Task 2:

Ứng dụng mã hóa và giải mã bằng Caesar Cipher gồm có các thành phần sau:  
 + Khung text để đưa dữ liệu đầu vào (đoạn text muốn mã hóa hoặc giải mã)  
 + Khung nhập key (1 – 25)  
 + Nút mã hóa (Encrypt)  
 + Nút giải mã (Decrypt)  
 + Nút cho phép thử tất cả các khóa để giải mã (Brute-force Decrypt)

Thực thi file CaesarCipher.py sẽ xuất hiện một giao diện như hình bên dưới:  
A screenshot of a computer

Description automatically generated  
 *Ứng dụng mã hóa và giải mã bằng mật mã Caesar*

Kiểm thử chức năng mã hóa:

Nhập một đoạn văn bản bất kỳ và so sánh kết quả khi mã hóa bằng các công cụ trực tuyến khác.

A screenshot of a computer

Description automatically generated

*Kết quả của ứng dụng*

A screenshot of a computer

Description automatically generated

*Kết quả của dcode*

Kiểm thử chức năng giải mã:

Nhập một đoạn văn bản bất kỳ và so sánh kết quả khi giải mã bằng các công cụ trực tuyến khác.

A screenshot of a computer

Description automatically generated

*Kết quả của ứng dụng*

*A screenshot of a computer

Description automatically generated*

*Kết quả của dcode*

Kiểm thử chức năng Brute-force Decrypt:

Nhập một đoạn văn bản bất kỳ và so sánh kết quả với các công cụ trực tuyến khác. Như ta thấy, thì cả ứng dụng và công cụ trực tuyến đều cho ra đoạn văn bản có ý nghĩa khi Key = 3.

*A screenshot of a computer

Description automatically generated*

*Kết quả của ứng dụng*

*A screenshot of a computer

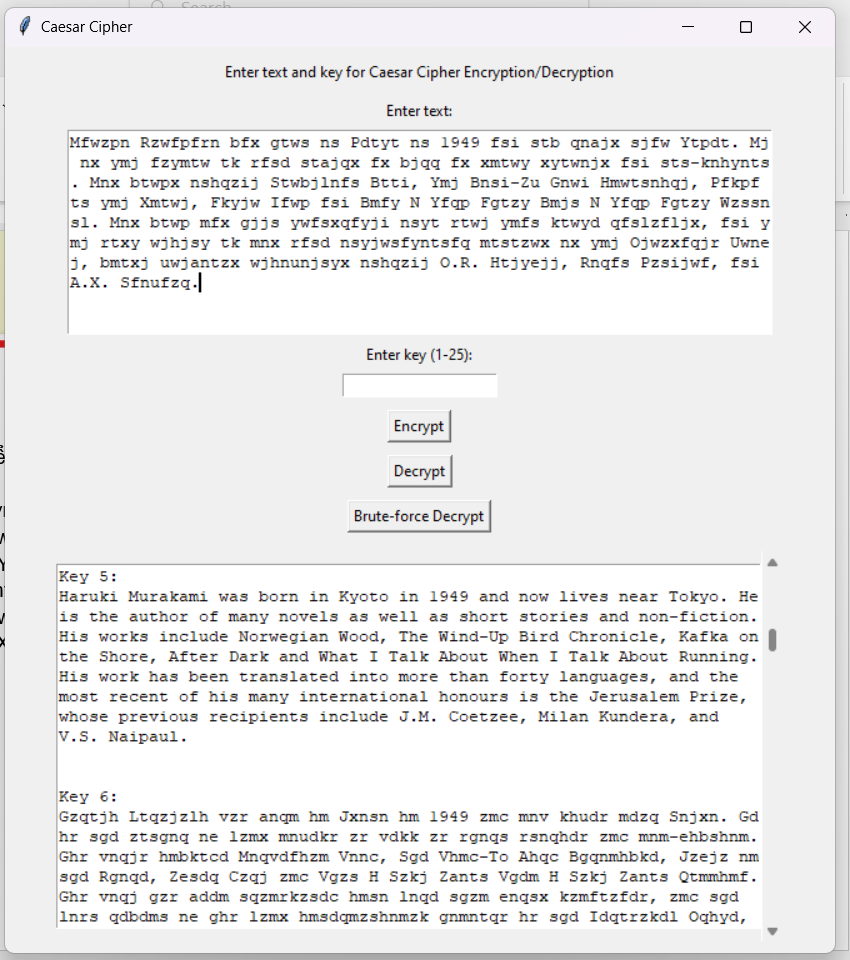
Description automatically generated*

*Kết quả của dcode*

Kiểm tra lại chức năng Brute-force Decrypt với đoạn text:

Mfwzpn Rzwfpfrn bfx gtws ns Pdtyt ns 1949 fsi stb qnajx sjfw Ytpdt. Mj nx ymj fzymtw tk rfsd stajqx fx bjqq fx xmtwy xytwnjx fsi sts-knhynts. Mnx btwpx nshqzij Stwbjlnfs Btti, Ymj Bnsi-Zu Gnwi Hmwtsnhqj, Pfkpf ts ymj Xmtwj, Fkyjw Ifwp fsi Bmfy N Yfqp Fgtzy Bmjs N Yfqp Fgtzy Wzssnsl. Mnx btwp mfx gjjs ywfsxqfyji nsyt rtwj ymfs ktwyd qfslzfljx, fsi ymj rtxy wjhjsy tk mnx rfsd nsyjwsfyntsfq mtstzwx nx ymj Ojwzxfqjr Uwnej, bmtxj uwjantzx wjhnunjsyx nshqzij O.R. Htjyejj, Rnqfs Pzsijwf, fsi A.X. Sfnufzq.

Như vậy, đoạn văn bản trên có nghĩa khi Key = 5.



*Kết quả của ứng dụng*

Task 7:

Cách tìm cờ của file hình ảnh ‘crypto01.jpg’ đã được mã hóa XOR bằng 6 chữ cái:

* Tìm khóa:  
  + Vì khóa dài 6 ký tự, chúng ta sẽ thử tất cả các khóa khả thi (hoặc đoán các khóa phổ biến) bằng phương pháp brute-force và thực hiện XOR với tệp để giải mã.  
  + Tệp này có thể là một ảnh JPEG, vì vậy sau khi giải mã, chúng ta sẽ tìm kiếm dữ liệu có thể đọc được hoặc dữ liệu có cấu trúc trong kết quả giải mã.
* Viết mã Python để giải mã XOR:  
  + Chúng ta có thể sử dụng Python để đọc tệp đã mã hóa và áp dụng XOR cipher để thử giải mã với tất cả các khóa 6 ký tự khả thi.
* Kết quả:  
  Sau khi giải mã, kết quả sẽ là một flag là một ảnh mà chúng ta có thể mở và kiểm tra.