BÁO CÁO THỰC HÀNH

Bài thực hành số 1: Classical cryptography

Môn học: Nhập môn Mạng máy tính

Lớp: NT101.N12.MMCL.1

THÀNH VIÊN THỰC HIỆN (Nhóm TH1.02):

|  |  |  |
| --- | --- | --- |
| ***STT*** | ***Họ và tên*** | ***MSSV*** |
| **1** | **Hoàng Văn Anh Đức** | **20520890** |
| **2** | **Nguyễn Mạnh Cường** | **20520421** |
| **3** | **Nguyễn Trần Đức Anh** | **20520392** |
| **4** | **Lê Quang Minh** | **20520245** |

|  |
| --- |
| **Điểm tự đánh giá** |
| **10** |

ĐÁNH GIÁ KHÁC:

|  |  |
| --- | --- |
| Tổng thời gian thực hiện |  |
| Phân chia công việc |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

**Mục lục**

[**A.** BÁO CÁO CHI TIẾT 3](#_Toc115456003)

[1. Kick off : crack the code 3](#_Toc115456004)

[2. Caesar cipher 3](#_Toc115456005)

[3. Mono-alphabetic substitution cipher and frequency analysis : 6](#_Toc115456006)

[a. Nội dung 1 : Mono-alphabetic substitution cipher 6](#_Toc115456007)

[b. Nội dung 2 : Frequency analysis 9](#_Toc115456008)

[4. Block cipher 11](#_Toc115456009)

[a. Nội dung 1 :Tạo một tệp văn bản 100 byte bắt đầu bằng tên và ID sinh viên của bạn. Mã hóa tệp này dưới dạng văn bản rõ với ít nhất ba chế độ sử dụng OpenSSL (key và IV (nếu cần) là do bạn chọn). 11](#_Toc115456010)

[5. Encryption Mode – ECB vs. CBC 12](#_Toc115456011)

[a. Nội dung 1 : Mã hóa dùng ECB && CBC : 12](#_Toc115456012)

[b. Nội dung 2: Chọn hình ảnh khác, lặp lại thử nghiệm ở trên và báo cáo quan sát 14](#_Toc115456013)

[6. Padding : 15](#_Toc115456014)

[a. Nội dung 1 : Sử dụng các chế độ ECB, CBC, CFB và OFB để mã hóa tệp (bạn có thể chọn bất kỳ mật mã). Vui lòng báo cáo chế độ nào có đệm và chế độ nào không. Đối với những trường hợp không cần đệm, vui lòng giải thích lý do. 15](#_Toc115456015)

[b. Nội dung 2 : Luyện tập đệm của mật mã khối 16](#_Toc115456016)

[**B.** TÀI LIỆU THAM KHẢO 17](#_Toc115456017)

# BÁO CÁO CHI TIẾT

## Kick off : crack the code

Dựa vào hình để tìm code 3 chữ số

Text

Description automatically generated with low confidence

291 : One number is correct and in the right place

245 : One number is correct but in the wrong place

463 : Two numbers are correct but in the wrong place

578 : Nothing is correct

569 : One number is correct but in the wrong place

1+2 => 2 sai (vì nếu 2 thỏa mãn 1 thì sẽ không thỏa mãn 2 và ngược lại ) => 9 ,1,4,5 có thể đúng

3 => 6,3,9,1,4,5 có thể đúng

4 => loại 5 => 9,1,6,3,4 có thể đúng

3+5 => loại 6 => 9,1,3,4 có thể đúng

1+5 => 9 đúng , 1 sai => 9,3,4 đúng => ? 9 ?

3 => 3 9 4 là số cần tìm

## Caesar cipher

Viết ứng dụng bằng ngôn ngữ lập trình bạn đã chọn để mã hóa và giải mã một tin nhắn bằng mật mã Caesar. Ứng dụng của bạn phải đáp ứng các yêu cầu sau:

• Cho phép nhập một khóa và một bản rõ để mã hóa hoặc bản mã để giải mã bằng một khóa nhất định.

• Cho phép brute-force tất cả các khóa có thể k để tìm bản rõ của bản mã đã cho mà không có khóa của nó.

Text

Description automatically generated

* Đoạn code có chức năng mã hóa: nhập thông điệp, và key vào từ bàn phím. Thông điệp này sẽ được lưu vào một mảng ký tự (message[100]). Cho chạy vòng lặp từ ký tự đầu tiên của mảng. Gán giá trị phần tử trong mảng vào biến ch. Ta sẽ cộng ký tự với giá trị key để ra được ký tự mã hóa. Nếu ký tự sau khi cộng có giá trị lớn hơn ‘z’ hoặc ‘Z’ (với các ký tự viết hoa) thì ta sẽ sử dụng công thức “ch = ch – ‘z’ (‘Z’) + ‘a’ (‘A’) – 1”. Sau đó, ta sẽ gán ký tự đã xử lý vào lại mảng và tiếp tục xử ký tự tiếp theo trong mảng và lặp lại cho đến khi hết mảng ký tự . Vì kí tự chỉ trong 1 khoảng nhất định nên phải làm v để kí tự nằm trong khoảng đó . vd : a = 65 , kí tự 64 sẽ là z .

z=122 , 123 = a

Text

Description automatically generated

* Đoạn code có chức năng giải mã: Cho chạy vòng lặp từ ký tự đầu tiên của mảng. Gán giá trị phần tử trong mảng vào biến ch. Ta sẽ trừ ký tự với giá trị key để ra được ký tự mã hóa. Nếu ký tự sau khi cộng có giá trị nhỏ hơn ‘a’ hoặc ‘A’ (với các ký tự viết hoa) thì ta sẽ sử dụng công thức “ch = ch – ‘a’ (‘A’) + ‘z’ (‘Z’) – 1”. Sau đó, ta sẽ gán ký tự đã xử lý vào lại mảng và tiếp tục xử ký tự tiếp theo trong mảng và lặp lại cho đến khi hết mảng ký tự

Text

Description automatically generated

* Giải mã đoạn mã cho trước mà không cần key: lưu thông điệp muốn giải mã vào trong một mảng ký tự. Rồi ta cho chạy vòng lặp để thử từng trường hợp j trong bảng chữ cái. Sau đó, ta cho chạy vòng lặp thứ hai (bên trong vòng for đầu tiên) từ ký tự đầu tiên của mảng. Gán giá trị phần tử trong mảng vào biến ch. Ta sẽ trừ ký tự với giá trị j để ra được ký tự mã hóa. Nếu ký tự sau khi cộng có giá trị nhỏ hơn ‘a’ hoặc ‘A’ (với các ký tự viết hoa) thì ta sẽ sử dụng công thức “ch = ch – ‘a’ (‘A’) + ‘z’ (‘Z’) – 1”. Sau đó, ta sẽ gán ký tự đã xử lý vào lại mảng và tiếp tục xử ký tự tiếp theo trong mảng và lặp lại cho đến khi hết mảng ký tự. Tiếp tục xử lý cho trường hợp j tiếp theo và tuần tự cho đến khi hết các giá trị trong bảng chữ cái

Text

Description automatically generated

* Input và output của đoạn code mã hóa và giải mã dùng key

Text

Description automatically generated

* Output của đoạn code giải mã đoạn mã cho trước mà không cần key

## Mono-alphabetic substitution cipher and frequency analysis :

### Nội dung 1 : Mono-alphabetic substitution cipher

Mã hóa : mess[i] = alpha[j] => encrypted = keyword[j]

Giải mã : encrypted[i] = keyword [j] => plain = alpha [j]

Text

Description automatically generated

* Hàm dùng để nhập key và xác định người dùng đang cần giải mã hay mã hóa: Người dùng nhập key từ bàn phím. Chạy vòng lặp để chuyển các ký tự sang ký tự viết in. Sau đó, chạy 2 vòng lặp for để kiểm tra xem các ký tự trong chuỗi keyword có trùng nhau hay không. Nếu có thì ta thoát chương trình bằng câu lệnh exit (EXIT\_FAILURE)

Text

Description automatically generated

* Tạo bảng chữ cái mới với keyword: tạo ra chuỗi ***temp*** với giá trị rỗng để nạp lần lượt các ký tự vào. Ta dùng vòng for đầu tiên để nạp lần lượt các ký tự trong chuỗi keyword vào chuỗi temp. Ta dùng thêm một vòng for nữa để thêm các ký tự còn lại trong bảng chữ cái vào chuỗi. Bằng cách ép kiểu char cho giá trị (i+65) (ký tự ASCII) –
* ***temp = keyword+ abc…xyz***

Text

Description automatically generated

* Loại bỏ các kí tự trong keyword khỏi bảng chữ cái: Ta chạy hai vòng for để kiểm tra xem trong chuỗi keyword có ký tự nào trùng với ký tự trong chuỗi temp không? Sử dụng vòng for đầu tiên để kiểm tra chuỗi temp và tạo biến found kiểu bool. Vòng for thứ 2 được lồng vào bên trong vòng for đầu tiên và dùng để kiểm tra chuỗi keyword. Nếu ký tự thứ i của chuỗi temp trùng với ký tự thứ j của chuỗi keyword thì ta sẽ gán biến found thành true và thoát vòng lặp. Sau khi thoát khỏi vòng lặp thứ 2 thì ta sẽ xét biến found có bằng false hay không. Nếu có thì ta sẽ thêm ký tự thứ i trong chuỗi temp vào keyword

(mục đích : tạo 1 chuỗi có keyword và thêm các kí tự lần lượt trong bảng chữ cái vào keyword [ các kí tự lặp lại (ở trong temp) sẽ k đc thêm vào ])

Vd : keyword : abc

Chuỗi mới : abc d e f (không thêm abc đã có)

Text

Description automatically generated

* Hàm giải mã: Nhập thông điệp muốn mã hóa từ bàn phím. Sử dụng vòng for và hàm toupper để chuyển lần lượt các ký tự chuỗi message thành ký tự in hoa. Tạo ra chuỗi decryText có giá trị là rỗng. Chạy vòng for để xét chuỗi message. Nếu ký tự rỗng ((char) 32 ⬄ dấu cách) thì ta sẽ thêm dấu cách vào trong chuỗi. Nếu không, ta tạo biến counter bằng 0, sau đó chạy vòng for để kiểm tra chuỗi alpha. Nếu ký tự thứ i của chuỗi message bằng ký tự thứ j của chuỗi keyword thì ta thêm vào chuỗi decryText phần tử thứ ‘count’ của chuỗi alpha. Trường hợp không bằng ta cộng biến counter lên 1.

Text

Description automatically generated

* Input và output khi chạy chương trình

Ví dụ : keyword a c

mess a c b

alpha a b c … x y z

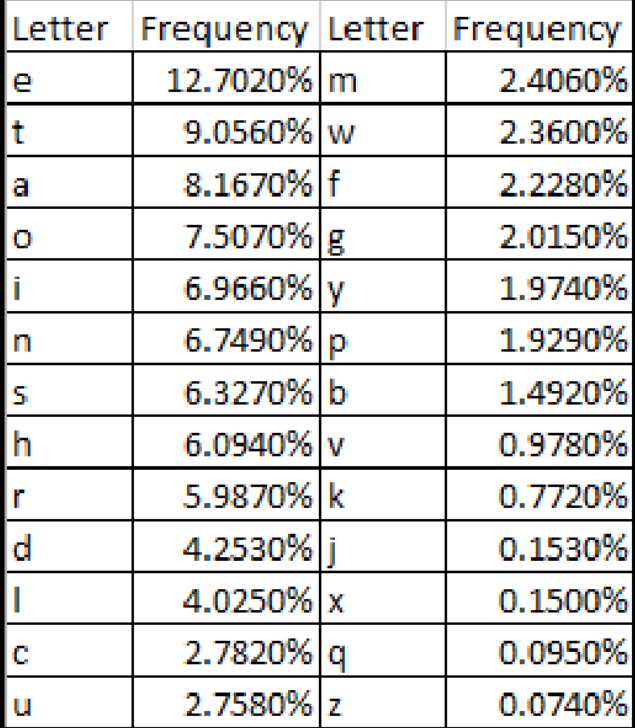
keyword mới a c b .. x y z

cipher a b c

plain a c b

### Nội dung 2 : Frequency analysis

Bước 1 :Tìm mức độ xuất hiện của các kí tự trong văn bản



Bước 2 : Dựa trên văn bản mật mã, cần đưa ra các giả định và thay thế từng chữ cái một và sau đó phân tích kết quả cuối cùng để chắc chắn rằng câu trả lời có ý nghĩa. Càng đoán đúng, bạn sẽ càng tiến gần hơn và cuối cùng sẽ giải mã đc cypher text

A picture containing table

Description automatically generated

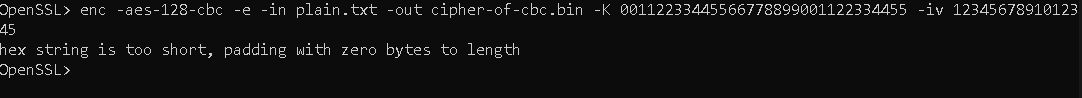
* Plain text :

the oscars turn on sunday which seems about right after this long strange awards trip the bagger feels like a nonagenarian too the awards race was bookended by the demise of harvey weinstein at its outset and the apparent implosion of his film company at the end and it was shaped by the emergence of metoo times up blackgown politics armcandy activism and a national conversation as brief and mad as a fever dream about whether there ought to be a president winfrey the season didnt zust seem extra long it was extra long because the oscars were moved to the first weekend in march to avoid conflicting with the closing ceremony of the winter olympics thanks pyeongchang one big question surrounding this years academy awards is how or if the ceremony will address metoo especially after the golden globes which became a zubilant comingout party for times up the movement spearheaded by powerful hollywood women who helped raise millions of dollars to fight sexual harassment around the country signaling their support golden globes attendees swathed themselves in black sported lapel pins and sounded off about sexist power imbalances from the red carpet and the stage on the air e was called out about pay inequity after its former anchor catt sadler quit once she learned that she was making far less than a male cohost and during the ceremony natalie portman took a blunt and satisfying dig at the allmale roster of nominated directors how could that be topped as it turns out at least in terms of the oscars it probably wont be women involved in times up said that although the globes signified the initiatives launch they never intended it to be zust an awards season campaign or one that became associated only with redcarpet actions instead a spokeswoman said the group is working behind closed doors and has since amassed million for its legal defense fund which after the globes was flooded with thousands of donations of or less from people in some countries no call to wear black gowns went out in advance of the oscars though the movement will almost certainly be referenced before and during the ceremony especially since vocal metoo supporters like ashley zudd laura dern and nicole kidman are scheduled presenters another feature of this season no one really knows who is going to win best picture arguably this happens a lot of the time inarguably the nailbiter narrative only serves the awards hype machine but often the people forecasting the race socalled oscarologists can make only educated guesses the way the academy tabulates the big winner doesnt help in every other category the nominee with the most votes wins but in the best picture category voters are asked to list their top movies in preferential order if a movie gets more than percent of the firstplace votes it wins when no movie manages that the one with the fewest firstplace votes is eliminated and its votes are redistributed to the movies that garnered the eliminated ballots secondplace votes and this continues until a winner emerges it is all terribly confusing but apparently the consensus favorite comes out ahead in the end this means that endofseason awards chatter invariably involves tortured speculation about which film would most likely be voters second or third favorite and then equally tortured conclusions about which film might prevail in it was a tossup between boyhood and the eventual winner birdman in with lots of experts betting on the revenant or the big short the priWe went to spotlight last year nearly all the forecasters declared la la land the presumptive winner and for two and a half minutes they were correct before an envelope snafu was revealed and the rightful winner moonlight was crowned this year awards watchers are unequally divided between three billboards outside ebbing missouri the favorite and the shape of water which is the baggers prediction with a few forecasting a hail mary win for get out but all of those films have historical oscarvoting patterns against them the shape of water has nominations more than any other film and was also named the years best by the producers and directors guilds yet it was not nominated for a screen actors guild award for best ensemble and no film has won best picture without previously landing at least the actors nomination since braveheart in this year the best ensemble sag ended up going to three billboards which is significant because actors make up the academys largest branch that film while divisive also won the best drama golden globe and the bafta but its filmmaker martin mcdonagh was not nominated for best director and apart from argo movies that land best picture without also earning best director nominations are few and far between

## Block cipher

### Nội dung 1 :Tạo một tệp văn bản 100 byte bắt đầu bằng tên và ID sinh viên của bạn. Mã hóa tệp này dưới dạng văn bản rõ với ít nhất ba chế độ sử dụng OpenSSL (key và IV (nếu cần) là do bạn chọn).

+Mã hóa dùng AES 128 bit mode **CBC** :



Kết quả :

Graphical user interface, text, application, website

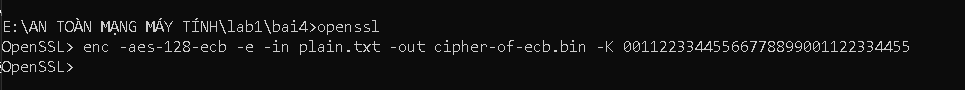
Description automatically generated

Chuyển qua .text :

A picture containing text

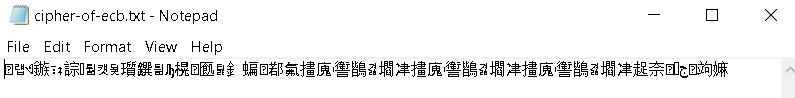
Description automatically generated

+Mã hóa mode **ECB**: Không cần iv

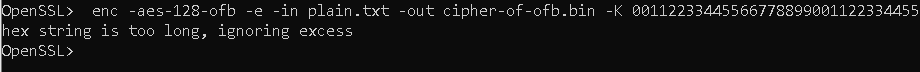


Graphical user interface, text

Description automatically generated



+Mã hóa mode **OFB** :





Graphical user interface, text, application

Description automatically generated

## Encryption Mode – ECB vs. CBC

### Nội dung 1 : Mã hóa dùng ECB && CBC :





A picture containing text

Description automatically generated

+ Cắt head của plaintext và body của 2 file .bmp khi đã mã hóa :

Text

Description automatically generated





2. Gắn head của plaintext vào 2 body của 2 file .bmp

Text

Description automatically generated

=> Kết quả :

Graphical user interface, application, Teams

Description automatically generated

Ta thấy thuật toán mã hóa **CBC** mã hóa tốt hơn **ECB vì :**

1. **ECB** không cần dùng tới IV ( IV tạo sự ngẫu nhiên khá tốt trong việc giải mã )
2. Từ block thứ 2 trở đi của **CBC** cần ciphertext của block trước đó để đảm bảo rằng plaintext có cùng nội dung sẽ ra được ciphertext khác nhau
3. **ECB** tạo ra cùng 1 ciphertext nếu plaintext có nội dung giống nhau

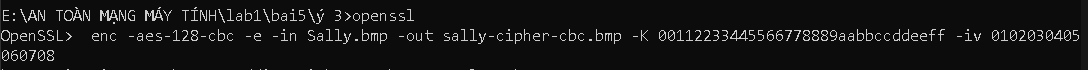
Chart, box and whisker chart

Description automatically generated

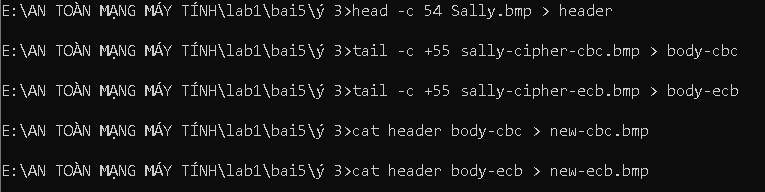
Diagram

Description automatically generated

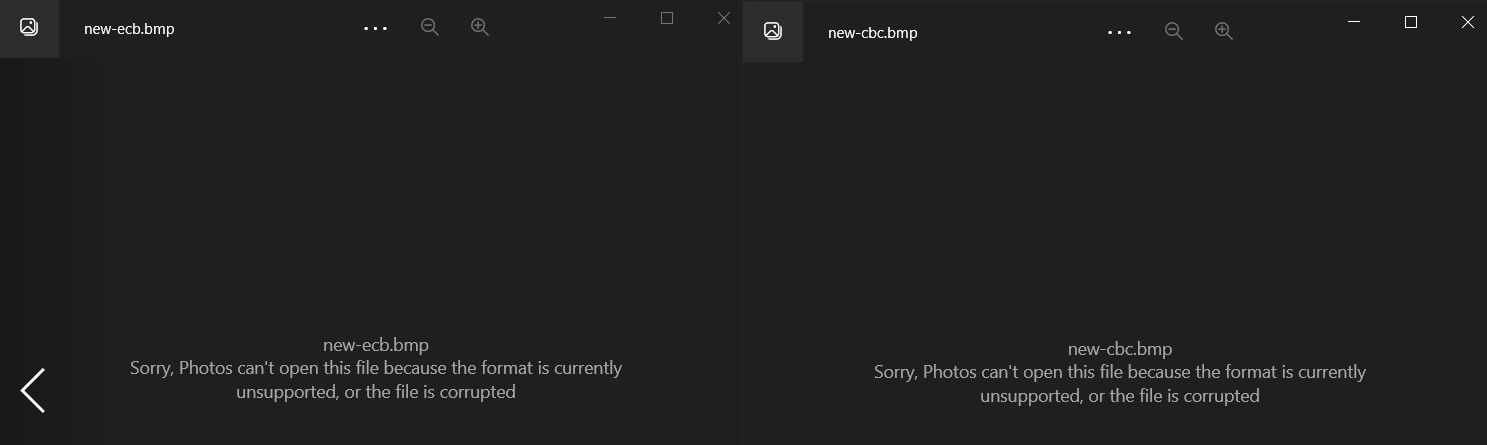
### Nội dung 2: Chọn hình ảnh khác, lặp lại thử nghiệm ở trên và báo cáo quan sát











Không nhận được vì file gốc của tấm ảnh này không phải .bmp

## Padding :

### Nội dung 1 : Sử dụng các chế độ ECB, CBC, CFB và OFB để mã hóa tệp (bạn có thể chọn bất kỳ mật mã). Vui lòng báo cáo chế độ nào có đệm và chế độ nào không. Đối với những trường hợp không cần đệm, vui lòng giải thích lý do.

**+ ECB :**

Text

Description automatically generated

Text

Description automatically generated

Cần padding

**+ CBC :**

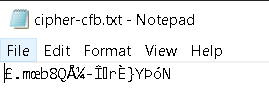


Text

Description automatically generated with low confidence

+CFB :



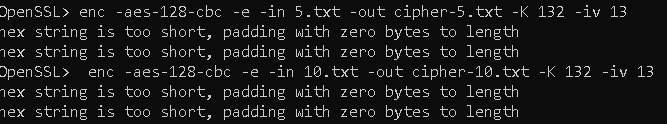


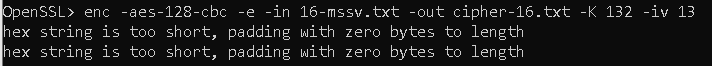
+OFB :



### Nội dung 2 : Luyện tập đệm của mật mã khối

+ Mã hóa file 5,10,16 bytes .File 16 bytes chứa mssv :





Text

Description automatically generated

File 5 bytes sau khi mã hóa có 16 bytes

File 10 bytes sau khi mã hóa có 16 bytes

File 16 bytes sau khi mã hóa có 32 bytes

+ Giải mã 3 file :



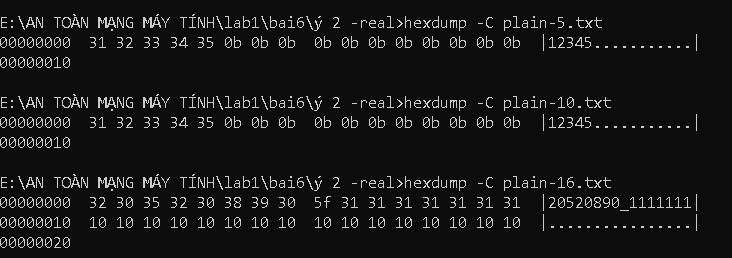
Text

Description automatically generated

Graphical user interface, application

Description automatically generated

+ Gõ lệnh để xem nội dung **đệm** thêm là gì :



# TÀI LIỆU THAM KHẢO