Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin

2

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Thuật toán mã hoá AES

Thực hành môn Mật mã học

Tháng 3/2023

Lưu hành nội bộ

Mọi góp ý về tài liệu, vui lòng gửi về email inseclab@uit.edu.vn

BEE SECURE
INSECLAB

A. TỔNG QUAN

1. Mục tiêu

- Hiểu được thuật toán AES và mode CBC và các mode khác.
- Lập trình sử dụng được thư viện cryptopp trên đa nền tảng (window và linux)
- Tìm hiểu được một vài cuộc tấn công trên các thuật toán này

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

1. Phần mềm visual studio code

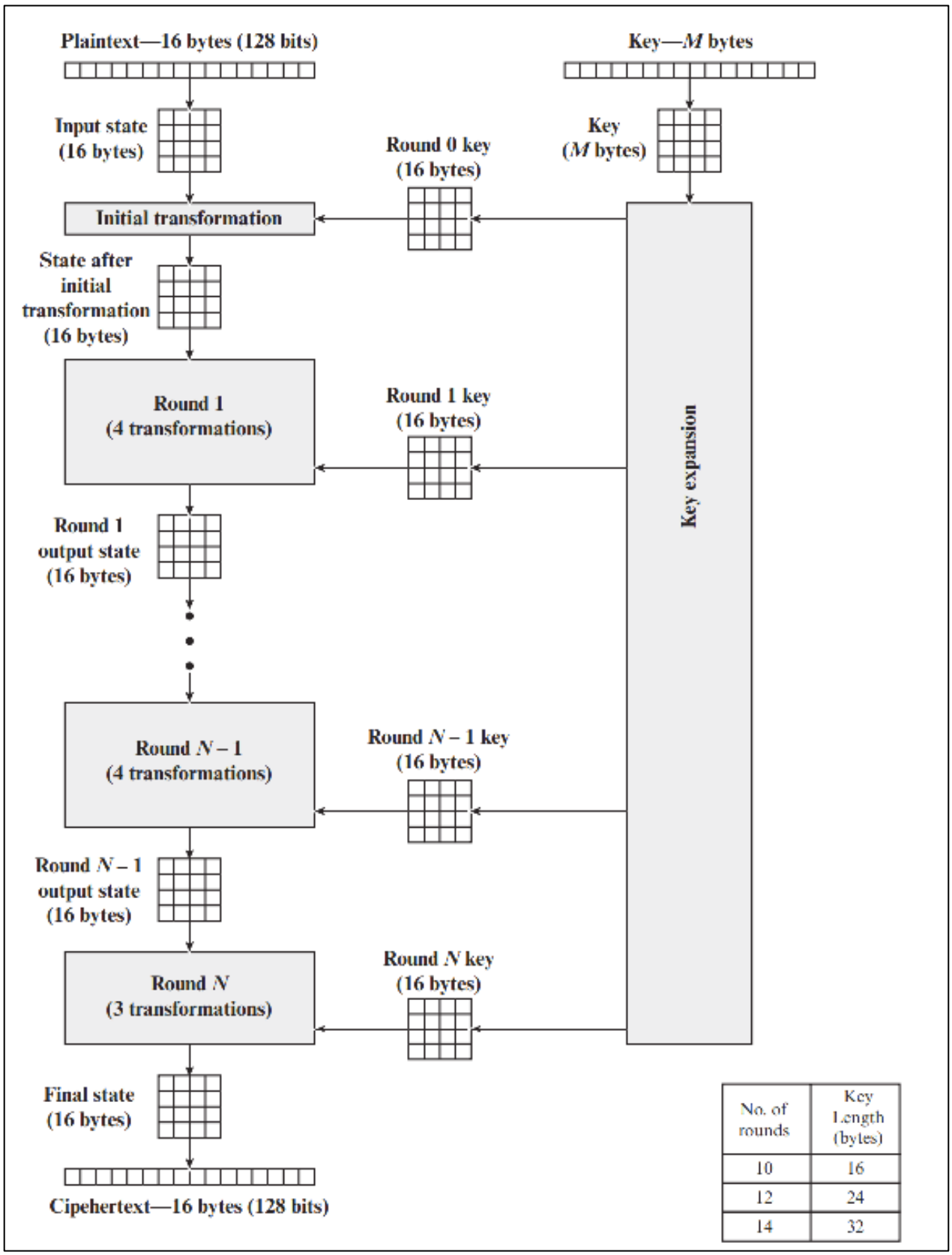
2. Hệ điều hành

- Sử dụng cả hệ điều hành linux và window để kiểm tra thuật toán.

C. THỰC HÀNH

1. Tìm hiểu mã hoá AES sử dụng thư viện cryptopp

Thuật toán AES



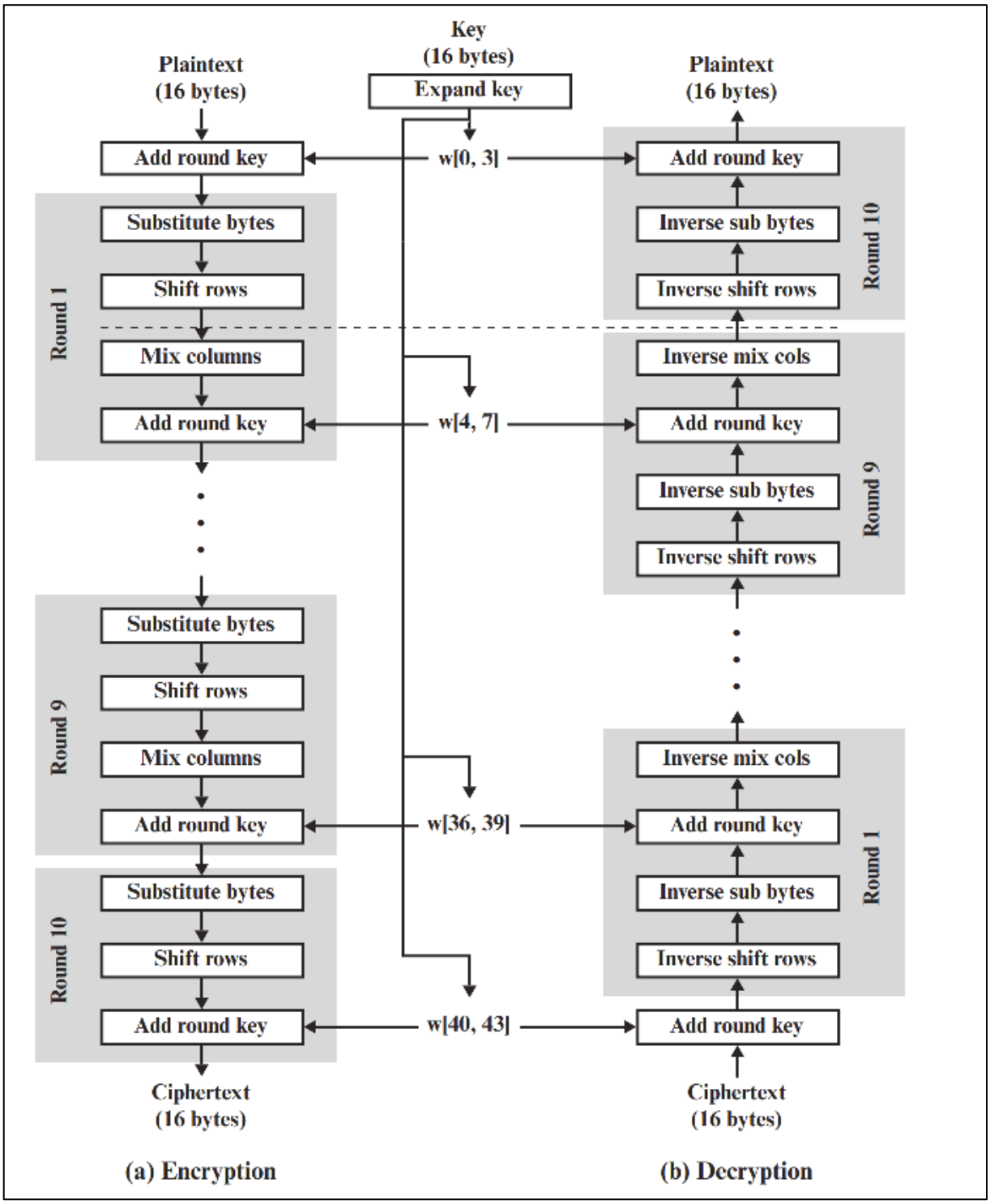
a) Mã hoá:

- Mã rõ có kích thước đầu vào là 16 bytes. Độ dài khoá có thể là 16,24, 32 bytes thì tên gọi thuật toán có thể thay đổi theo tên độ dài key như: AES-128, AES-192, AES-256.

- Đầu vào của thuật toán mã hoá và giải mã là một khối 16 byte. Mật mã sẽ bao gồm N vòng, tròn đó số vòng phụ thuộc vào độ dài khoá: 10 vòng cho khoá 16 byte, 12 cho 24 byte và 14 cho 32 byte.

b) Giải mã

- Quá trình giải mã sẽ ngược lại với quá trình mã hoá



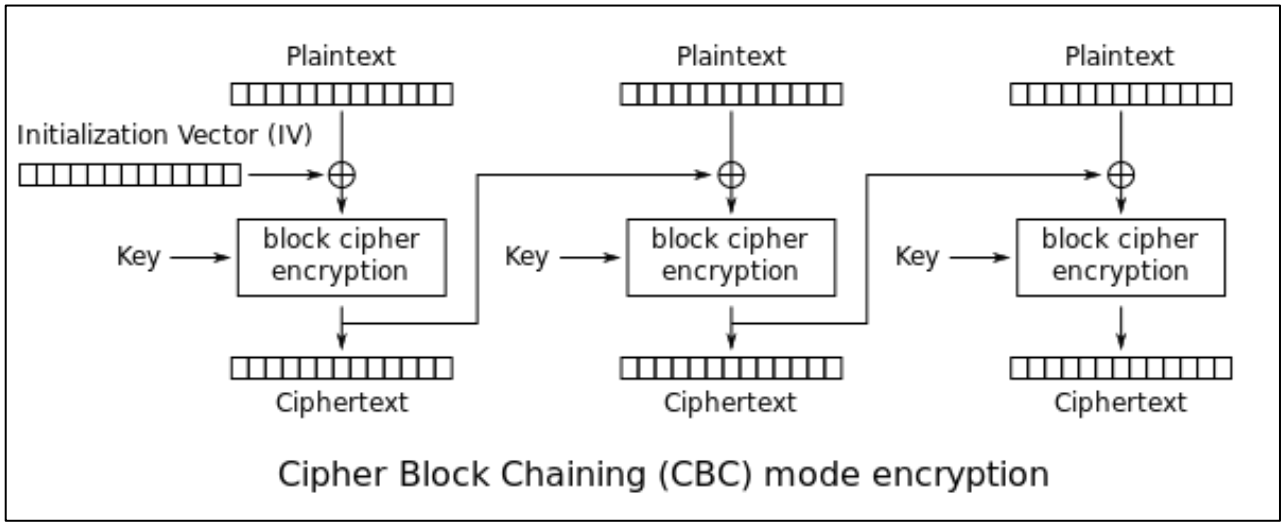
c) Thực hành viết chương trình mã hoá sử dụng thuật toán AES bằng thư viện cryptopp sử dụng mode CBC và so sánh với thuật toán DES.

- **Bước 1**: Sử dụng code mẫu được cung cấp:

```
AutoSeededRandomPool prng;

byte key[AES::DEFAULT_KEYLENGTH];
prng.GenerateBlock(key, sizeof(key));

byte iv[AES::BLOCKSIZE];
prng.GenerateBlock(iv, sizeof(iv));

string plain = "CBC Mode Test";
string cipher, encoded, recovered;
```

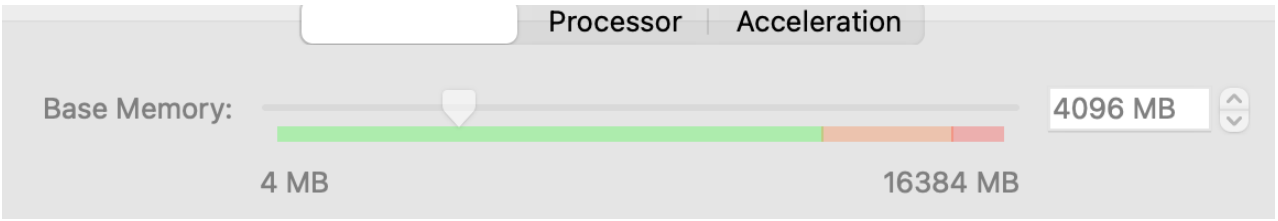
Chậm lại và suy nghĩ 1: AES::DEFAULT_KEYLENGTH và AES::BLOCKSIZE bằng bao nhiêu?

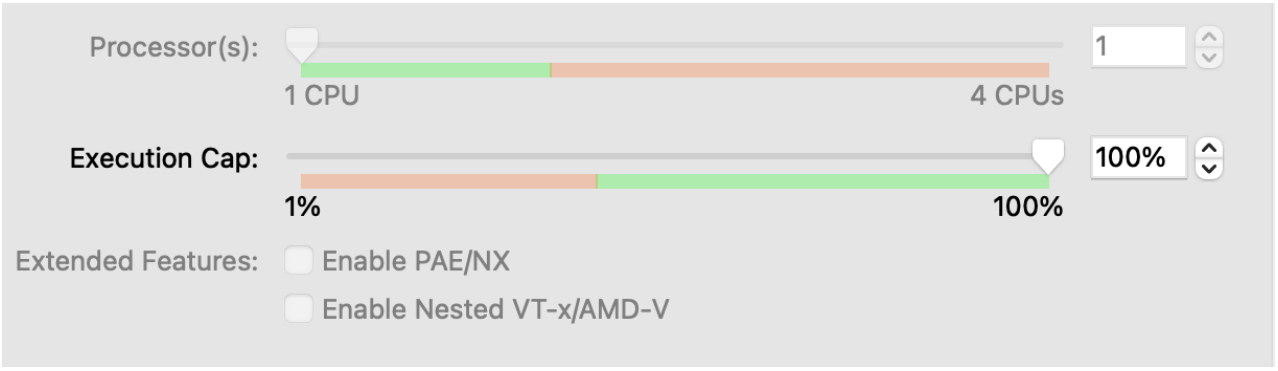
- **Bước 2**: Mã hoá:



- Sử dụng code mẫu benchmarks_AES.cpp được cung cấp, chạy thử và ghi nhận lại thông tin phần cứng thiết bị đang sử dụng

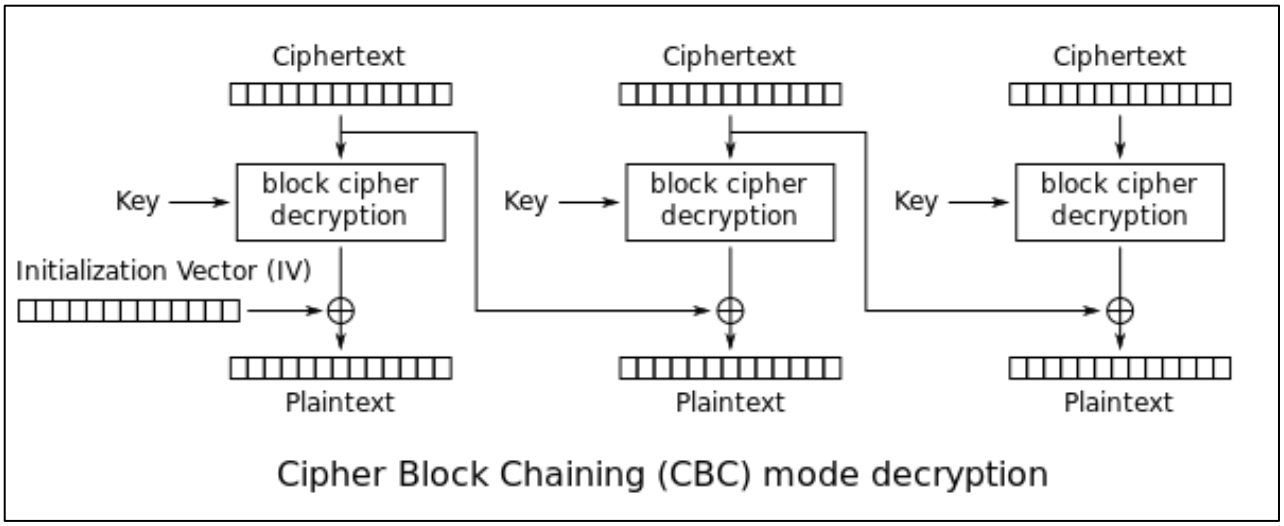
```
AES/CTR benchmarks...
  2.7 GHz cpu frequency
  0.936678 cycles per byte (cpb)
  2748.99 MiB per second (MiB)
```





Chậm lại và suy nghĩ 2: CTR_Mode là gì, các thông số trong code mẫu có ý nghĩa như thế nào? Tham khảo thêm tại: https://www.cryptopp.com/wiki/Benchmarks

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



- **Bài tập 2:** Tương tự với quá trình mã hoá, so sánh tốc độ của quá trình giải mã AES so với DES
- Các phần bài tập về lập trình thuật toán AES mode CBC, tương tự với DES
- **Bài tập 3:** plaintext hỗ trợ đầu vào bao gồm các kí tự thuộc UTF-16
- **Bài tập 4:** Đầu vào plaintext được nhập thủ công vào chương trình.
- **Bài tập 5:** Secret Key và IV nhập vào thủ công từ chương trình
- **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

2. Tấn công thuật toán và lược đồ

1. Khai thác mode ECB của thuật toán AES

- **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. Xem thêm tại: https://zachgrace.com/posts/attacking-ecb/

3. Bài tập luyện tập

- **Bài tập luyện tập 1:** Đánh giá hiệu năng của thuật toán AES với các mode ECB, CBC, OFB, CFB, CTR, XTS, CCM, GCM
  1. Trường hợp 1: Dữ liệu nhỏ hơn 64-bit
  2. Trường hợp 2: Dữ liệu dạng utf-16
  3. Trường hợp 3: Dữ liệu lớn hơn 1MB
  4. Báo cáo với 2 thông số Cycles Per Byte và MiB/Second. Có thể tham khảo công cụ đánh giá tại https://www.cryptopp.com/wiki/Benchmarks
- **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 sau:
  1. IV, key cố định (giả định là chỉ biết được IV, key là bí mật)
  2. Plaintext có độ dài đủ lớn và cố định.
  3. Chỉ cần trình bày logic của chương trình, không cần thực hiện thành công quá trình tấn công.
- **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)

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm Code, CSDL được export và chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1.
  - Ví dụ: [NT219.K11.ANTN.1]-Lab1_1852xxxx-.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

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

HẾT

Chúc các bạn hoàn thành tốt!