µs
Decryption time: 1609 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_64.txt
File contains 64 bytes
Encryption time: 43 µs
Decryption time: 1418 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_64.txt
File contains 64 bytes
Encryption time: 40 µs
Decryption time: 1390 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_64.txt
File contains 64 bytes
Encryption time: 43 µs
Decryption time: 1385 µs
(base) wlan-napt-002:Lab2 thoatran$ ./temprsa test_64.txt
File contains 64 bytes
Encryption time: 44 µs
Decryption time: 1405 µs
(base) wlan-napt-002:Lab2 thoatran$
```

Because in the implementation we use the RSA_PKCS1_PADDING mode, it just can encrypt the file having the number of bytes smaller than the number of key minus 11 bytes, therefore, it just can encrypt the file test_8.txt and file test_64.txt



We have the graph showing the relation between the number of bytes and the time consuming(μs) of RSA encryption/decryption:

(*) SHA1 encryption:

The implement code is in the file 2019.07.15.s1242006.tempsha1.c

To compile and run the file, run the following command lines:

```
gcc -o tempsha1 2019.07.15.s1242006.tempsha1.c -lssl -lcrypto -L/usr/local/opt/openssl/lib -I/usr/local/opt/openssl/include  
.tempdes [input_file]
```

With the input file here is test_8.txt, test_64.txt, test_512.txt,... ,respectively.

+) For the file test_8.txt

```
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_8.txt  
File contains 8 bytes  
Encryption time: 8 μs  
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_8.txt  
File contains 8 bytes  
Encryption time: 8 μs  
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_8.txt  
File contains 8 bytes  
Encryption time: 8 μs  
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_8.txt  
File contains 8 bytes  
Encryption time: 9 μs  
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_8.txt  
File contains 8 bytes  
Encryption time: 8 μs
```

+) For the file test_64.txt

```
Lab2 -- bash -- 80x15
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_64.txt
File copntains 64 bytes
Encryption time: 11 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_64.txt
File copntains 64 bytes
Encryption time: 7 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_64.txt
File copntains 64 bytes
Encryption time: 23 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_64.txt
File copntains 64 bytes
Encryption time: 7 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_64.txt
File copntains 64 bytes
Encryption time: 11 µs
```

+) For the file test_512.txt

```
Lab2 -- bash -- 80x15
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_512.txt
File copntains 512 bytes
Encryption time: 11 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_512.txt
File copntains 512 bytes
Encryption time: 12 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_512.txt
File copntains 512 bytes
Encryption time: 8 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_512.txt
File copntains 512 bytes
Encryption time: 13 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_512.txt
File copntains 512 bytes
Encryption time: 10 µs
```

+) For the file test_4096.txt

```
Lab2 -- bash -- 80x15
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_4096.txt
File copntains 4096 bytes
Encryption time: 24 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_4096.txt
File copntains 4096 bytes
Encryption time: 24 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_4096.txt
File copntains 4096 bytes
Encryption time: 36 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_4096.txt
File copntains 4096 bytes
Encryption time: 17 µs
][(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_4096.txt
File copntains 4096 bytes
Encryption time: 16 µs
```

+) For the file test_32768.txt

```
Lab2 — bash — 80x15
File copntains 32768 bytes
Encryption time: 74 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_32768.txt]
File copntains 32768 bytes
Encryption time: 73 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_32768.txt]
File copntains 32768 bytes
Encryption time: 139 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_32768.txt]
File copntains 32768 bytes
Encryption time: 185 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_32768.txt]
File copntains 32768 bytes
Encryption time: 73 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_32768.txt]
```

+) For the file test_262144.txt

```
Lab2 — bash — 80x15
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_262144.txt]
File copntains 262144 bytes
Encryption time: 543 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_262144.txt]
File copntains 262144 bytes
Encryption time: 548 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_262144.txt]
File copntains 262144 bytes
Encryption time: 586 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_262144.txt]
File copntains 262144 bytes
Encryption time: 623 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_262144.txt]
File copntains 262144 bytes
Encryption time: 526 µs
```

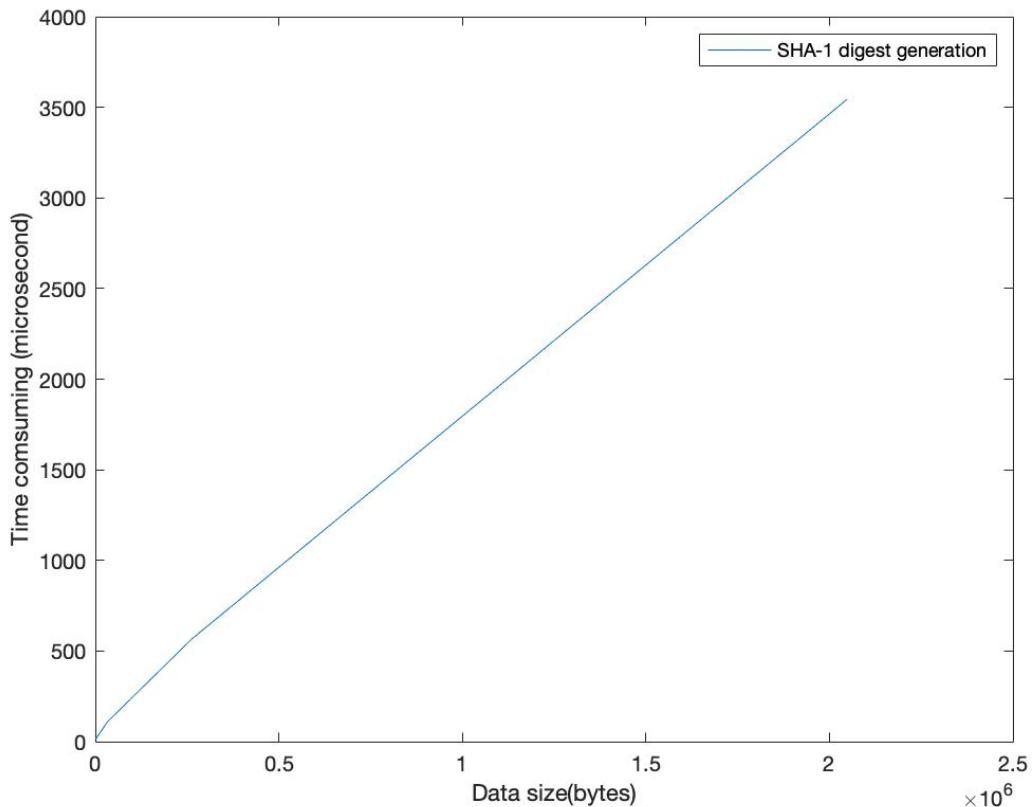
+For the file test_2047512.txt

```
Lab2 — bash — 80x15
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_2047512.txt]
File copntains 2047512 bytes
Encryption time: 4802 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_2047512.txt]
File copntains 2047512 bytes
Encryption time: 2963 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_2047512.txt]
File copntains 2047512 bytes
Encryption time: 3615 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_2047512.txt]
File copntains 2047512 bytes
Encryption time: 3270 µs
[(base) wlan-napt-002:Lab2 thoatran$ ./tempsha1 test_2047512.txt]
File copntains 2047512 bytes
Encryption time: 3065 µs
```

We have the average time consuming of SHA-1 digest generation:

Data size (bytes)	8.	64	512	4096	32768	262144	2047512
SHA1 digest generation.	8.	10.8.	11.8.	23.4	108.8	565.2	3543

Therefore, we have the gray showing the SHA-1 digest generation time when increasing the data size:



From the above graph and figure, we can see that:

+) The RSA encryption time is significantly much bigger than DES encryption time or in other way, DES is much faster than RSA encryption. The reason is while DES encryption is symmetric key encryption, RSA is asymmetric key encryption, involving doing computation with very large numbers, in particular deciphering is computing a large number to a huge power.

+) The DES encryption time consuming and SHA-1 digest generation time consuming increase when increasing the number of bytes in data, but we can see that the SHA-1 digest generation time increasing speed is much slower compared to DES encryption's one. That's because SHA-1 (and many other hashes designed to be cryptographically strong) are based on repeated application of an encryption or decryption routine to fixed-sized blocks of data. Consequently, when computing a hash value of a long string, the algorithm takes proportionally more time than computing the hash value of a small string. Mathematically, we say that the

runtime to hash a string of length N is $O(N)$ when using SHA-1, whereas DES works with the plaintext with 64 bit key. The DES imposes 16 complex rounds to encrypt the data. The 16 rounds are iterated and the ciphers are same but it uses a different key derived, therefore when increasing the data size, the encryption time consuming increases promptly.

+) The RSA decryption time is significantly higher than the RSA encryption time or in other way, the RSA decryption is much slower than RSA encryption, that's because both RSA encryption and decryption involve modular exponentiation, but whereas the public encryption exponent is normally small and fixed, the secret decryption exponent is usually almost as long as the modulus. Thus, doubling the modulus size makes encryption take twice as long, but makes decryption take *four times* as long