UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

UIT
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

Report Lab 3

Lecturer: Nguyen Ngoc Tu

Report Lab 3

Student Information

Full Name: Trương Đức Hào

Student ID Number: 22520407

Class: ATTT2022.1

Device Information

CPU: AMD Ryzen7-5800H @ 3.2 GHz

Ram: 8 GB DDR4

SSD: 500GB

Display chip name: AMD Radeon Graphics – RTX 3050 NVIDIA

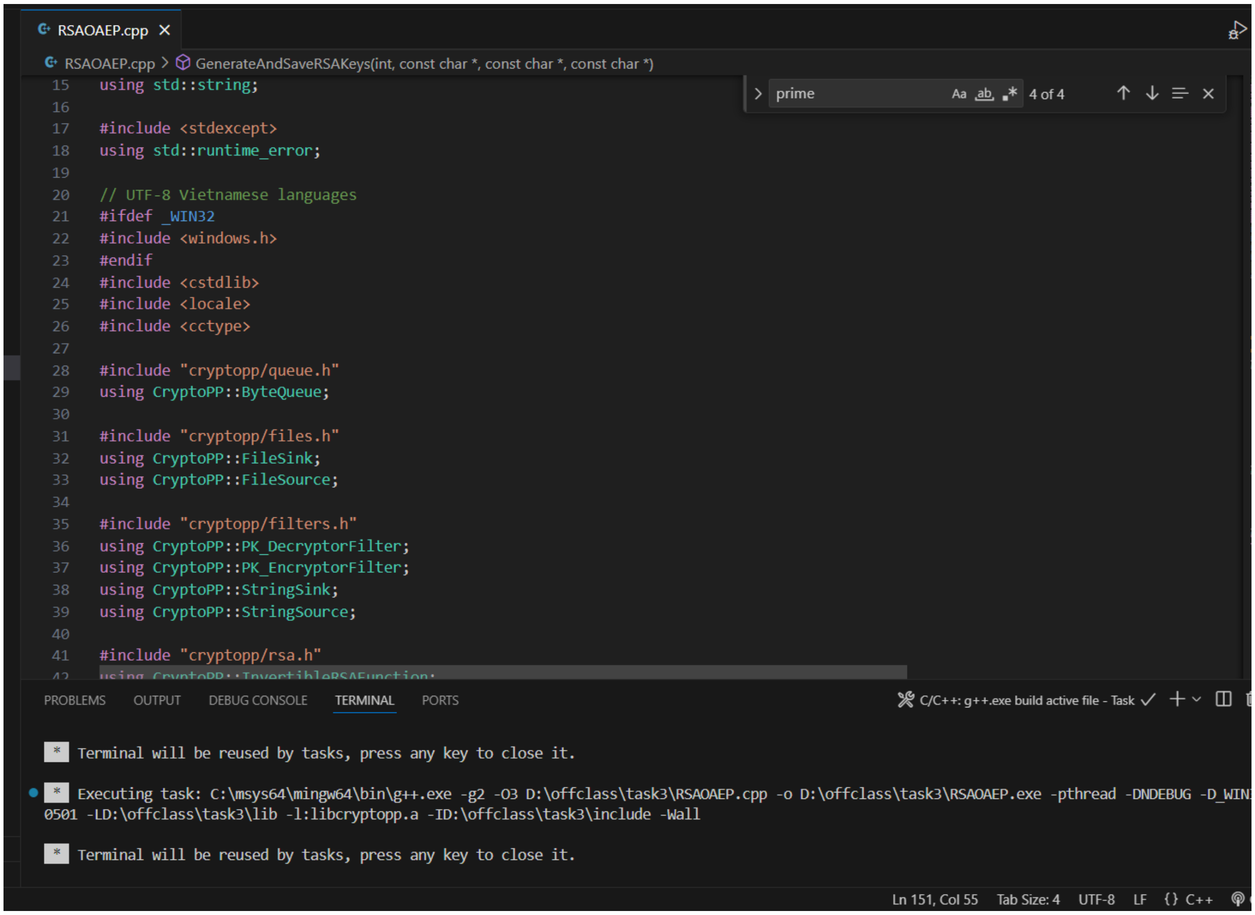
RSAOAEP

Plaintext	Trương Đức Hào – 22520407 – ATTTK17.1 (1kb)
Keysize	3072 bits
Modulo N	514956159860022839763435931121809441133695571638726252546640022006163577282052728658920638260219315737452777247341856117228201194924346362401589855712992727861549915776805933750995426747746122916611774128382482378310872854788546662740497246604218729487781433102299878914784604735543049514838611112648207063622109893212144086889611447025354894740872531416368321833803229467470703152425321737611797552223470439810489677881422078102956772791836093959954397167501975302500946998418879231362724234919007209294696324521159113654667973804945554669760601620356896905237079869734098989086925437198879676909498097080344898409231842689679655098445216665186866342117472714904867567677159057620995546653620827127915305911715459656250454700382573759112371460120181175103394279747984778488543600189876092853641661047755789637241483318011711477559004961197103079871296324865511868290475556888728732769408458272608158396786458528474985418627 1
Prime1 P	238182305176472191262654446343426688553301971186085613843000555733406674860561368996980157264327901732717110466413850344757759035994522800854694032909441792138030165328040520972177592522012328705101405683151354546376453831670905967466918023995718087085740638620491651204853123961921913131716660059808500121109130328360710311254372216582504136744378223986200465827552695899178440608346210601846041570328592204720144442210279972801581912317259114514688104746772613 1
Prime2 Q	216202525825117657197349075092421936226617626605106209317135865093614800783755008052426813662709965173829059114418416576526267157

	52942677913067626296628383418802443158086890694268895249316047339014363132778565531648649685350563116124947163367772491855490744948584322905735704863773131075129284371211402913779106174900768564236143886285205536752714613291170090864628364305793586795998572893825617932658349302255260771513957778032435839532687946129283447459355879 41
PublicExponent E	17
PrivateExponent D	272623849337659150462995492946840292364897655573443310171750599885616011502263209290016808490704343625710293836828041473826694750254065721271429923612760855926702896587720788456409343572336182720559174538555431847341050334888054115568498542319880503846472523407099935896062437801169849743149852941990227268976411119935840987176853119013423179568697222514547935088484062659249195786578111508147422233530072585782023947113694041348624173830972049743505269088677516096061473174791839820131342658331378933198581576468471975392013195355954658422379527642380807576843032936004744906551766904620833845684662529728849482597202920571514395041244453893398627089637552778165335863294450926590164313591084058626136393659905198298438890311148282584732820368356863734729211836174619582627540946243841311375474119905544921353880074632337361104175319448352753690081518000223619682696896150425243673306170470058276742842582109356062400340293

Deploy

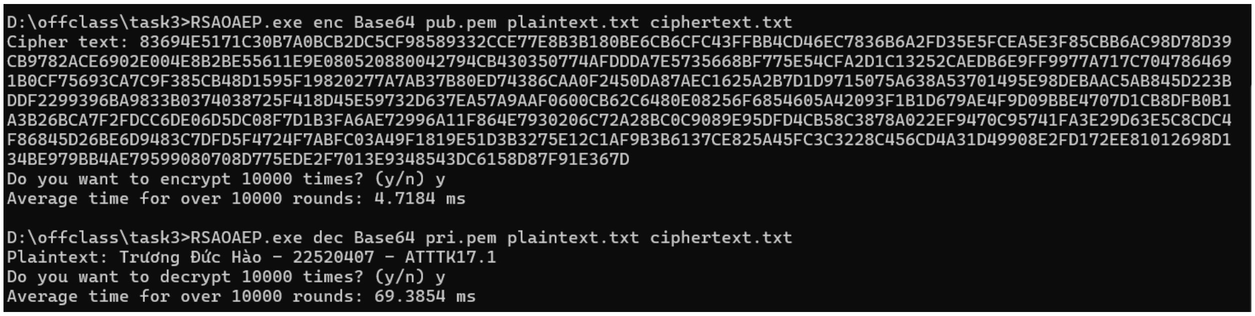
TimeCounter mili seconds	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
Plaintext	4.7184	69.3854	3.3562	52.362
200 Char	5.4543	73.1621	3.8756	63.2542
300 Char	4.5125	65.1652	4.2365	64.3698



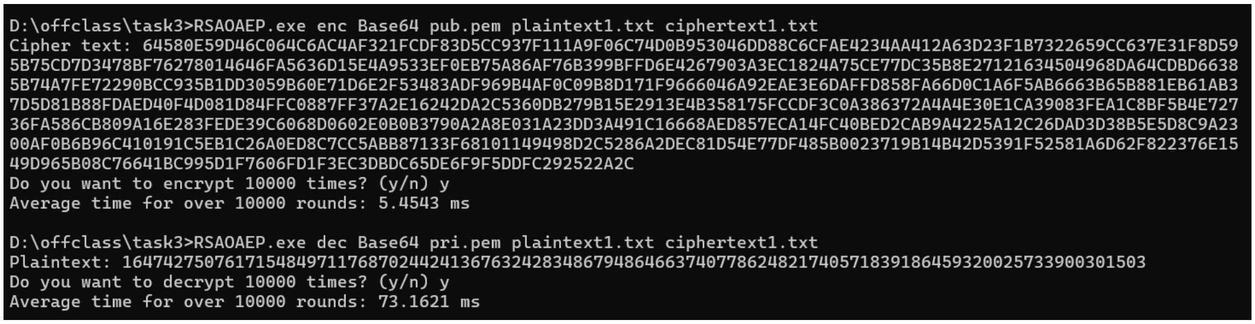
RSAOAEP.cpp
RSAOAEP.cpp > GenerateAndSaveRSAKeys(int, const char *, const char *, const char *)
prime
Aa
ab
.*
4 of 4
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
C/C++: g++.exe build active file - Task
Ln 151, Col 55
Tab Size: 4
UTF-8
LF
{} C++

```
using std::string;

#include <stdexcept>
using std::runtime_error;

// UTF-8 Vietnamese languages
#ifdef _WIN32
#include <windows.h>
#endif
#include <cstdlib>
#include <locale>
#include <cctype>

#include "cryptopp/queue.h"
using CryptoPP::ByteQueue;

#include "cryptopp/files.h"
using CryptoPP::FileSink;
using CryptoPP::FileSource;

#include "cryptopp/filters.h"
using CryptoPP::PK_DecryptorFilter;
using CryptoPP::PK_EncryptorFilter;
using CryptoPP::StringSink;
using CryptoPP::StringSource;

#include "cryptopp/rsa.h"
using CryptoPP::InvertibleRSAFunction;
```

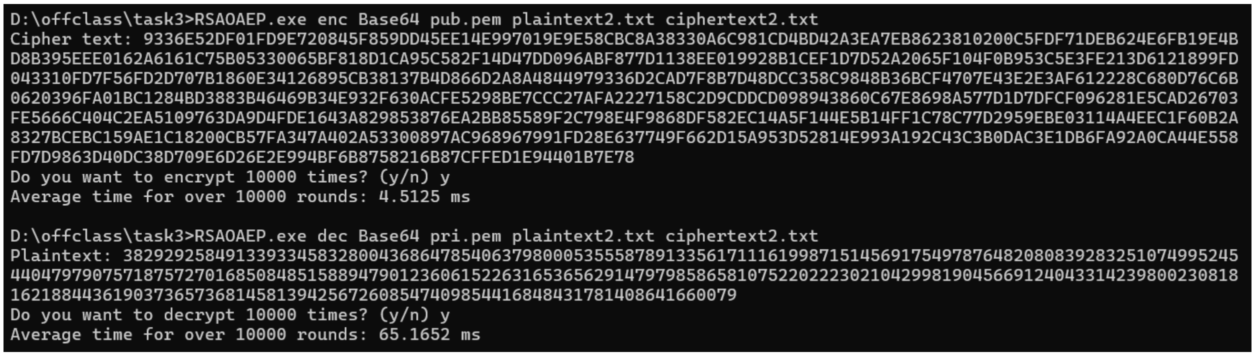
```
 *  Terminal will be reused by tasks, press any key to close it.

 *  Executing task: C:\msys64\mingw64\bin\g++.exe -g2 -O3 D:\offclass\task3\RSAOAEP.cpp -o D:\offclass\task3\RSAOAEP.exe -pthread -DNDEBUG -D_WIN
0501 -LD:\offclass\task3\lib -l:libcryptopp.a -ID:\offclass\task3\include -Wall

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



```
D:\offclass\task3>RSAOAEP.exe enc Base64 pub.pem plaintext.txt ciphertext.txt
Cipher text: 83694E5171C30B7A0BCB2DC5CF98589332CCE77E8B3B180BE6CB6CFC43FFBB4CD46EC7836B6A2FD35E5FCEA5E3F85CBB6AC98D78D39
CB9782ACE6902E004E8B2BE55611E9E080520880042794CB430350774AFDDDA7E5735668BF775E54CFA2D1C13252CAEDB6E9FF9977A717C704786469
1B0CF75693CA7C9F385CB48D1595F19820277A7AB37B80ED74386CAA0F2450DA87AEC1625A2B7D1D9715075A638A53701495E98DEBAAC5AB845D223B
DDF2299396BA9833B0374038725F418D45E59732D637EA57A9AAF0600CB62C6480E08256F6854605A42093F1B1D679AE4F9D09BBE4707D1CB8DFB0B1
A3B26BCA7F2FDCC6DE06D5DC08F7D1B3FA6AE72996A11F864E7930206C72A28BC0C9089E95DFD4CB58C3878A022EF9470C95741FA3E29D63E5C8CDC4
F86845D26BE6D9483C7DFD5F4724F7ABFC03A49F1819E51D3B3275E12C1AF9B3B6137CE825A45FC3C3228C456CD4A31D49908E2FD172EE81012698D1
34BE979BB4AE79599080708D775EDE2F7013E9348543DC6158D87F91E367D
Do you want to encrypt 10000 times? (y/n) y
Average time for over 10000 rounds: 4.7184 ms

D:\offclass\task3>RSAOAEP.exe dec Base64 pri.pem plaintext.txt ciphertext.txt
Plaintext: Trương Đức Hào - 22520407 - ATTTK17.1
Do you want to decrypt 10000 times? (y/n) y
Average time for over 10000 rounds: 69.3854 ms
```

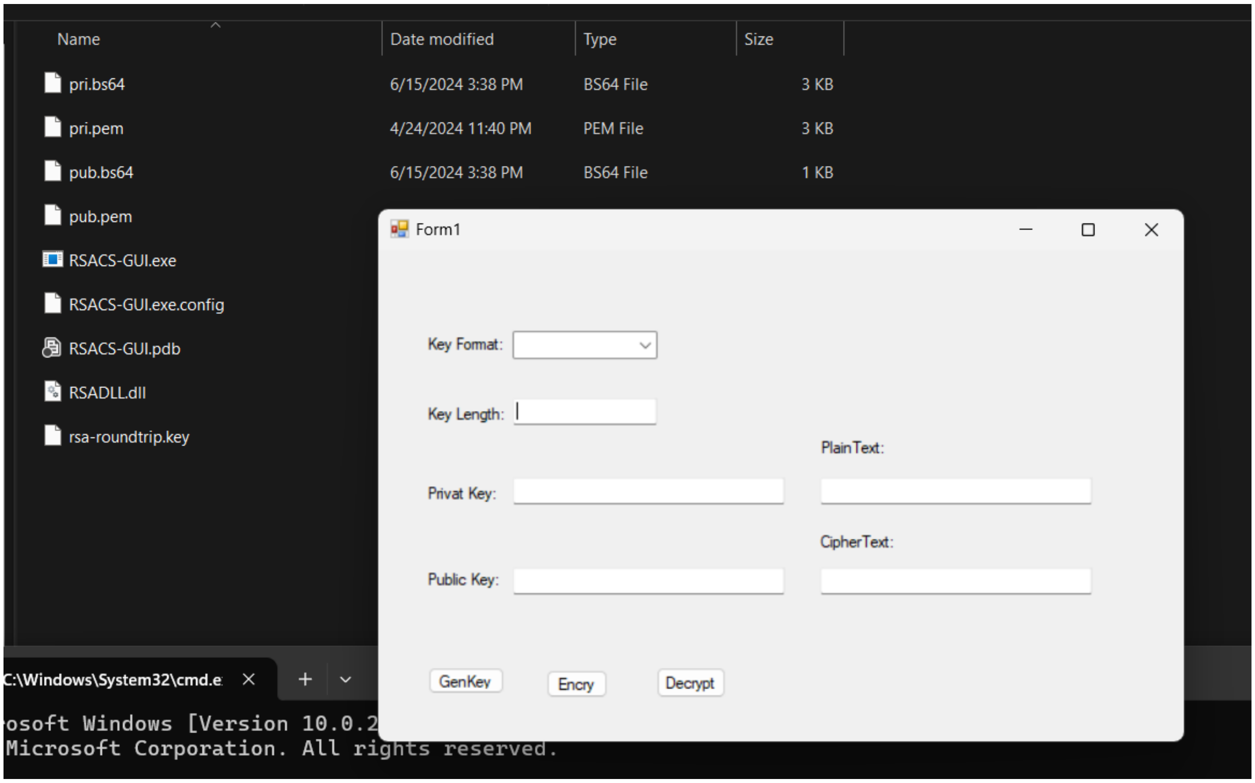


```
D:\offclass\task3>RSAOAEP.exe enc Base64 pub.pem plaintext1.txt ciphertext1.txt
Cipher text: 64580E59D46C064C6AC4AF321FCDF83D5CC937F111A9F06C74D0B953046DD88C6CFAE4234AA412A63D23F1B7322659CC637E31F8D59
5B75CD7D3478BF76278014646FA5636D15E4A9533EF0EB75A86AF76B399BFFD6E4267903A3EC1824A75CE77DC35B8E27121634504968DA64CDBD6638
5B74A7FE72290BCC935B1DD3059B60E71D6E2F53483ADF969B4AF0C09B8D171F9666046A92EAE3E6DAFFD858FA66D0C1A6F5AB6663B65B881EB61AB3
7D5D81B88FDAED40F4D081D84FFC0887FF37A2E16242DA2C5360DB279B15E2913E4B358175FCCDF3C0A386372A4A4E30E1CA39083FEA1C8BF5B4E727
36FA586CB809A16E283FEDE39C6068D0602E0B0B3790A2A8E031A23DD3A491C16668AED857ECA14FC40BED2CAB9A4225A12C26DAD3D38B5E5D8C9A23
00AF0B6B96C410191C5EB1C26A0ED8C7CC5ABB87133F68101149498D2C5286A2DEC81D54E77DF485B0023719B14B42D5391F52581A6D62F822376E15
49D965B08C76641BC995D1F7606FD1F3EC3DBDC65DE6F9F5DDFC292522A2C
Do you want to encrypt 10000 times? (y/n) y
Average time for over 10000 rounds: 5.4543 ms

D:\offclass\task3>RSAOAEP.exe dec Base64 pri.pem plaintext1.txt ciphertext1.txt
Plaintext: 1647427507617154849711768702442413676324283486794864663740778624821740571839186459320025733900301503
Do you want to decrypt 10000 times? (y/n) y
Average time for over 10000 rounds: 73.1621 ms
```



```
D:\offclass\task3>RSAOAEP.exe enc Base64 pub.pem plaintext2.txt ciphertext2.txt
Cipher text: 9336E52DF01FD9E720845F859DD45EE14E997019E9E58CBC8A38330A6C981CD4BD42A3EA7EB8623810200C5FDF71DEB624E6FB19E4B
D8B395EEE0162A6161C75B05330065BF818D1CA95C582F14D47DD096ABF877D1138EE019928B1CEF1D7D52A2065F104F0B953C5E3FE213D6121899FD
043310FD7F56FD2D707B1860E34126895CB38137B4D866D2A8A4844979336D2CAD7F8B7D48DCC358C9848B36BCF4707E43E2E3AF612228C680D76C6B
0620396FA01BC1284BD3883B46469B34E932F630ACFE5298BE7CCC27AFA2227158C2D9CDDCD098943860C67E8698A577D1D7DFCF096281E5CAD26703
FE5666C404C2EA5109763DA9D4FDE1643A829853876EA2BB85589F2C798E4F9868DF582EC14A5F144E5B14FF1C78C77D2959EBE03114A4EEC1F60B2A
8327BCEBC159AE1C18200CB57FA347A402A53300897AC968967991FD28E637749F662D15A953D52814E993A192C43C3B0DAC3E1DB6FA92A0CA44E558
FD7D9863D40DC38D709E6D26E2E994BF6B8758216B87CFFED1E94401B7E78
Do you want to encrypt 10000 times? (y/n) y
Average time for over 10000 rounds: 4.5125 ms

D:\offclass\task3>RSAOAEP.exe dec Base64 pri.pem plaintext2.txt ciphertext2.txt
Plaintext: 3829292584913393345832800436864785406379800053555878913356171116199871514569175497876482080839283251074995245
4404797907571875727016850848515889479012360615226316536562914797985865810752202223021042998190456691240433142398002308l8
1621884436190373657368145813942567260854740985441684843178140864166007
Do you want to decrypt 10000 times? (y/n) y
Average time for over 10000 rounds: 65.1652 ms
```

GUI BUILD:



Name	Date modified	Type	Size
pri.bs64	6/15/2024 3:38 PM	BS64 File	3 KB
pri.pem	4/24/2024 11:40 PM	PEM File	3 KB
pub.bs64	6/15/2024 3:38 PM	BS64 File	1 KB
pub.pem			
RSACS-GUI.exe			
RSACS-GUI.exe.config			
RSACS-GUI.pdb			
RSADLL.dll			
rsa-roundtrip.key			

```
C:\Windows\System32\cmd.e
osoft Windows [Version 10.0.2
Microsoft Corporation. All rights reserved.
```

Comments and Comparison:

- Thời gian thực thi trên Linux nhanh hơn Window, đây là vấn đề về quản lý hệ thống và cấp phát tài nguyên giữa hai hệ điều hành.
- Thời gian giải mã lâu hơn rất nhiều mã hóa vì số lượng phép toán cần tính toán để giải mã là nhiều hơn đáng kể.
- Thời gian thực thi càng lâu khi file có kích thước càng lớn.
- Với những file có kích thước lớn, nên giải phóng bộ nhớ sau khi sử dụng để thực thi tốt hơn.