Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: Mật mã học

Kỳ báo cáo: Buổi 02 (Session 02)

Tên chủ đề: chủ đề môn học

Ngày báo cáo: 28/03/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT219.N22.ATCL

STT	Họ và tên	MSSV	Email
1	Lê Thị Huyền Trang	21522694	21522694@gm.uit.edu.vn
2	Phạm Thái Bảo	21520156	21520156@gm.uit.edu.vn
3	Trần Tấn Hải	21522036	21522036@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Chậm lại và suy nghĩ 1	100%	
2	Chậm lại và suy nghĩ 2	100%	
3	Bài tập 1	100%	
4	Bài tập 2	100%	
5	Bài tập 3	100%	
6	Bài tập 4	100%	
7	Bài tập 5	100%	
8	Bài tập 6	100%	
9	Bài tập 7	0%	
10	Bài tập luyện tập 1	0%	
11	Bài tập luyện tập 2	0%	
12	Bài tập luyện tập 3	0%	

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

1. **Chậm lại và suy nghĩ 1: AES::DEFAULT_KEYLENGTH và AES::BLOCKSIZE bằng bao nhiêu?**

   AES::DEFAULT_KEYLENGTH = 16 byte. Trong thuật toán AES, key có thể là 128 bit, 192 bit hoặc 256 bit

   AES::BLOCKSIZE = 16 byte

```
PS C:\ThucHanh> ./aes_cbc_sample.exe
AES::DEFAULT_KEYLENGTH = 16
AES::BLOCKSIZE = 16
```

2. **Chậm lại và suy nghĩ 2: CTR_Mode là gì, các thông số trong code mẫu có ý nghĩa như thế nào?**

   The Counter (CTR) mode is a typical block cipher mode of operation using block cipher algorithm. CTR involves XOR-ing a sequence of pad vectors with the plaintext and ciphertext blocks. In the CTR mode, we start off with a random seed, *s*, and compute pad vectors according to the formula:

$$V_i = E_K(s+i-1)$$

   : where E_K denotes the block encryption algorithm using key *K*, V_i is a pad vector, and *i* is the vector's offset starting from 1.

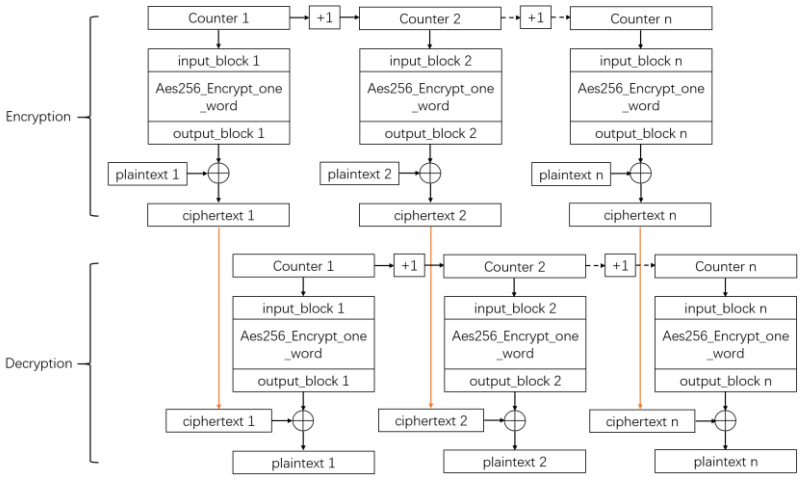
   Now that the vectors have been generated, encryption can proceed using the following formula:

$$C_i = V_i \oplus B_i$$

   Decryption is carried out in a similar way:

$$B_i = V_i \oplus C_i$$

   CTR makes use of a single encryption algorithm for both encryption and decryption.



```
PS D:\ThucHanh> ./benchmarks.exe
AES/CTR benchmarks...
  2.7 GHz cpu frequency
  0.451837 cycles per byte (cpb)
  5698.78 MiB per second (MiB)
PS D:\ThucHanh>
```

The first line indicates the algorithm name, which is AES using CTR mode in this case.

The second line indicates CPU frequency. CPU frequency is measured in Hertz (Hz), which represents the number of clock cycles per second. A lower CPU frequency means that the CPU can execute instructions and process data more slowly.

The third line indicates Cycles per byte. Cycles per byte is measured in cpb, which represents the number of clock cycles required to process one byte of data. A lower cpb means that the algorithm is faster, as it can process more data in a shorter amount of time.

The last line indicates Throughput. Throughput is typically measured in MiB/s (mebibytes per second), which represents the amount of data that can be processed per second. It is calculated as the product of the CPU frequency and cpb, divided by 1024.

3. Bài tập 1: Code thêm để so sánh tốc độ AES so với tốc độ mã hoá của thuật toán DES

According to cycles per byte (cpb) metric, we can conclude that the AES system is significant faster than DES system (35.6755 cpb of DES > 2.13149 cpb of AES)

DES result:

```
Nhap plain: Test with input less than 64-bit
key: 5073F55768297BFF
iv: 8DA894AD1845C686
cipher text: CCD46F67EA8C675903714299310C816DA874D45795C445A7FBD24AED63EA13FDAB33169514F5045C
DES/CBC benchmarks...
Benchmark for Encryption
  2.7 GHz cpu frequency
  35.6755 cycles per byte (cpb)
  72.1762 MiB per second (MiB)
```

AES result:

```
Nhap plain: Test with input less than 64-bit
key: 4A473A8700E284C0AF75AB1B5EFB86AA
iv: 9725E87D4C61033DFC4DBE797FBD544F
plain text: Test with input less than 64-bit
Benchmark for encryption
AES/CBC benchmarks...
  2.7 GHz cpu frequency
  2.13149 cycles per byte (cpb)
  1208.04 MiB per second (MiB)
```

4. Bài tập 2: Tương tự với quá trình mã hoá, so sánh tốc độ của quá trình giải mã AES so với DES

Note that the plaintext, key, and iv are the same as previous exercise.

According to cycles per byte (cpb) metric, we can conclude that the AES system is significant faster than DES system (35.6755 cpb of DES > 2.13149 cpb of AES)

DES result:

```
recovered text: Test with input less than 64-bit
DES/CBC benchmarks...
Benchmark for decryption
  2.7 GHz cpu frequency
  80.1519 cycles per byte (cpb)
  32.1255 MiB per second (MiB)
Press any key to continue . . .
```

AES result:

```
AES/CBC benchmarks...
Benchmark for decryption
  2.7 GHz cpu frequency
  0.399041 cycles per byte (cpb)
  6452.78 MiB per second (MiB)
recovered text: Test with input less than 64-bit
Press any key to continue . . .
```

5. Bài tập 3: plaintext hỗ trợ đầu vào bao gồm các kí tự thuộc UTF-16

```
D:\Studying_stuffs\2_HK2\NT219\ThucHanh\Test.exe
key: F3F8DEB11EA03201F1D36D45697BEB91
iv: 80F56B6F2B2FE68596A92202859E28BB
plain text: Input hỗ trợ dữ liệu dạng UTF16 (tiếng việt)
cipher text: 723945E0B120194F850C42E558F6855AEEBBEF40C49967DD6610D1ED0FED58A07EDB2863B7DAEDD85F46D5B601711F947D50F4EED71
4BE63F13C20FC506615D0
recovered text: Input hỗ trợ dữ liệu dạng UTF16 (tiếng việt)
Press any key to continue . . .
```

6. Bài tập 4: Đầu vào plaintext được nhập thủ công vào chương trình.

```
string plain;
wstring wplain;
wcout<<L"Nhập plain: ";
std::getline(wcin,wplain);
plain = ws2s(wplain);
```

7. Bài tập 5: Secret Key và IV nhập vào thủ công từ chương trình

```
D:\Studying_stuffs\2_HK2\NT219\ThucHanh\Test.exe
Nhập plain: Dữ liệu test có hỗ trợ UTF16 (tiếng việt)
Nhập key hay random:
1. Nhập
2. Random
Lựa chọn: 1
Nhập dữ liệu key: Test key
Nhập iv hay random:
1. Nhập
2. Random
Lựa chọn: 1
Nhập dữ liệu iv: Test IV
key: 546573742068657900006FD839010000
iv: 54657374204956000000000000000000
plain text: Dữ liệu test có hỗ trợ UTF16 (tiếng việt)
cipher text: 234523055F3EF687663C131269AF6C06644318D25A0206DEA39069EC4EA412D7F61A26362E5DB62020889A21080C497C1B2ED4707DF
4E0A7627D0FB80D0316A0
recovered text: Dữ liệu test có hỗ trợ UTF16 (tiếng việt)
Press any key to continue . . .
```

8. Bài tập 6: Sử dụng thuật toán mã hoá AES với các mode còn lại được hỗ trợ ECB, CBC, OFB, CFB, CTR, XTS, CCM, GCM

ECB:

```
key: 0649EA109604CEFE418303C80FDA0E9D
plain text: ECB Mode Test
cipher text: 4BB38AA8D122F35351D746CF732D1034
recovered text: ECB Mode Test
```

CBC:

```
key: CE2CAEDF1195F870128D8B12B0B0448F
iv: 921A82064D299FC2414EB06E3F2EA254
plain text: CBC Mode Test
cipher text: D522CD6A52BFF5FA223BF771F4502349
recovered text: CBC Mode Test
```

OFB:

```
key: F9A2A091D704B398E7164AF103F35BE3
iv: B0AF15F74052D2B9D8CAE808B969F431
plain text: OFB Mode Test
cipher text: 07B5535516CB2C51EE22D65C53
recovered text: OFB Mode Test
```

CFB:

```
key: 45B456B1F6E12A586A607E596DAFBAF2
iv: F904974CE93B05C003CC4D9CA2297371
plain text: CFB Mode Test
cipher text: E75628B172D84152ADCD2C2089
recovered text: CFB Mode Test
```

CTR:

```
key: 561C3E814AFD2B1065F95FDEE4F99DD5
iv: 21D22904BC91355DCA5068F5420B9288
plain text: CTR Mode Test
cipher text: DACB09C2E20749216DD7A304CE
recovered text: CTR Mode Test
```

XTS:

```
key: 914E405D2326F8982B4FD2CE710A92A4640CAF99B824F2F0181D9203F501AC8F
iv: A1C3EC7CDE2D9863437C00D2DCEBC901
plain text: XTS (XEX-based Tweaked Codebook Mode with Cipher Text Stealing) là một mode of operation trong mật mã đối xứng được sử dụng để mã
hóa dữ liệu trên các thiết bị lưu trữ như ổ đĩa cứng hoặc USB. Nó sử dụng hai khóa để tăng cường tính bảo mật so với các mode khác.
cipher text: CDBCB77B4A5AC3CCD84FF7F64C3C4FB23D756395D7AB8E75A8607749474C0F0CB1916E88BDE8887B0E93E096ED9717FA4DB63CC5EFB10CBC14D68B77415D03A5B
3CF6064683755B61397854557EDA0791F8F3DC9EAF83603B57378A63171761FF020189737550C5DF0D6928F4250C5B5EF804BC1807AEB561C4469D60C40AA3ECC3BE44AD37BE87
019C0FD5A5D5115FC498F486CF4788B84AD764C7E9111E84747A19F041B5E3DA965346E9C7BF49C6CD77C66501A980F1848B4D58097AE1A520EEB38B1CD1E1120C570938344 2B7
88AF1586DD9D12ADCF0AB437A742437BE8A07743D289FF438118382EAA8B976984840180DD8FE6C42AABBF69531691C8AC0B1471EECFD98082E65CF408849219DE284E756832D7
CA457191475C6E158FF53EC5207C8429D26A5F4F1DFA376548B51BD2B5DFF9CC6051EF4B774ADB3BEC71F72C1AD82471EC30D0A
recovered text: XTS (XEX-based Tweaked Codebook Mode with Cipher Text Stealing) là một mode of operation trong mật mã đối xứng được sử dụng để
 mã hóa dữ liệu trên các thiết bị lưu trữ như ổ đĩa cứng hoặc USB. Nó sử dụng hai khóa để tăng cường tính bảo mật so với các mode khác.
```

CCM:

```
key: 7ACE2215CE37DF7DAED28B9EE5060B35
iv: 77ABF544682311A8B0B77768D6C311BE
plain text: CCM Mode Test
cipher text: 4CEDDA93773262889D7B034FA472635C7B6978A64D0111F86AC18FD6E1
recovered text: CCM Mode Test
```

GCM:

```
key: F09CD29AA470E21036A2DB03C1773E0F
iv: 8A8EE79F5D848719BA97BB9EB66889B5
plain text: GCM Mode Test
cipher text: A7D61C5512DE5CD97417A789893311241C699A48A3D41A9B93F0E09A65
recovered text: GCM Mode Test
Press any key to continue . . .
```

9. **Bài tập 7: Tìm hiểu điểm yếu của mode ECB và khai thác trên code AES có hỗ trợ nhập đầu vào đã build, với key và iv cố định.**

10. **Bài tập luyện tập 1: Đánh giá hiệu năng của thuật toán AES với các mode ECB, CBC, OFB, CFB, CTR, XTS, CCM, GCM**

11. **Bài tập luyện tập 2: Đưa ra điểm yếu của thuật toán AES và viết chương trình tấn công tìm ra được plaintext của thuật toán với các điều kiện**

12. **Bài tập luyện tập 3: Đưa ra điểm yếu của mode CBC và viết chương trình tấn công. (Chỉ cần trình bày logic của chương trình, không cần thực hiện thành công quá trình tấn công)**