UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

UIT
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN

REPORT

Subject: Cryptography

Report Lab 1

Lecturer: Nguyen Ngoc Tu

Report Lab 1

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

DES

plaintext: Trương Đức Hào - 22520407 – ATTTK17.1 (testcase1)

key: BF2DDCD77E4C2368

iv: 432BEE020A8B48EF

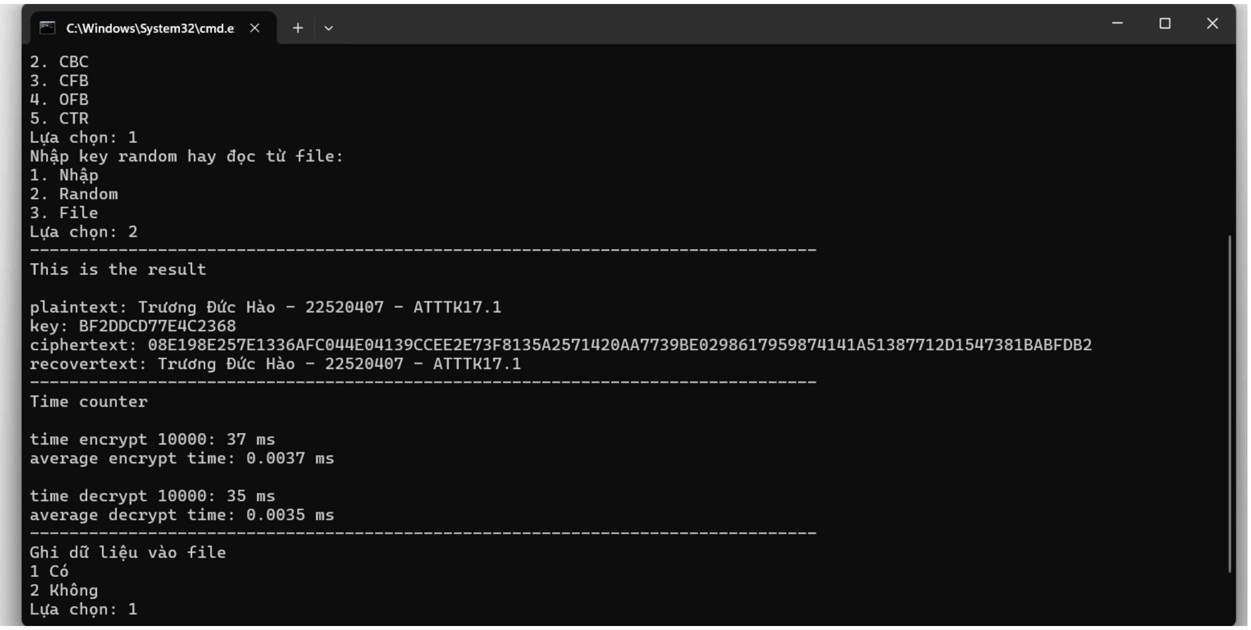
number of iterations: 10000

time counter: mili seconds

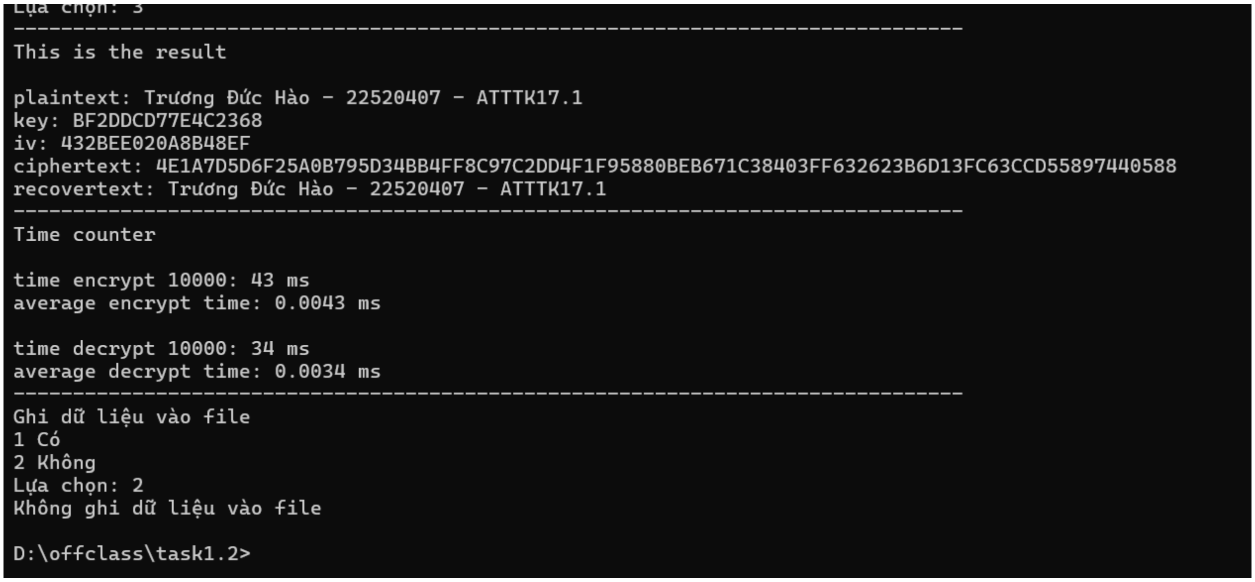
testcase1.txt (1 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0037	0.0035	0.0026049	0.0026058
CBC	0.0035	0.0033	0.0027666	0.00274
CFB	0.003	0.0035	0.0027456	0.0026576
OFB	0.0035	0.0031	0.0029246	0.002877
CTR	0.0043	0.0034	0.0027964	0.0027436

ECB vs CTR:



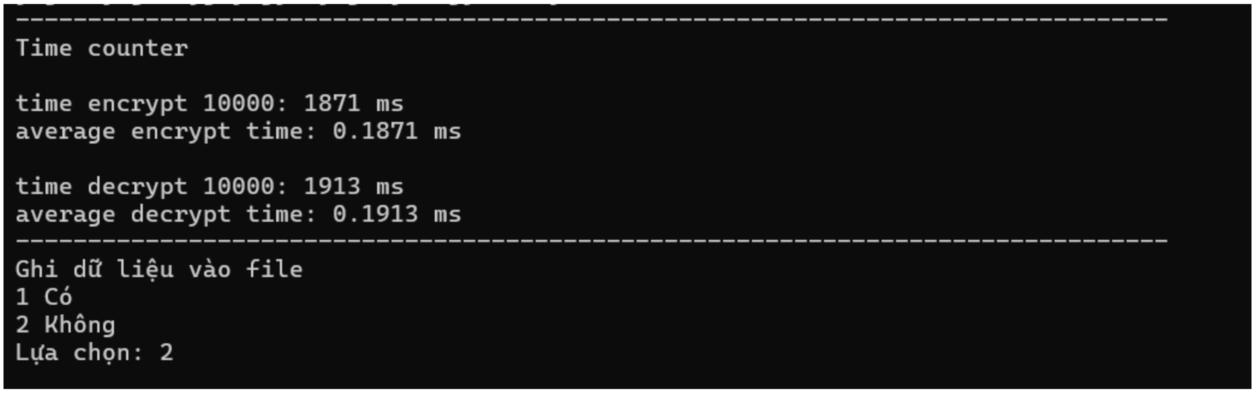
```
2. CBC
3. CFB
4. OFB
5. CTR
Lựa chọn: 1
Nhập key random hay đọc từ file:
1. Nhập
2. Random
3. File
Lựa chọn: 2
--------------------------------------------------------------------------------
This is the result

plaintext: Trương Đức Hào - 22520407 - ATTTK17.1
key: BF2DDCD77E4C2368
ciphertext: 08E198E257E1336AFC044E04139CCEE2E73F8135A2571420AA7739BE0298617959874141A51387712D1547381BABFDB2
recovertext: Trương Đức Hào - 22520407 - ATTTK17.1
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 37 ms
average encrypt time: 0.0037 ms

time decrypt 10000: 35 ms
average decrypt time: 0.0035 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: 1
```



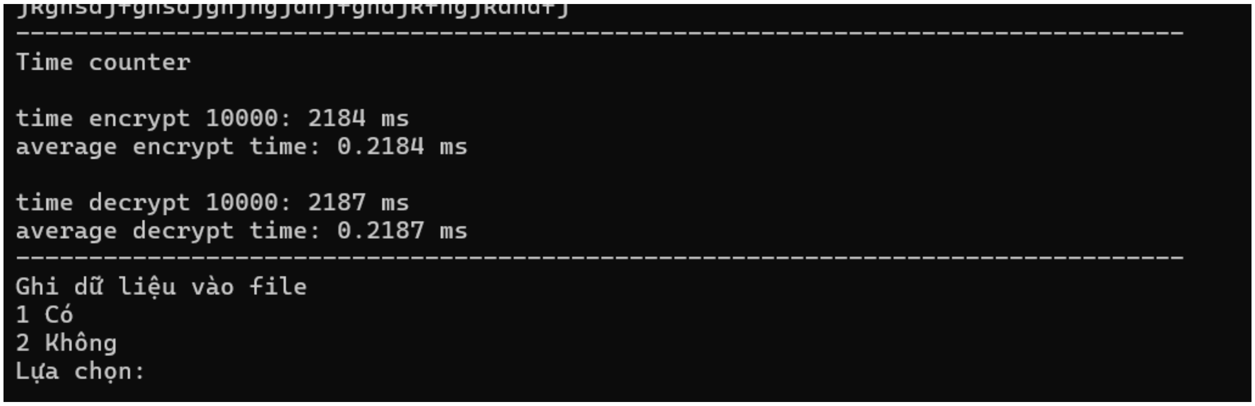
```
Lựa chọn: 3
--------------------------------------------------------------------------------
This is the result

plaintext: Trương Đức Hào - 22520407 - ATTTK17.1
key: BF2DDCD77E4C2368
iv: 432BEE020A8B48EF
ciphertext: 4E1A7D5D6F25A0B795D34BB4FF8C97C2DD4F1F95880BEB671C38403FF632623B6D13FC63CCD55897440588
recovertext: Trương Đức Hào - 22520407 - ATTTK17.1
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 43 ms
average encrypt time: 0.0043 ms

time decrypt 10000: 34 ms
average decrypt time: 0.0034 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: 2
Không ghi dữ liệu vào file

D:\offclass\task1.2>
```

testcase2.txt (20 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.1871	0.1913	0.15591	0.156237
CBC	0.1845	0.1756	0.174245	0.156908
CFB	0.1875	0.1789	0.177004	0.156958
OFB	0.2153	0.2106	0.177	0.176939
CTR	0.2184	0.2187	0.185067	0.184701



```
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 1871 ms
average encrypt time: 0.1871 ms

time decrypt 10000: 1913 ms
average decrypt time: 0.1913 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: 2
```

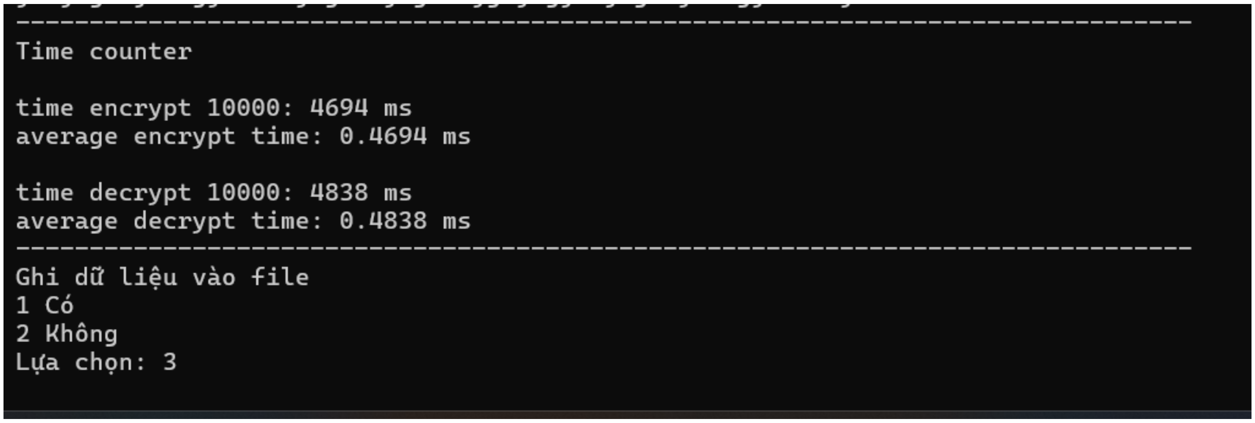


```
jkghsdjfghsdjghjhgjdhjfghdjkfhgjkdhdfj
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 2184 ms
average encrypt time: 0.2184 ms

time decrypt 10000: 2187 ms
average decrypt time: 0.2187 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

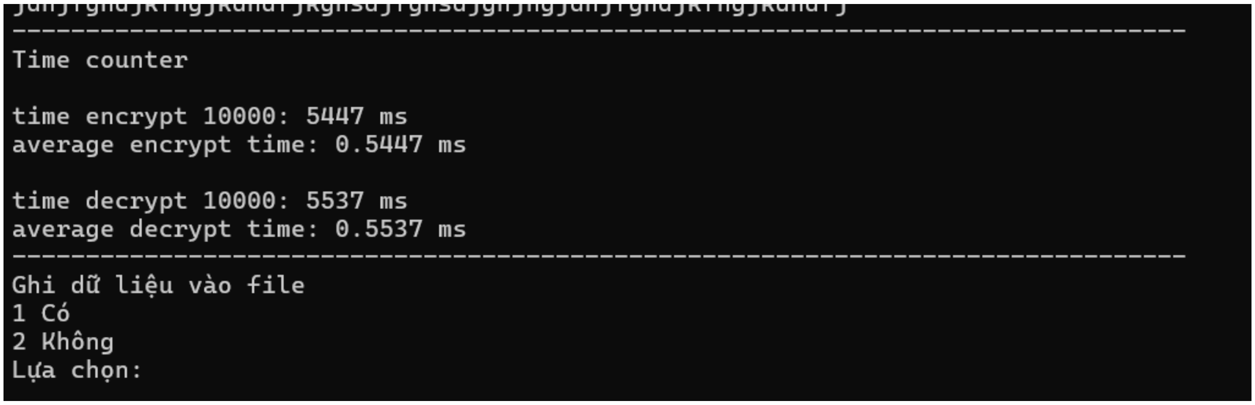
testcase3.txt (50 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.4694	0.4838	0.39205	0.392449
CBC	0.4210	0.3746	0.46387	0.394245
CFB	0.6003	0.610	0.444534	0.39462
OFB	0.4863	0.5203	0.445113	0.445177
CTR	0.5447	0.5537	0.464835	0.464436

ECB vs CTR:



```
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 4694 ms
average encrypt time: 0.4694 ms

time decrypt 10000: 4838 ms
average decrypt time: 0.4838 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: 3
```

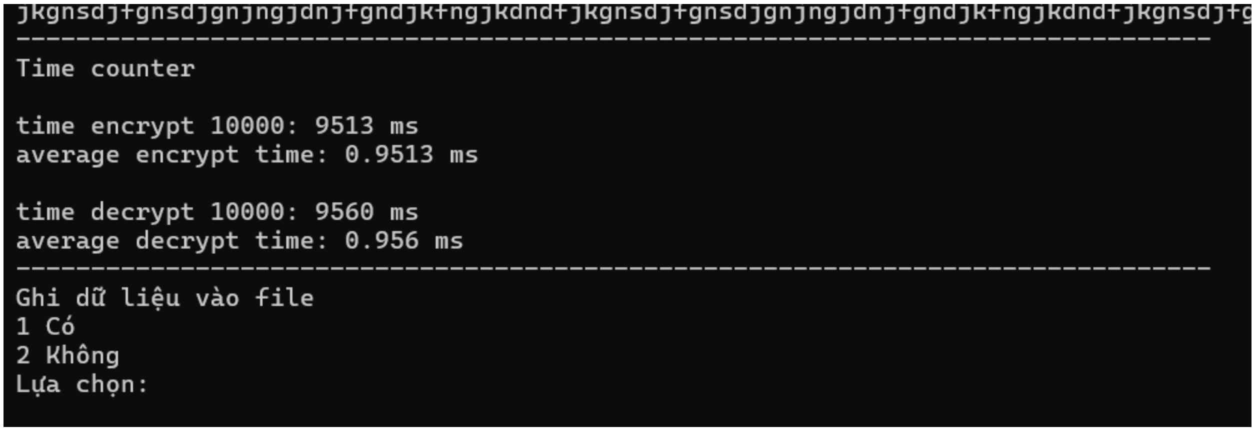


```
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 5447 ms
average encrypt time: 0.5447 ms

time decrypt 10000: 5537 ms
average decrypt time: 0.5537 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

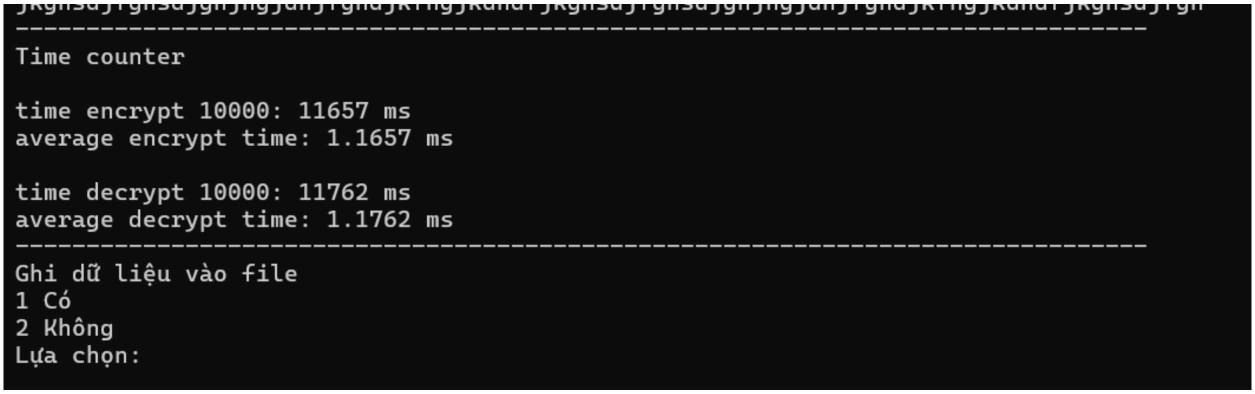
testcase4.txt (100 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.9513	0.956	0.790493	0.790547
CBC	0.9786	0.9102	0.929154	0.788597
CFB	1.2301	1.2356	0.896158	0.794559
OFB	1.156	1.230	0.922937	0.923643
CTR	1.1657	1.762	0.933519	0.932912

ECB vs CTR:



```
jkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfg
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 9513 ms
average encrypt time: 0.9513 ms

time decrypt 10000: 9560 ms
average decrypt time: 0.956 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

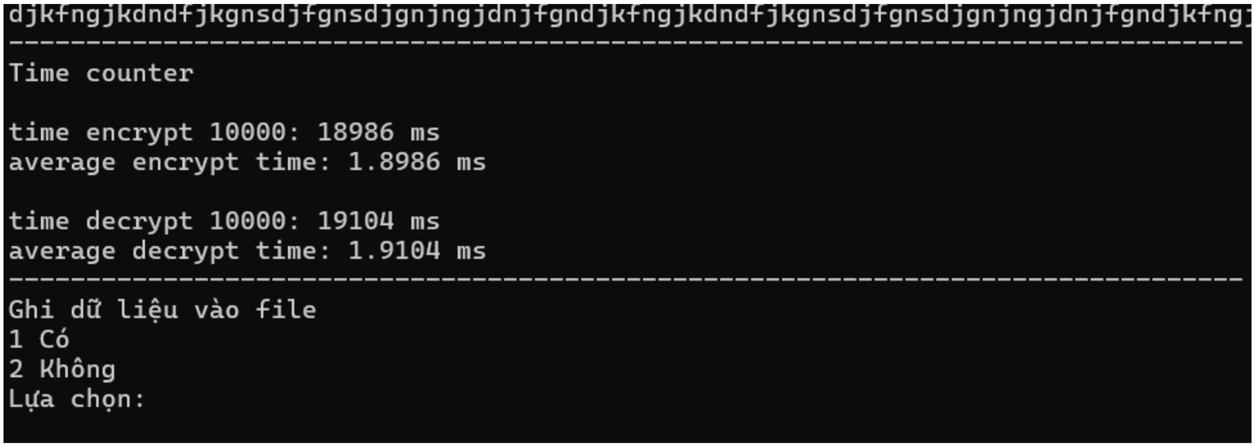


```
jkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgn
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 11657 ms
average encrypt time: 1.1657 ms

time decrypt 10000: 11762 ms
average decrypt time: 1.1762 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

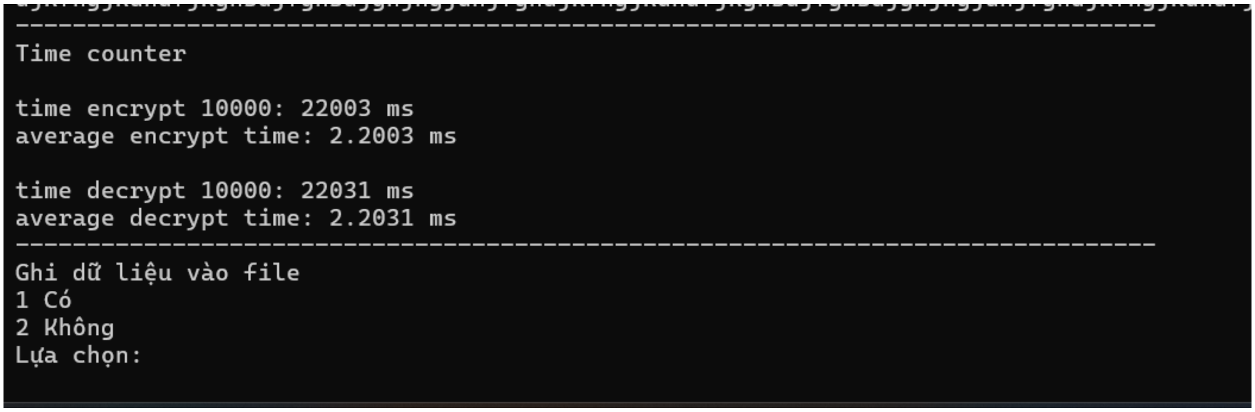
testcase5.txt (200 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	1.8986	1.9104	1.57201	1.57121
CBC	2.1035	1.9624	1.85131	1.56704
CFB	2.0236	1.9231	1.78779	1.57931
OFB	1.9632	1.9836	1.79383	1.79079
CTR	2.2003	2.2031	1.87095	1.86667

ECB vs CTR:



```
djkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngj
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 18986 ms
average encrypt time: 1.8986 ms

time decrypt 10000: 19104 ms
average decrypt time: 1.9104 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

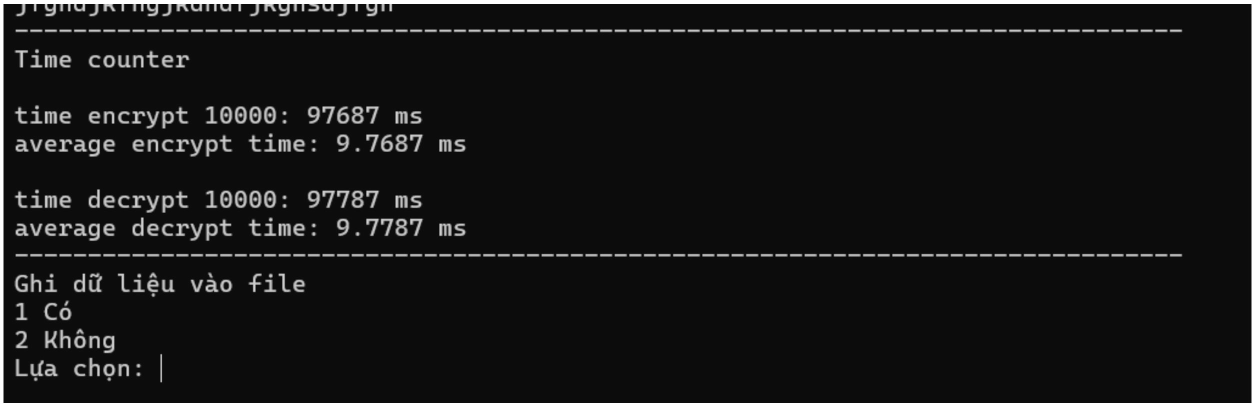


```
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 22003 ms
average encrypt time: 2.2003 ms

time decrypt 10000: 22031 ms
average decrypt time: 2.2031 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

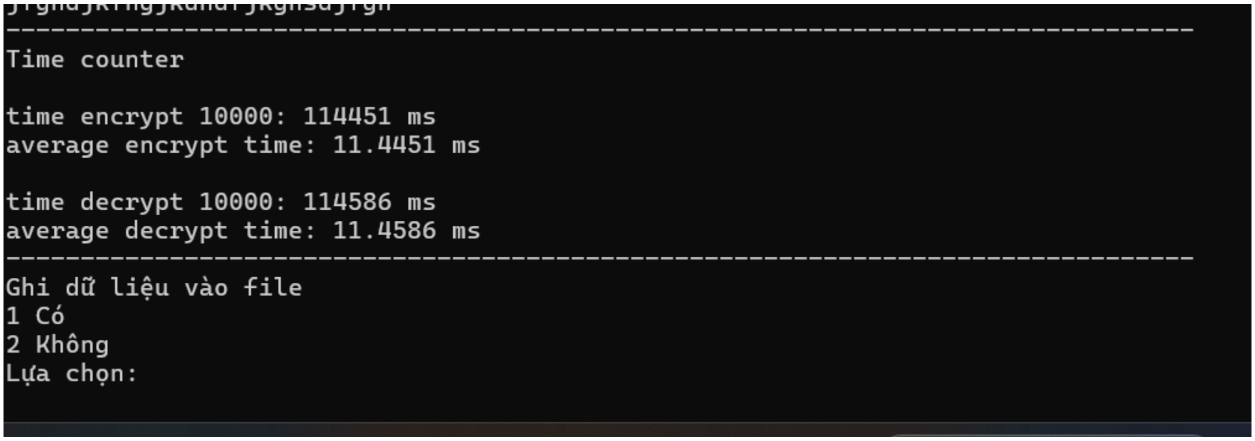
testcase6.txt (1024 KB = 1 MB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	9.7687	9.7787	8.04969	8.05198
CBC	10.4598	9.6526	9.51168	8.05622
CFB	10.5632	9.7856	9.20892	8.12086
OFB	12.3526	12.7785	9.21188	9.20689
CTR	11.4451	11.4586	9.60558	9.60156

ECB vs CTR:



```
jrghdjkrhgjkdhdrjkghsdjrgh
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 97687 ms
average encrypt time: 9.7687 ms

time decrypt 10000: 97787 ms
average decrypt time: 9.7787 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```



```
jrghdjkrhgjkdhdrjkghsdjrgh
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 114451 ms
average encrypt time: 11.4451 ms

time decrypt 10000: 114586 ms
average decrypt time: 11.4586 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

AES

plaintext: Trương Đức Hào - 22520407 – ATTTK17.1 (testcase1)

key: 9800A318AEFF1DD5CEF5925B04A4217A195833F2FA095762CD61DDF12BF4AAB0

iv: 1B4BB83084BAF338

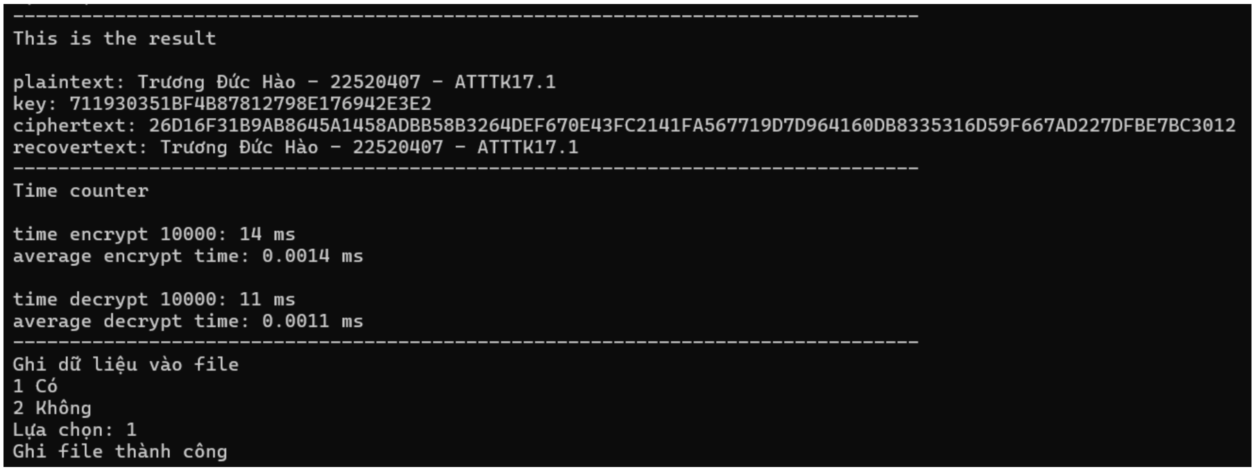
auth data: 22520407

time counter: mili seconds

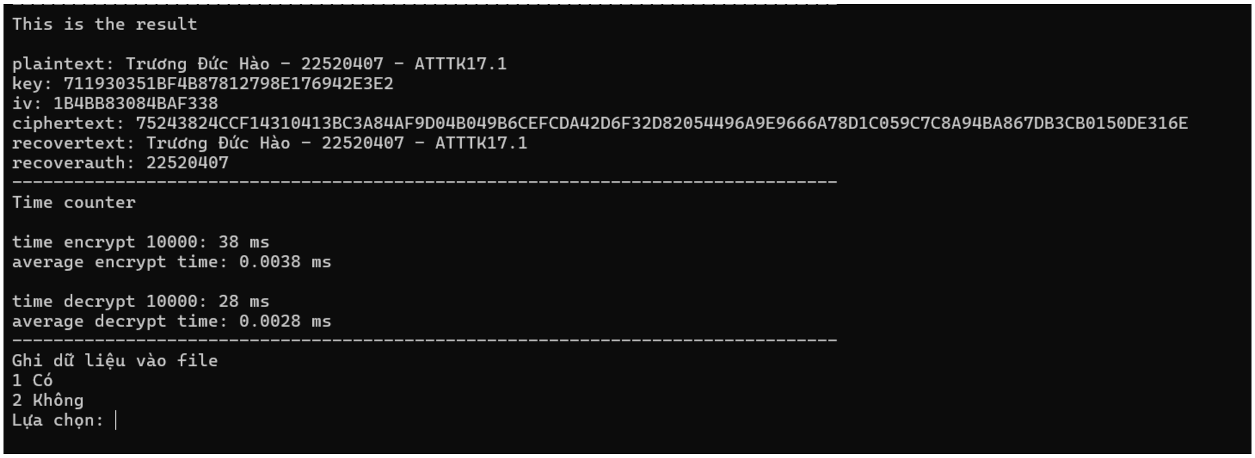
testcase1.txt (1 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0014	0.0011	0.00127	0.00167
CBC	0.0021	0.0020	0.0009	0.00102
CFB	0.0029	0.0031	0.0007	0.0015
OFB	0.0014	0.0015	0.0033	0.0027
CTR	0.0024	0.0024	0.001	0.0013
XTS	0.0030	0.0032	0.0042	0.002
GCM	0.0026	0.0025	0.0016	0.004
CCM	0.0038	0.0028	0.0027	0.0047

ECB vs CCM:



```
--------------------------------------------------------------------------------
This is the result

plaintext: Trương Đức Hào - 22520407 - ATTTK17.1
key: 711930351BF4B87812798E176942E3E2
ciphertext: 26D16F31B9AB8645A1458ADBB58B3264DEF670E43FC2141FA567719D7D964160DB8335316D59F667AD227DFBE7BC3012
recovertext: Trương Đức Hào - 22520407 - ATTTK17.1
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 14 ms
average encrypt time: 0.0014 ms

time decrypt 10000: 11 ms
average decrypt time: 0.0011 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: 1
Ghi file thành công
```

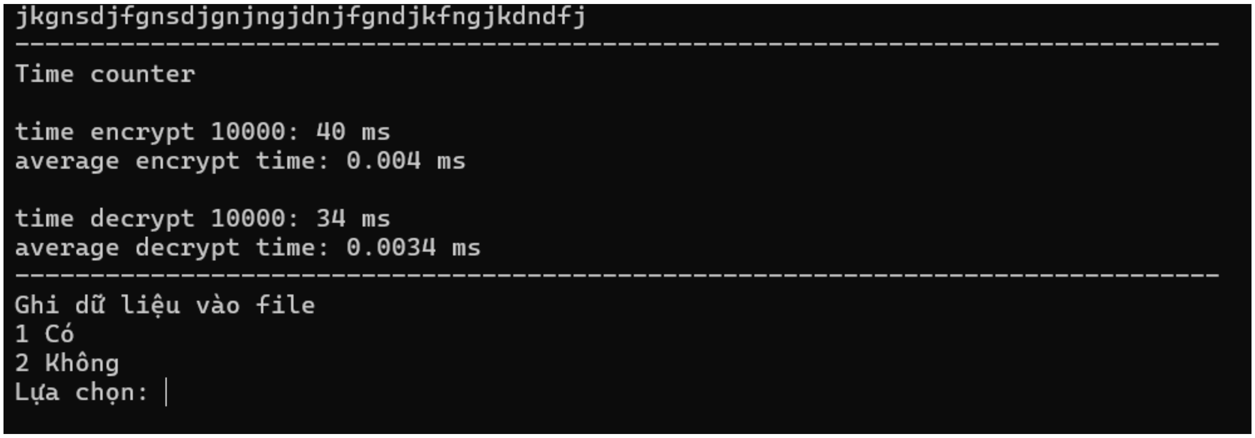


```
This is the result

plaintext: Trương Đức Hào - 22520407 - ATTTK17.1
key: 711930351BF4B87812798E176942E3E2
iv: 1B4BB83084BAF338
ciphertext: 75243824CCF14310413BC3A84AF9D04B049B6CEFCDA42D6F32D82054496A9E9666A78D1C059C7C8A94BA867DB3CB0150DE316E
recovertext: Trương Đức Hào - 22520407 - ATTTK17.1
recoverauth: 22520407
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 38 ms
average encrypt time: 0.0038 ms

time decrypt 10000: 28 ms
average decrypt time: 0.0028 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: 
```

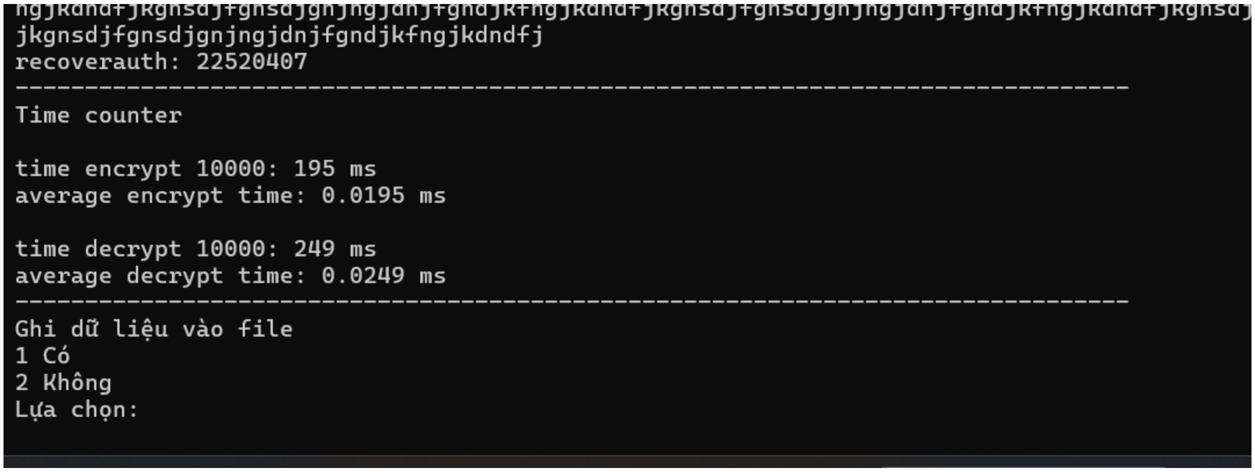
testcase2.txt (20 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.004	0.0034	0.0087086	0.0089201
CBC	0.0141	0.0047	0.0291228	0.0302103
CFB	0.012	0.0081	0.0291984	0.0280123
OFB	0.0158	0.0157	0.0282953	0.0027321
CTR	0.0047	0.0057	0.0098595	0.0097851
XTS	0.0144	0.014	0.0204288	0.0210521
GCM	0.0083	0.013	0.0125633	0.0125012
CCM	0.0195	0.0249	0.0340690	0.0363210

ECB vs CCM:



```
jkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfj
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 40 ms
average encrypt time: 0.004 ms

time decrypt 10000: 34 ms
average decrypt time: 0.0034 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: 
```

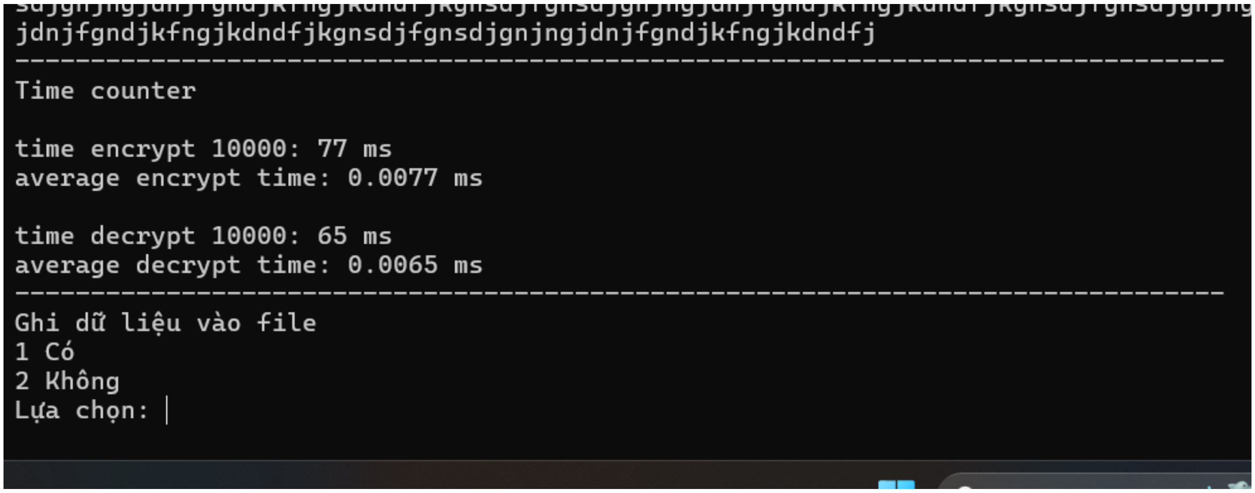


```
ngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdj
jkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfj
recoverauth: 22520407
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 195 ms
average encrypt time: 0.0195 ms

time decrypt 10000: 249 ms
average decrypt time: 0.0249 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

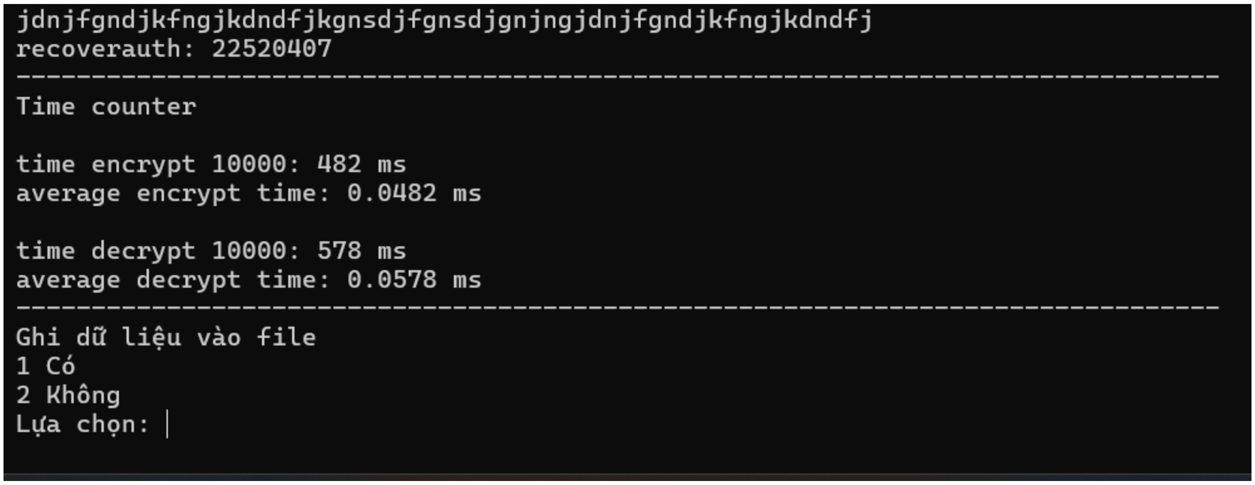
testcase3.txt (50 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0077	0.0065	0.0183947	0.0195214
CBC	0.0335	0.0117	0.0669401	0.0670123
CFB	0.0355	0.0187	0.0662011	0.0672143
OFB	0.0333	0.0335	0.0670936	0.0681420
CTR	0.0069	0.008	0.0180896	0.0184102
XTS	0.037	0.0358	0.0485905	0.0471252
GCM	0.0129	0.0213	0.0264517	0.0263517
CCM	0.0482	0.0578	0.0801763	0.0802014

ECB vs CCM:



```
sdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjng
jdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfj
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 77 ms
average encrypt time: 0.0077 ms

time decrypt 10000: 65 ms
average decrypt time: 0.0065 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

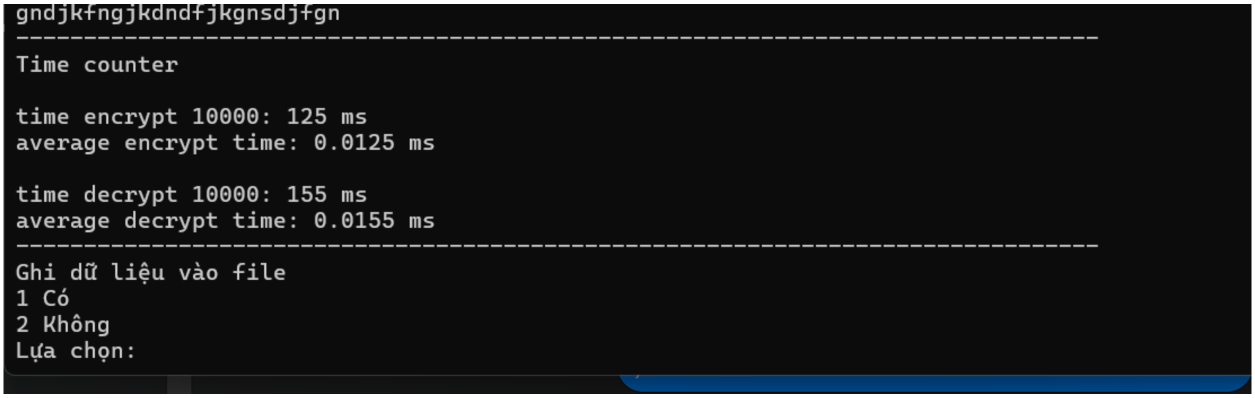


```
jdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfj
recoverauth: 22520407
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 482 ms
average encrypt time: 0.0482 ms

time decrypt 10000: 578 ms
average decrypt time: 0.0578 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

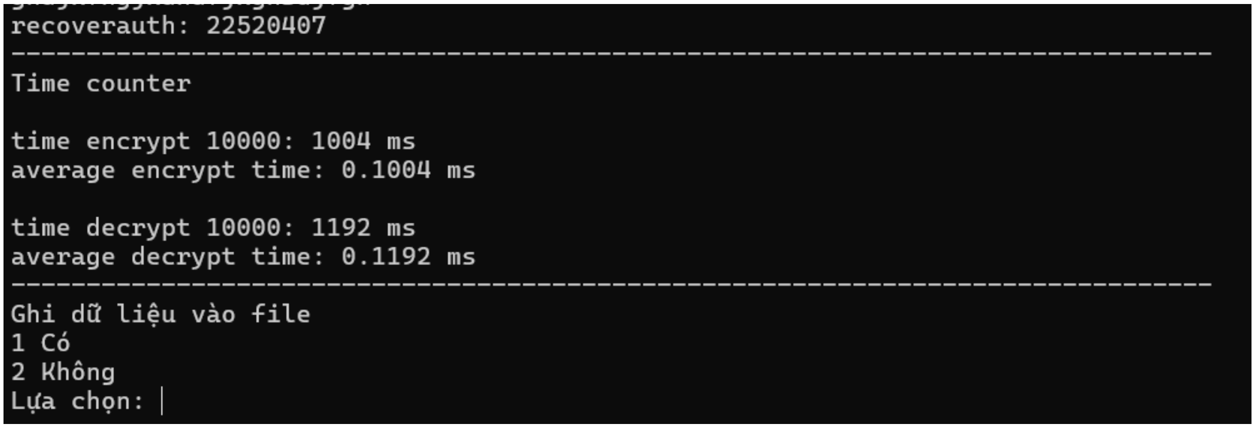
testcase4.txt (100 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0125	0.0155	0.0325843	0.0337514
CBC	0.0614	0.0182	0.1322160	0.1420240
CFB	0.0658	0.0297	0.1356760	0.1375214
OFB	0.0624	0.0634	0.1329210	0.1324853
CTR	0.0169	0.0175	0.0337018	0.0347512
XTS	0.0774	0.0806	0.0970175	0.0915142
GCM	0.0357	0.0541	0.0488964	0.0452032
CCM	0.1004	0.1192	0.1212740	0.1356201

ECB vs CCM:



```
gndjkfngjkdndfjkgnsdjfgn
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 125 ms
average encrypt time: 0.0125 ms

time decrypt 10000: 155 ms
average decrypt time: 0.0155 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

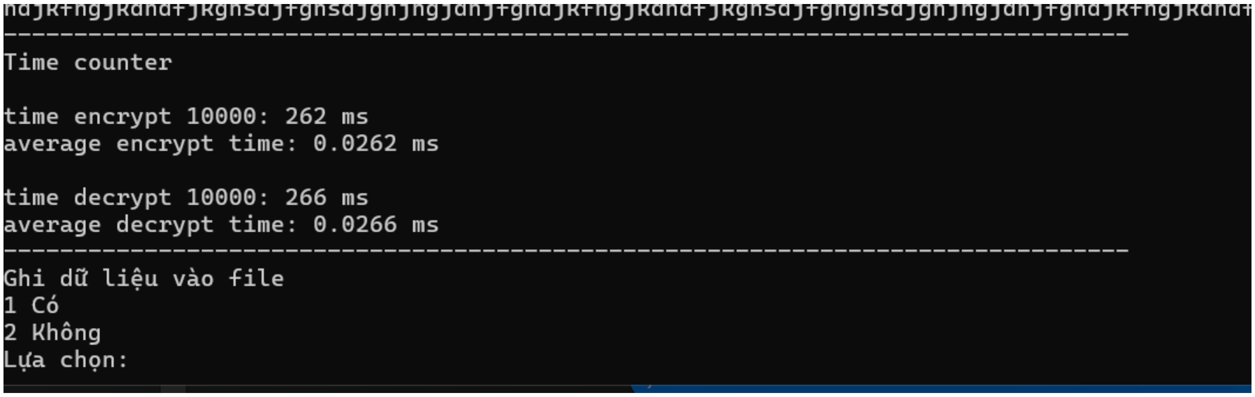


```
recoverauth: 22520407
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 1004 ms
average encrypt time: 0.1004 ms

time decrypt 10000: 1192 ms
average decrypt time: 0.1192 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

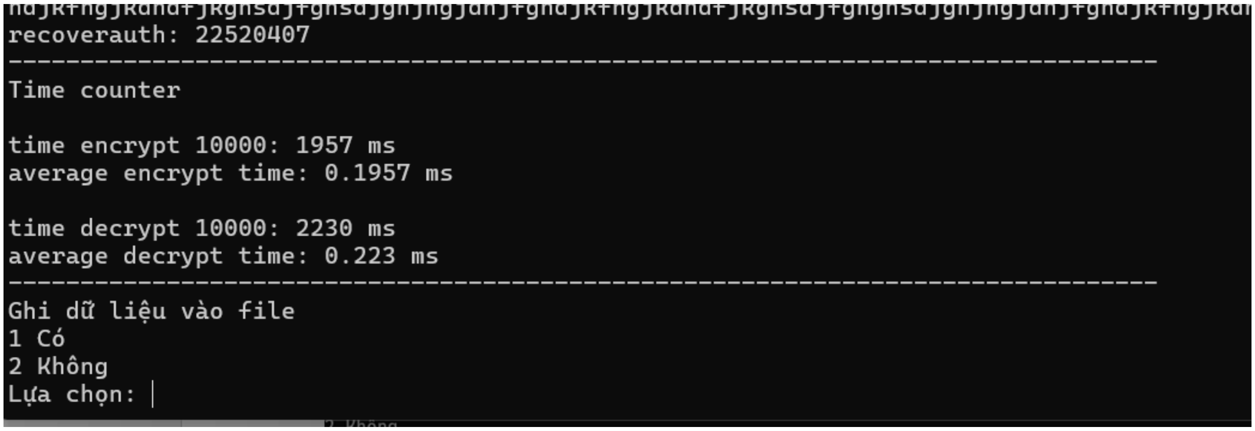
testcase5.txt (200 KB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.0262	0.0266	0.0461604	0.0452173
CBC	0.1119	0.0329	0.1921180	0.2014253
CFB	0.1203	0.0534	0.1949320	0.2102541
OFB	0.123	0.1239	0.1978380	0.1952302
CTR	0.0305	0.0274	0.0493176	0.0486231
XTS	0.1405	0.1324	0.1878430	0.1935620
GCM	0.0549	0.0815	0.0743966	0.0813201
CCM	0.1957	0.223	0.2343270	0.2475325

ECB vs CCM:



```
hdjkfngjkdndfjkghsdjfghsdjghjngjdnjfghdjkfngjkdndfjkghsdjfghghsdjghjngjdnjfghdjkfngjkdndf
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 262 ms
average encrypt time: 0.0262 ms

time decrypt 10000: 266 ms
average decrypt time: 0.0266 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

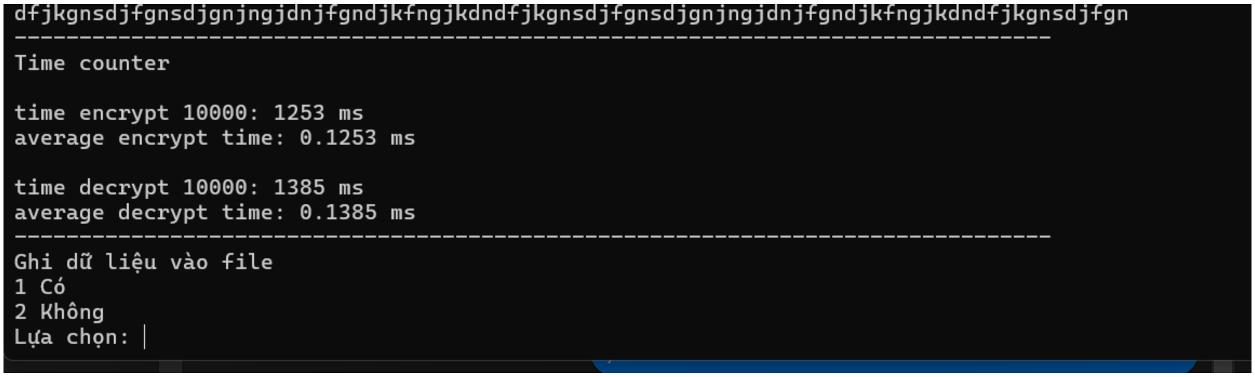


```
ndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgngnsdjgnjngjdnjfgndjkfngjkdn
recoverauth: 22520407
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 1957 ms
average encrypt time: 0.1957 ms

time decrypt 10000: 2230 ms
average decrypt time: 0.223 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: |
```

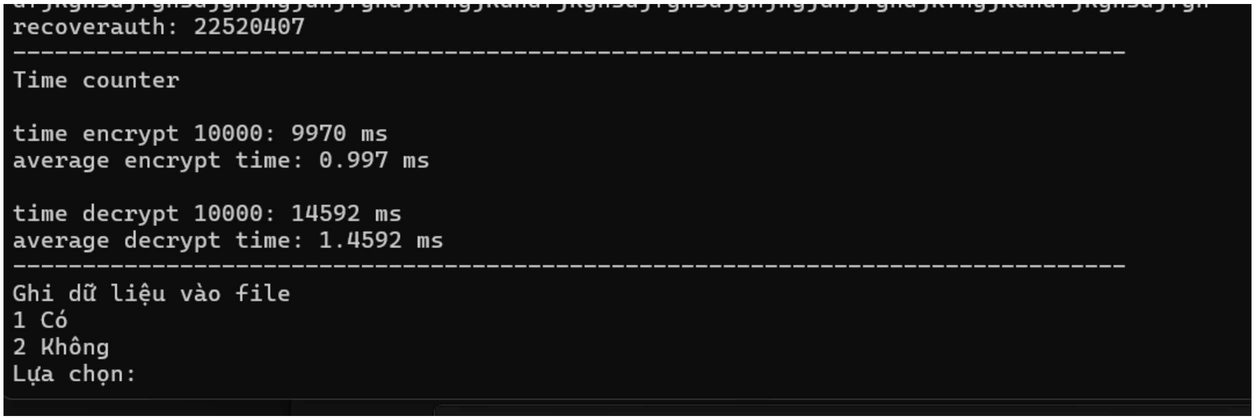
testcase6.txt (1024 KB = 1 MB)

Mode	Encrypt (Window)	Decrypt (Window)	Encrypt (Linux)	Decrypt (Linux)
ECB	0.1253	0.1385	0.326627	0.331456
CBC	0.6156	0.1672	1.325160	1.312521
CFB	0.6628	0.2531	1.116080	1.214232
OFB	0.6927	0.639	1.389250	1.365215
CTR	0.2012	0.1463	0.240121	0.253123
XTS	0.77	0.751	0.947407	0.938215
GCM	0.2727	0.6684	0.415180	0.423652
CCM	0.997	1.492	1.233940	1.223145

ECB vs CCM:

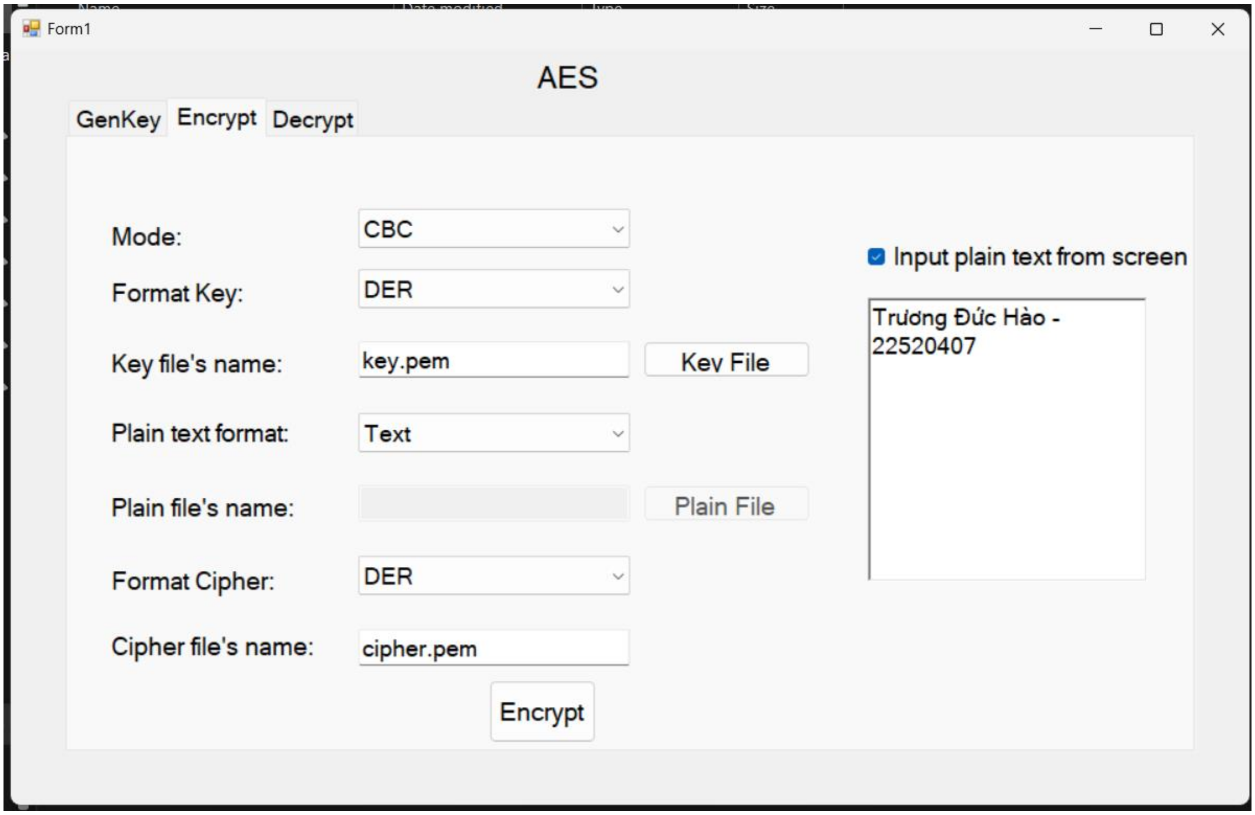


```
dfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgnsdjgnjngjdnjfgndjkfngjkdndfjkgnsdjfgn
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 1253 ms
average encrypt time: 0.1253 ms

time decrypt 10000: 1385 ms
average decrypt time: 0.1385 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn: |
```



```
recoverauth: 22520407
--------------------------------------------------------------------------------
Time counter

time encrypt 10000: 9970 ms
average encrypt time: 0.997 ms

time decrypt 10000: 14592 ms
average decrypt time: 1.4592 ms
--------------------------------------------------------------------------------
Ghi dữ liệu vào file
1 Có
2 Không
Lựa chọn:
```

GUI BUILD:



Form1

AES

GenKey | Encrypt | Decrypt

Mode: CBC

Format Key: DER

Key file's name: key.pem

Plain text format: Text

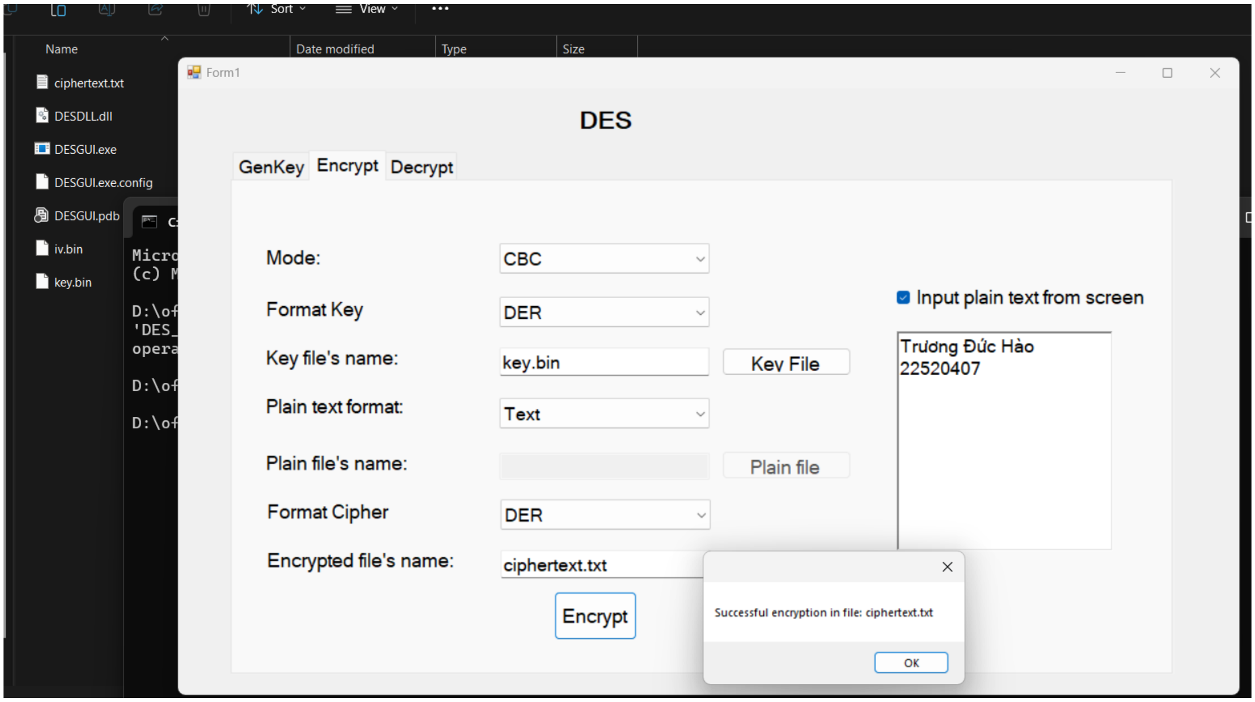
Plain file's name:

Format Cipher: DER

Cipher file's name: cipher.pem

☑ Input plain text from screen

Trương Đức Hào - 22520407



DES

Mode: CBC

Format Key: DER

Key file's name: key.bin

Plain text format: Text

Plain file's name:

Format Cipher: DER

Encrypted file's name: ciphertext.txt

☑ Input plain text from screen

Trương Đức Hào
22520407

Successful encryption in file: ciphertext.txt

Comments and Comparison:

- AES mode nhanh hơn DES mode trong cả 6 testcases trên cả Window hoặc Linux
- Thời gian thực thi trên Linux nhanh hơn Window ở mode DES và ngược lại, vấn đề có thể đến từ cài đặt hệ thống, quản lý tài nguyên giữa 2 hệ điều hành này.
- Thời gian thực thi càng lâu khi file có kích thước càng lớn
- Mode ECB, CTR, GCM có thời gian thực thi ngắn hơn đáng kể so với những mode khác trong AES
- Với những file có kích thước lớn, nên giải phóng bộ nhớ sau khi sử dụng để thực thi tốt hơn.