ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

THÁI NGỌC DIỄM TRINH – 22521541

CLASS: NT219.O22.ANTT

OFF-CLASS LABS

LAB 4: ECC-BASED DIGITAL SIGNATURE WITH CRYPTOPP/OPENSSL

TP. HỒ CHÍ MINH, NĂM 2024

ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

THÁI NGỌC DIỄM TRINH - 22521541

OFF-CLASS LABS

LAB 4: ECC-BASED DIGITAL SIGNATURE WITH CRYPTOPP/OPENSSL

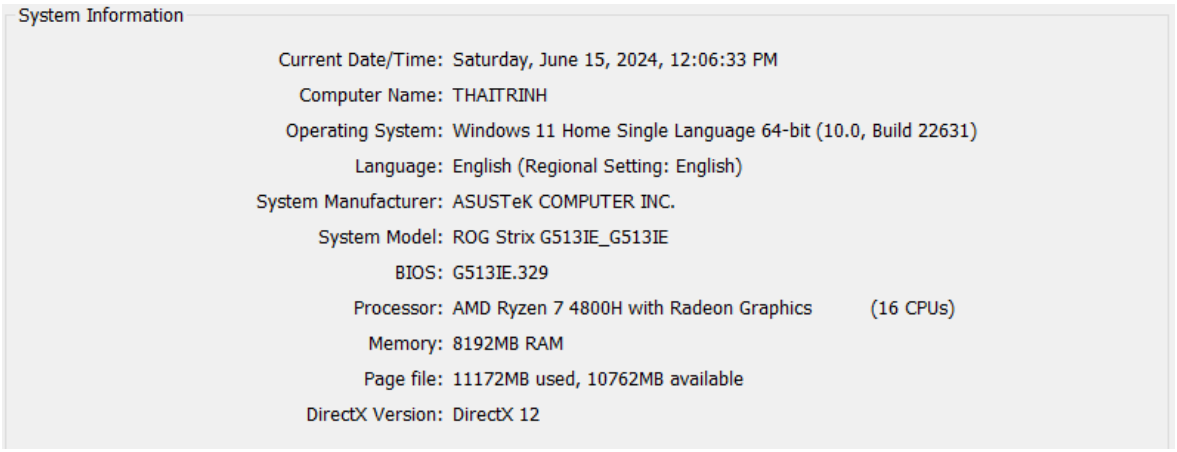
GIẢNG VIÊN HƯỚNG DẪN

TS. NGUYỄN NGỌC TỰ

TP. HỒ CHÍ MINH, NĂM 2024

MỤC LỤC

Chương 1. **HARDWARE RESOURCE**

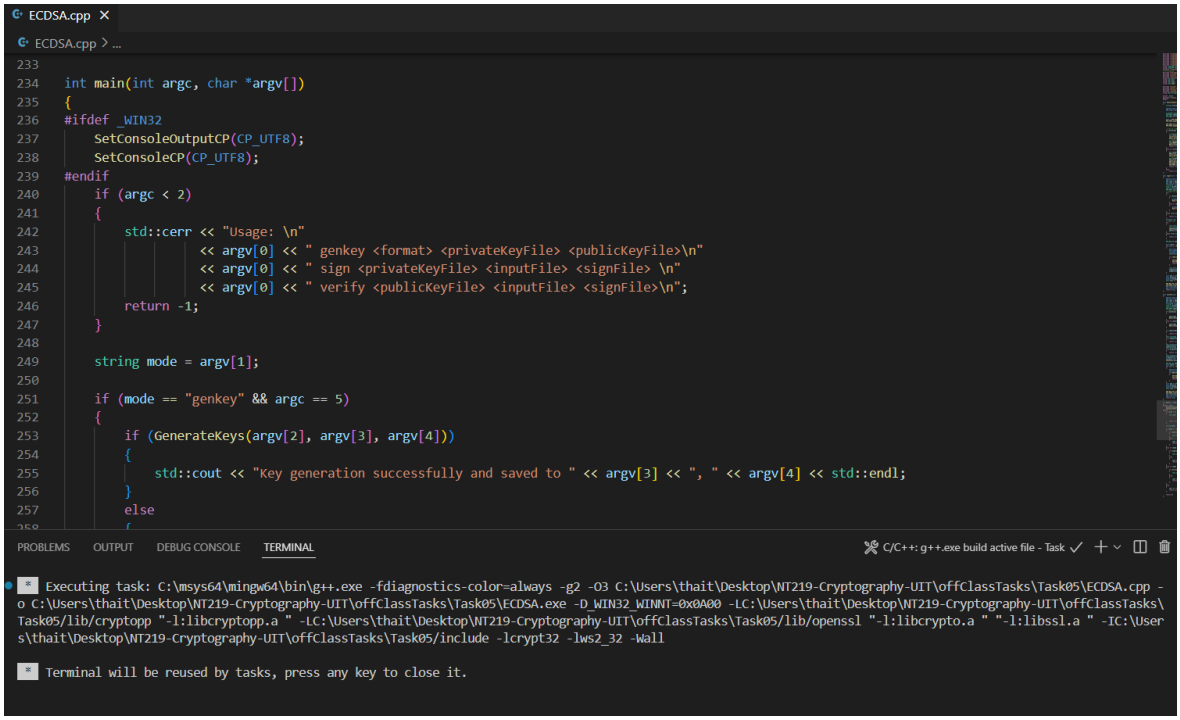


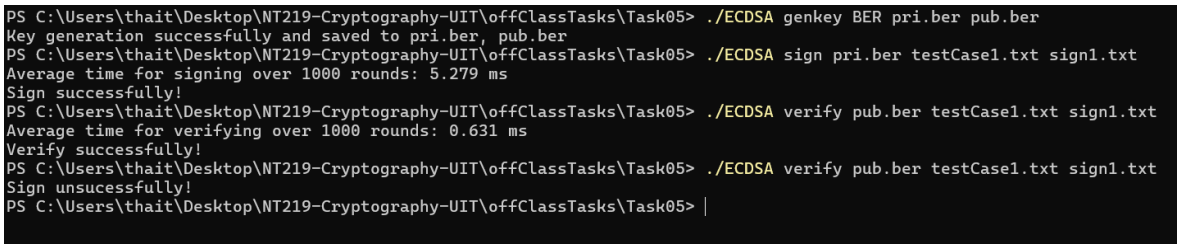
Chương 2. **BUILD TASKS**

2.1. ECDSA

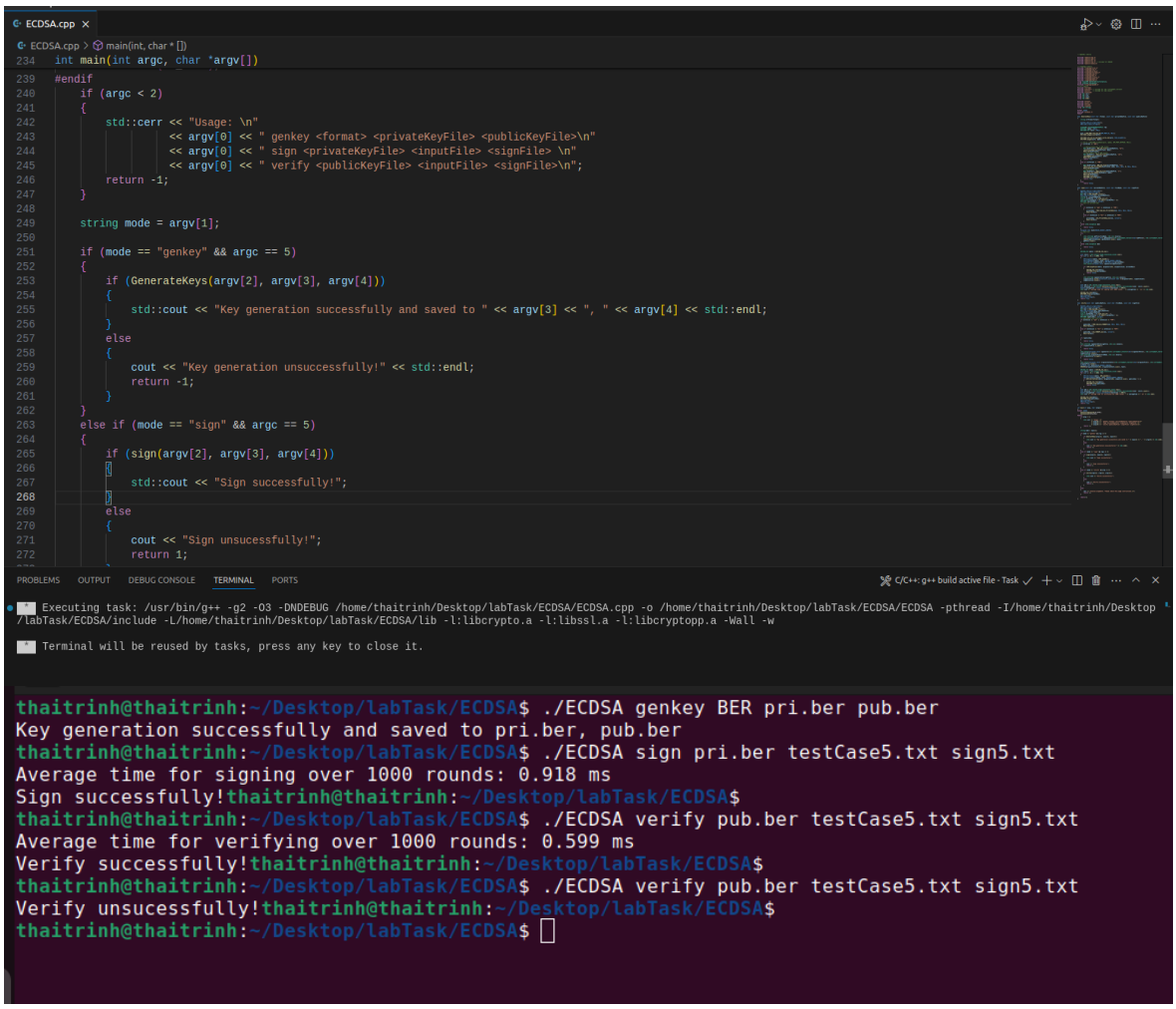
2.1.1. Command Line:

- Windows:



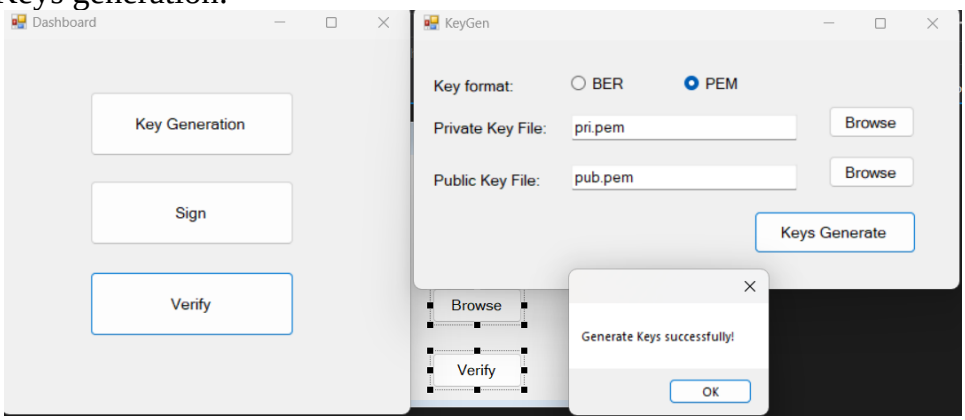


- Ubuntu:

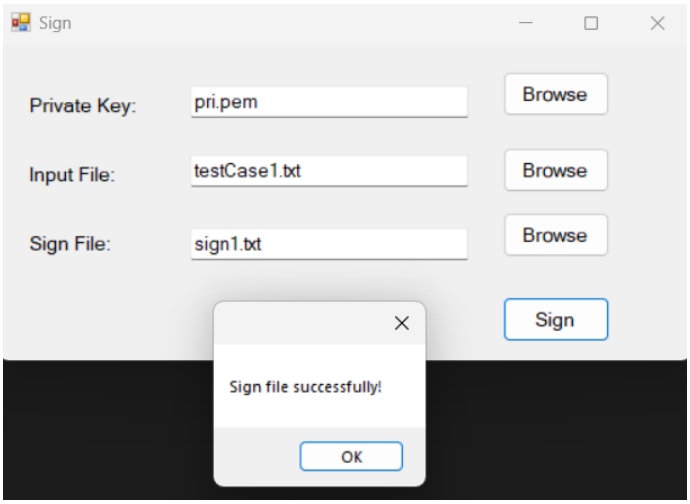

ECDSA.cpp
ECDSA.cpp > main(int, char * [])
int main(int argc, char *argv[])
#endif
if (argc < 2)
{
std::cerr << "Usage: \n"
<< argv[0] << " genkey <format> <privateKeyFile> <publicKeyFile>\n"
<< argv[0] << " sign <privateKeyFile> <inputFile> <signFile> \n"
<< argv[0] << " verify <publicKeyFile> <inputFile> <signFile>\n";
return -1;
}
string mode = argv[1];
if (mode == "genkey" && argc == 5)
{
if (GenerateKeys(argv[2], argv[3], argv[4]))
{
std::cout << "Key generation successfully and saved to " << argv[3] << ", " << argv[4] << std::endl;
}
else
{
cout << "Key generation unsuccessfully!" << std::endl;
return -1;
}
}
else if (mode == "sign" && argc == 5)
{
if (sign(argv[2], argv[3], argv[4]))
{
std::cout << "Sign successfully!";
}
else
{
cout << "Sign unsucessfully!";
return 1;
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
C/C++: g++ build active file - Task
Executing task: /usr/bin/g++ -g2 -O3 -DNDEBUG /home/thaitrinh/Desktop/labTask/ECDSA/ECDSA.cpp -o /home/thaitrinh/Desktop/labTask/ECDSA/ECDSA -pthread -I/home/thaitrinh/Desktop/labTask/ECDSA/include -L/home/thaitrinh/Desktop/labTask/ECDSA/lib -l:libcrypto.a -l:libssl.a -l:libcryptopp.a -Wall -w
Terminal will be reused by tasks, press any key to close it.
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./ECDSA genkey BER pri.ber pub.ber
Key generation successfully and saved to pri.ber, pub.ber
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./ECDSA sign pri.ber testCase5.txt sign5.txt
Average time for signing over 1000 rounds: 0.918 ms
Sign successfully!thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./ECDSA verify pub.ber testCase5.txt sign5.txt
Average time for verifying over 1000 rounds: 0.599 ms
Verify successfully!thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./ECDSA verify pub.ber testCase5.txt sign5.txt
Verify unsuccessfully!thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$

2.1.2. GUI

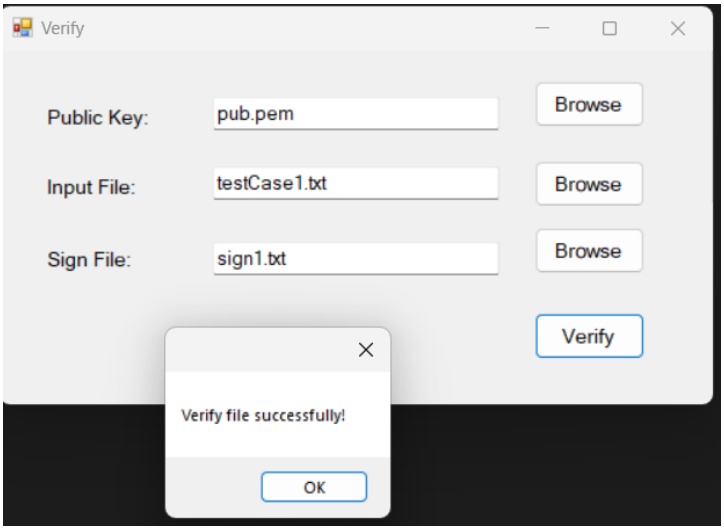
- Keys generation:



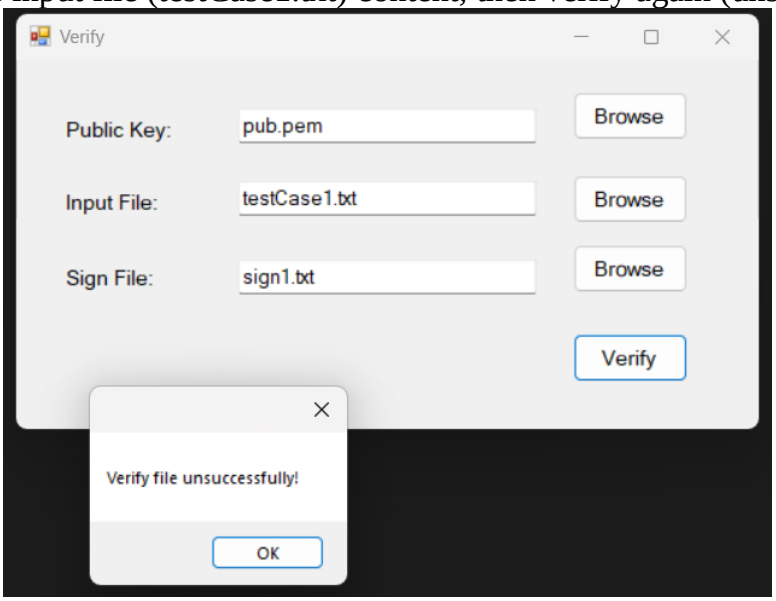
- Sign:



- Verify:

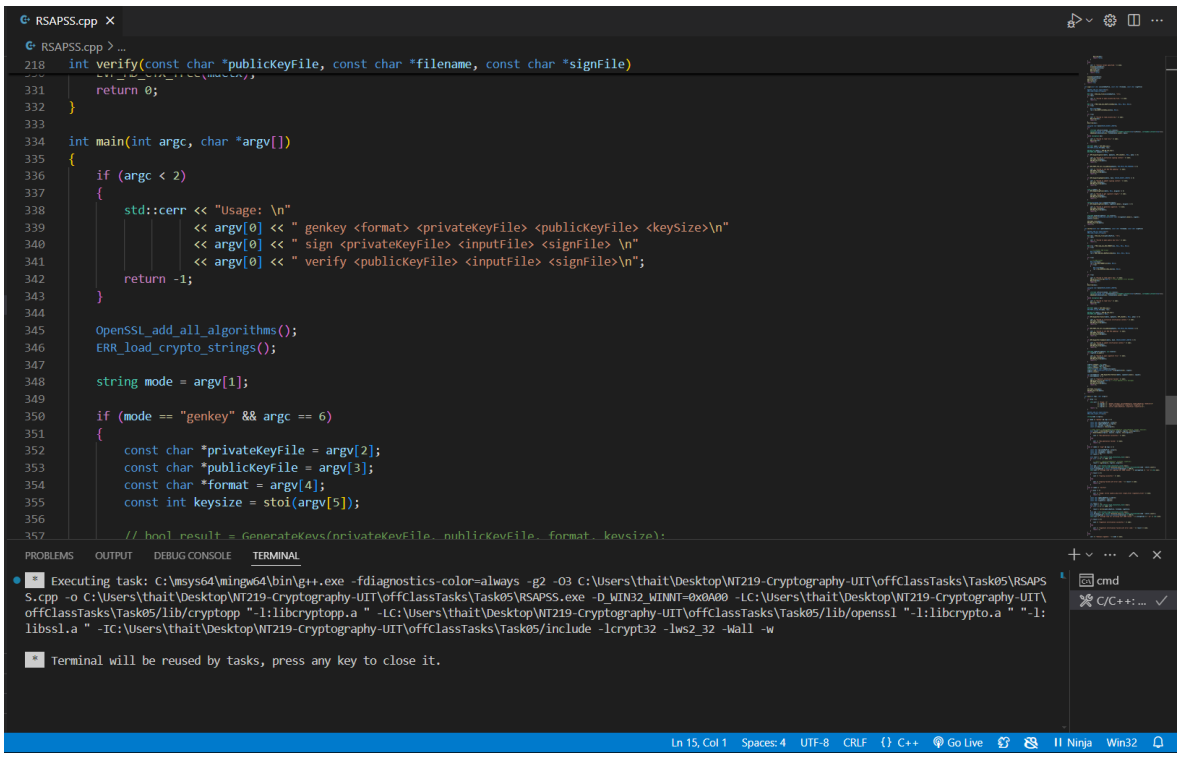


- Change input file (testCase1.txt) content, then verify again (unsuccessfully):



2.2. RSAPSS

- Windows:



```
PS C:\Users\thait\Desktop\NT219-Cryptography-UIT\offClassTasks\Task05> ./RSAPSS genkey PEM pri.pem pub.pem 3072
Key generation successful.
PS C:\Users\thait\Desktop\NT219-Cryptography-UIT\offClassTasks\Task05> ./RSAPSS sign pri.pem testCase1.txt sign1.txt
Average time for signing over 1000 rounds: 6.609 ms
Signing successful.
PS C:\Users\thait\Desktop\NT219-Cryptography-UIT\offClassTasks\Task05> ./RSAPSS verify pub.pem testCase1.txt sign1.txt
Average time for verifying over 1000 rounds: 0.183 ms
Signature verification successful.
PS C:\Users\thait\Desktop\NT219-Cryptography-UIT\offClassTasks\Task05> ./RSAPSS verify pub.pem testCase1.txt sign1.txt
Average time for verifying over 1000 rounds: 0.169 ms
```

- Ubuntu:

RSAPSS.cpp

RSAPSS.cpp > main(int, char * [])

```cpp
}

int main(int argc, char *argv[])
{
    if (argc < 2)
    {
        std::cerr << "Usage: \n"
                  << argv[0] << " genkey <format> <privateKeyFile> <publicKeyFile> <keySize>\n"
                  << argv[0] << " sign <privateKeyFile> <inputFile> <signFile> \n"
                  << argv[0] << " verify <publicKeyFile> <inputFile> <signFile>\n";
        return -1;
    }

    OpenSSL_add_all_algorithms();
    ERR_load_crypto_strings();

    string mode = argv[1];

    if (mode == "genkey" && argc == 6)
    {
        const char *privateKeyFile = argv[2];
        const char *publicKeyFile = argv[3];
        const char *format = argv[4];
        const int keysize = stoi(argv[5]);

        // bool result = GenerateKeys(privateKeyFile, publicKeyFile, format, keysize);
        bool result = GenerateKeys(argv[2], argv[3], argv[4], stoi(argv[5]));
        if (GenerateKeys(argv[2], argv[3], argv[4], stoi(argv[5])))
        {
            cout << "Key generation successful." << endl;
        }
        else
        {
            cerr << "Key generation failed." << endl;
            return -1;
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
*  Executing task: /usr/bin/g++ -g2 -O3 -DNDEBUG /home/thaitrinh/Desktop/labTask/ECDSA/RSAPSS.cpp -o /home/thaitrinh/Desktop/labTask/ECDSA/RSAPSS -pthread -I/home/thaitrinh/Desktop/labTask/ECDSA/include -L/home/thaitrinh/Desktop/labTask/ECDSA/lib -l:libcrypto.a -l:libssl.a -l:libcryptopp.a -Wall -w

*  Terminal will be reused by tasks, press any key to close it.
```

```
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./RSAPSS genkey BER pri.ber pub.ber 3072
Key generation successful.
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./RSAPSS sign pri.ber testCase1.txt sign1.txt
Average time for signing over 1000 rounds: 2.696 ms
Sign file sucessfully!
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./RSAPSS verify pub.ber testCase1.txt sign1.txt
Average time for verifying over 1000 rounds: 0.075 ms
Verify file sucessfully!
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$ ./RSAPSS verify pub.ber testCase1.txt sign1.txt
Average time for verifying over 1000 rounds: 0.077 ms
Verify file unsucessfully! 8
thaitrinh@thaitrinh:~/Desktop/labTask/ECDSA$
```

Chương 3. **COMPUTATION PERFORMANCE**

Number of iterations: 1000

Time counter: mili seconds

3.1. Sign

	ECDSA		**RSAPSS**	
Test case	**Windows**	**Linux**	**Windows**	**Linux**
1 (1KB)	6.803	1.109	6.655	2.37
2 (20KB)	7.458	0.906	6.654	2.376
3 (50KB)	7.63	1.173	6.766	2.46
4 (100KB)	7.944	0.924	6.876	2.755
5 (200KB)	8.195	0.976	6.934	2.937
6 (1MB)	7.832	1.007	7.524	10.257
7 (5MB)	7.844	1.079	17.881	26.167

3.2. Verify

	ECDSA		RSAPSS	
Test case	**Windows**	**Linux**	**Windows**	**Linux**
1 (1KB)	0.635	0.615	0.197	0.076
2 (20KB)	0.635	0.611	0.242	0.11
3 (50KB)	0.63	0.608	0.306	0.185
4 (100KB)	0.643	0.612	0.418	0.323
5 (200KB)	0.658	0.616	0.636	0.594
6 (1MB)	0.682	0.614	3.166	3.942
7 (5MB)	0.658	0.606	13.982	17.371

Chương 4. **COMMENT AND COMPARSION**

4.1. ECDSA

For sign algorimth, Ubuntu has much superior performance compared to Windows, nearly 6 times faster.

For verify algorimth, the difference between Linux and Windows is not large, but Linux is still slightly faster than Windows in all test cases.

With files of different sizes, the time to sign and verify is not significantly different.

4.2. RSAPSS

For both sign and verify algorimthh, Ubuntu has a shorter average run time than Windows.

The larger the file, the slower the running time.

4.3. Conclusion

For files smaller than 200KB in size, running time on RSAPSS can be faster or equal to that on ECDSA.

But for larger files, RSAPSS runs much slower, if the file size is larger, it is slower, while ECDSA has no difference in running time with files of different sizes.