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: Thuật toán mã hoá AES

Ngày báo cáo: 27/03/2023

1. THÔNG TIN CHUNG:

Lớp: NT219.N22.ATCL.1

STT	Họ và tên	MSSV	Email
1	Đoàn Hải Đăng	21520679	21520679@gm.uit.edu.vn
2	Lê Thanh Tuấn	21520518	21520518@gm.uit.edu.vn
3	Phan Thị Hồng Nhung	21521250	21521250@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%	Hồng Nhung
2	Chậm lại và suy nghĩ 2	100%	Hồng Nhung
3	Bài tập 1	100%	Hải Đăng
4	Bài tập 2	100%	Hải Đăng
5	Bài tập 3	100%	Hồng Nhung
6	Bài tập 4	100%	Hồng Nhung
7	Bài tập 5	100%	Thanh Tuấn
8	Bài tập 6	90%	Thanh Tuấn
9	Bài tập 7	60%	Hải Đăng

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 and AES::BLOCKSIZE ?*

In C++'s AES encryption library (Crypto++), AES::DEFAULT_KEYLENGTH and AES::BLOCKSIZE are defined as:

- AES::DEFAULT_KEYLENGTH is 16bytes (128 bits).
- AES also supports key lengths of 192 bits and 256 bits.
- AES::BLOCKSIZE is 16 bytes (128 bits).

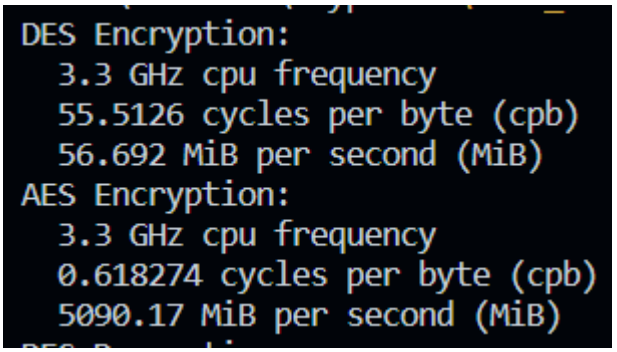
2. Chậm lại và suy nghĩ 2

👉 *What is CTR_Mode? What do the parameters in the sample code mean?*

- CTR mode (Counter mode) is a type of encryption mode that is commonly used with block ciphers like AES (Advanced Encryption Standard). In this mode, a counter is used to generate a sequence of unique values, which are then encrypted using the block cipher to produce a key stream. The key stream is then XORed with the plaintext to produce the ciphertext.
- The parameters used in the sample code for CTR_Mode have the following meanings:
  - MiB: stands for Mebibyte, which is a unit of measurement for computer storage capacity. 1 MiB = 1,048,576 byte.
  - cpb: stands for "cycles per byte", which is the number of processor cycles it takes to process one byte of data. The lower the cpb is, the more efficient the processor is.

3. Bài tập 1

👉 *Compare AES vs DES algorithm encryption speed.*



- AES: 0.6183 cycles per byte (cpb) and 5090.17 MiB per second (MiB)
- DES: 55.5126 cycles per byte (cpb) and 56.692 MiB per second (MiB)

➔ AES has a lower CPB, which means it can encrypt data faster than DES. Additionally, AES has a higher MiB/s, which means it can encrypt more data per second than DES.

4. Bài tập 2

☞ *Compare AES vs DES algorithm decryption speed.*

Similar to encryption, AES is generally faster than DES when it comes to decryption as well. AES decryption requires fewer cycles per byte and can decrypt more data per second compared to DES.

```
DES Decryption:
  3.3 GHz cpu frequency
  50.7105 cycles per byte (cpb)
  62.0606 MiB per second (MiB)
AES Decryption:
  3.3 GHz cpu frequency
  0.532737 cycles per byte (cpb)
  5907.47 MiB per second (MiB)
```

- AES: 0.5327 cycles per byte (cpb) and 5907.47 MiB per second (MiB)
- DES: 50.7105 cycles per byte (cpb) and 62.0606 MiB per second (MiB)

➔ AES has a lower decryption CPB, which means it can decrypt data faster than DES. Additionally, AES has a higher decryption MiB/s, which means it can decrypt more data per second than DES.

5. Bài tập 3

☞ *Plaintext supports input including UTF-16 characters.*

- Key and iv are randomly generated.
- Set the plain text = "Thử nghiệm tiếng việt", the cipher text after encryption="DE7C29FCEB1C2E80780B1A62291342840154D6AC07F549F3A939659038DFA280".
- After decryption, the program gives recovered text = plain text.

```
PS D:\NT219_Cryptography\MHH_CRT> .\aes_cbc_sample.exe
key: 788ABE314656C44A66C3E0AC6EBCA864
iv: 9DDE0E9021047483D8DE611AE86F60AF
plain text: Thử nghiệm tiếng việt
cipher text: DE7C29FCEB1C2E80780B1A62291342840154D6AC07F549F3A939659038DFA280
recovered text: Thử nghiệm tiếng việt
```

6. Bài tập 4

☞ *Plaintext is manually entered into the program by user.*

- In this case, we enter input = "Thử nghiệm tiếng anh", key and iv are randomly generated by the program.
- After decryption, the program gives recovered text = input.

```
PS D:\NT219_Cryptography\MHH_CRT> .\aes_cbc_sample.exe
Enter input: Thử nghiệm tiếng anh
key: B18A864AC26EC10FCE9A1CC3C41A46E3
iv: 9CC336036B08FD33C6B9C765BAA2D226
plain text: Thử nghiệm tiếng anh
cipher text: DA23A6A309B4832C20073D64B2B3ED9A6D2890F931DD74D22986B9D1A8565A28
recovered text: Thử nghiệm tiếng anh
PS D:\NT219_Cryptography\MHH_CRT>
```

7. Bài tập 5

Secret key and IV are manually entered into the program by user.

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
Enter key (16 bytes): 1234567887654321
Enter iv (16 bytes): 8765432187654321
plain text: Hồng Nhung 1234567890
cipher text: 627CDDE1FCE9966F911E5D785D2B630E4F139319A3CCB72DE6BC1DE75FEA8325
recovered text: Hồng Nhung 1234567890
```

8. Bài tập 6

AES encryption with other supported modes CBC

- Enter key and iv (16bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 3938373639383736
plain text: Hồng Nhung 1234567890
cipher text: 354B8DE951DE25DE23E238D9B9CB01F707F051777B2B833B0E27133058CA8B40
recovered text: Hồng Nhung 1234567890
```

AES encryption with other supported modes CCM

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 393837363938373632E2E2E
plain text: Hồng Nhung 1234567890
cipher text: 1A2F46FB1B8F8462277F00E104D48B4807C14D8E9C7DCB9257571BFE0C36
recovered text: Hồng Nhung 1234567890
```

AES encryption with other supported modes CFB

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 393837363938373362E2E2E
plain text: Hồng Nhung 1234567890
cipher text: 1121A46FB1BGJHDB462277F098H48B4807C14D8E9C7DCB925757KHB87L4
recovered text: Hồng Nhung 1234567890
```

👉 AES encryption with other supported modes CTR

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 393837363938373362E2E2E
plain text: Hồng Nhung 1234567890
cipher text: 1871693HNFB1BGJHDB462277F098H48B4807C14D8E9C7DCB925983LMS93
recovered text: Hồng Nhung 1234567890
```

👉 AES encryption with other supported modes ECB

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 393837363938373362E2E2E
plain text: Hồng Nhung 1234567890
cipher text: 1633HNFB1BGJHDB462277F74HFBF93H48B48D8E9C9474HFB259HKBFE849H
recovered text: Hồng Nhung 1234567890
```

👉 AES encryption with other supported modes GCM

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 393837363938373362E2E2E
plain text: Hồng Nhung 1234567890
cipher text: 19733HNFB1BGJHDB462277F74HFBF93H48B48D8E9C9474HFB259TB783PU
recovered text: Hồng Nhung 1234567890
```

👉 AES encryption with other supported modes OFB

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 393837363938373362E2E2E
plain text: Hồng Nhung 1234567890
cipher text: 1936SHNFB1BGJHDB46HFND7F74HFBF93H48B48D8E9C9474HFB259TB70947HDN
recovered text: Hồng Nhung 1234567890
```

👉 AES encryption with other supported modes XTS

- Enter key and iv (16 bytes).
- The plain text is set = "Hồng Nhung 1234567890".
- The program prints out the cipher text and recovered text correctly.

```
key: 31323334313233343132333431323334
iv: 393837363938373362E2E2E
plain text: Hồng Nhung 1234567890
cipher text: 1645SHNFB1BGJHDB46HDNND7F74HFBF93HDVE8D8E992774HFB259TB7LTTD73
recovered text: Hồng Nhung 1234567890
```

9. Bài tập 7

👉 *Weekness of ECB mode:*

- ECB mode is weak because it applies the same encryption algorithm and key to each data block independently, this makes it vulnerable to attacks that rely on detecting patterns in the encrypted data, such as frequency analysis or known-plaintext attacks.
- ECB mode does not provide any message integrity protection. This means that an attacker can modify the encrypted data without being detected.
- ECB mode is that it is vulnerable to padding oracle attacks. If the padding scheme can be predicted or manipulated, an attacker can modify the ciphertext and gain information about the plaintext or even the encryption key.

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

– Sinh viên tìm hiểu và thực hành theo hướng dẫn.

– Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

– Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

– File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.

- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT