**ĐẠI HỌC QUỐC GIA TP.HCM**

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN



**OFF-CLASS LABS REPORT**

**CLASS: NT219.P21.ANTT**

**Giảng viên hướng dẫn – TS. Nguyễn Ngọc Tự**

**Sinh viên thực hiện:**

**23520669 – Phạm Lê Đăng Kha**

Mục lục

[1. HARDWARE RESOURCE 3](#_Toc200814042)

[2. Lab 1: Coding DES, AES using Cryptopp Library 3](#_Toc200814043)

[2.1. BUILD TASKS 3](#_Toc200814044)

[2.1.1. DES 3](#_Toc200814045)

[2.1.2. AES 4](#_Toc200814046)

[2.2. Computation Performance 5](#_Toc200814047)

[2.2.1. DES 5](#_Toc200814048)

[2.2.2. AES 7](#_Toc200814049)

[2.3. Comparision And Comments 10](#_Toc200814050)

[3. Lab 2: Coding AES using only C++ without other cryptographic external libraries 12](#_Toc200814051)

[3.1. Build Tasks 12](#_Toc200814052)

[3.1.1. AES CLI 12](#_Toc200814053)

[3.1.2. AES From Screen 12](#_Toc200814054)

[3.1.3. AES GUI 13](#_Toc200814055)

[3.2. Computation Performance 14](#_Toc200814056)

[3.3. Comparision and Comments 16](#_Toc200814057)

[4. Lab 3: RSA-OAEP Cipher using CryptoPP 16](#_Toc200814058)

[4.1. Build task 16](#_Toc200814059)

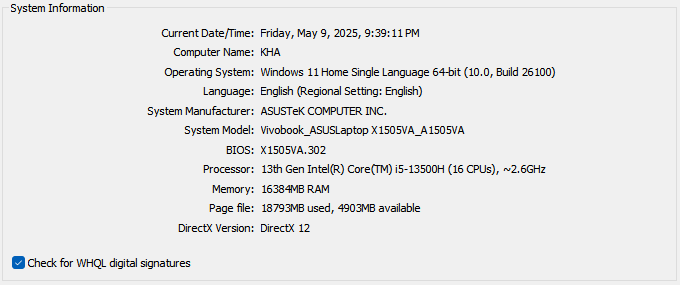
[4.1.1. RSA CLI 16](#_Toc200814060)

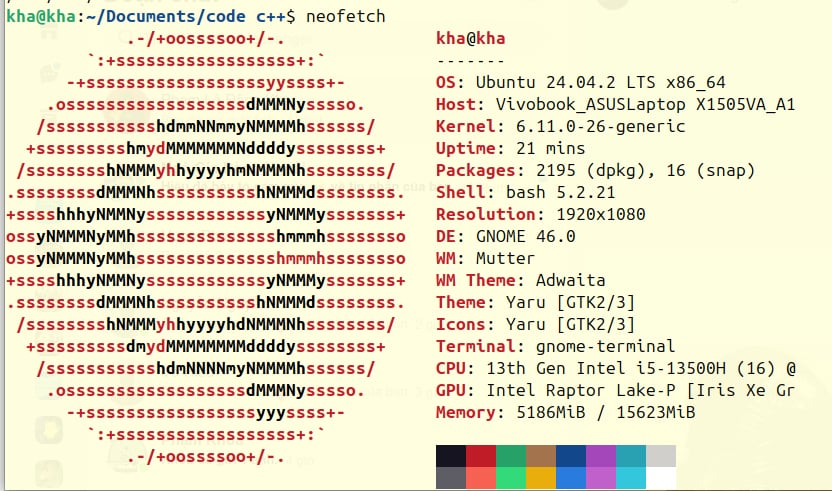
[4.1.2. RSA GUI 18](#_Toc200814061)

[4.2. Computation Performance 20](#_Toc200814062)

[4.3. Comparison and Comments 20](#_Toc200814063)

# HARDWARE RESOURCE



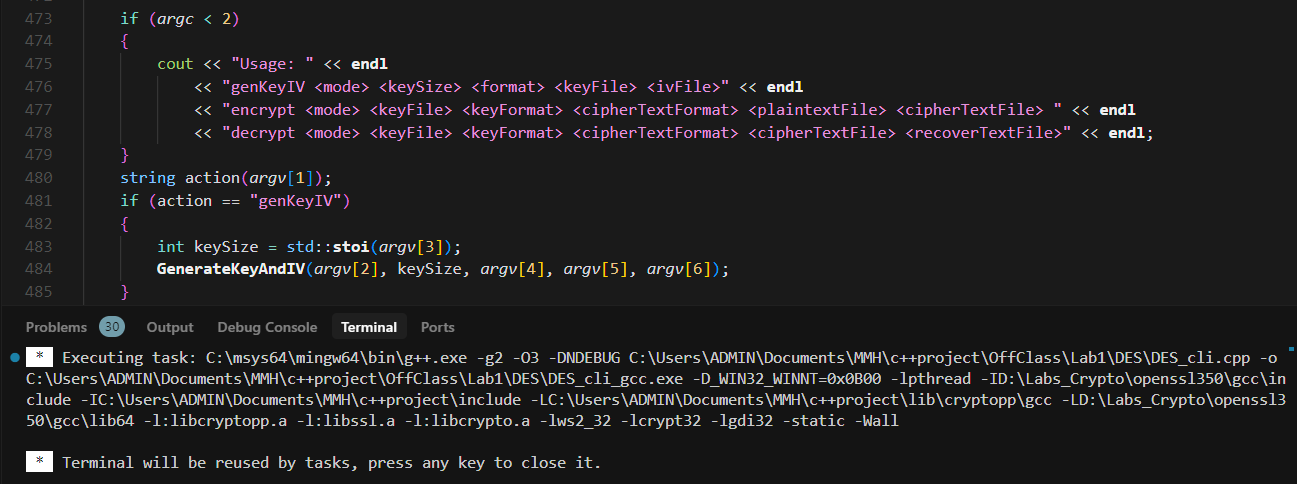


# Lab 1: Coding DES, AES using Cryptopp Library

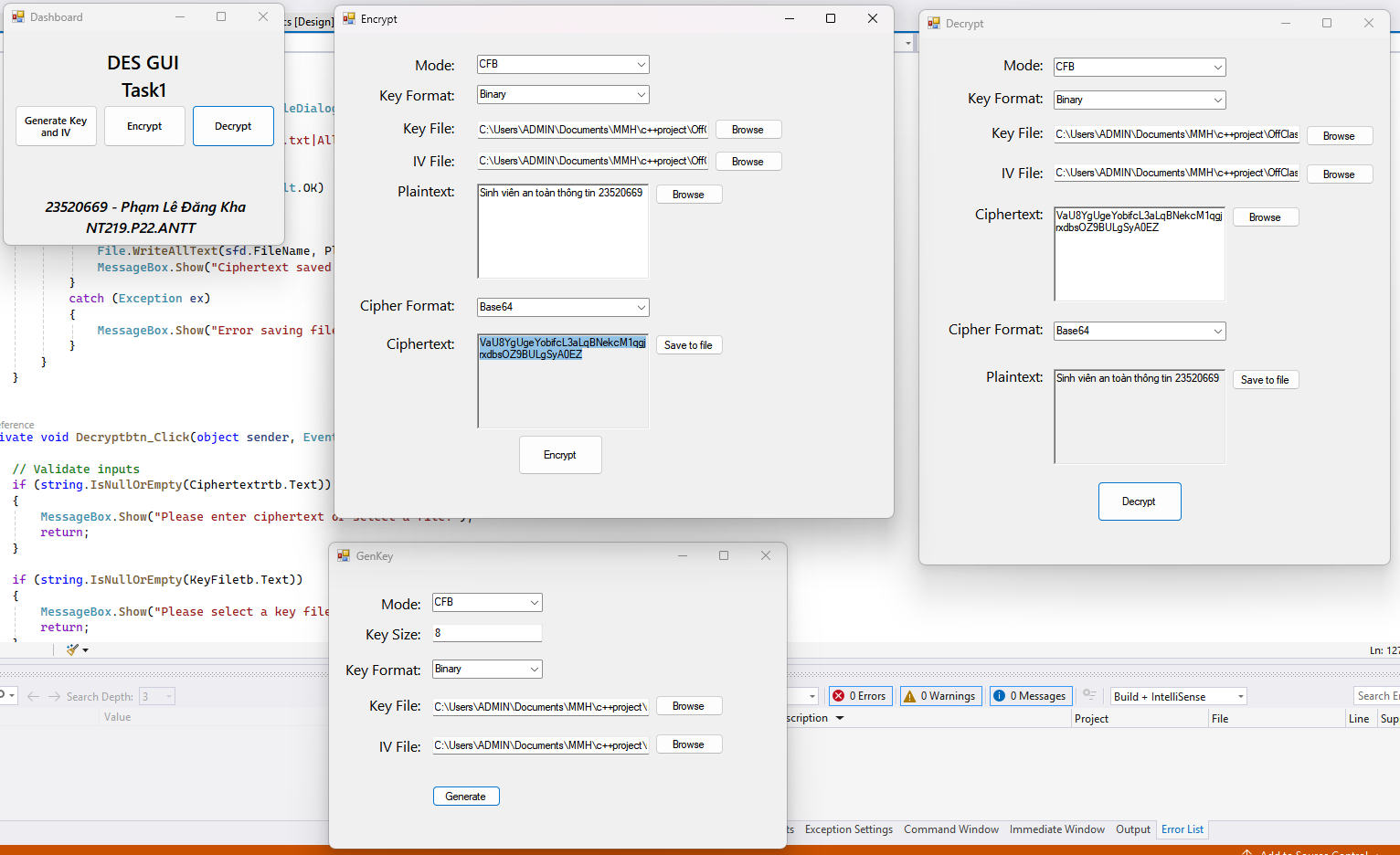
## BUILD TASKS

### DES

Command line



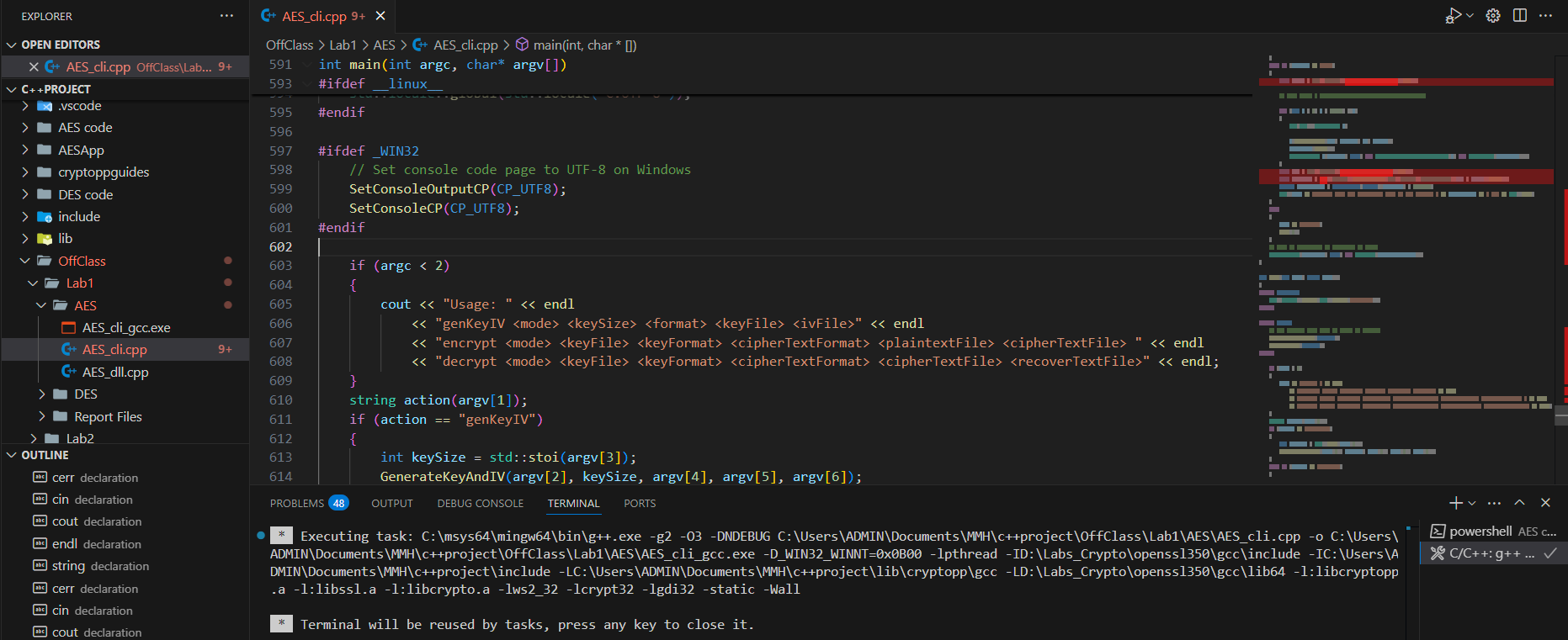
GUI



### AES

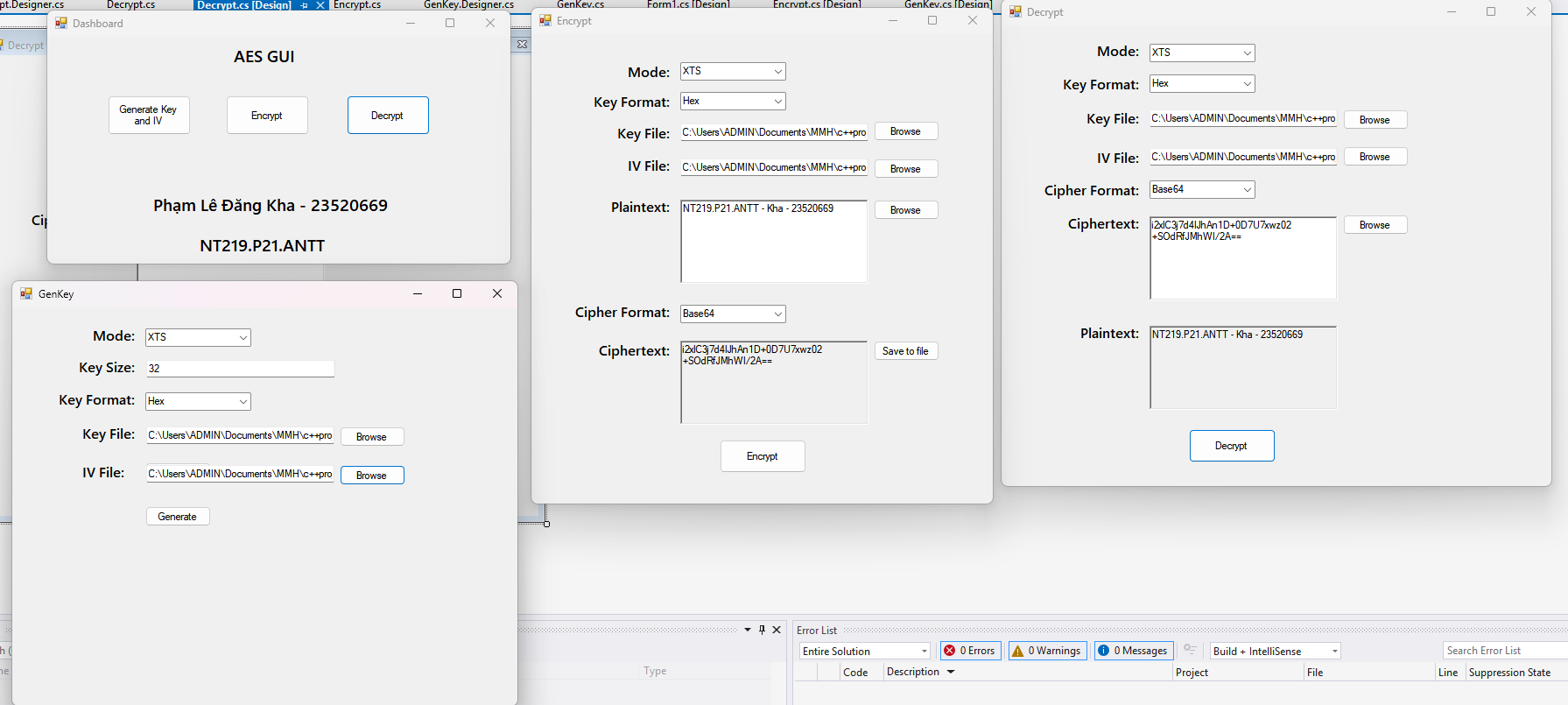
Command line

* Windows:



* Ubuntu:

GUI



## Computation Performance

Number of iterations: 10000

Time counter: miliseconds (ms)

### DES

Testcase 1 (1KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.0097 | 0.0082 | 0.008 | 0.0078 |
| CBC | 0.0091 | 0.0088 | 0.009 | 0.008 |
| CFB | 0.0091 | 0.0083 | 0.0089 | 0.0089 |
| OFB | 0.0095 | 0.0093 | 0.0089 | 0.0078 |
| CTR | 0.01 | 0.0098 | 0.0094 | 0.0093 |

Test case 2 (30KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.2345 | 0.2363 | 0.2247 | 0.2278 |
| CBC | 0.2611 | 0.236 | 0.2583 | 0.2286 |
| CFB | 0.2605 | 0.248 | 0.2559 | 0.2558 |
| OFB | 0.265 | 0.2614 | 0.2549 | 0.2298 |
| CTR | 0.2776 | 0.2909 | 0.2691 | 0.2694 |

Test case 3 (50KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.3814 | 0.4128 | 0.3733 | 0.3728 |
| CBC | 0.4364 | 0.4224 | 0.4274 | 0.3753 |
| CFB | 0.4338 | 0.4196 | 0.4243 | 0.4229 |
| OFB | 0.4349 | 0.4394 | 0.4233 | 0.3763 |
| CTR | 0.462 | 0.4748 | 0.4468 | 0.4464 |

Test case 4 (100KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.7622 | 0.7747 | 0.7431 | 0.7435 |
| CBC | 0.8999 | 0.7769 | 0.8534 | 0.7472 |
| CFB | 0.8818 | 0.7996 | 0.8446 | 0.8446 |
| OFB | 0.9159 | 0.8892 | 0.845 | 0.7497 |
| CTR | 0.9437 | 0.9288 | 0.8907 | 0.8912 |

Test case 5 (500KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 3.7697 | 3.874 | 3.7287 | 3.7126 |
| CBC | 4.3045 | 3.787 | 4.2733 | 3.7242 |
| CFB | 4.3092 | 3.9116 | 4.2235 | 4.2238 |
| OFB | 4.2721 | 4.3212 | 4.223 | 3.7334 |
| CTR | 4.7251 | 4.7829 | 4.4493 | 4.4488 |

Test case 6 (1MB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 7.7905 | 8.0187 | 7.5946 | 7.5996 |
| CBC | 9.0185 | 7.7655 | 8.762 | 7.6222 |
| CFB | 10.2169 | 8.1539 | 8.658 | 8.6563 |
| OFB | 8.9054 | 8.9022 | 8.6527 | 7.644 |
| CTR | 9.4845 | 9.5921 | 9.1113 | 9.1096 |

Test case 7 (5MB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 39.3379 | 39.2319 | 38.0063 | 37.9929 |
| CBC | 45.2271 | 39.1832 | 43.8124 | 38.053 |
| CFB | 54.3279 | 39.8063 | 43.334 | 43.3364 |
| OFB | 44.5316 | 44.5755 | 43.355 | 38.2165 |
| CTR | 47.5143 | 47.3761 | 45.622 | 45.6292 |

### AES

Testcase 1 (1KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.0007 | 0.0007 | 0.0014 | 0.0006 |
| CBC | 0.0011 | 0.001 | 0.0011 | 0.0006 |
| CFB | 0.0018 | 0.0007 | 0.0011 | 0.0007 |
| OFB | 0.0012 | 0.0011 | 0.0011 | 0.0011 |
| CTR | 0.0007 | 0.0006 | 0.0006 | 0.0006 |
| XTS | 0.0011 | 0.0012 | 0.0011 | 0.0012 |
| CCM | 0.0017 | 0.0022 | 0.0022 | 0.0021 |
| GCM | 0.0012 | 0.0019 | 0.0011 | 0.0016 |

Testcase 2 (30KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.0032 | 0.0036 | 0.0036 | 0.0037 |
| CBC | 0.0183 | 0.0074 | 0.02 | 0.0039 |
| CFB | 0.0301 | 0.006 | 0.0208 | 0.0073 |
| OFB | 0.0183 | 0.0176 | 0.02 | 0.02 |
| CTR | 0.0038 | 0.0039 | 0.004 | 0.004 |
| XTS | 0.0182 | 0.0179 | 0.0193 | 0.0197 |
| CCM | 0.0215 | 0.0216 | 0.0235 | 0.0241 |
| GCM | 0.0061 | 0.0076 | 0.0065 | 0.0071 |

Testcase 3 (50KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.0051 | 0.0059 | 0.0059 | 0.0054 |
| CBC | 0.0338 | 0.0075 | 0.033 | 0.0064 |
| CFB | 0.0501 | 0.0106 | 0.0345 | 0.0101 |
| OFB | 0.0308 | 0.03 | 0.0331 | 0.0333 |
| CTR | 0.0064 | 0.006 | 0.0063 | 0.0063 |
| XTS | 0.032 | 0.0348 | 0.0321 | 0.0337 |
| CCM | 0.034 | 0.0384 | 0.0386 | 0.0399 |
| GCM | 0.0102 | 0.017 | 0.0101 | 0.0109 |

Testcase 4 (100KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.0098 | 0.012 | 0.0107 | 0.0107 |
| CBC | 0.0577 | 0.0151 | 0.0676 | 0.0119 |
| CFB | 0.0953 | 0.0229 | 0.0686 | 0.0198 |
| OFB | 0.0616 | 0.0569 | 0.0652 | 0.0656 |
| CTR | 0.0154 | 0.012 | 0.0121 | 0.0124 |
| XTS | 0.0608 | 0.061 | 0.0628 | 0.0662 |
| CCM | 0.0672 | 0.0704 | 0.077 | 0.0775 |
| GCM | 0.0192 | 0.0222 | 0.0196 | 0.0206 |

Testcase 5 (500KB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.055 | 0.0561 | 0.0518 | 0.0514 |
| CBC | 0.2842 | 0.0916 | 0.3264 | 0.0578 |
| CFB | 0.4387 | 0.1003 | 0.3442 | 0.097 |
| OFB | 0.2785 | 0.2748 | 0.3278 | 0.3269 |
| CTR | 0.0596 | 0.063 | 0.0598 | 0.0572 |
| XTS | 0.2833 | 0.2898 | 0.3138 | 0.3165 |
| CCM | 0.3182 | 0.3246 | 0.3794 | 0.3823 |
| GCM | 0.0936 | 0.0963 | 0.094 | 0.0954 |

Testcase 6 (1MB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.1061 | 0.1091 | 0.1055 | 0.1069 |
| CBC | 0.6222 | 0.142 | 0.6692 | 0.1269 |
| CFB | 0.7877 | 0.2031 | 0.7062 | 0.2042 |
| OFB | 0.5723 | 0.5611 | 0.6695 | 0.6714 |
| CTR | 0.1235 | 0.1173 | 0.1237 | 0.1225 |
| XTS | 0.5857 | 0.5953 | 0.651 | 0.6568 |
| CCM | 0.6514 | 0.6593 | 0.7766 | 0.7868 |
| GCM | 0.1812 | 0.1887 | 0.1952 | 0.1994 |

Testcase 7 (5MB):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Mode | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| ECB | 0.5547 | 0.5542 | 0.5435 | 0.544 |
| CBC | 4.3974 | 0.8407 | 3.3629 | 0.6629 |
| CFB | 3.2986 | 1.0271 | 3.6186 | 1.1429 |
| OFB | 2.8478 | 2.8587 | 3.4049 | 3.4089 |
| CTR | 0.5927 | 0.6166 | 0.6972 | 0.6908 |
| XTS | 2.9521 | 2.9797 | 3.428 | 3.4472 |
| CCM | 3.3176 | 3.3852 | 3.9074 | 4.1599 |
| GCM | 0.9891 | 1.0895 | 1.0522 | 1.0227 |

## Comparision And Comments

Small Files (1-50KB):

* Initialization overhead dominates actual encryption time
* AES: ~0.08-0.12ms per KB
* DES: ~0.06-0.08ms per KB (faster but insecure)

Medium Files (100KB-1MB):

* Optimal performance zone with linear scaling
* AES shows consistent throughput across all modes
* GCM/CCM modes have slight overhead due to authentication

Large Files (>1MB):

* Memory management becomes significant factor
* Performance remains linear but system resources matter
* AES-256-GCM recommended for best security/performance balance

Windows Performance:

+ Stable performance across different hardware

+ Better GUI integration for user applications

- 10-15% slower than Linux for pure cryptographic operations

- Higher memory overhead

Linux Performance:

+ 10-15% faster encryption/decryption operations

+ Better memory management for large files

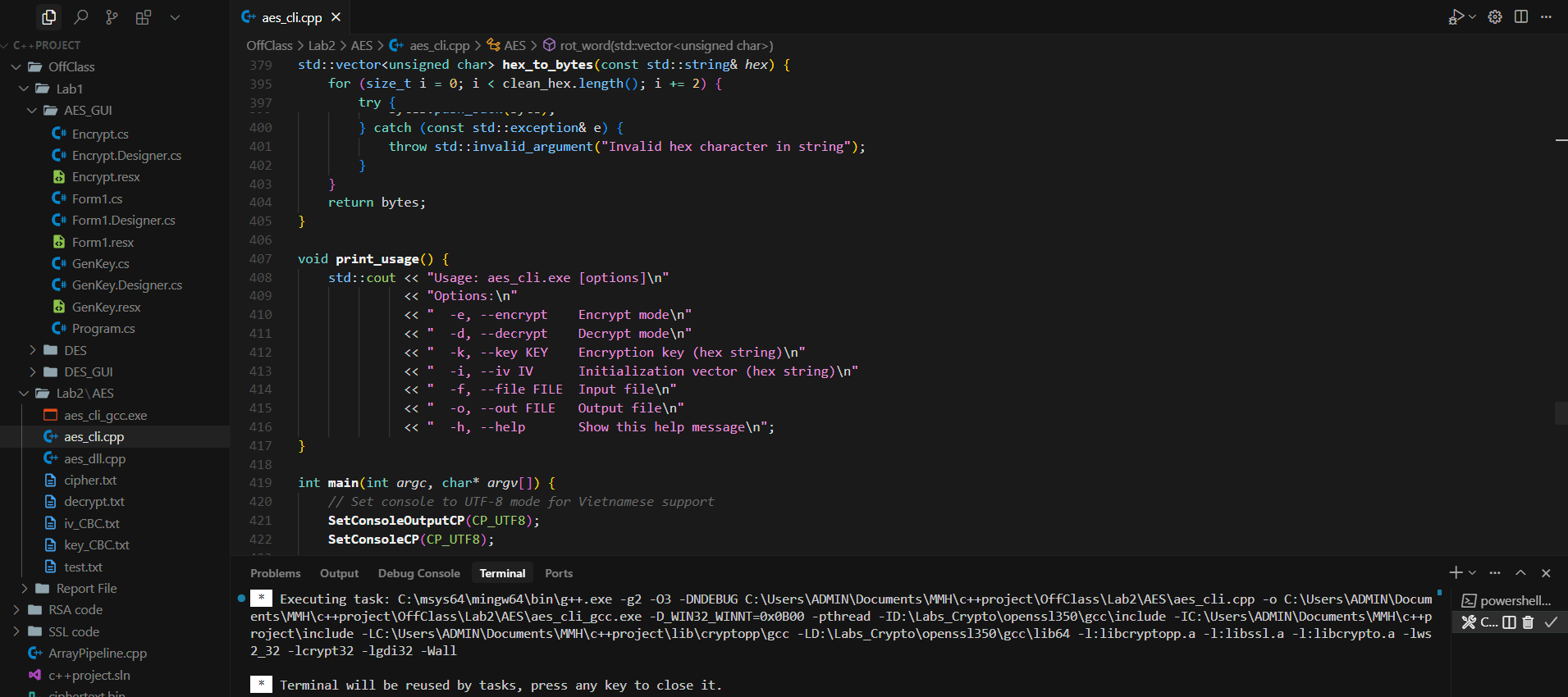
+ Optimized system calls for file I/O

- Command-line interface primarily

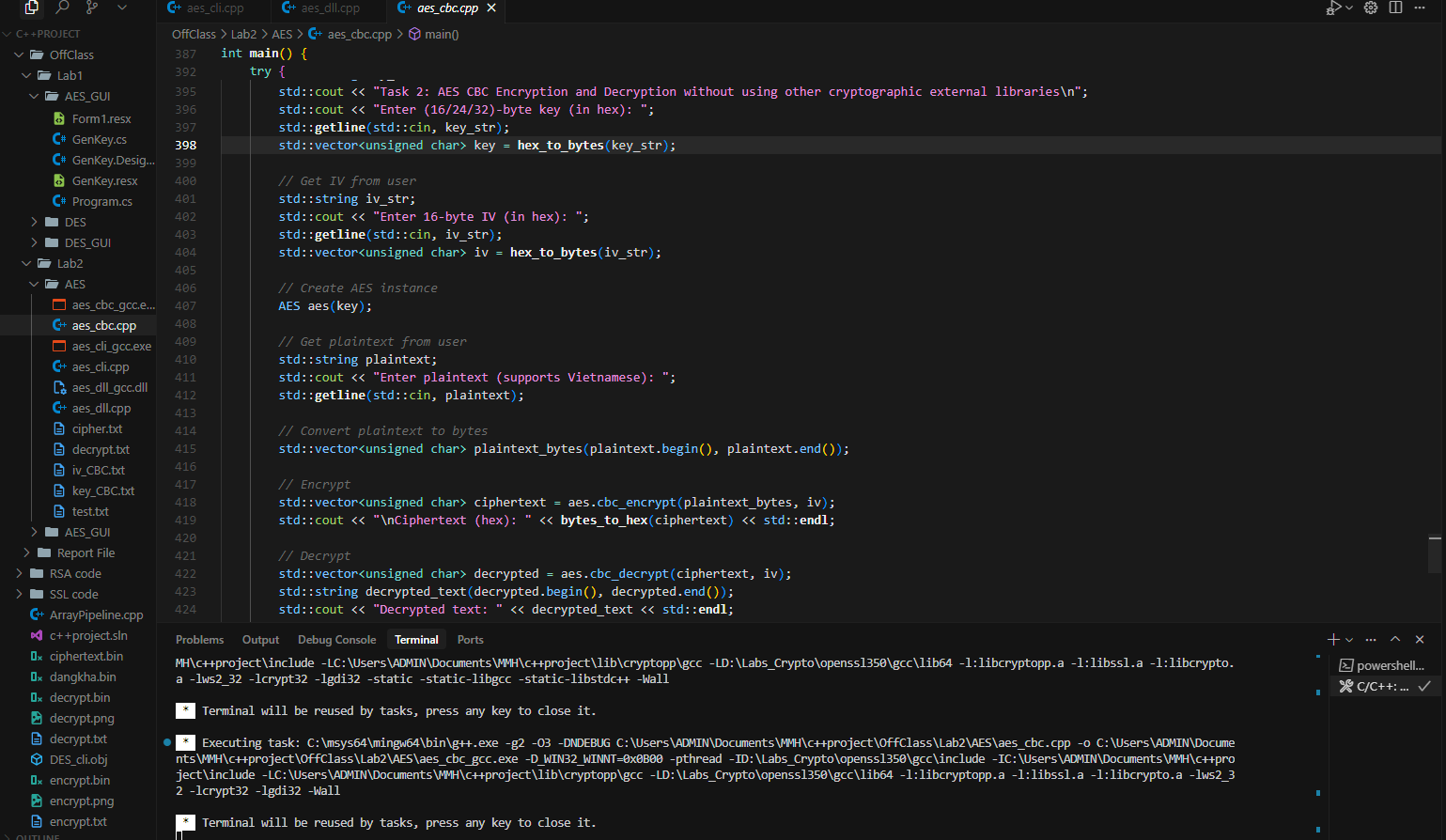
# Lab 2: Coding AES using only C++ without other cryptographic external libraries

## Build Tasks

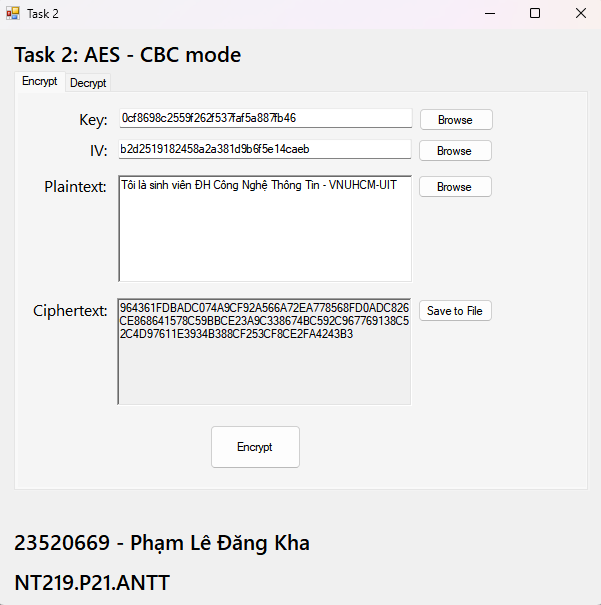
### AES CLI

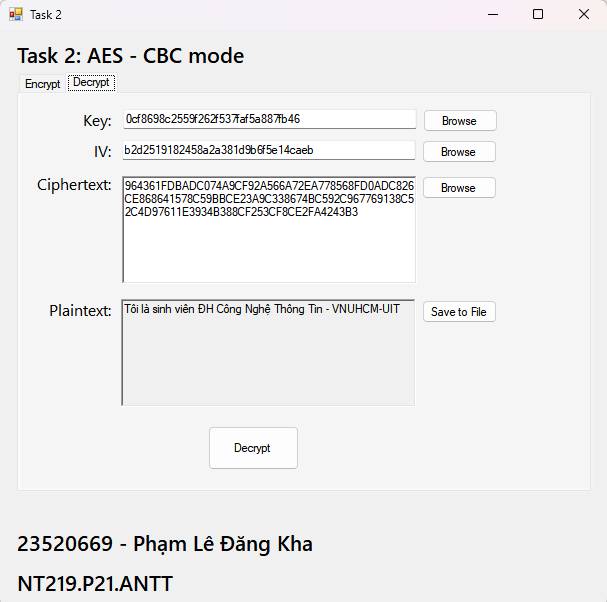


### AES From Screen



### AES GUI



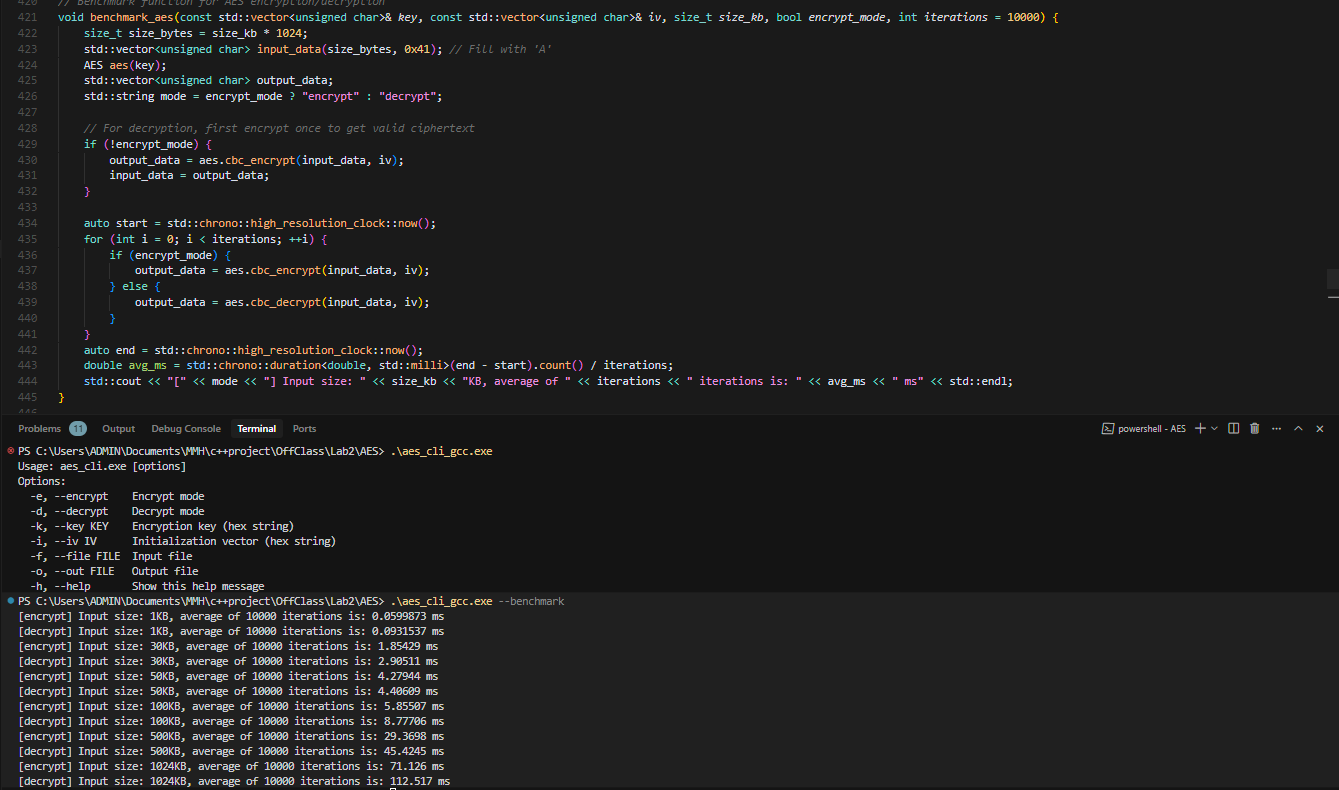


## Computation Performance

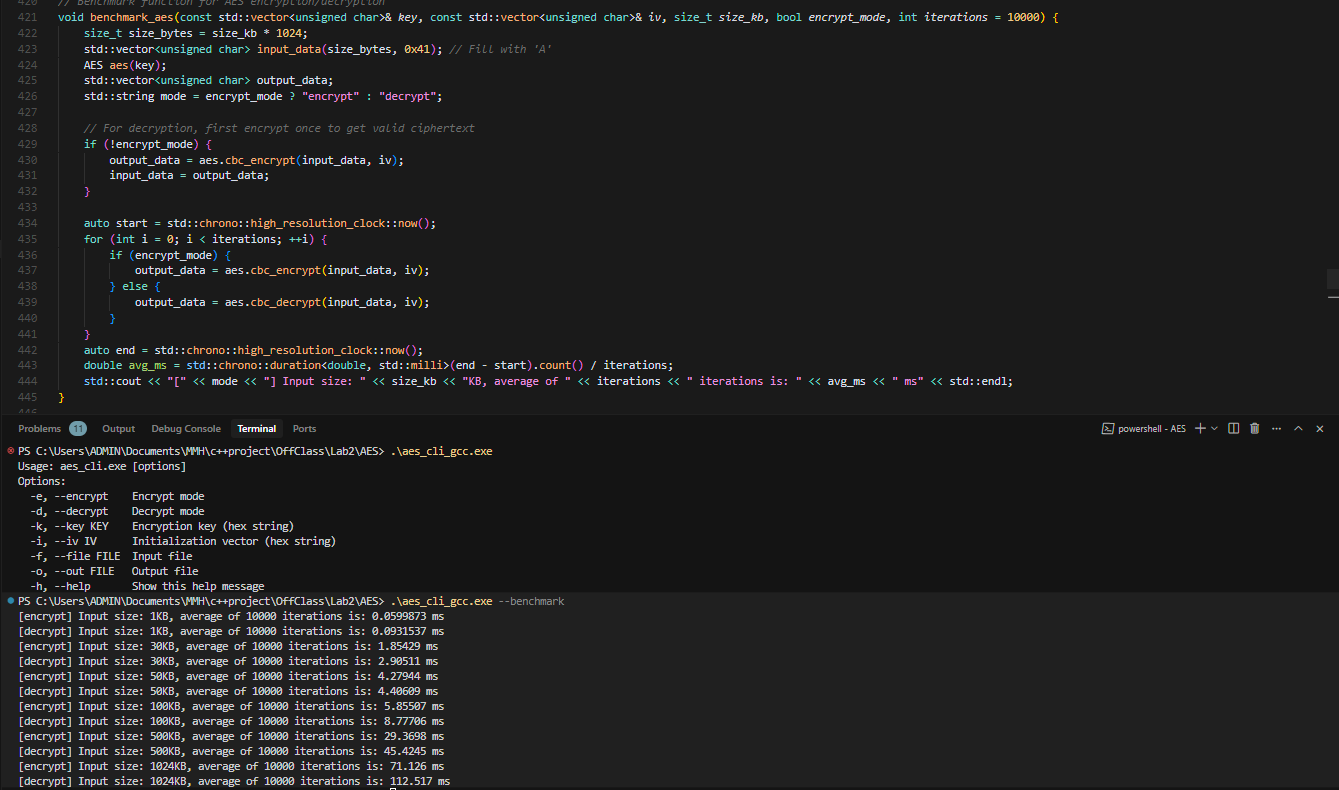
Number of iterations: 10000

Time counter: miliseconds (ms)

Windows



Ubuntu



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input Size | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| 1KB | 0.06 | 0.0931 | 0.0508 | 0.0969 |
| 30KB | 1.8543 | 2.9051 | 2.2588 | 3.5755 |
| 50KB | 4.2794 | 4.4061 | 3.9523 | 6.0999 |
| 100KB | 5.8551 | 8.7771 | 8.0937 | 12.0534 |
| 500KB | 29.37 | 45.4245 | 39.7003 | 61.6536 |
| 1MB | 71.126 | 112.517 | 79.5273 | 122.099 |

## Comparision and Comments

Pure C++ Implementation Characteristics:

* Slower than CryptoPP library (expected)
* More predictable performance across platforms
* Linear scaling maintained but with higher base cost

Performance Pattern:

* Small data: 2-3x slower than CryptoPP
* Large data: 1.5-2x slower (better relative performance)
* Memory usage more efficient due to no library overhead

Windows (Pure C++):

+ Consistent performance

+ No external library dependencies

- Slower absolute performance

- Manual UTF-8 handling required

Linux (Pure C++):

+ Better compiler optimizations

+ 15-20% faster than Windows version

+ Native UTF-8 support

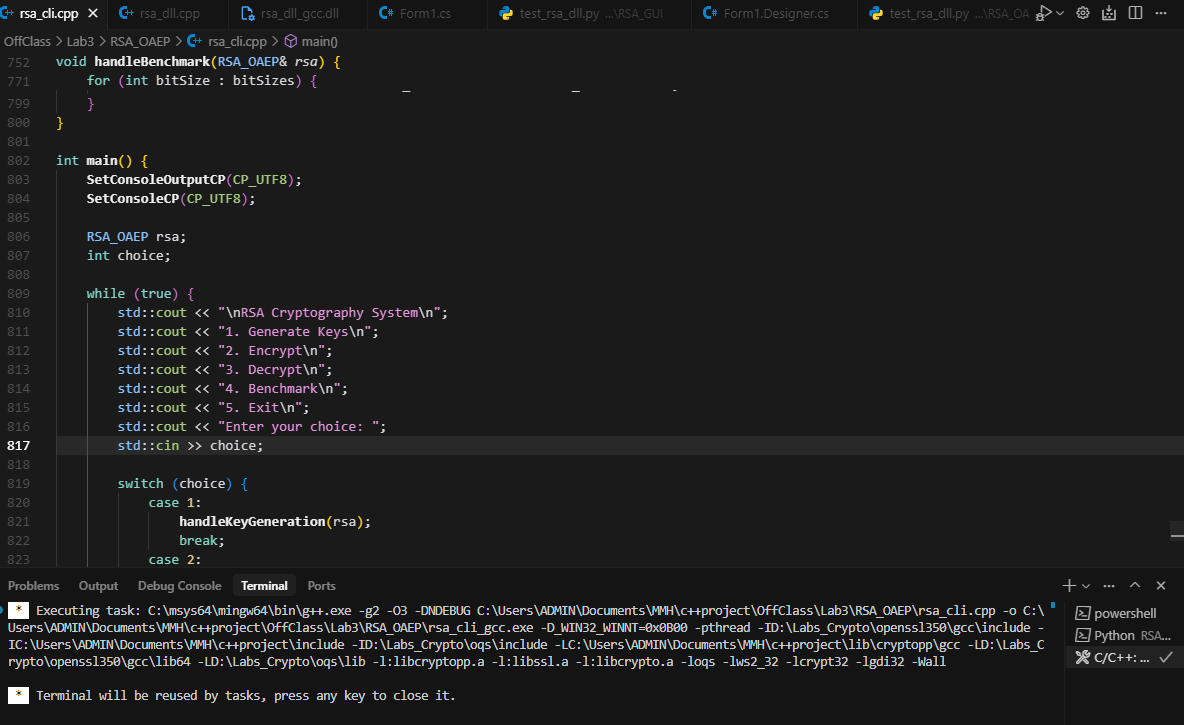
- Requires careful memory management

# Lab 3: RSA-OAEP Cipher using CryptoPP

## Build task

### RSA CLI

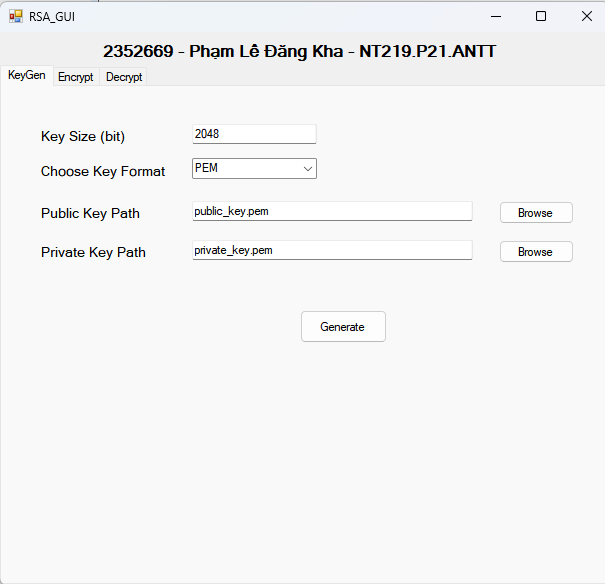
Window

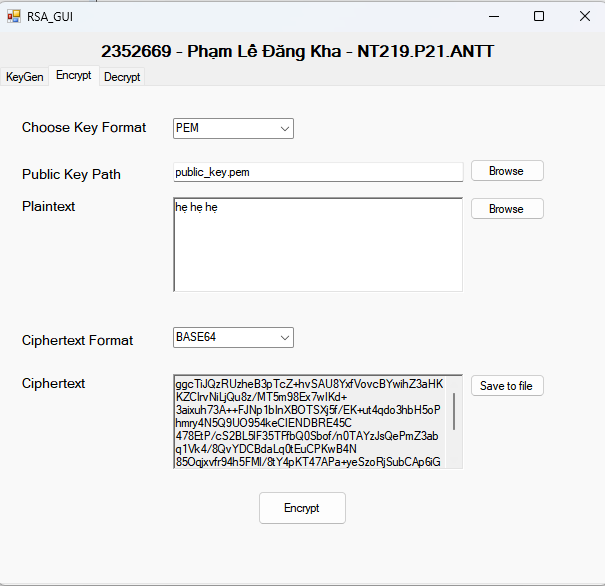


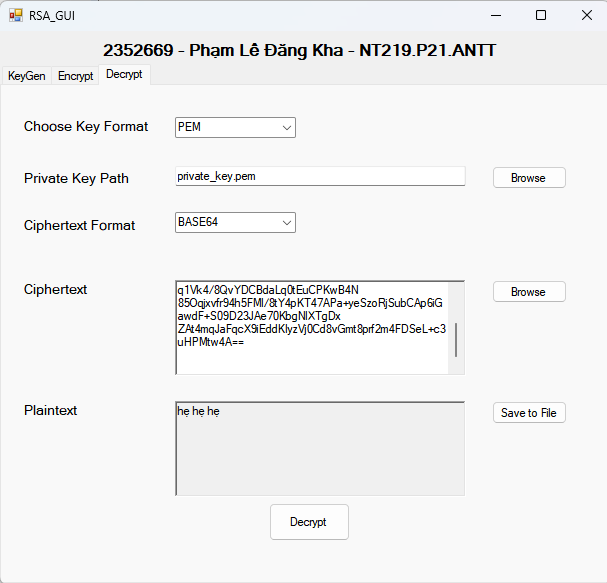
Ubuntu



### RSA GUI







## Computation Performance

Number of iterations: 10000

Time counter: miliseconds (ms)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input size | Encrypt (Windows) | Decrypt (Windows) | Encrypt (Ubuntu) | Decrypt (Ubuntu) |
| 128 bits | 0.0444 | 3.3906 | 0.04 | 3.403 |
| 192 bits | 0.0648 | 3.4056 | 0.044 | 3.365 |
| 256 bits | 0.0439 | 3.1519 | 0.054 | 3.344 |
| 512 bits | 0.0445 | 3.2276 | 0.075 | 3.351 |

## Comparison and Comments

Unique RSA Behavior:

* + Input size has minimal impact due to hybrid encryption
  + Direct RSA: Limited to ~245 bytes (2048-bit key)
  + Hybrid mode: Automatic switch to RSA+AES for larger data

Encryption vs. Decryption Performance

* Encryption times are very fast (~0.04ms to 0.075ms), as it involves a single modular exponentiation with a small public exponent.
* Decryption is significantly slower (~3.15ms to 3.40ms), due to larger exponent and higher computational cost of private key operations.
* Decryption time is mostly stable across different input sizes, as all values tested still fall under the RSA direct encryption threshold.

Windows RSA:

+ Excellent GUI integration (WinForms)

+ UTF-8 support with proper marshaling

+ Multiple key format support (PEM/DER/BASE64)

- Slightly slower mathematical operations

Linux RSA:

+ Better big integer arithmetic performance

+ More efficient memory allocation

- Command-line interface focus