1

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

**<Classical Cryptography>**

**Môn học: An toàn mạng máy tính**

**Lớp: NT101.P21.1**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn** | Nguyễn Xuân Hà |
| **Sinh viên thực hiện** | Nguyễn Minh Quyền (23521325) |
| Nguyễn Văn B (18520002) |
| **Mức độ hoàn thành** | Hoàn thành |
| **Thời gian thực hiện** | 06/03/2025 – 00/03/2025 |
| **Tự chấm điểm** | 10/10 |

* 1. **CÁC BƯỚC THỰC HÀNH**

**Gợi ý:** *Ghi rõ từng bước thực hành, chụp hình ảnh screenshot để báo cáo thêm trực quan*

* 1. **TRẢ LỜI CÁC CÂU HỎI**

## Task 1. Kickoff: Crack the code

Task 1.1. Let’s begin with a straightforward task that does not use any cipher algorithm. Try to solve the following codes:

1. We need to find the code to open the lock in Figure 4. The lock has a three-digit pin that satisfies five conditions (hints). Can you crack this code? If it’s possible, explain how.

A number padlock with numbers

AI-generated content may be incorrect.

1 | 9 | 3 : 1 số đúng và ở đúng vị trí

2 | 7 | 3: 1 số đúng nhưng không ở đúng vị trí

8 | 1 | 3 : 2 số đúng nhưng không ở đúng vị trí

4 | 0 | 3 : không có cái nào đúng

5 | 7 | 8 : 1 số đúng nhưng ở không ở đúng vị trí

**Giải:**

xét 4 | 0 | 3 : loại 4, 0, 3.

Xét 1 | 9 | 3 : số 1 hoặc số 9 đúng và ở đúng vị trí.

Xét 8 | 1 | 3 : chắc chắn số 1 và số 8 đúng nhưng sai vị trí => số 9 bị loại.

* Vị trí thứ nhất là số 1 => 1 | \* | \* .

Xét 5 | 7 | 8 : số 8 đã đúng nhưng sai vị trí lần 2 và số 5 với số 7 bị loại.

* Vị trí thứ hai là số 8 => 1 | 8 | \*

Xét 2 | 7 | 3 : số 2 đúng nhưng sai vị trí vì số 3 và số 7 đã bị loại.

* Vị trí thứ ba là số 2 => 1 | 8 | 2.

**Vậy đáp án là 1 | 8 | 2.**

## 2. Caesar cipher

Task 2.1 In this task, you must write an application using your chosen programming language to encrypt and decrypt a message using Caesar cipher. Your application should satisfy the following requirements:

Allow to input a key and a plaintext to encrypt or ciphertext to decrypt using a given key.

Allow brute-force all possible keys k to find the plaintext of given ciphertext without its key.

Test your program with a message of at least 100 words and compare the result with other cryptography tools (like Cryptool 2) to verify. Then use your program to crack the following ciphertext:

Max NBM bl t extwbgz bglmbmnmbhg ngwxk OGN-AVF, lixvbtebsbgz bg max ybxew hy bgyhkftmbhg mxvaghehzr. Xlmtueblaxw pbma t fbllbhg mh yhlmxk bgghotmbhg tgw xqvxeexgvx bg BM xwnvtmbhg tgw kxlxtkva, NBM hyyxkl t pbwx ktgzx hy ngwxkzktwntmx tgw ihlmzktwntmx ikhzktfl tbfxw tm ikhwnvbgz abzaer ldbeexw ikhyxllbhgtel. Max ngboxklbmr bl kxvhzgbsxw yhk bml vnmmbgz-xwzx kxlxtkva bg tkxtl ebdx vruxklxvnkbmr, tkmbybvbte bgmxeebzxgvx, tgw lhymptkx xgzbgxxkbgz. Pbma lmtmx-hy-max-tkm ytvbebmbxl tgw t lmkhgz xfiatlbl hg vheetuhktmbhg pbma bgwnlmkr, NBM xjnbil lmnwxgml pbma uhma maxhkxmbvte dghpexwzx tgw iktvmbvte ldbeel mh makbox bg max ktibwer xoheobgz mxva bgwnlmkr.

Do you find any special concerning the key used to encrypt this ciphertext?

**Giải:**

A screenshot of a computer program

AI-generated content may be incorrect.

A screen shot of a computer program

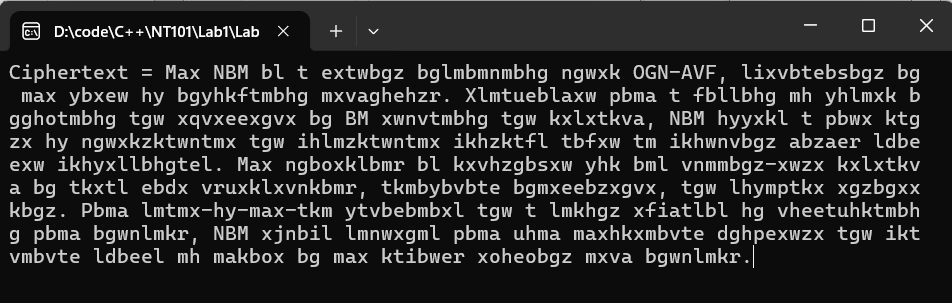
AI-generated content may be incorrect.

Giải thích code:

* Hàm EnCrytion được dùng để mã hóa ký tự và hàm DeCrytion được dùng để giải mã ký tự theo thuật toán Caeser Cipher.
* Đầu tiên kiểm tra ký tự có viết hoa hay không viết hoa, còn không thì sẽ là các ký tự đặc biệt, sau đó trả về 1 ký tự theo biểu thức sau: 'A' + (input - 'A' - key + 26) % 26.
* Input – ‘A’ : lấy ra thứ tự của input trong bảng chữ cái.
* input - 'A' – key : dịch chuyển input về trước 1 khoảng key hay lấy khoảng cách từ ‘A’ tới chữ cái mới khi chuẩn bị dịch chuyển.
* input - 'A' - key + 26 : cộng thêm 26 để kết quả luôn dương.
* % 26 : lấy dư để số luôn nằm trong khoảng [0, 25].
* ‘A’ + : để chuyển từ chỉ số qua lại ký tự chữ cái.
* Tương tự cho các biểu thức khác.
* Dòng 39: Nhập vào 1 chuỗi văn bản (s).
* Dòng 40: Lấy độ dài chuỗi.
* Dòng 42 – 47: Người dùng chọn phương thức mã hóa (Encryt) hoặc giải mã (Decryt).
* Dòng 49 – 59: Nhập key, sau đó duyệt và mã hóa tuần tự từng ký tự của chuỗi văn bản theo key vừa nhập để cho ra chuỗi mã hóa (Ciphertext).
* Dòng 61 – 72: Để giải mã thì duyệt qua từng key (1 - 25) với chuỗi văn bản, với từng key thì duyệt tuần tự từng ký tự để giải mã và cho ra chuỗi giải mã (Plaintext). Từ đây kiểm tra từng đáp án để tìm ra đáp án chính xác.

**Quá trình chạy chương trình:**

Nhập chuỗi ciphertext:



Chọn giải mã (Decryt) và tìm kiếm kết quả đúng với từng key (1 - 25) được duyệt: 

A screenshot of a computer screen

AI-generated content may be incorrect.

Kết quả sau khi tìm kiếm tại key = 19:

Tương tự cho việc mã hóa (Encryt):

A screenshot of a computer

AI-generated content may be incorrect.

## 4. Playfair cipher

**Task 4.1** Encrypt and decrypt using Playfair cipher. You are able to use public tools or your own tool that was developed in the advanced task 4.2. Given the cipher text:

ARYWYPHCBVEBYGMPNCYGCNTDNCWTMGRMFTQPLEWTMLREFBEBQEBIYGBFLPHVOAEHKDHEUNGQFEROLEWTMLOPHEQGOSBEROQDWTLCMTHBWLNRKXRYLORYYPHCBVEBYRLGYDMKYGGWKLROANDBWGNERMNGYRLGHEWRTRLMBRHMUDGVODVTEGMCHLGWCMTFODNRRYCMZKODDUTDXGEOPOYRMFRMGUKXRYGHABROVTGQMCEHPRPEOTSEGEQLARYWYPOTMGQDOEXGOAUDHGUTULTNEHFTFHPGXGVPHGURBDMEGWKLETCBOTNTFQLTAEHMTUGEOAHEVEROXGVPHGDEWTEWGQIEDLPILERWPMOATNGQKQEAHBMVRFKBRMKLXODXFREBHMNUKXRYKLRMFLWDDNCN

The key used was Harry Potter. Let’s decrypt the message.

**Giải:**

A screenshot of a computer

AI-generated content may be incorrect.

**Advanced Task 4.2** In this extra task, you have to write an application using your own programming language to encrypt and decrypt a message using Playfair cypher. Your application should satisfy the following requirements:

* Allow you to input a key and the plain text to encrypt or a cypher text to decrypt.
* Display the Playfair matrix (5x5) corresponding with the given key.

Test your program with a message of at least 100 words and compare the result with other cryptography tools (like Cryptool 2) to verify.

**Giải:**

A screen shot of a computer screen

AI-generated content may be incorrect.

A computer screen shot of a program code

AI-generated content may be incorrect.

A computer screen shot of a program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screen shot of a computer program

AI-generated content may be incorrect.

**Giải thích code:**

1. Hàm fillMatrix:

* Hàm dùng để điền 1 ma trận kích thước 5x5 với khóa key đầu vào và sau đó điền các ký tự chữ cái còn thiếu ( ‘I’ và ‘J’ là một) dựa trên thuật toán Playfair.
* Sử dụng set<char> used để lưu các ký tự chữ cái đã điền và ma trận nhằm tránh trùng lặp ký tự.
* Tiếp theo điền các ký tự của khóa key vào ma trận khóa, ký tự sẽ được viết hoa để đồng bộ dữ liệu khóa.
* Tiếp đến thay ký tự ‘J’ thành ‘I’ để đủ 25 ký tự chữ cái cho ma trận 5x5, kế đến kiểm tra xem ký tự này đã được điền hay chưa bằng cách sử dụng used để kiểm tra.
* Sau khi đã điền xong khóa thì sẽ điền các ký tự chữ cái còn thiếu vào ma trận, cũng thay ‘J’ bằng ‘I’ và kiểm tra chữ cái đã được sử dụng hay chưa.

1. Hàm printMatrix: dùng để in ma trận khóa.
2. Hàm processString:

* Hàm dùng để biến chuỗi văn bản thành 1 chuỗi có từng cặp 2 ký tự liền nhau và từng cặp cách nhau bởi 1 khoảng trắng, với mỗi 1 cặp ký tự giống nhau thì sẽ tách ra và thêm ‘X’ vào sau ký tự đầu tiên đó, còn ký tự còn lại sẽ liên kết với các ký tự sau của chuỗi văn bản theo thuật toán của Playfair.
* Dòng 46 – 49: Loại bỏ khoảng trắng trong văn bản và biến chuỗi thành chuỗi in hoa.
* Dòng 51: chia chuỗi thành từng cặp ký tự.
* Dòng 52 – 53: lấy ký tự đầu của cặp và ký tự sau của cặp, nếu mà cặp cuối của chuỗi chỉ có 1 ký tự thì sẽ thêm ‘X’ vào sau ký tự đó để thành 1 cặp hoàn chỉnh.
* Dòng 54 – 58: xử lý 2 ký tự trùng nhau, chèn thêm ‘X’ vào giữa chúng, i-- để nó lặp lại ở cặp tiếp theo.
* Dòng 59 – 62: nếu 2 ký tự không trùng thì giữ nguyên cặp đó.
* Dòng 63 – 64: sau đó thêm khoảng trắng vào giữa mỗi cặp.
* Cuối cùng trả về chuỗi đã chỉnh sửa.

1. Struct Point: Tạo 1 kiểu biến Point để lưu giữ tọa độ của ký tự trong ma trận khóa.
2. Hàm EnCrytion và DeCrytion:

* Hàm EnCrytion và DeCrytion dùng để mã hóa và giải mã ký tự theo thuật toán Playfair.
* Dòng 78 – 79: Khai báo biến Point nhằm lưu trữ tọa độ cho 2 ký tự cần mã hóa.
* Dòng 81 – 96: tìm kiếm tọa độ 2 ký tự mã hóa trong ma trận khóa.
* Dòng 97 – 101: nếu 2 ký tự mã hóa cùng hàng (row) thì cả 2 sẽ dịch qua phải 1 đơn vị, nếu ký tự ở cuối hàng (row) thì sẽ quay lại từ ký tự đầu hàng (row).
* Dòng 102 – 106: nếu 2 ký tự mã hóa cùng cột (col) thì cả 2 sẽ dịch xuống 1 đơn vị, nếu ký tự ở cuối cột (col) thì sẽ quay lại từ ký tự đầu cột (col).
* Dòng 107 – 108: Trường hợp cuối là khi 2 ký tự mã hóa tọa nên 1 hình chữ nhật trong ma trận khóa, khi đó cả 2 sẽ trao đổi tọa độ cột cho nhau.
* Dòng 109 – 110: 2 ký tự mã hóa sẽ lấy ký tự mới dựa trên tọa độ mới của mình.
* Tương tự cho DeCrytion nhưng ngược lại so với EnCrytion.

1. Hàm main:

* Nhập vào chuỗi văn bản, sau đó chuỗi văn bản sẽ được chỉnh sửa dựa vào hàm processString.
* Sau đó nhập chuỗi khóa (key), khi đó sẽ tạo ra ma trận khóa dựa vào hàm fillMatrix.
* Chọn các phương thức Encryt hoặc Decryt để mã hóa hoặc giải mã chuỗi văn bản.
* Với mỗi phương thức thì sẽ duyệt qua từng cặp ký tự để mã hóa hoặc giải mã.

**Quá trình chạy chương trình:**

Với văn bản “*Doan trich Xuan Toc Do cuu quoc la mot phan quan trong trong tac pham So Do cua nha van Vu Trong Phung Khong chi la mot cau chuyen no con la mot buc tranh song dong ve cuoc song va thoi dai Voi chi tiet va su sac net tac gia da tao ra mot buc tranh chan thuc ve xa hoi Viet Nam trong giai doan lich su day bien dong Tac pham khong chi tap trung vao nhan vat chinh ma con phan anh sau sac ve tinh hinh chinh tri xa hoi va tam ly con nguoi Su tuong tac giua cac nhan vat cung voi nhung hinh anh ve cuoc song hang ngay voi nhung rac roi trong quan he con nguoi da khien doc gia dam chim trong the gioi ma tac gia tao ra Dieu nay lam noi bat kha nang cua tieu thuyet trong viec phan anh va lam sang to nhung khia canh sau sac cua xa hoi va con nguoi Qua doan trich chung ta co the thay duoc kha nang sang tao da dang cua van hoc va ky thuat viet de mo ta cuoc song phong phu va da chieu cung voi thong diep tu tuong ma tac gia muon truyen dat qua nhung trang van*” thành chuỗi mã hóa với Key = “maytinh”:

A screenshot of a computer

AI-generated content may be incorrect.

A black and white screen with white letters

AI-generated content may be incorrect.

## 5. Polyalphabetic ciphers – Vigenère

**Task 5.1** In this task, your job is to write an application using your chosen programming language to encrypt and decrypt a message using Vigenère cipher.

Test your program with a message of at least 100 words and compare the result with other cryptography tools (like Cryptool 2) to verify.

**Giải:**

A screen shot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a program code

AI-generated content may be incorrect.

**Giải thích code:**

* Hàm EnCrytion và DeCrytion được dùng để mã hóa và giải mã ký tự ứng dụng theo thuật toán Vigenère cipher.
* Đầu tiên kiểm tra ký tự có viết hoa hay không viết hoa, còn không thì sẽ là các ký tự đặc biệt, sau đó trả về 1 ký tự theo biểu thức sau: 'A' + (input - 'A' - key + 26) % 26.
* Input – ‘A’ : lấy ra thứ tự của input trong bảng chữ cái.
* Key – ‘A’ : lấy ra thứ tự của key trong bảng chữ cái.
* input - 'A' + (key – ‘A’) : dịch chuyển input về trước 1 khoảng shift hay lấy khoảng cách từ ‘A’ tới chữ cái mới khi chuẩn bị dịch chuyển.
* input - 'A' + (key – ‘A’) + 26 : cộng thêm 26 để kết quả luôn dương.
* % 26 : lấy dư để số luôn nằm trong khoảng [0, 25].
* ‘A’ + : để chuyển từ chỉ số qua lại ký tự chữ cái.
* Tương tự cho DeCrytion.
* Dòng 41 – 43: Nhập chuỗi văn bản (s) và lấy độ dài chuỗi.
* Dòng 45 – 47: Nhập chuỗi key và lấy độ dài key.
* Dòng 50 – 55: Người dùng chọn phương thức mã hóa (Encryt) hoặc giải mã (DeCryt).
* Dòng 49: Biến j dùng để duyệt qua từng ký tự của chuỗi key, nếu j = độ dài chuỗi key thì sẽ qua trở lại bằng 0.
* Dòng 56 – 68: Duyệt qua từng ký tự của chuỗi văn bản và tương ứng với đó là ký tự của chuỗi key để mã hóa từng ký tự, sau đó cho ra chuỗi mã hóa (Ciphertext).
* Dòng 69 – 81: Duyệt qua từng ký tự của chuỗi văn bản và tương ứng với đó là ký tự của chuỗi key để giải mã từng ký tự, sau đó cho ra chuỗi giải mã (Plaintext).

**Quá trình chạy chương trình:**

Mã hóa chuỗi văn bản “hello world” với key = “maytinh”:

A screenshot of a computer program

AI-generated content may be incorrect.

Giải mã lại chuỗi mã hóa vừa rồi “tejew jvdlb” với cùng key = “maytinh”:

A screenshot of a computer program

AI-generated content may be incorrect.