BÁO CÁO THỰC HÀNH

**Bài thực hành số 01**

**MÃ HÓA BẤT ĐỐI XỨNG**

|  |  |
| --- | --- |
| **Môn học:** An toàn Mạng máy tính | **Điểm tự đánh giá** |
| **Lớp:** NT101.N11.1  **Giảng viên hướng dẫn:** Văn Thiên Luân | **10** |

**PHÂN CÔNG NHIỆM VỤ NHÓM 1:**

|  |  |  |
| --- | --- | --- |
| **MSSV** | **Họ và Tên** | **Nhiệm vụ** |
| 20521086 | Trang Kỳ Anh | - Đảm nhiệm nội dung thực hành và báo cáo bài 1 và bài 2.  - Góp ý, nhận xét các bài còn lại cho các thành viên khác.  - Tổng hợp, chỉnh sửa báo cáo. |
| 20521280 | Lê Thanh Hằng | - Đảm nhiệm nội dung thực hành và báo cáo bài 3 và bài 4.  - Góp ý, nhận xét các bài còn lại cho các thành viên khác. |
| 20520131 | Dương Đức Anh | - Đảm nhiệm nội dung thực hành và báo cáo bài 5 và bài 6.  - Góp ý, nhận xét các bài còn lại cho các thành viên khác. |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện | 80 tiếng |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị | - Bài dài, tốn nhiều thời gian để hiểu vì ban đầu bị mất 1 tiết lý thuyết.  - Bài thực hành viết bằng tiếng anh gây một chút khó khăn trong việc đọc – hiểu một số thuật từ. |

**MỤC LỤC**

[I. BÁO CÁO CHI TIẾT 3](#_Toc115728150)

[**1.** **Khởi động: Bẻ khóa** 3](#_Toc115728151)

[*a.* *Mở khóa gồm 3 chữ số trong hình 8 dựa vào các dữ liệu có sẵn* 3](#_Toc115728152)

[*b.* *Tìm bảng mã tương ứng với các số từ 1 đến 9 theo manh mối* 3](#_Toc115728153)

[**2.** **Mật mã Caesar** 6](#_Toc115728154)

[*a.* *Màn hình ứng dụng* 6](#_Toc115728155)

[*b.* *Mô tả ứng dụng* 6](#_Toc115728156)

[*c.* *Các hàm đã triển khai* 7](#_Toc115728157)

[*d.* *Thực nghiệm* 9](#_Toc115728158)

[*e.* *Vấn đề sau thực nghiệm* 10](#_Toc115728159)

[**3.** **Mật mã đơn chữ cái và phân tích tần suất** 11](#_Toc115728160)

[**4.** **Tương tự mật mã khối** 13](#_Toc115728161)

[**5.** **Chế độ mã hóa ECB và BCB** 14](#_Toc115728162)

[**6.** **Bộ đệm** 15](#_Toc115728163)

[II. TÀI LIỆU THAM KHẢO 26](#_Toc115728164)

1. **BÁO CÁO CHI TIẾT**
2. **Khởi động: Bẻ khóa**
3. *Mở khóa gồm 3 chữ số trong hình 8 dựa vào các dữ liệu có sẵn*

Ta có các dữ liệu đề bài cho như sau:

1. Trong các số 2, 9, 1 có một số đúng và nằm đúng vị trí
2. Trong các số 2, 4, 5 có một số đúng nhưng không nằm đúng vị trí
3. Trong các số 4, 6, 3 có 2 số đúng nhưng không nằm đúng vị trí
4. Trong các số 5, 7, 8 không có số nào đúng
5. Trong các số 5, 6, 9 có 1 số đúng và không nằm đúng vị trí

**Giải thích:**

(1), (2) => số 2 không thể là số đúng (6)

(2), (5), (6) => số 4 là số đúng nhưng không nằm đúng vị trí (7)

(3), (7) => số 4 nằm ở vị trí thứ ba **(i)**

(3), (5) => số 6 không phải số đúng (8)

(5), (8) => số 9 là số đúng nhưng không nằm đúng vị trí (9)

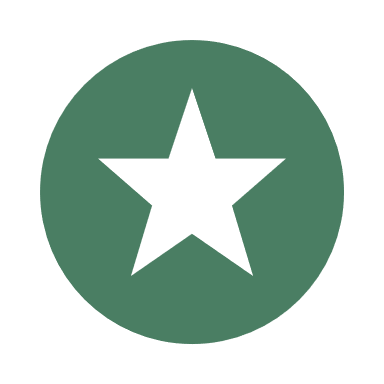
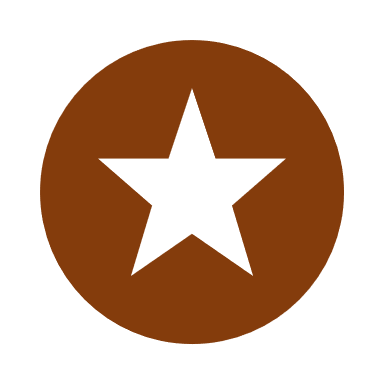
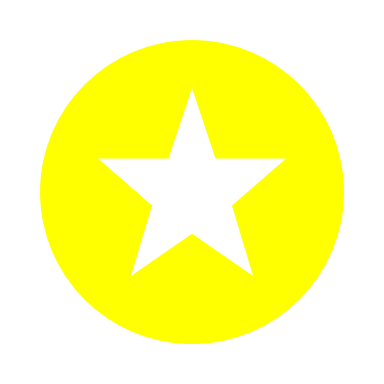
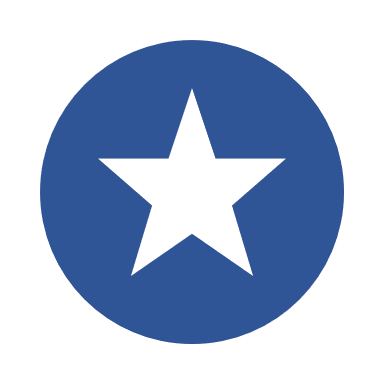
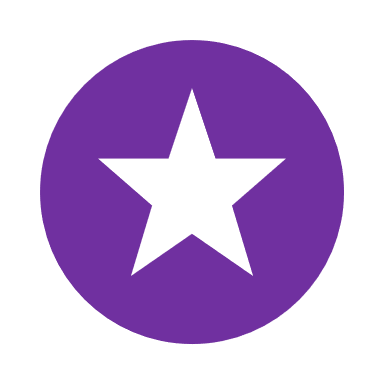
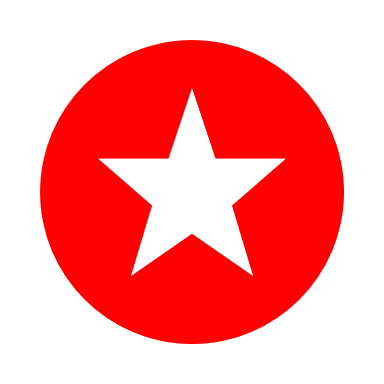
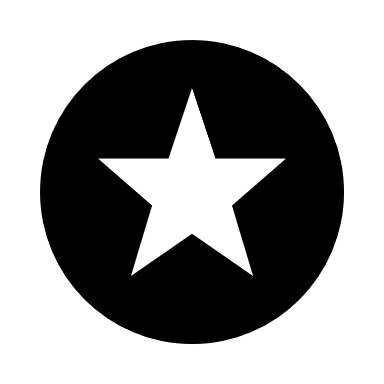
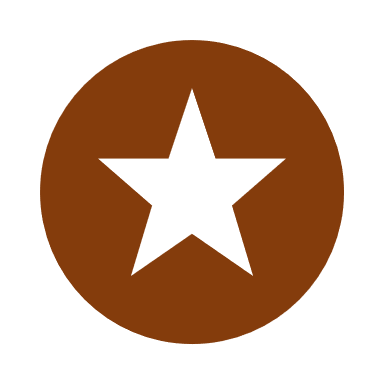
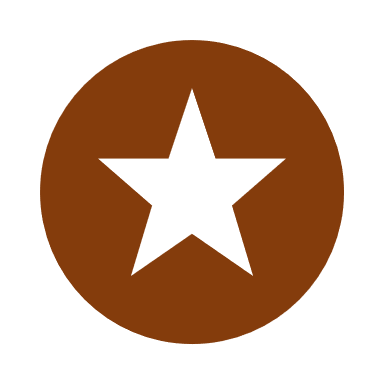
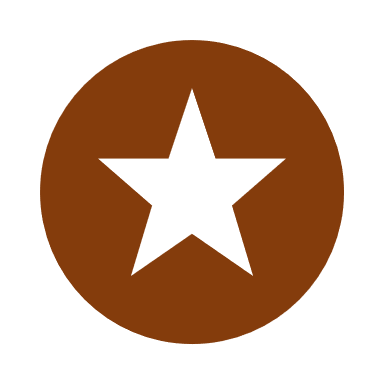
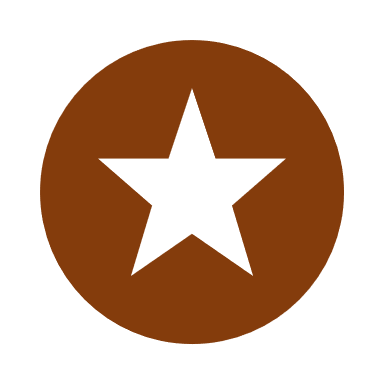
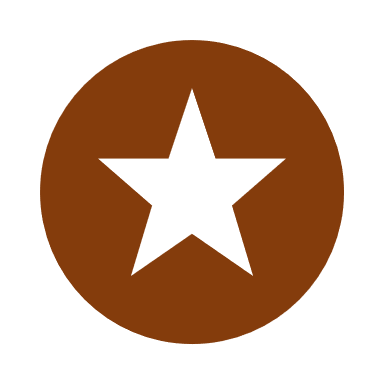
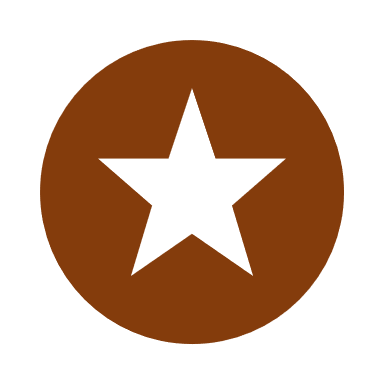
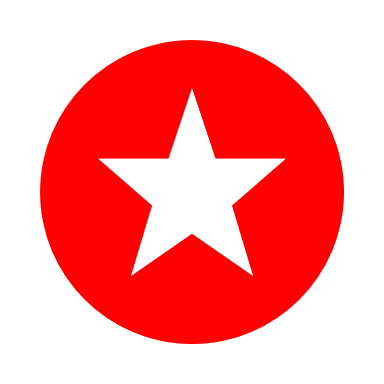
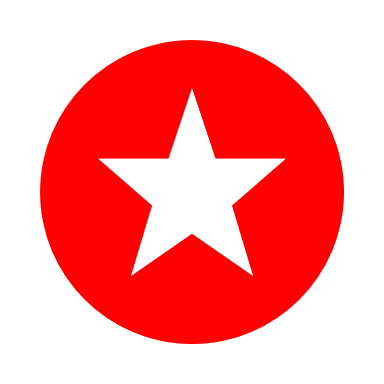
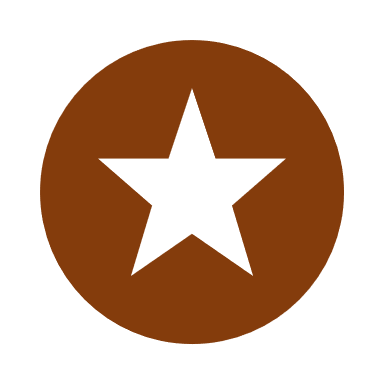
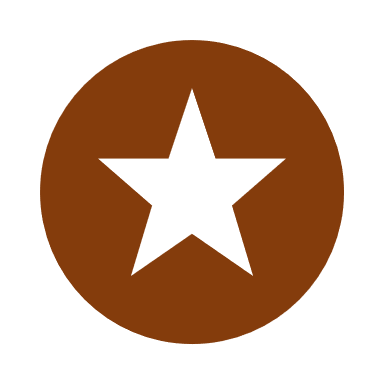
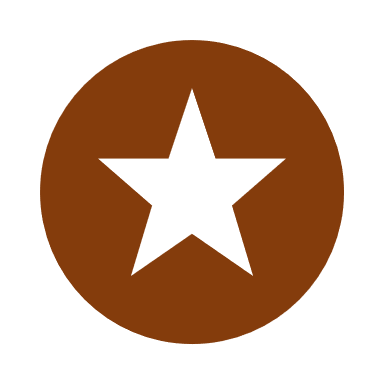
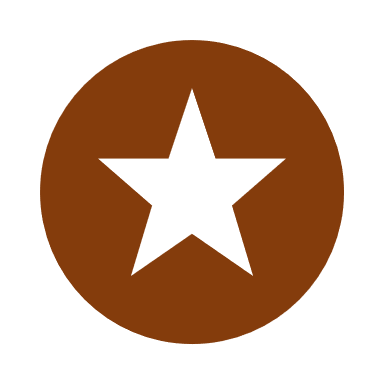
(1), (9) => số 9 nằm ở vị trí thứ hai **(ii)**

(3), (8) => số 3 là số đúng và nằm ở vị trí thứ nhất **(iii)**

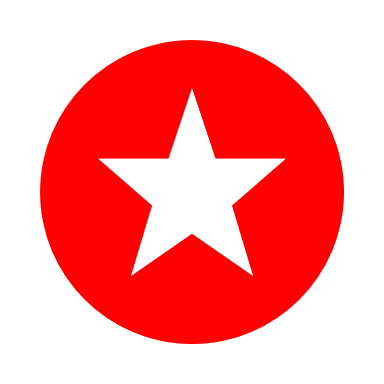
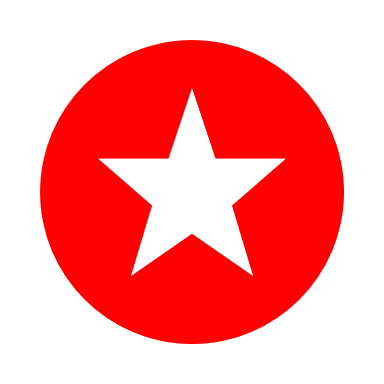
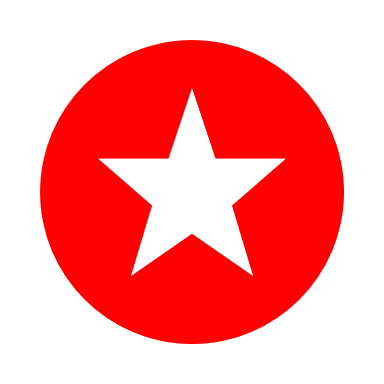
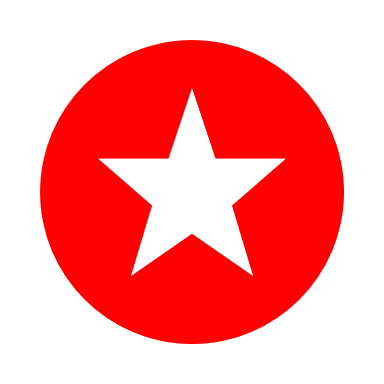
**(i), (ii), (iii)** => Đáp án sẽ là **394**

1. *Tìm bảng mã tương ứng với các số từ 1 đến 9 theo manh mối*

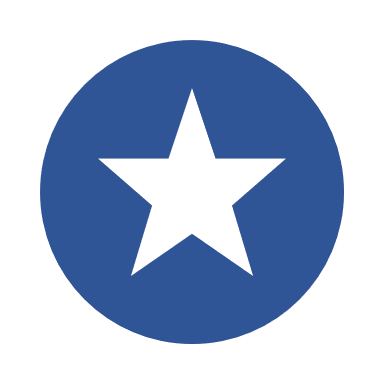
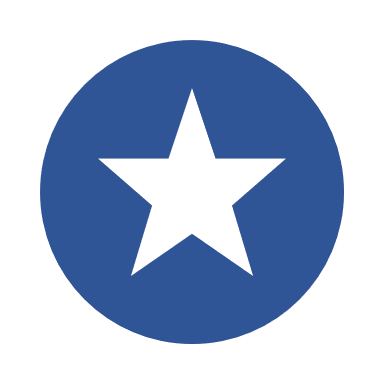
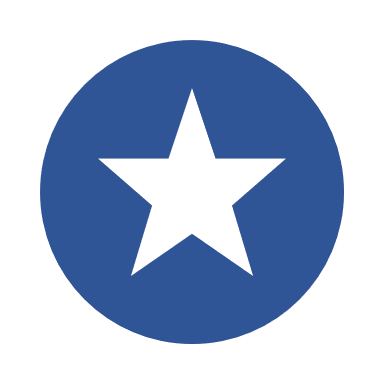
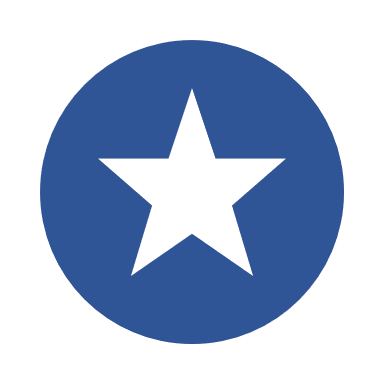
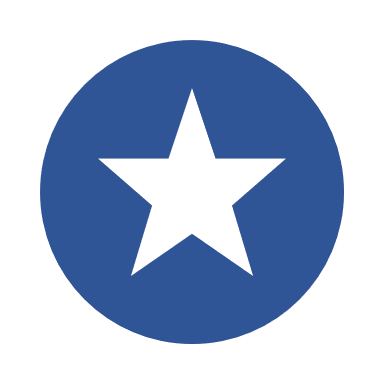
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | ? |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |
| ? | ? | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |
| ? | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |
| Badge New with solid fillBadge New with solid fill | Badge New with solid fillBadge New with solid fill | Badge New with solid fillBadge New with solid fill | Badge New with solid fillBadge New with solid fill |  |

* Mỗi kí hiệu  biểu thị cho một con số duy nhất trong các số từ 1 đến 9.
* Cột ngoài cùng bên phải là tổng của các hàng
* Hàng cuối cùng chính là tổng của các cột
* Mỗi dấu “?” thể hiện 1 hoặc 2 chữ số.
* Ta sẽ dựa vào tổng các hàng và các cột để dự đoán
* Ta thấy  và  là các số giống nhau mà các ngôi sao chỉ biểu thị cho con số từ **1** đến **9** nên  và  chỉ có thể là **11**, **22**, **33**.
* Ở cột thứ 3,  =  +  +  +  nên  chỉ có thể là số chẵn. Trong các số **11**, **22**, **33** chỉ có **22** là số chẵn nên  chắc chắn sẽ đại diện cho số **2**.
* Ta bắt đầu thay thế tạm thời các  thành số **2** ta sẽ có bảng sau:

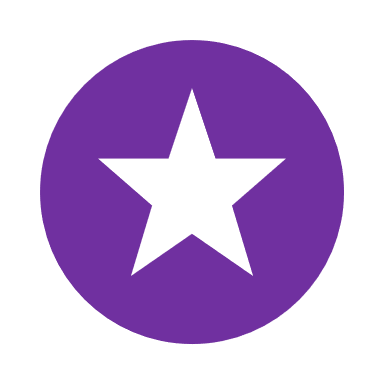
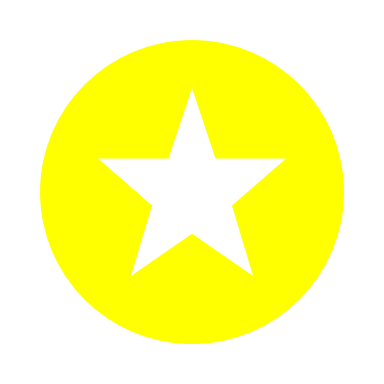
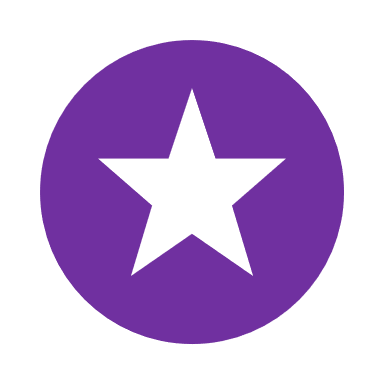
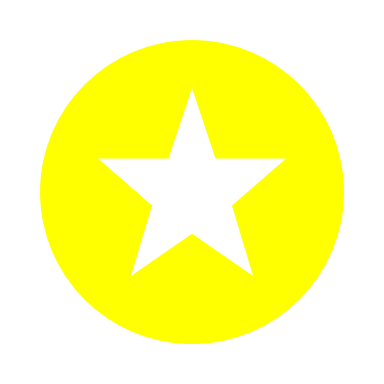
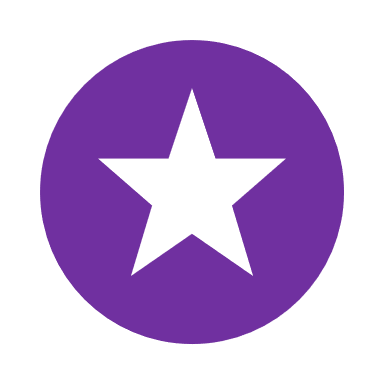
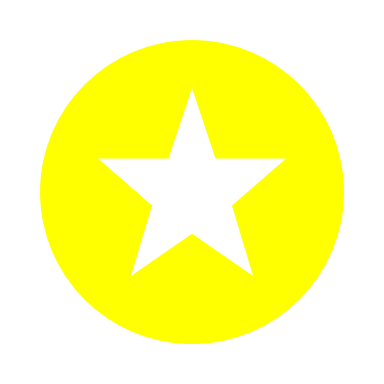
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | ? |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |
| ? | ? | Badge New with solid fill | Badge New with solid fill | 22 |
| ? | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | 2Badge New with solid fill |
| 2Badge New with solid fill | Badge New with solid fillBadge New with solid fill | 22 | 2Badge New with solid fill |  |

* Vì  +  +  +  = **22** nên  và  chỉ có thể là các cặp số mà tổng của chúng bằng **11**, ví dụ như **5 – 6**, **4 – 7**, **3 – 8**, **2 – 9**.
* Ta chọn  = **5** và  = **6** để tiếp tục làm tiếp. Nếu các trường hợp sau không khớp ta sẽ quay lại thử cặp số khác.
* Sau khi chọn ta thêm trực tiếp vào bảng để dễ dàng tính toán tiếp

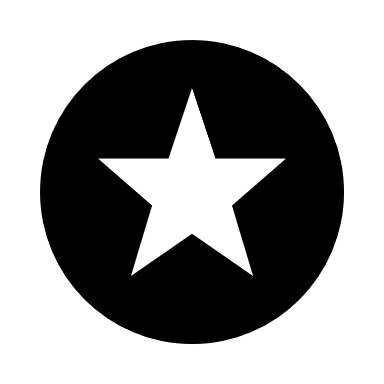
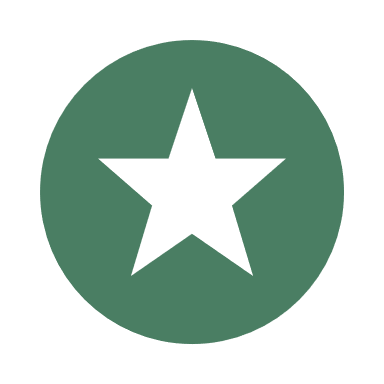
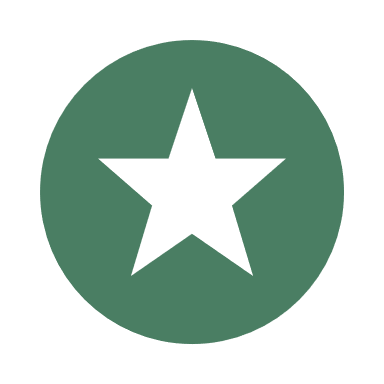
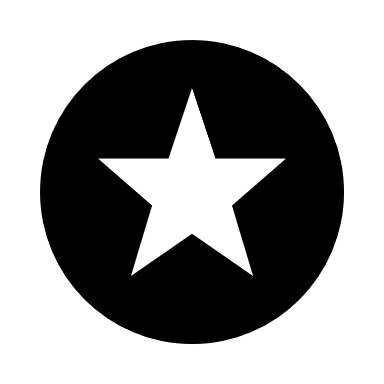
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Badge New with solid fill | Badge New with solid fill | 5 | Badge New with solid fill | ? |
| Badge New with solid fill | Badge New with solid fill | 6 | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |
| ? | ? | 5 | Badge New with solid fill | 22 |
| ? | Badge New with solid fill | 6 | Badge New with solid fill | 2Badge New with solid fill |
| 2Badge New with solid fill | Badge New with solid fillBadge New with solid fill | 22 | 2Badge New with solid fill |  |

* Tiếp đến, ta sẽ xét  là số **11** hay **33**.
* Nếu  là **11** thì không có chữ số nào thỏa để  +  + **6** +  == **11**
* Nếu  là **33** thì  = **9** sẽ thỏa **9** + **9** + **6** + **9** = **33**.
* Vậy  = **9** và  = **3**. Ta tiếp tục thay vào bảng như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Badge New with solid fill | Badge New with solid fill | 5 | Badge New with solid fill | ? |
| 9 | 9 | 6 | 9 | 33 |
| ? | ? | 5 | Badge New with solid fill | 22 |
| ? | 9 | 6 | 9 | 2Badge New with solid fill |
| 29 | 33 | 22 | 23 |  |

* Ta có ở cột thứ 3,  + **9** +  + **9** = **23**. Vậy  +  = **5.**
* Vì số **2** và số **3** đã đại diện cho 2 ngôi sao khác nên chỉ còn lại số **1** và **4** có tổng là **5**. Ta thử chọn  = **4** và  = **1** và cập nhật lại bảng như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Badge New with solid fill | Badge New with solid fill | 5 | 4 | ? |
| 9 | 9 | 6 | 9 | 33 |
| ? | ? | 5 | 1 | 22 |
| ? | 9 | 6 | 9 | 2Badge New with solid fill |
| 29 | 33 | 22 | 23 |  |

* Hiện tại chỉ còn lại  và , đồng thời cũng chỉ còn số **7** và số **8** chưa đại diện cho ngôi sao nào nên mình sẽ thử chọn  = **7** và  = **8** và cập nhật lại bảng như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | 8 | 5 | 4 | ? |
| 9 | 9 | 6 | 9 | 33 |
| ? | ? | 5 | 1 | 22 |
| ? | 9 | 6 | 9 | 27 |
| 29 | 33 | 22 | 23 |  |

* Tiếp đến ta sẽ điền vào các dấu **“?”** sao cho thỏa điều kiện: Cột cuối cùng là tổng của các hàng và hàng cuối cùng là tổng của các cột.
* Ở hàng đầu tiên, dấu **“?”** nằm ở cột cuối cùng nên sẽ là tổng của 4 số trong hàng đó: **8 + 8 + 5 + 4 = 25**
* Ở cột thứ hai, ta có: **8 + 9 + ? + 9 = 33** nên **“?”** ở cột này sẽ là số **7**
* Ở hàng thứ 3 ta có: **“?” + 7 + 5 + 1 = 22** nên **“?”** ở hàng này (không phải coojt 2) sẽ là số **9**
* Ở hàng thứ 4 ta có: **“?” + 9 + 6 + 9 = 27** nên **“?”** ở hàng này sẽ là số **3**
* Kiểm tra các dấu **“?”** đã điền có thỏa cột thứ nhất không: **8 + 9 + 9 + 3 = 29** (đúng) nên ta sẽ có bảng hoàn chỉnh như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | 8 | 5 | 4 | ? |
| 9 | 9 | 6 | 9 | 33 |
| 9 | 7 | 5 | 1 | 22 |
| 3 | 9 | 6 | 9 | 27 |
| 29 | 33 | 22 | 23 |  |

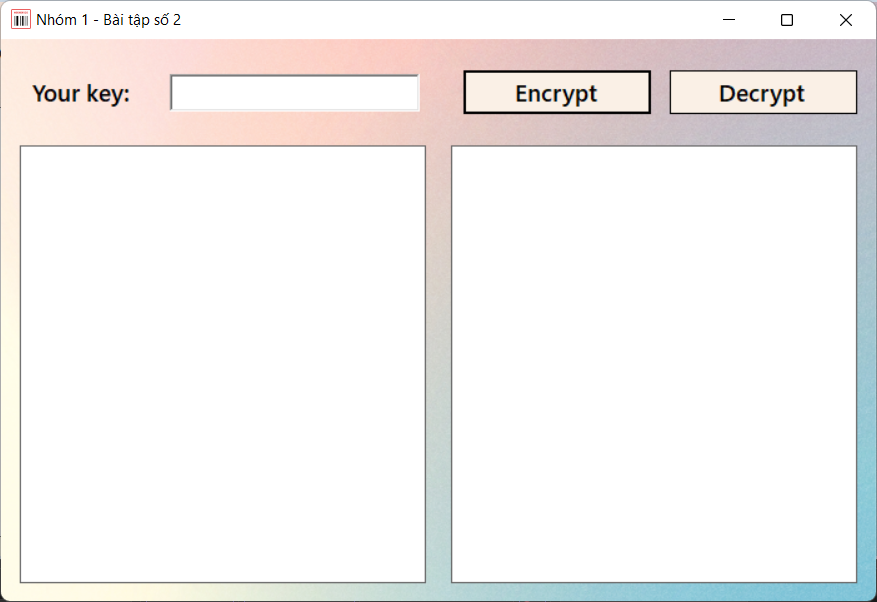
Vậy đáp án cho bài này là:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |  |  |  |  |  |  |  |  |  |  |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill | với | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill |
| Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fill | Badge New with solid fillBadge New with solid fill |  |  |  |  |  |  |  |  |  |  |
| Badge New with solid fillBadge New with solid fill | Badge New with solid fillBadge New with solid fill | Badge New with solid fillBadge New with solid fill | Badge New with solid fillBadge New with solid fill |  |  |  |  |  |  |  |  |  |  |  |

1. **Mật mã Caesar**
2. *Màn hình ứng dụng*

Nút giải mã

Nút mã hóa



Kết quả sẽ hiện ở đây

Nhập đoạn văn cần mã hóa hoặc giải mã ở đây

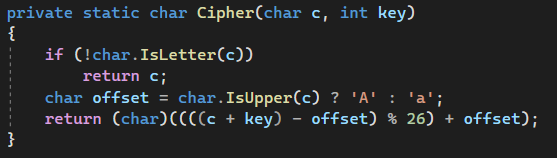
Nhập key ở đây

1. *Mô tả ứng dụng*

* Sau khi nhập đoạn văn, nếu bạn nhấn nút Encrypt thì đoạn văn đó sẽ là plaintext còn nếu bạn nhấn nút Decrypt thì đoạn văn đó sẽ là ciphertext.
* Nếu bạn nhập key thì khi nhấn nút Encrypt hoặc Decrypt thì chương trình sẽ mã hóa hoặc giải mã theo key bạn nhập.
* Nếu bạn không nhập key thì khi nhấn nút Encrypt sẽ tạo key ngẫu nhiên để mã hóa và hiện key đã tạo vào ngay ô nhập key.
* Nếu bạn không nhập key thì khi nhấn nút Decrypt thì chương trình sẽ tự dò tìm key để có thể mã hóa bất kì đoạn văn nào mà không có sẵn key.
* Đây là thuật toán dựa vào tần suất xuất hiện của các chữ cái của một ngôn ngữ để tìm ra key và ngôn ngữ mà nhóm mình chọn để viết ứng dụng này là Tiếng Anh (vì đây là ngôn ngữ Quốc tế và các đoạn văn trong bài thực hành cũng là Tiếng Anh)
* Theo Wikipedia, trong Tiếng Anh tần suất chữ e xuất hiện là nhiều nhất với tỉ lệ 12,70 % nên trước khi mã hóa, chương trình của nhóm mình sẽ làm một thao tác quét tần suất xuất hiện của các chữ cái trong đoạn văn.
* Sau khi quét được tần suất thì chữ cái xuất hiện nhiều nhất trong đoạn văn bất kì sẽ được thay bằng chữ e.
* Từ đó ta có thể tìm được key bằng cách lấy vị trí của chữ có tần suất xuất hiện nhiều nhất trừ cho vị trí của chữ e.
* Trong nội dung bài thực hành, đề bài có yêu cầu sử dụng Brute-force để tìm ra plaintext mà không cần key. Thuật toán này sẽ tìm được hết tất cả các trường hợp có thể xảy ra kể cả trường hợp đúng và trường hợp sai nên mình đã tìm một thuật toán tối ưu hơn là quét tần số như trên.

1. *Các hàm đã triển khai*

* Hàm Cipher



* Hàm mã hóa

Text

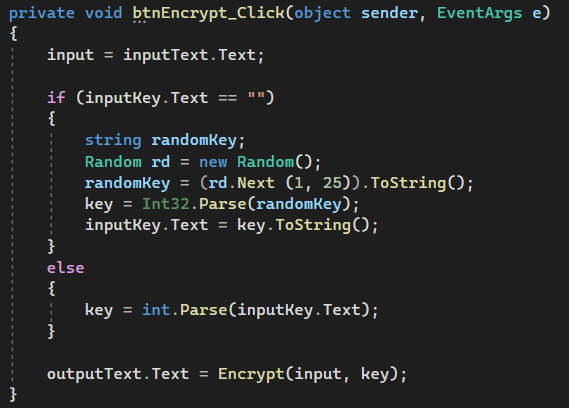
Description automatically generated

* Hàm giải mã

Text

Description automatically generated

* Hàm thực hiện hành động khi nhấn nút Encrypt



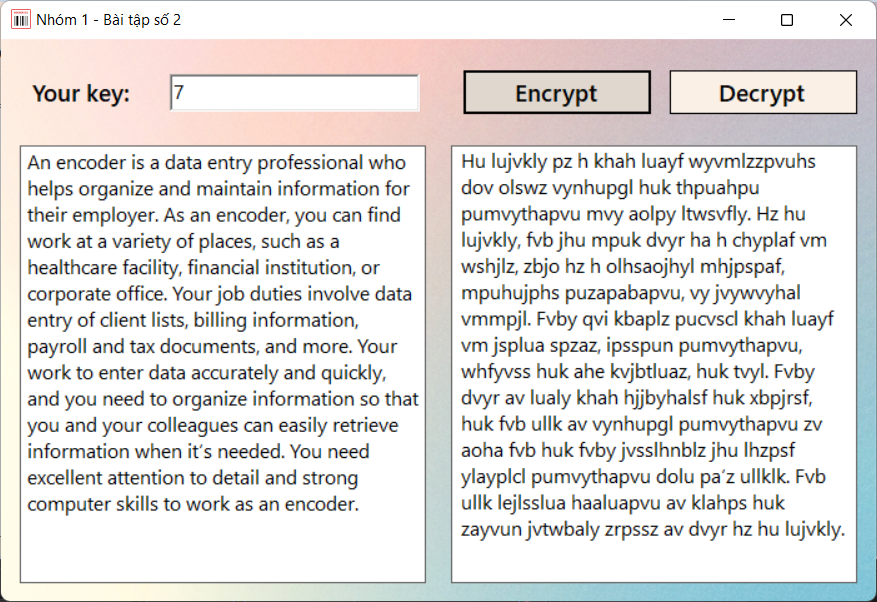
* Hàm thực hiện hành động khi nhấn nút Decrypt

Text

Description automatically generated

1. *Thực nghiệm*

* Đầu tiên, ta copy 1 đoạn văn Tiếng Anh bất kì trên Internet và giải mã với key là 7, ta được kết quả như sau:

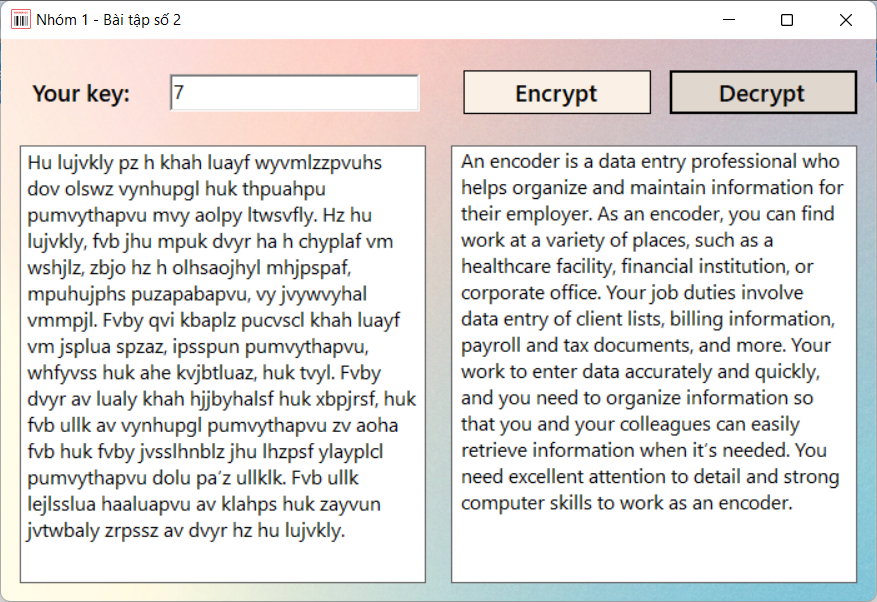


* Sau đó ta so sánh với kết quả từ công cụ mã hóa Cryptool thấy kết quả hoàn toàn khớp.

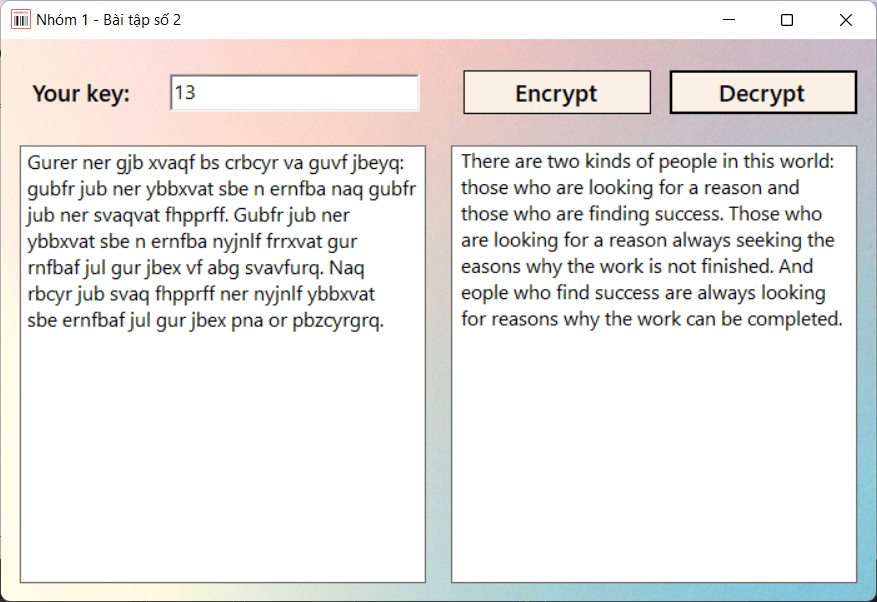
Application, Word

Description automatically generated

* Khi giải mã lại đoạn văn trên, ta thu được đoạn văn ban đầu



* Ta thử giải mã đoạn văn trong bài thực hành mà không cần key ta có kết quả như hình sau với key không cần nhập.

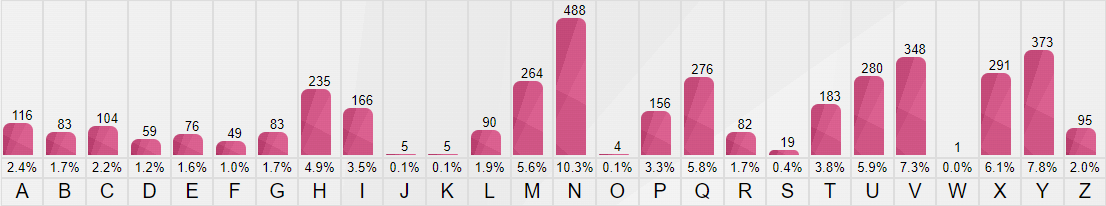


1. *Vấn đề sau thực nghiệm*

* Vấn đề chỉ xảy ra khi mã hóa đoạn văn bản mà không có key. Trong quá trình quét tần suất nếu như có từ 2 chữ cái có cùng tần suất xuất hiện thì chương trình có thể chạy sai. Vấn đề này đang được nhóm đau đầu nghĩ cách khắc phục.

1. **Mật mã đơn chữ cái và phân tích tần suất**

* Phân tích tần suất của các chữ cái trong file ciphertext.txt (bằng web frequency analysis tool), ta được tần suất các từ đơn như sau:



* Bigram phổ biến nhất trong file là: yt
* Trong ngôn ngữ tiếng anh thì từ đơn phổ biến trong các văn bản là e, t, a, o và các từ ít phổ biến là z, j, x, q. Bigram phổ biến là: th
* Giả sử:
* n ~ e, y ~ t, v ~ a, x ~ o (vì n, t, x, v có tần suất cao nhất)
* w ~ z, o ~ j, j ~ x, k ~ q (vì w, o, x, j có tần suất thấp nhất)
* bigram yt ~ th
* **Đoạn đầu ciphertext:**

the oqaahq tzhu ou qzupad lhmah qeecq agozt hmrht abteh thmq iour qthaure alahpq thme the garreh beeiq imse a uouareuahmau too.

* Xét từ ‘oqaahq’ có 6 kí tự có thể viết lại dưới dạng 0.1.2.3.4.1 (với mỗi kí tự thay thế bằng một số và kí tự giống nhau có số giống nhau). Kí tự 0 là ‘o’, kí tự 3 là ‘a’ và có 2 kí tự giống nhau là kí tự thứ 1 và 5 (đánh số 1). Trong tiếng anh chỉ có ‘oscars’ là phù hợp. Vậy: q ~ s, a ~ c, h ~ r.
* Xét từ ‘uouareuarmau’ có 12 kí tự được viết lại 0.1.0.2.3.4.0.2.5.6.2.0. Kí tự 1 là ‘o’, kí tự 4 là ‘e’kí tự 5 là ‘r’, kí tự thứ 3, 7, 10 giống nhau là ‘a’ (đánh số 2), kí tự thứ 0, 2, 6, 11 giống nhau (đánh số 0). Trong tiếng anh có từ ‘nonagenarian’ là phù hợp. Vậy u ~ n, r ~ g, m ~ i.
* Đoán văn bản đoạn đầu sau khi giải mã:

the Oscars turn on Sunday which seems about right after this long, strange awards trip the bagger feels like a nonagenarian too.

- **Ta có bảng giải mã:**



* **Vậy đáp án sau khi giải mã đoạn ciphertext là:**

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, Time’s Up, black-gown politics, arm-candy activism and a national conversation as brief and mad as a fever dream about whether there ought to be a President Winfrey. The season didn’t just 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 year’s Academy Awards is how or if the ceremony will address MeToo especially after the Golden Globes which became a jubilant coming-out party for Time’s 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 all-male roster of nominated directors. How could that be topped.

As it turns out at least in terms of the Oscars, it probably won’t be.

Women involved in Time’s Up said that although the Globes signified the initiatives launch, they never intended it to be just an awards season campaign or one that became associated only with red-carpet 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 Judd, 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, so-called Oscar ologists, can make only educated guesses.

The way the academy tabulates the big winner doesn’t 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 first-place votes, it wins. When no movie manages that, the one with the fewest first-place votes is eliminated and its votes are redistributed to the movies that garnered the eliminated ballots’ second-place 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 end-of-season 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 2015, it was a tossup between “Boyhood” and the eventual winner, “Birdman.” In 2016, with lots of experts betting on “The Revenant” or “The Big Short,” the prize 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 Bagger’s prediction), with a few forecasting a Hail Mary win for “Get Out.”

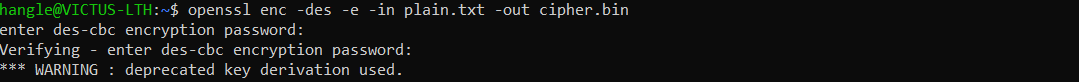
But all of those films have historical Oscar-voting patterns against them. “The Shape of Water” has 13 nominations, more than any other film, and was also named the year’s best by the producers’ and directors’ guilds. Yet it was not nominated for a Screen Actors Guild Award for best ensemble; and no film has won best picture without previously landing at least the actors’ nomination since “Braveheart,” in 1996. This year, the best ensemble SAG ended up going to “Three Billboards,” which is significant because actors make up the academy’s 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.

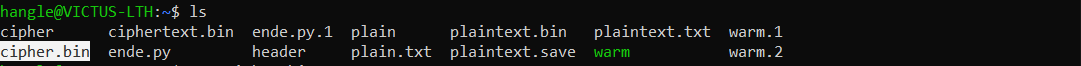
1. **Tương tự mật mã khối**

* Tạo file plain.txt có nội dung

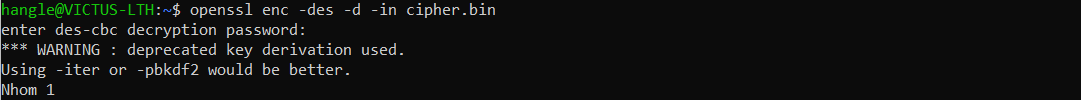


* Mã hóa file plain.txt bằng mã hóa des và lấy file cipher.bin làm file đích





* Giải mã file cipher.bin được nội dung của file plain.txt



1. **Chế độ mã hóa ECB và BCB**

* Pic\_original.bmp ban đầu

Shape, circle

Description automatically generated

* Giả thuyết đưa ra trước khi thực hiện mã hóa CBC: sau khi thực hiện, tệp hình ảnh sau đó sẽ bị mất đi độ sắc nét ban đầu
* Thực hiện mã hóa CBC



* Sau khi mã hóa tệp pic\_original.bmp thành pic.bmp, mở tệp pic.bmp lên bằng image viewer

Graphical user interface, application

Description automatically generated

* Cắt 54 bit đầu của tệp pic\_original.bmp ban đầu làm file header, cắt tệp pic.bmp từ bit thứ 55 trở đi, ghép lại để tạo ra tệp new.bmp



* Kết quả thu được tệp hình ảnh newcbc.bmp

Background pattern

Description automatically generated

* Kết luận: Sau khi thực hiện mã hóa CBC, do bản chất của mã hóa CBC, lấy kết quả mã hóa ở lần trước đó làm phép xor với phần đang mã hóa dẫn đến các khối sau đó đều bị biến đổi và mất đi tính chất ban đầu nên dẫn đến việc tệp hình ảnh bit map sau đó giống như bị nhòe, biến dạng
* Giả thuyết đưa ra trước khi thực hiện mã hóa ecb: sau khi thực hiện, tệp hình ảnh sau cùng sẽ mất đi màu sắc, chỉ còn tông màu trắng đen
* Thực hiện mã hóa ECB



* Cắt 54 bit đầu của tệp pic\_original.bmp ban đầu làm file header, cắt tệp picecb.bmp từ bit thứ 55 trở đi, ghép lại để tạo ra tệp newecb.bmp



* Kết quả thực nghiệm:

Background pattern

Description automatically generated

* Kết luận: Sau khi thực hiện mã hóa ECB, do bản chất của ECB là mã hóa từng khối, khối sau không có liên quan đến khối phía trước nên hình ảnh của tệp được mã hóa không thay đổi, chỉ có màu sắc cho hình ảnh bị đổi đôi chút thành những màu khác nhau.

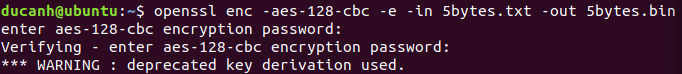
1. **Bộ đệm**

* Lần lượt tạo các tệp tin .txt với 5 số 1, 10 số 1 và 16 số 1 để được các file 5,10 và 16 bytes.

Graphical user interface, text, application

Description automatically generated

* Mã hóa tệp tin 5bytes.txt bằng mã hóa CBC và lấy tệp tin đích là 5bytes.bin



* Tệp tin 5bytes.bin sẽ nặng hơn và trở thành định dạng số nhị phân và không thể mở bằng trình duyệt “text editor” hoặc “image viewer” mà phải mở bằng lệnh “xxd 5bytes.bin”

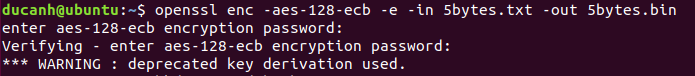
A screenshot of a computer

Description automatically generated with low confidence

Graphical user interface, text, application

Description automatically generated

* Mã hóa ECB cũng cho kết quả tương tự



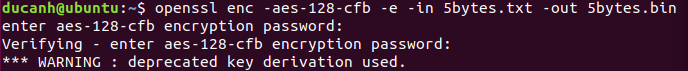
Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* Mã hóa bằng CFB



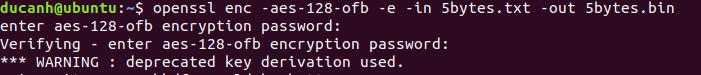
* Tệp đã được mã hóa



Graphical user interface, text, application, email

Description automatically generated

* Mã hóa OFB



* Tệp sau khi mã hóa



Graphical user interface, application

Description automatically generated

=> Các tệp tin được mã hóa bằng OFB và CFB không có padding vì những chế độ mã hóa này chuyển các tệp tin được mã hóa thành dạng khối và khối cuối cùng sẽ được cắt ra để bảo toàn khối lượng của tệp tin được mã hóa.

* Quy trình làm tương tự với các tệp tin 10bytes.txt và 16bytes.txt
* Mã hóa CBC



Graphical user interface, application

Description automatically generated

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* Mã hóa ECB

Text

Description automatically generated

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* Mã hóa CFB

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

Graphical user interface, application

Description automatically generated

* Mã hóa OFB

Text

Description automatically generated

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* Lần lượt giải mã các tệp tin mã hóa ECB, CBC, CFB và OFB tương ứng với các tệp 5bytes.txt, 10bytes.txt, 16bytes.txt cos khóa là “1”

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

* Thực hiện giải mã CBC



Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* Thực hiện giải mã ECB

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* Thực hiện giải mã CFB

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* Thực hiện giải mã OFB

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

=> Padding thường được dùng để thêm vào các tệp này là bit 0 (Ký tự rỗng khi giải mã ra)

1. **TÀI LIỆU THAM KHẢO**

[1] <https://youtu.be/3en7PBeS_kA>

[2] <https://en.wikipedia.org/wiki/Frequency_analysis>