X

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ X**

**<Tên Lab>**

**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.

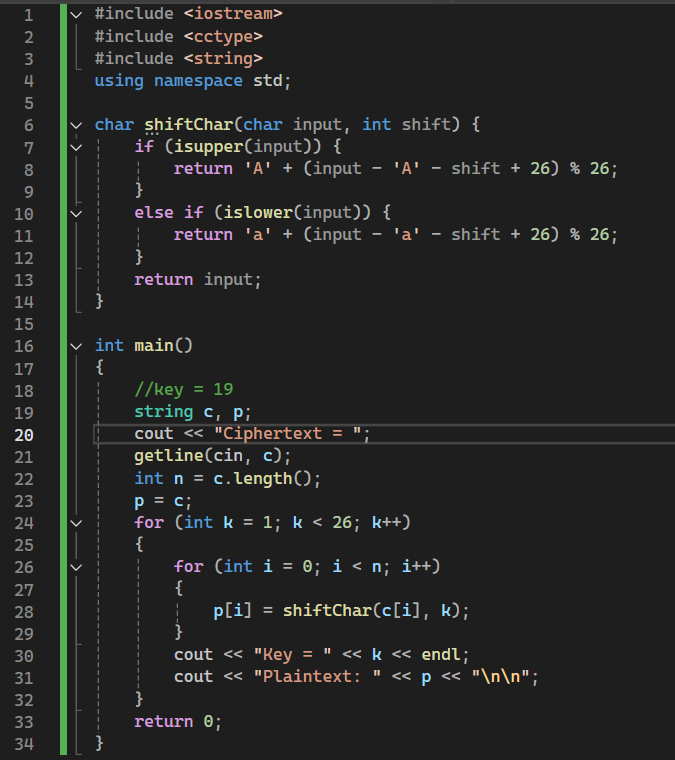
Allow brute-force all possible keys k to find the plaintext of given ciphertext without its key.

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:**

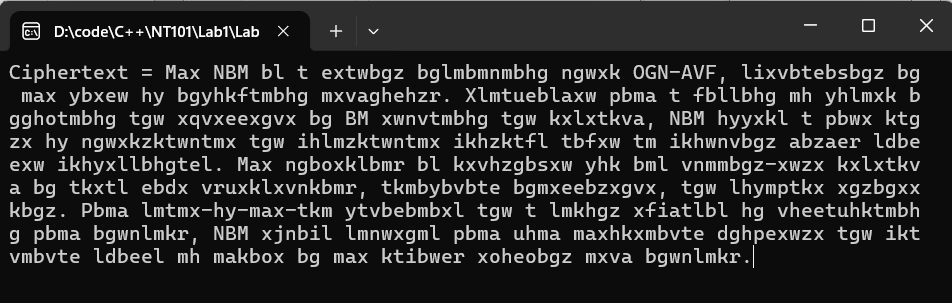


Giải thích code:

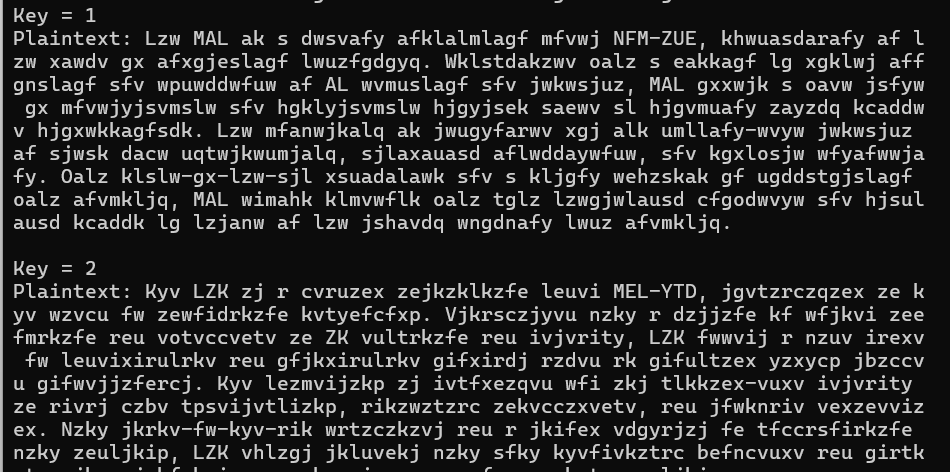
* Hàm shiftChar ban đầu được dùng để mã hóa ký tự nhưng sau khi thay đổi thì đã dùng để giải mã ký tự.
* Đầu tiên kiểm tra ký tự có viết hoa hay không viết hoa, còn không thì sẽ là các ký tự đặc biệt.
* 'A' + (input - 'A' - shift + 26) % 26
* Input – “A” : lấy ra thứ tự của input trong bảng chữ cái.
* input - 'A' – shift : dịch chuyển input về trước 1 khoảng shift.
* input - 'A' - shift + 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.
* Dòng 20: Nhập vào 1 chuỗi cần mã hóa (c)
* Dòng 21: lấy độ dài chuỗi.
* Dòng 22: copy chuỗi mã hóa để lấy độ dài cho chuỗi giải mã (p).
* Duyệt từng ký tự trong chuỗi để giải mã từng ký tự.
* Duyệt key từ 1 – 25 để tìm kiếm kết quả theo công thức p = (c – key) mod 26
* Sau đó kiểm tra từng kết quả với mỗi key

**Quá trình chạy chương trình:**

Nhập chuỗi ciphertext:



Tìm kiếm kết quả với mỗi key từ 1 – 25:



Kết quả sau khi tìm kiếm tại key = 19:

