BÁO CÁO THỰC HÀNH

Môn học: Nhập môn bảo đảm và an ninh thông tin

Lab 3:

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: IE105.P13.CNVN

STT	Họ và tên	MSSV	Email
1	Hoàng Bảo Long	22520807	22520807@gm.uit.edu.vn
2	Đặng Trần Long	22520805	22520805@gm.uit.edu.vn
3	Nguyễn Duy Phương	22521165	22521165@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]2

STT	Công việc	Kết quả tự đánh giá
1	Task 1 (1.1, 1.2)	60%
2	Task 2	100%
3	Task 3 (3.1)	0%
4	Task 4	100%
5	Task 5	100%
6	Task 6	100%
7	Task 7 (7.1 done)	50%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

Task 1:

Ex.1. Key for lock is 042

EX.2.
Approached using brute force technique since the test case is quite low (1->9)

Label each symbol as alphabel letter from a to i

Column 3 re write as 2b+2f=10i+i => ii%11=0

After brute force I came out as 2

Continue brute force

7	7	5	1
9	9	6	9
5	8	5	4
8	9	6	9

Final result:

a	b	c	d	e	f	g	h	i
7	5	8	1	9	6	3	4	2

Task 2:

Encrypts or decrypts text based on the key and mode.

Attempts to decrypt ciphertext using all possible keys.

Prints the application menu.

Prompts the user to choose an option (1, 2, or 3).

Option 1 (Encrypt):

- Prompt for plaintext and key.

- Encrypt the plaintext.
- Print the ciphertext.

Option 2 (Decrypt):

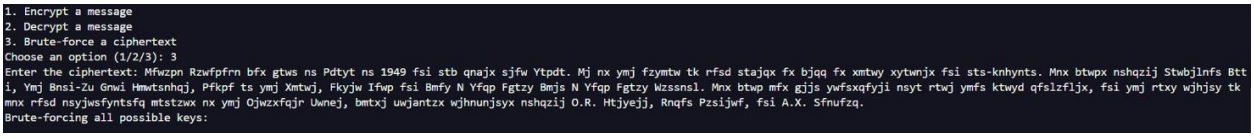
- Prompt for ciphertext and key.
- Decrypt the ciphertext.
- Print the plaintext.

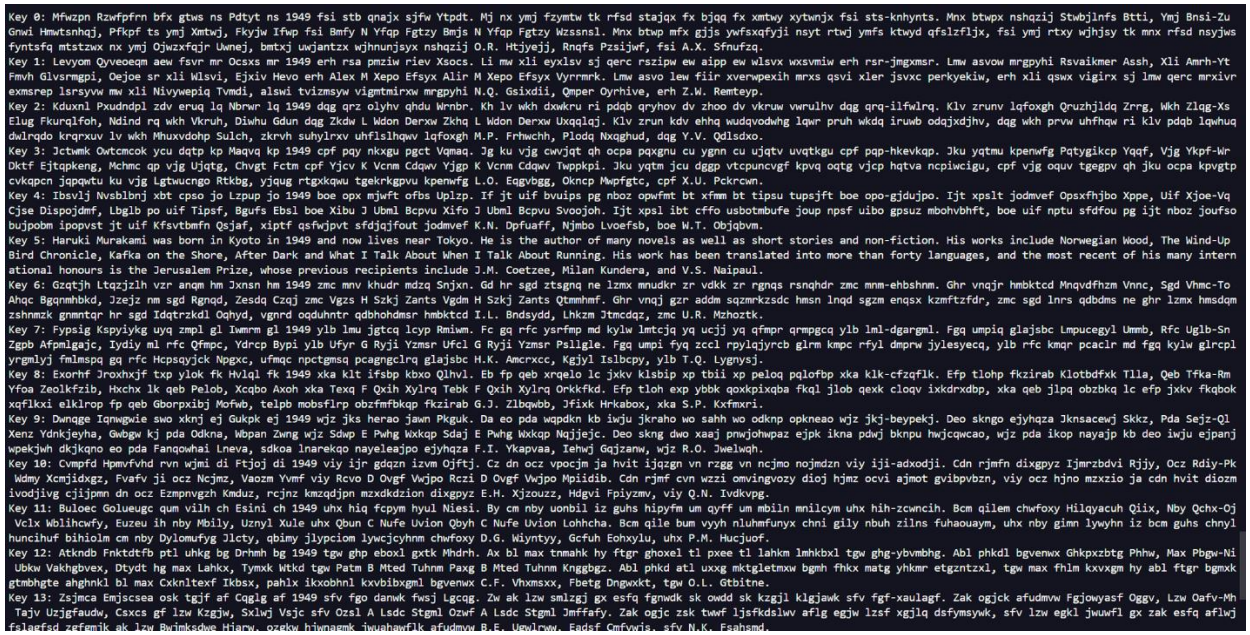
Option 3 (Brute-force):

- Prompt for ciphertext.
- Attempt to decrypt using all possible keys.

Invalid choice:

- Print an error message.





The correct is 5

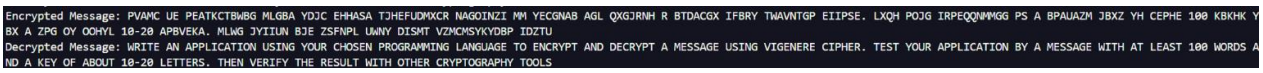
Task 4:

1. Convert the key to uppercase, replace “J” with “I,” and combine it with the alphabet to build a unique 5×5 matrix.
2. Remove spaces and non-letter characters from the plaintext, pad it if necessary, then split it into pairs.
3. For each pair, locate their positions in the matrix and apply Playfair cipher rules to encrypt or decrypt (adjusting columns, rows, or performing a rectangle swap).
4. Return or print the resulting encrypted or decrypted text.

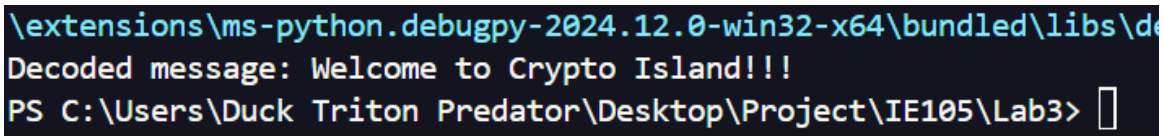
```
Enter the key: K
Enter the plain-text to encrypt: IE105 UIT N15 Long Long Phuong

Playfair Matrix:
K A B C D
E F G H I
L M N O P
Q R S T U
V W X Y Z


Encrypted Message: EFZPSOMPSNMPSNOITPSN
Decrypted Message: IEUITNLONGLONGPHUONG
```

Task 5:

1. Define generate_key function to extend the key to match the message length.
2. Define encrypt function to encrypt the message using the Vigenere cipher.
3. Define decrypt function to decrypt the encrypted message using the Vigenere cipher.
4. Set the message and key variables with example values.
5. Generate the extended key using generate_key.
6. Encrypt the message using the encrypt function.
7. Decrypt the encrypted message using the decrypt function.
8. Print the original message.
9. Print the encrypted message.
10. Print the decrypted message.

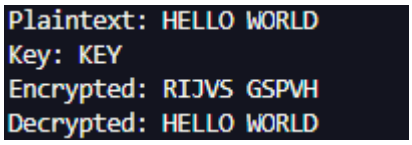


Task 6:



1. Defines a list ascii_codes containing ASCII integer values.
2. Converts each integer to its corresponding character using chr(code).
3. Joins all characters into a single string decoded_message with ".join(...).
4. Prints the message "Decoded message:" followed by the decoded string.
5. Outputs the human-readable message represented by the ASCII codes.

Task 7.1:



Vigenère cipher for encrypting and decrypting messages. The process involves the following steps:

1. Key Generation: The generate_key function extends the given key to match the length of the message by repeating its characters.

2. Encryption: The encrypt function shifts each character of the message based on the corresponding character in the key. Letters are shifted alphabetically (considering case), while non-alphabetic characters remain unchanged.

3. Decryption: The decrypt function reverses the encryption process by shifting the characters back using the key.

Finally, the main function demonstrates the process by encrypting and decrypting the message "HELLO WORLD" using the key "KEY". It prints the original plaintext, the key, the encrypted ciphertext, and the decrypted text to verify correctness.

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

HẾT