

**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 1: CODING DES, AES USING CRYPTOPP**  
**LIBRARY**

**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 1: CODING DES, AES USING CRYPTOPP**  
**LIBRARY**

**GIẢNG VIÊN HƯỚNG DẪN**  
**TS. NGUYỄN NGỌC TỰ**

**TP. HỒ CHÍ MINH, NĂM 2024**

## MỤC LỤC

Chương 1.	HARDWARE RESOURCE.....	1
Chương 2.	BUILD TASKS.....	2
2.1.	DES: .....	2
2.1.1.	Command line:.....	2
2.1.2.	GUI: .....	2
2.2.	AES: .....	3
2.2.1.	Arguments:.....	3
2.2.2.	GUI: .....	4
Chương 3.	COMPUTATION PERFORMANCE.....	5
3.1.	DES: .....	5
3.1.1.	Test case 1 (1KB): .....	5
3.1.2.	Test case 2 (20KB): .....	5
3.1.3.	Test case 3 (50KB): .....	6
3.1.4.	Test case 4 (100KB): .....	6
3.1.5.	Test case 5 (500KB): .....	6
3.1.6.	Test case 6 (1MB):.....	7
3.1.7.	Test case 7 (5MB):.....	7
3.2.	AES: .....	8
3.2.1.	Test case 1 (1KB): .....	8
3.2.2.	Test case 2 (20KB): .....	8
3.2.3.	Test case 3 (50KB): .....	9
3.2.4.	Test case 4 (100KB): .....	9

3.2.5.	Test case 5 (200KB): .....	10
3.2.6.	Test case 6 (1MB):.....	10
3.2.7.	Test case 7 (5MB):.....	11
Chương 4.	COMMENTS AND COMPARSION .....	12

## Chương 1. **HARDWARE RESOURCE**

System Information

Current Date/Time: Saturday, June 15, 2024, 12:06:33 PM

Computer Name: THAITRINH

Operating System: Windows 11 Home Single Language 64-bit (10.0, Build 22631)

Language: English (Regional Setting: English)

System Manufacturer: ASUSTeK COMPUTER INC.

System Model: ROG Strix G513IE\_G513IE

BIOS: G513IE.329

Processor: AMD Ryzen 7 4800H with Radeon Graphics (16 CPUs)

Memory: 8192MB RAM

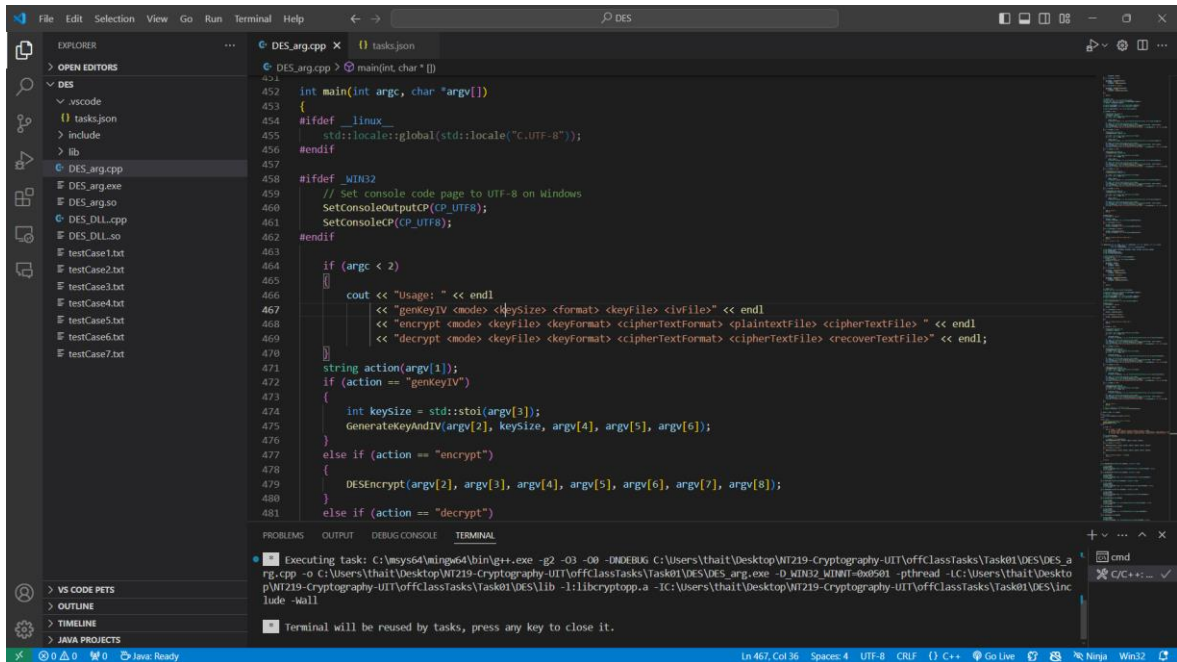
Page file: 11172MB used, 10762MB available

DirectX Version: DirectX 12

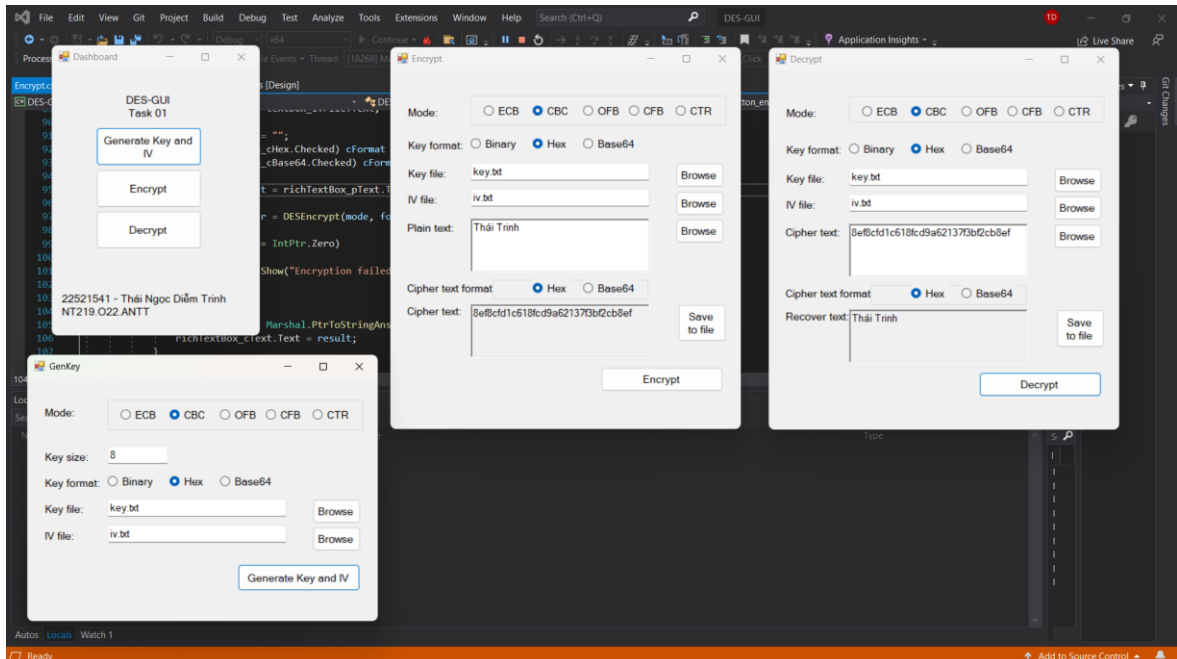
## Chương 2. BUILD TASKS

### 2.1. DES:

#### 2.1.1. Command line:



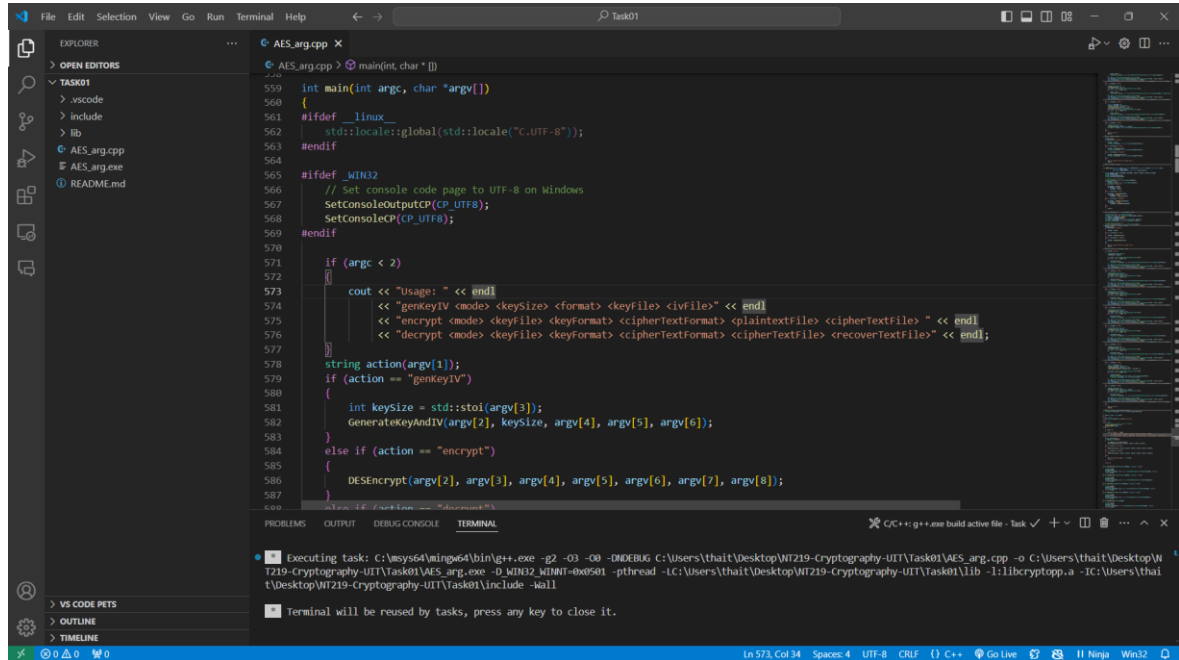
#### 2.1.2. GUI:



## 2.2. AES:

### 2.2.1. Arguments:

- Windows:



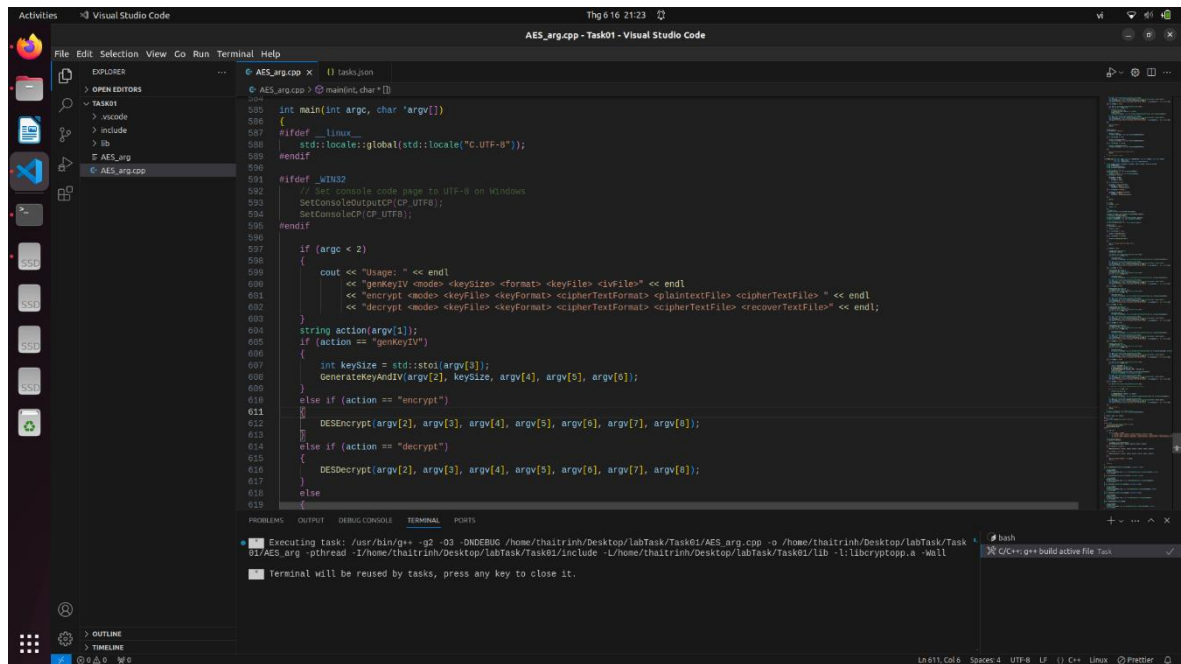
The screenshot shows the Visual Studio Code interface with the file `AES_arg.cpp` open in the editor. The code is a C++ program that implements AES encryption and decryption. It uses `std::string` for file paths and `std::cout` for output. The program is compiled and run in the terminal, showing the execution command and the output.

```
559 int main(int argc, char *argv[])
560 {
561     #ifdef __linux__
562         std::locale::global(std::locale("C.UTF-8"));
563     #endif
564
565     #ifdef _WIN32
566         // Set console code page to UTF-8 on Windows
567         SetConsoleOutputCP(CP_UTF8);
568         SetConsoleCP(CP_UTF8);
569     #endif
570
571     if (argc < 2)
572     {
573         cout << "Usage: " << endl;
574         cout << "genkeyIV <mode> <keySize> <format> <keyfile> <ivfile>" << endl;
575         cout << "encrypt <mode> <keyfile> <keyformat> <cipherTextFormat> <plaintextFile> <cipherTextFile>" << endl;
576         cout << "decrypt <mode> <keyfile> <keyformat> <cipherTextFormat> <cipherTextFile> <recoverTextFile>" << endl;
577     }
578     string action(argv[1]);
579     if (action == "genkeyIV")
580     {
581         int keySize = stoi(argv[3]);
582         GenerateKeyAndIV(argv[2], keySize, argv[4], argv[5], argv[6]);
583     }
584     else if (action == "encrypt")
585     {
586         DESencrypt(argv[2], argv[3], argv[4], argv[5], argv[6], argv[7], argv[8]);
587     }
588     else if (action == "decrypt")
589     {
590         DESdecrypt(argv[2], argv[3], argv[4], argv[5], argv[6], argv[7], argv[8]);
591     }
592 }
```

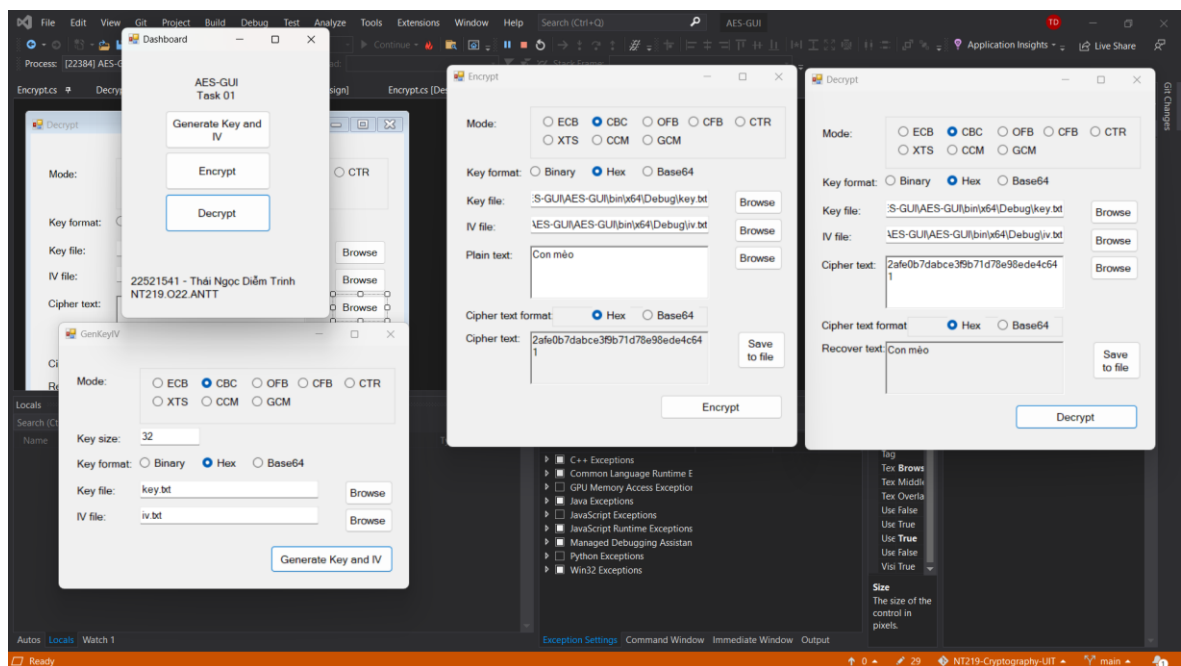
Terminal output:

```
Executing task: C:\msys64\mingw64\bin\g++.exe -g2 -O3 -O0 -DDEBUG C:\Users\thait\Desktop\WT219-Cryptography-UIT\Task01\AES_arg.cpp -o C:\Users\thait\Desktop\WT219-Cryptography-UIT\Task01\AES_arg.exe -D_WIN32_WINNT=0x0501 -pthread -LC:\Users\thait\Desktop\WT219-Cryptography-UIT\Task01\lib -l:libcryptopp.a -IC:\Users\thait\Desktop\WT219-Cryptography-UIT\Task01\include -Wall
```

- Ubuntu:



## 2.2.2. GUI:





### Chương 3. COMPUTATION PERFORMANCE

Number of iterations: 10000

Time counter: mili seconds

#### 3.1. DES:

##### 3.1.1. Test case 1 (1KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0081	0.0082	0.0075	0.0074
CBC	0.0091	0.0082	0.0082	0.0075
OFB	0.0087	0.0087	0.008	0.0081
CFB	0.0091	0.0085	0.0085	0.0083
CTR	0.009	0.0089	0.0083	0.0084

##### 3.1.2. Test case 2 (20KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.1747	0.176	0.1781	0.1773
CBC	0.1966	0.1755	0.1973	0.1783
OFB	0.1916	0.1916	0.1929	0.1928
CFB	0.1934	0.1741	0.1936	0.1779
CTR	0.198	0.1982	0.2002	0.1995

### 3.1.3. Test case 3 (50KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.4526	0.4512	0.4636	0.4615
CBC	0.5104	0.4538	0.5118	00.4624
OFB	0.5016	0.499	0.5046	0.5002
CFB	0.5378	0.486	0.5381	0.4984
CTR	0.5119	0.5148	0.5186	0.5187

### 3.1.4. Test case 4 (100KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.9199	0.9037	0.9376	0.9228
CBC	1.0276	0.9086	1.0251	0.9247
OFB	1.0659	1.0073	1.002	1.009
CFB	1.0647	0.9729	1.0751	0.9971
CTR	1.0415	1.0365	1.0378	1.0384

### 3.1.5. Test case 5 (500KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	1.8212	1.8322	1.9014	1.8461
CBC	2.0725	1.8442	2.0546	1.854
OFB	2.0726	2.0035	2.0034	2.0131

CFB	1.9929	1.813	2.0142	1.9948
CTR	2.0996	1.0686	2.1274	2.1277

### 3.1.6. Test case 6 (1MB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	10.6298	10.6554	11.3112	11.2253
CBC	12.0514	10.794	13.2832	13.0011
OFB	11.7781	11.7676	11.4992	11.593
CFB	11.849	10.7516	12.0194	11.9854
CTR	12.256	12.1608	12.4583	12.4590

### 3.1.7. Test case 7 (5MB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	46.1354	46.062	47.1324	46.9201
CBC	52.1045	47.4282	53.2784	53.1029
OFB	50.7912	79.5167	50.0101	50.3281
CFB	50.7612	49.8213	52.1974	51.0834
CTR	52.4434	52.6886	52.7933	52.7810

### 3.2. AES:

#### 3.2.1. Test case 1 (1KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0017	0.0017	0.0008	0.0008
CBC	0.24	0.0017	0.0016	0.0009
OFB	0.0022	0.0022	0.0017	0.0015
CFB	0.0027	0.0026	0.0018	0.0017
CTR	0.0018	0.0017	0.001	0.0009
XTS	0.0023	0.0023	0.0014	0.0013
CCM	0.0038	0.0052	0.0025	0.0029
GCM	0.0033	0.0046	0.0017	0.0023

#### 3.2.2. Test case 2 (20KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0048	0.0047	0.004	0.0037
CBC	0.0208	0.0051	0.0198	0.0041
OFB	0.0211	0.0211	0.0204	0.0203
CFB	0.0295	0.0261	0.0274	0.0231
CTR	0.0055	0.0055	0.0047	0.0048
XTS	0.0146	0.0147	0.0147	0.0135
CCM	0.0255	0.027	0.0243	0.0261

GCM	0.0094	0.0107	0.008	0.0086
-----	--------	--------	-------	--------

### 3.2.3. Test case 3 (50KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0099	0.0096	0.0094	0.0096
CBC	0.0518	0.0104	0.0505	0.0093
OFB	0.0526	0.0527	0.0521	0.0518
CFB	0.0801	0.0779	0.0765	0.0729
CTR	0.0117	0.0117	0.0112	0.0115
XTS	0.0349	0.0354	0.0375	0.0343
CCM	0.0618	0.0534	0.0607	0.0613
GCM	0.0197	0.0209	0.0183	0.019

### 3.2.4. Test case 4 (100KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0184	0.0187	0.0173	0.0167
CBC	0.102	0.0192	0.1004	0.18
OFB	0.1039	0.1038	0.1032	0.1031
CFB	0.1587	0.1699	0.1569	0.1408
CTR	0.0218	0.0218	0.0211	0.0212
XTS	0.0684	0.0693	0.0704	0.0675
CCM	0.1211	0.1227	0.1206	0.1206

GCM	0.0362	0.0376	0.035	0.036
-----	--------	--------	-------	-------

### 3.2.5. Test case 5 (200KB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0346	0.0337	0.0353	0.033
CBC	0.2032	0.0372	0.2017	0.0358
OFB	0.2063	0.2066	0.2061	0.2074
CFB	0.2946	0.2585	0.2874	0.2339
CTR	0.0418	0.0418	0.0417	0.0416
XTS	0.1354	0.1375	0.1381	0.1335
CCM	0.2405	0.2426	0.2397	0.2411
GCM	0.0701	0.0716	0.0694	0.0706

### 3.2.6. Test case 6 (1MB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.1965	0.19	0.2052	0.1885
CBC	1.1907	0.2134	1.1999	0.2214
OFB	1.203	1.2114	1.2095	1.2079
CFB	1.5418	1.1605	1.4874	1.0242
CTR	0.2355	0.2372	0.2453	0.2424
XTS	0.7952	0.8262	0.8078	0.7898

CCM	1.4328	1.4718	1.4011	1.4047
GCM	0.4137	0.4225	0.4024	0.4067

### 3.2.7. Test case 7 (5MB):

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	1.5337	1.4876	1.8676	1.9008
CBC	5.4134	0.7334	5.8107	2.0626
OFB	5.498	5.5543	6.0019	5.9886
CFB	7.7629	6.9828	7.8876	6.6229
CTR	1.6886	1.7265	1.9577	1.9306
XTS	3.7403	3.7862	4.2896	4.1836
CCM	6.486	6.7983	6.6031	6.6721
GCM	2.1584	2.1463	2.6328	2.564

#### Chương 4. **COMMENTS AND COMPARSION**

AES mode is faster than DES mode in 7 testcases in both Window and Linux

Executing the code in Window is faster than Linux in 7 testcases

Time execute increase as same as the increase of file size

There are not much different in time execute in 5 modes in DES among 7 testcases

Mode ECB, CTR, GCM have the time execute faster than the other modes in scheme AES

With the files, the size of which are under 1 MB have the time execute faster than the file from 1 MB and above. With the file greater than 1 MB, must have the clean data function to cut down the time execute



