TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO GIỮA KỲ MÔN XÁC SUẤT THỐNG KÊ**

*Người hướng dẫn*: **TS NGUYỄN QUỐC BÌNH**

*Người thực hiện*: **PHẠM TRÍ HÙNG**

Lớp **: 20050201**

Khoá  **: 24**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO GIỮA KỲ XÁC SUẤT THỐNG KÊ**

Người hướng dẫn: **TS NGUYỄN QUỐC BÌNH**

Người thực hiện: **PHẠM TRÍ HÙNG**

Lớp **: 20050201**

Khoá  **: 24**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

LỜI CẢM ƠN

Xin gửi lời cảm ơn đến thầy vì đã cung cấp cho em đủ kiến thức trong quá trình học tập nhằm thực hiện được báo cáo này một cách tốt nhất.

**CÔNG TRÌNH ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi và được sự hướng dẫn khoa học của TS Nguyễn Quốc Bình;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong luận văn còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung luận văn của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Phạm Trí Hùng*

TÓM TẮT

Trong báo cáo này em sẽ dùng kiến thức mình đã học được trong học kỳ vừa rồi nhằm giải quyết các vẫn đề liên quan đến môn học cấu trúc rời rac.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc101465228)

[TÓM TẮT iii](#_Toc101465229)

[MỤC LỤC 1](#_Toc101465230)

[DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT 2](#_Toc101465231)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 3](#_Toc101465232)

[PHẦN 1: 4](#_Toc101465233)

[1.1 Introduction: 4](#_Toc101465234)

[1.1.1 phần câu hỏi: 4](#_Toc101465235)

[1.1.2 phần trả lời: 4](#_Toc101465236)

[1.2 Monoalphabetic substitution cipher 6](#_Toc101465237)

[1.2.1 phần câu hỏi: 6](#_Toc101465238)

[1.2.2 phần trả lời: 6](#_Toc101465239)

[1.3 Frequency Analysis: 16](#_Toc101465240)

[1.3.1 phần câu hỏi: 16](#_Toc101465241)

[1.3.2 phần trả lời: 16](#_Toc101465242)

[1.4 Experiments: 18](#_Toc101465243)

[1.4.1 phần câu hỏi: 18](#_Toc101465244)

[1.4.2 phần trả lời: 18](#_Toc101465245)

DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

**CÁC CHỮ VIẾT TẮT**

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

Hình 2.1 Thuật toán mã hóa atbash………………………………………………...........7

Hình 2.2 Thuật toán mã hóa caesar…………………………………………...…………9

Hình 2.3 Thuật toán mã hóa affine……………………………………………………..11

Hình 2.4 Thuật toán mã hóa mixed\_alphabet…………………………………………..13

Hình 2.5 Thuật toán mã hóa rot13……………………………………………………...15

Hình 3.1 Thuật toán frequency analysis………………………………………………..17

Hình 4.1 Thuật toán atbash kèm giải thích……………………………………………..19

Hình 4.2 Thuật toán caesar kèm giải thích……………………………………………..20

Hình 4.3 Thuật toán affine kèm giải thích……………………………………………...21

Hình 4.4 Thuật toán rot13 kèm giải thích……………………………………………....22

Hình 4.5 Thuật toán mixed\_alphabet giải thích………………………………………..23

Hình 4.6 Thuật toán frequency analysis kèm giải thích………………………………...25

Hình 4.7 Minh họa sử dụng thuật toán atbash để mã hóa chuỗi 50 từ…………………27

Hình 4.8 Minh họa sử dụng thuật toán caesar để mã hóa chuỗi 50 từ………………...28

Hình 4.9 Minh họa sử dụng thuật toán affine để mã hóa chuỗi 50 từ……………........29

Hình 4.10 Minh họa sử dụng thuật toán rot13 để mã hóa chuỗi 50 từ………………….30

Hình 4.11 Minh họa sử dụng thuật toán atbash để mã hóa chuỗi 100 từ………………32

Hình 4.12 Minh họa sử dụng thuật toán affine để mã hóa chuỗi 1000 từ………………43

PHẦN 1:

* 1. Introduction:
     1. phần câu hỏi:

Giới thiệu các khái niệm về mã hóa và giải mã, khóa đối xứng và khóa bất đối xứng, …

* + 1. phần trả lời:

Nhằm phục vụ nhu cầu bảo mật thông tin trong lúc vận chuyển, nhiều người đã tạo ra nhiều phương pháp khác nhau nhằm mã hóa, làm thay đổi nội dung gốc theo một trật tự, một khuôn mẫu nhất định nhằm đảm bảo tính bảo mật cũng như khả năng dịch trở lại thành văn bản gốc tại phía người nhận, việc mã hóa thực chất là một nhóm các thao tác được thực hiện chính xác và tuần tự nhằm chuyển văn bản gốc thành văn bản mã hóa, các phương pháp mã hóa này đa phần đều hoạt động dựa vào khóa, độ phức tạp và quá trình mã hóa phụ thuộc vào loại khóa được chọn, khóa bắt buộc phải được chọn trước quá trình mã hóa và trong đa phần trường hợp nếu không có khóa sẽ rất khó thậm chí không thể chuyển từ văn bản mã hóa sang văn bản gốc.

Việc mã hóa có thể hiểu đơn giản là quá trình biến bản rõ (plaintext) trở thành bản mã (ciphertext), thông thường chỉ có những người được ủy quyền (có được key mã hóa) mới có thể chuyển ngược lại từ bản mã thành bản rõ được, các key được dùng để tiến hành mã hóa thường được tạo ra từ các thuật toán tạo mã ngẫu nhiên.

Hiện tại các khóa dùng để mã hóa chia thành 2 dạng khác nhau đối xứng và bất đối xứng, cụ thể như sau:

Với khóa đối xứng việc mã hóa và giải mã sẽ được thực hiện bằng duy nhất một khóa, văn bản gốc ban đầu còn gọi là bản rõ sẽ được biến đổi thành dạng văn bản mà con người không thể đọc được, còn gọi là bản mã, sau đó khi bản mã gửi đến người nhận có thể sử dụng cùng một loại khóa đã dùng để mã hóa nhằm giải mã và lấy được thông tin.

Cách hoạt động: bên gửi sẽ tiến hành mã hóa bản rõ thành bãn mã thông qua một khóa đã được chọn lựa sẵn từ trước và được thông báo cho bên nhận, sau khi bên nhận có được thông tin sẽ tiến hành sử dụng chính xác loại khóa đã được bên gửi dùng để mã hóa nhằm tiến hành giải mã.

Ưu điểm:

Khóa đối xứng có ưu điểm là tốc độ tạo ra khóa nhanh, dễ dàng, dễ sử dụng.

Vì cả hai bên sử dụng cùng một loại khóa nên phương pháp mã hóa này có tốc độ truyền dữ liệu nhanh hơn.

Khuyết điểm:

Do sử dụng chung một loại khóa cho cả mã hóa và giải mã nên khi bên thứ 3 có được khóa thông tin sẽ ngay lập tức bị lộ.

Việc chia sẽ khóa giữa hai bên sẽ gặp khó khăn.

Cần tạo ra rất nhiều khóa nếu muốn giữ được tính bí mật của từng người khi trao đổi trong một nhóm người.

Không có tính ứng dụng cao trong các hệ thống có tính mở do khi đó sẽ có quá nhiều key cần phải được tạo ra nhằm đảm bảo được tính an toàn của thông tin.

Không thể sử dụng cho mục đích xác thực và chống thoái thoát

Trái lại với khóa đối xứng việc mã hóa và giải mã đối với khóa bất đối xứng sẽ cần 1 bộ chìa khóa, một bộ chìa khóa sẽ bao gồm 2 chiếc một chiếc khóa công khai (có thể cung cấp một cách công khai cho tất cả mọi người) và một chiếc khóa cá nhân(chỉ duy nhất một người giữ khóa này), vì các vấn đề bảo mật khóa bí mật khóa bí mật phải được đảm bảo bí mật với tất cả với tất cả mọi người.

Cách hoạt động:

Người gửi sẽ phải gửi thông tin đã được mã hóa bằng khóa công khai của người nhận.

Người nhận sẽ dùng khóa cá nhân của mình để giải mã thông tin.

Ưu điểm:

Khóa công khai không cần được chia sẽ một cách bí mật mà có thể được chia sẽ rộng rãi cho tất cả mọi người.

Khóa cá nhân chỉ có riêng một cá nhân được biết an toàn hơn và có khả năng xác thực được nguồn thông tin

Số lượng khóa cần tạo ra tuy vẫn nhiều nhưng ít hơn so với khóa đối xứng nếu muốn đảm bảo tính riêng tư của từng bên trong quá trình giao tiếp.

Cung cấp khả năng bảo mật dữ liệu cao hơn.

Nhược điểm:

Có khả năng bị tấn công thông qua phương pháp tấn công người đúng giữa.

Việc tạo ra và sử dụng tương đối khó.

* 1. Monoalphabetic substitution cipher
     1. phần câu hỏi:

Giới thiệu về các vấn đề, các ràng buộc, phương pháp và thuật toán nhằm mã hóa.

* + 1. phần trả lời:

Phương pháp mã hóa monoalphabetic substitution cipher có các đặc điểm sau:

Substitution: các dạng mã hóa xếp vào loại substitution này sẽ tiến hành thay thế ký tự trong văn bản gốc thành các ký tự khác trong quá trình mã hóa và thông qua một key nhất định được người thực hiện lựa chọn từ trước và trong quá trình mã hóa sẽ không làm thay đổi vị trí các ký tự.

Monoalphabetic: dạng mã hóa có tính chất monoalphabetic là dạng mã hóa chỉ dùng duy nhất một loại dạng substitution duy nhất trên toàn bộ bản rõ để tạo ra được bản mã, một ký tự trong bản rõ sẽ luôn trở thành một ký tự trong bản mã.

Thuật toán mã hóa bằng phương pháp atbash:



Hình 2.1 Thuật toán mã hóa atbash

Thuật toán atbash là một thuật toán mã hóa vô cùng đơn giản, việc mã hóa đơn giản này là một nhược điểm lớn và nên được cân nhắc khi quyết định sử dụng mã atbash. Với thuật toán atbash ta sẽ chỉ có duy nhất một lựa chọn duy nhất cho khóa nhằm mã hóa bản rõ thành bản mã, đó là đảo ngược toàn bộ bảng chữ cái (a-z => z-a) và do đó loại mật mã này khá rất dễ bị phá, trong trường hợp chỉ cần biết được văn bản được mã hóa bằng phương pháp atbash thì văn bản sẽ được phá ngay lập tức.

Ví dụ về quá trình mã hóa sử dụng mã atbash:

Mã hóa bản rõ “atbash” theo phương thức mã hóa atbash:

Bản rõ: atbash

Bảng chữ cái bản rõ và bản mã:

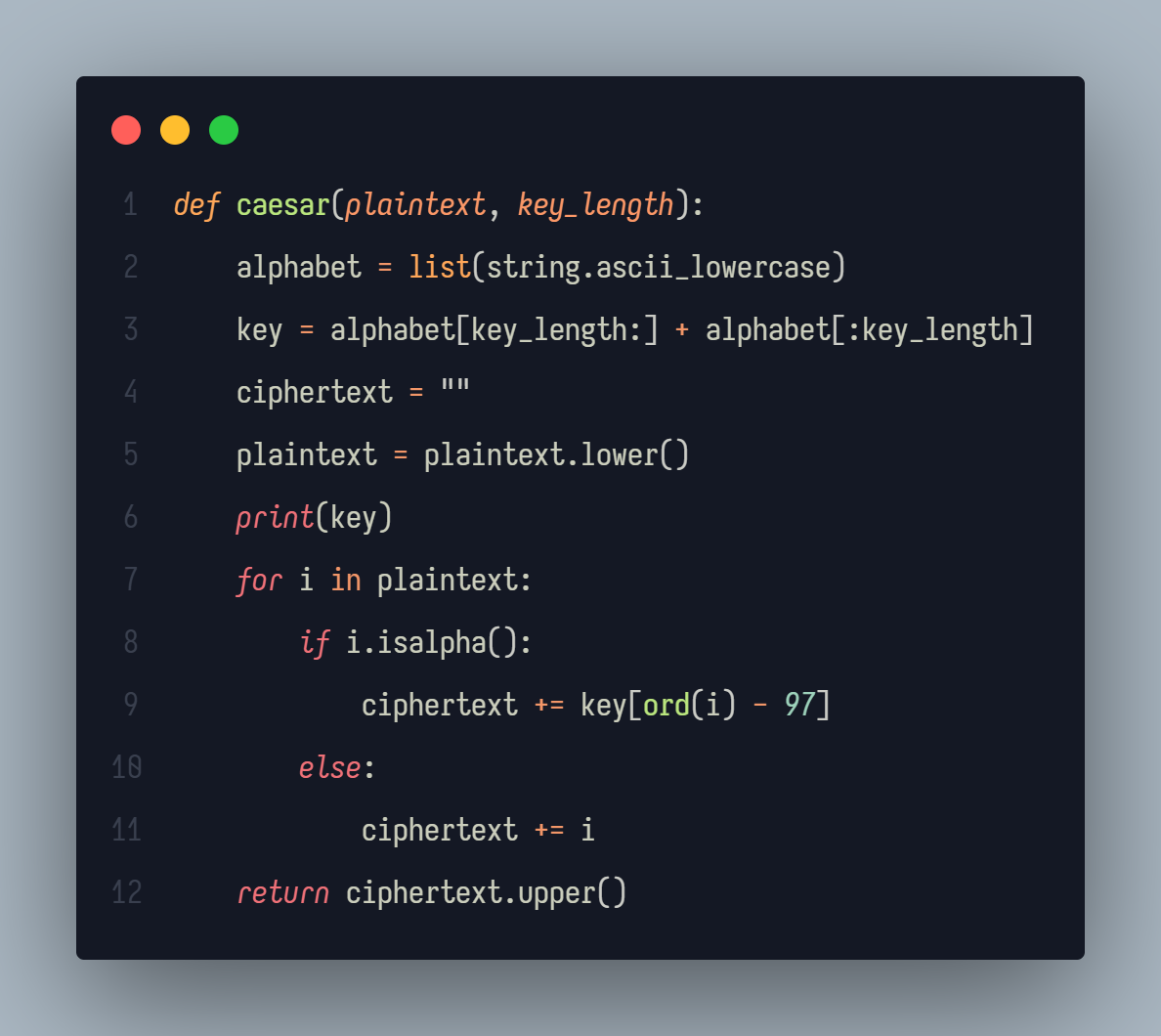
https://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/5266158_orig.jpg

Bảng 2.1 bảng chữ cái bản rõ và bản mã của phương pháp mã hóa atbash

Từ bảng trên ta sẽ có được a = Z, t = G, b = Y, a = Z, s = H, h = S

Kết quả cuối cùng thu được sau quá trình mã hóa bằng phương pháp mã hóa atbash là: ZGYZHS

thuật toán mã hóa theo phương pháp caesar:



Hình 2.2 Thuật toán mã hóa caesar

Thuật toán mã hóa caesar đã được tạo ra và đặt tên theo Julius Caesar nhằm truyền thông tin trong quân đôi, dù là độ phức tạp của thuật toán đã cao hơn atbash nhưng vẫn tương đối dễ phá đặc biệt là khi sử dụng các công nghệ hiện đại, việc tạo ra bảng mã trong phương pháp mã hóa caesar tương đối dễ dàng chỉ cần một một khóa là một số nguyên biểu thị độ dịch của bảng chữ cái từ đó tiến hành dịch phải đối với khóa dương và dịch trái đối với khóa âm với số ký tự tương ứng của khóa để tạo ra bản mã, và vì tính chất này mà t biết được rằng ta chỉ có thể tạo ra được tối đa 26 dạng khóa khác nhau, số lượng khóa có thể tạo ra không nhiều và do đó hoàn toàn có thể bị phá nếu sử dụng thuật toán vét cạn.

Trong ví dụ này ta sẽ dùng bảng mã caesar dịch 3 để tiến hành mã hóa văn bản “caesar”:

Bảng chử cái bản rõ và bản mã:

Picture

Bảng 2.2 Bảng chử cái bản rõ và bản mã của phương pháp mã hóa caesar

Từ bảng trên ta sẽ có được c = F, a = D, e = H, s = V a = D và r = U.

Và kết quả thu được bản mã sau khi tiến hành mã hóa bằng mã hóa caesar: FDHVDU.

Thuật toán mã hóa bằng phương pháp affine:



Hình 2.3 Thuật toán mã hóa affine

Quá trình tạo ra bảng mã của thuật toán mã hóa affine có chút khác biệt so với các dạng mã bên trên khi có sự xuât hiện của phép toán số học trong quá trình mã hóa, cụ thể khi muốn mã hóa văn bản gốc thành văn bản mã hóa ta cần sử dụng công thức (a \* x + b) % m, trong đó a và b chính là hai khóa để tiến hành mã hóa của dạng mã hóa này, theo mã hóa affine có thể tạo ra 312 loại key khác đã là một tiến bộ vượt bật so với những gì mà atbash và caesar có thể.

Mã hóa văn bản “affine” theo phương thức mã hóa affine:

Văn bản gốc: affine

Do đặc thù loại mã này thao tác nhiều trên số học nên điều đầu tiên ta làm sẽ là chuyển từ các ký tự trong bảng chữ cái latin thành các số nguyên từ 0 đến 25:

Picture

Bảng 2.3 Bảng chuyển từ các ký tự trong bảng chữ cái sang số nguyên

Quy đổi các ký tự bên trong văn bản gốc thành các số nguyên dương tương đương và tiến hành thực hiện phép toán để mã hóa, sau đó tra lại vào bảng và tìm ký tự ứng với kết quả vừa tính được:

a sẽ được chuyển thành số 0 và sau khi thực hiện phép tính với a = 5, b = 8, kết quả tính toán có được là 8 ứng với vị trí của chữ i trong bảng chử cái.

Tiếp tục tiến hành cho các ký tự khác trong chuỗi cho đến khi toàn bộ các ký tự được chuyển dổi, ta có được kết quả như sau



Bảng 2.4 Bảng chuyển từ chuỗi affine thành bản mã theo phương pháp mã hóa affine

IHHWVC

Thuật toán mã hóa bằng phương pháp mixed-alphabet:

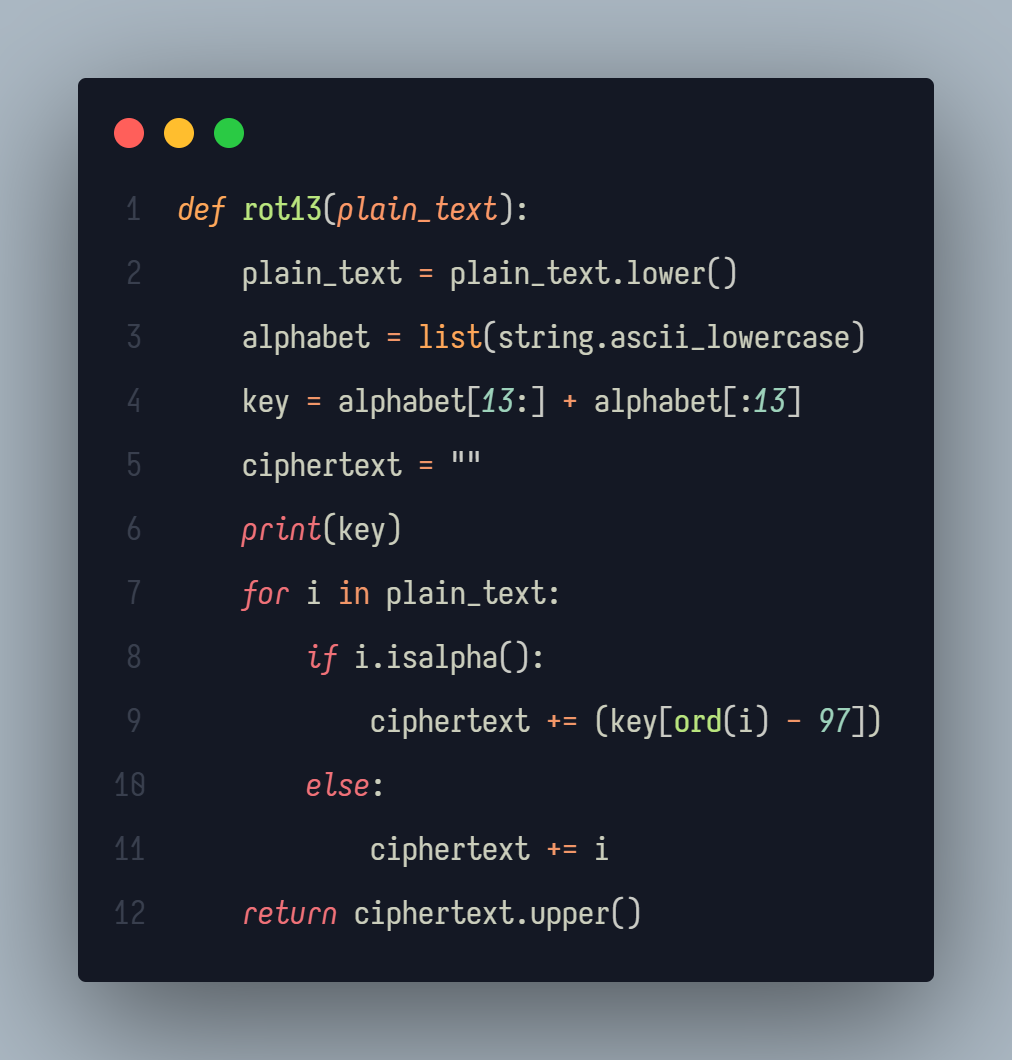


Hình 2.4 Thuật toán mã hóa mixed\_alphabet

Mixed-alphabet là một dạng mã hóa có khả năng tạo ra số lượng key rất lớn vì cách tạo ra key là trộn lẫn các chữ cái bên trong bảng chữ cái không theo bất cứ quy luật nào để tạo ra được key hoặc có thể dùng một keyword nào đó để tạo bảng mã trong trường hợp keyword được cung cấp t sẽ xếp tất cả các chữ cái có trong keyword đó lên đầu theo thứ tự xuất hiện của từng chữ cái còn lại các chữ cái khác viết theo thứ tự như bình thường:

Do đó ta sẽ có 26! = 403,291,461,126,605,635,584,000,000 cách khác nhau để tạo key và với mỗi key đó ta sẽ có một văn bản mã hóa khác nhau, do đó nếu không biết được key chính xác mà chỉ biết được loại mã hóa thì cũng tương đối khó để tiến hành giải mã văn bản được mã hóa bằng loại mã hóa này.

Thuật toán mã hóa bằng phương pháp rot13:



Hình 2.5 Thuật toán mã hóa rot13

Giống với loại mã hóa bằng phương pháp atbash, rot-13 chỉ có một lựa chọn key duy nhất đó là dịch từ bảng chữ cái gốc 13 ký tự từ trái sang phải, và cũng sẽ bị phá ngay lập tức nếu người giải mã nắm được loại mật mã được dử dụng là rot-13.

Mã hóa chuỗi “cipher” với thuật toán mã hóa rot-13:

Chuỗi gốc: “cipher”

Bàng chữ cái của bản rõ và bản mã:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |

Bảng 2.5 Bảng chữ cái của bản rõ và bản mã của phương pháp mã hóa rot13

Từ bảng trên ta tiến hành mã hóa chuỗi: “cipher” như sau:

c = P, i = V, p = C, h = U, e = R, r = E

sau khi hoàn tất quá trình mã hóa từ bản rõ bằng phương pháp rot13 ta thu được bản mã như sau:

PVCURE

* 1. Frequency Analysis:
     1. phần câu hỏi:

Giới thiệu về các vấn đề, các ràng buộc, phương pháp và thuật toán phân tích tần số.

* + 1. phần trả lời:

Việc phá mã không phải lúc nào cũng cần có sự xuất hiện của khóa, có thể dùng các dạng thuật toán liên quan nhằm tìm được bản rõ hoặc gần với bản rõ mà không cần khóa, ví dụ: thuật toán vét cạn brute force có thể hoatj động nếu đó là một số loại mã nhất định, nhưng trong các thuật toán mã hóa hiện đại hơn số lượng khóa được tạo ra sẽ là quá nhiều và thuật toán vét cạn sẽ là không khả thi, do đó ta cần tìm một phương pháp tốt hơn để tiến hành phá mã, và một trong số đó là phân tích tần số.

Hoàn cảnh: trong tất cả các ngôn ngữ có sử dụng bản chữ cái chắc chắn luôn luôn có các chữ cái sẽ có tần suất xuất hiện cao hơn các chữ cái còn lại, có thể lấy một ví dụ điển hình là bảng chữ cái tiếng anh, các chữ cái e, t, o, i, n được thống kê là những chữ cái có tần xuất xuất hiện nhiều nhất, với tính chất của substitution cipher là chỉ thay đổi từ một ký tự này sang một ký tự khác và không làm thay đổi vị trí, ta hoàn toàn có thể áp dụng việc phân tích tần số vào để phá mã, cụ thể như sau:

Bắt đầu bằng việc đếm tuần suất xuất hiện của toàn bộ các ký tự trong bản mã, ta sẽ thu được một danh sách các chữ cái trong bản mã được sắp xếp theo tần suất xuất hiện, ta sử dụng danh sách ký tự sắp xếp theo tần suất xuất hiện của ngôn ngữ muốn giải mã là đã chuẩn bị từ trước và tiến hành thay thế từng cặp cho giữa hai danh sách này cho nhau nhằm thu được kết quả.



Hình 3.1 Thuật toán frequency analysis

Theo ý kiến riêng của cá nhân phương pháp này có tương đối nhiều khuyết điểm, đầu tiên việc phân tích tần số này chỉ có ý nghĩa với các đoạn bản mã đủ lớn, cách làm này sẽ hoàn toàn vô nghĩa đối với các mật mã có quá ít nội dung vì không có đủ dữ kiện nhằm đếm được tần xuất xuất hiện và đảm bảo được thay thế đúng ký tự cần thiết

* 1. Experiments:
     1. phần câu hỏi:

chạy thử các thuật toán trong các phần trước

* + 1. phần trả lời:

1.4.2a phần giải thích code:

Từng bước thực thi của các loại mã đã được ghi chú ngắn gọn thông qua comment:

Mã atbash:



Hình 4.1 Thuật toán atbash kèm giải thích

Biến chuỗi nhận vào thành in thường nhằm đảm bảo tính đúng đắn của thuật toán, tạo ra khóa bằng cách đảo ngược bảo chữ cái latinh, duyệt qua các phần từ trong bản rõ và tiến hành thay thế để thu được bản mã

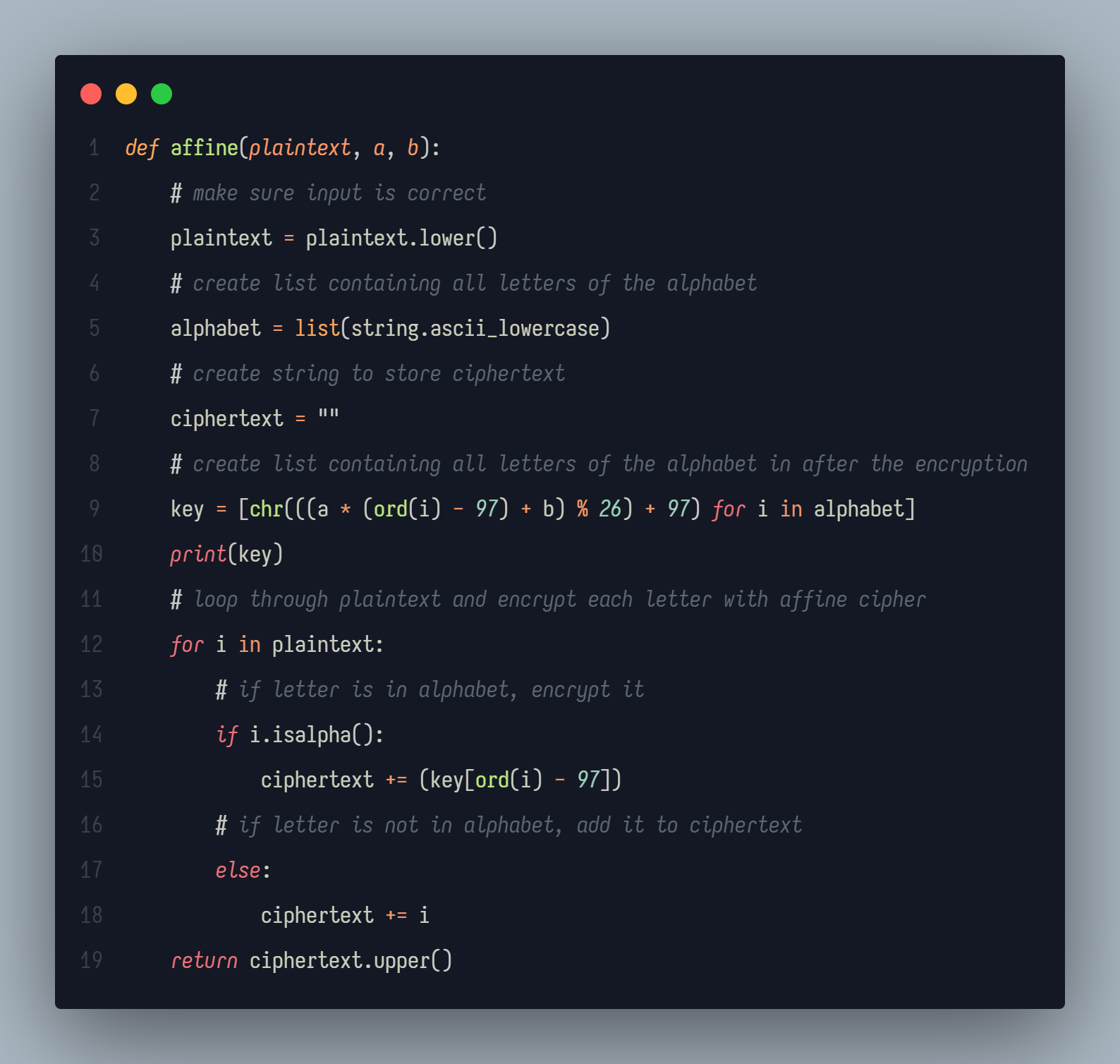
Mã caesar:



Hình 4.2 Thuật toán caesar kèm giải thích

Biến chuỗi nhận vào thành in thường nhằm đảm bảo tính đúng đắn của thuật toán, tạo ra khóa bằng cách dịch chuyển bảng chữ cái theo số ký tự đã truyền vào, duyệt qua các phần từ trong bản rõ và tiến hành thay thế để thu được bản mã

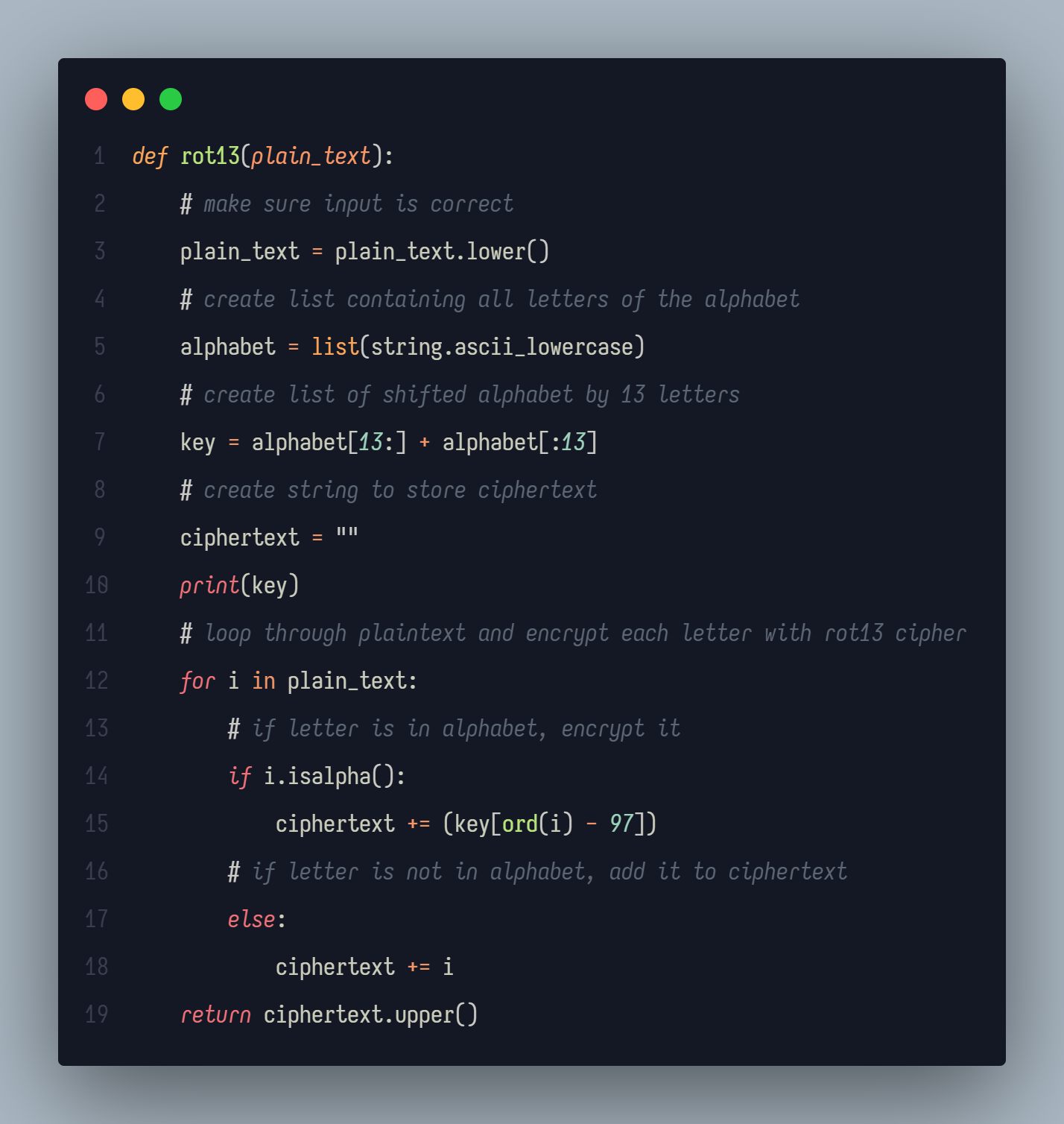
Mã affine:



Hình 4.3 Thuật toán affine kèm giải thích

Biến chuỗi nhận vào thành in thường nhằm đảm bảo tính đúng đắn của thuật toán, tạo ra khóa bằng cách lấy vị trí của chữ cái đó(có thể bắt đầu từ 0 hoặc 1) và làm theo công thức (a\*x +b) % 26, duyệt qua các phần từ trong bản rõ và tiến hành thay thế để thu được bản mã

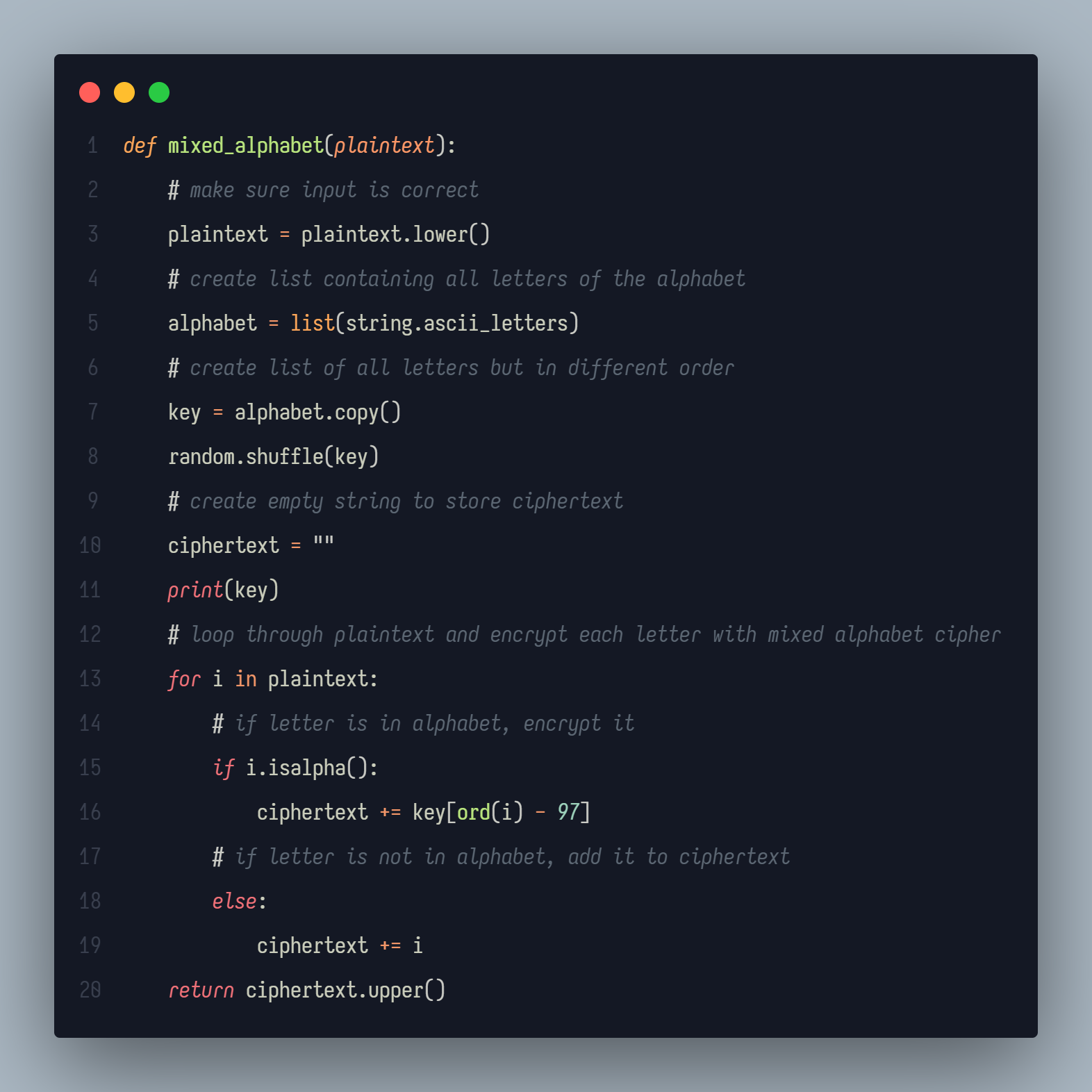
Mã rot13:



Hình 4.4 Thuật toán rot13 kèm giải thích

Biến chuỗi nhận vào thành in thường nhằm đảm bảo tính đúng đắn của thuật toán, tạo ra khóa bằng cách lấy 13 ký tự đầu bảng chữ cái chuyển xuống cuối duyệt qua các phần từ trong bản rõ và tiến hành thay thế để thu được bản mã

Mã mixed\_alphabet:



Hình 4.5 Thuật toán mixed\_alphabet giải thích

Biến chuỗi nhận vào thành in thường nhằm đảm bảo tính đúng đắn của thuật toán, tạo ra khóa bằng cách trộn lẫn các chữ cái trong bảng chữ cái một cách ngẫu nhiên, duyệt qua các phần từ trong bản rõ và tiến hành thay thế để thu được bản mã

Phân tích tần số:



Hình 4.6 Thuật toán frequency analysis kèm giải thích

Đếm tuần suất xuất hiện của từng ký tự bên trong bản mã, sắp xếp theo thứ tự giảm dần, tiến hành thay thế theo danh sách có sẵn để thu được kết quả.

1.4.2b Phần demo:

Nội dung file plaintext\_50:

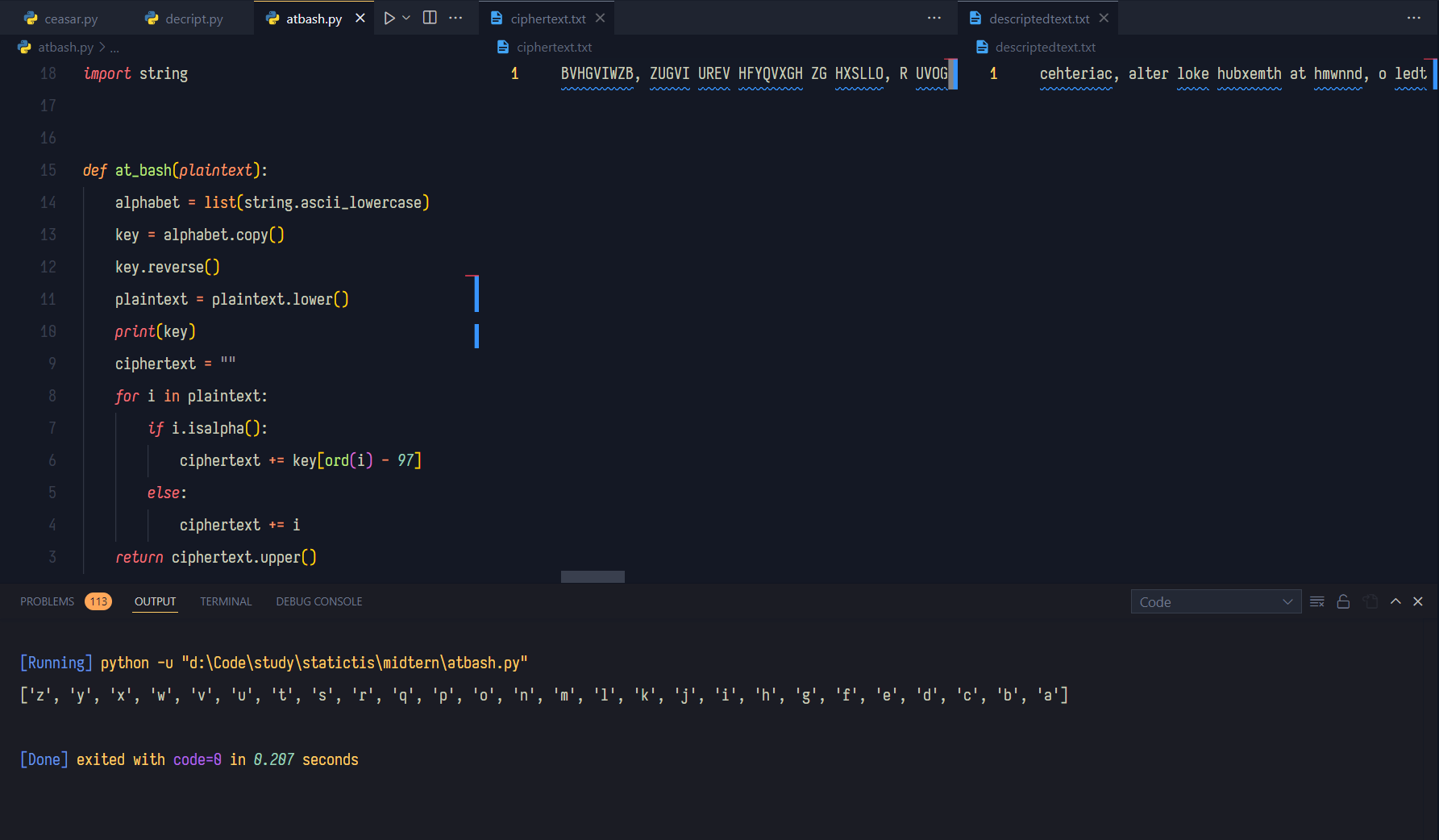
Yesterday, after five subjects at school, I felt so tired and hungry. So, I wanted to go home quickly. Because I was in hurried, I rode my bike so fast. Suddenly, a traffic accident happened, it made all people and me frightened. Fortunately, It didn't happened to me and I felt so lucky.

Nội dung file ciphertext sau khi sử dụng thuật toán atbash để mã hóa:

BVHGVIWZB, ZUGVI UREV HFYQVXGH ZG HXSLLO, R UVOG HL GRIVW ZMW SFMTIB. HL, R DZMGVW GL TL SLNV JFRXPOB. YVXZFHV R DZH RM SFIIRVW, R ILWV NB YRPV HL UZHG. HFWWVMOB, Z GIZUURX ZXXRWVMG SZKKVMVW, RG NZWV ZOO KVLKOV ZMW NV UIRTSGVMVW. ULIGFMZGVOB, RG WRWM'G SZKKVMVW GL NV ZMW R UVOG HL OFXPB.

Nội dung file decryptedtext sau khi dùng phân tích tần số nhằm phá mã:

cehteriac, alter loke hubxemth at hmwnnd, o ledt hn torei asi wusprc. hn, o vastei tn pn wnge juomydc. bemauhe o vah os wurroei, o rnie gc boye hn laht. huiiesdc, a trallom ammoiest waffesei, ot gaie add fenfde asi ge lropwtesei. lnrtusatedc, ot iois't waffesei tn ge asi o ledt hn dumyc.



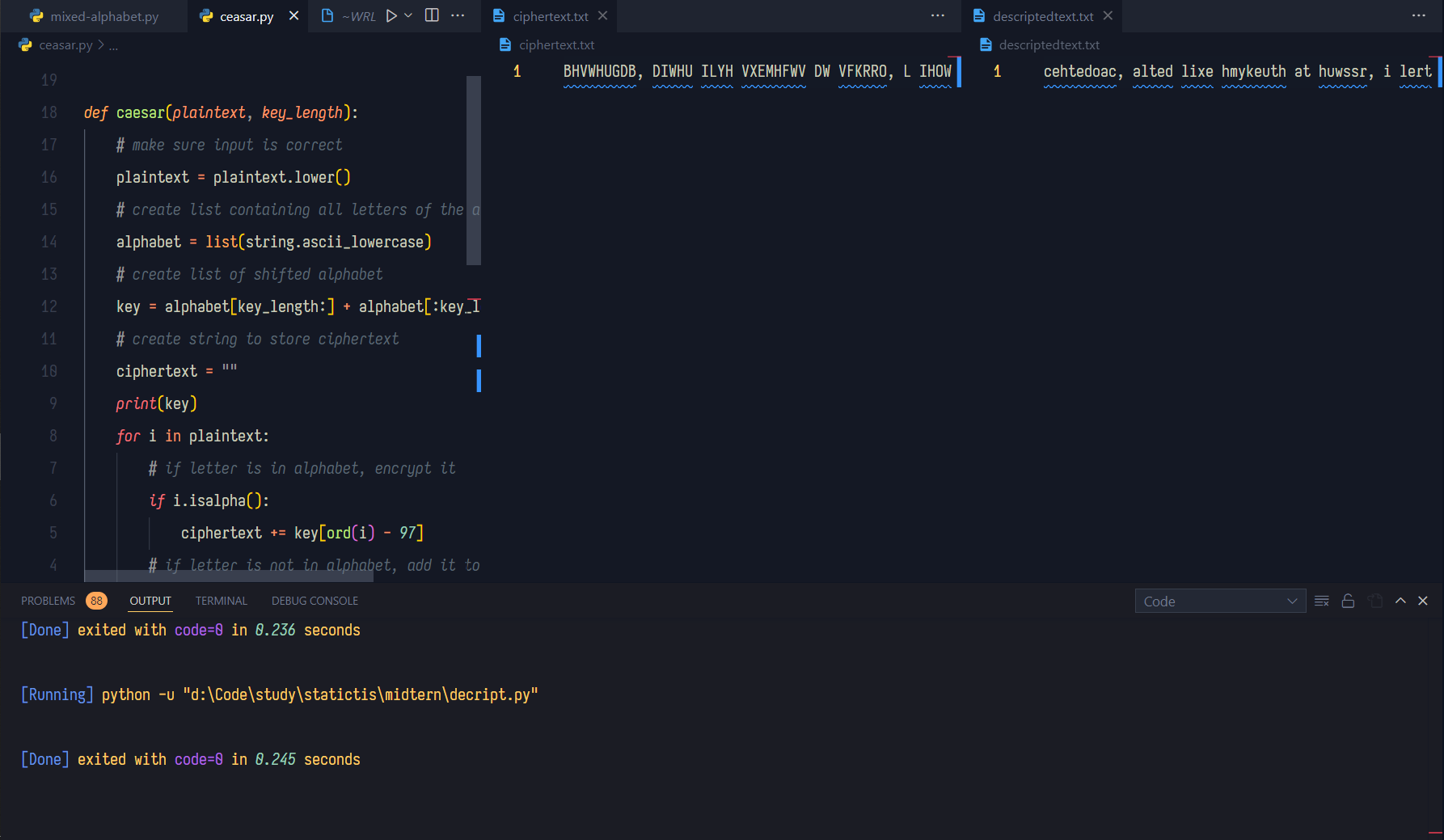
Hình 4.7 Minh họa sử dụng thuật toán atbash để mã hóa chuỗi 50 từ

Nội dung file ciphertext sau khi sử dụng thuật toán caesar với độ dịch là 3 để mã hóa:

BHVWHUGDB, DIWHU ILYH VXEMHFWV DW VFKRRO, L IHOW VR WLUHG DQG KXQJUB. VR, L ZDQWHG WR JR KRPH TXLFNOB. EHFDXVH L ZDV LQ KXUULHG, L URGH PB ELNH VR IDVW. VXGGHQOB, D WUDIILF DFFLGHQW KDSSHQHG, LW PDGH DOO SHRSOH DQG PH IULJKWHQHG. IRUWXQDWHOB, LW GLGQ'W KDSSHQHG WR PH DQG L IHOW VR OXFNB.

Nội dung file decryptedtext sau khi dùng phân tích tần số nhằm phá mã:

cehtedoac, alted lixe hmykeuth at huwssr, i lert hs tideo ano wmnpdc. hs, i vanteo ts ps wsge jmiubrc. yeuamhe i vah in wmddieo, i dsoe gc yibe hs laht. hmooenrc, a tdalliu auuioent waffeneo, it gaoe arr fesfre ano ge ldipwteneo. lsdtmnaterc, it oion't waffeneo ts ge ano i lert hs rmubc.



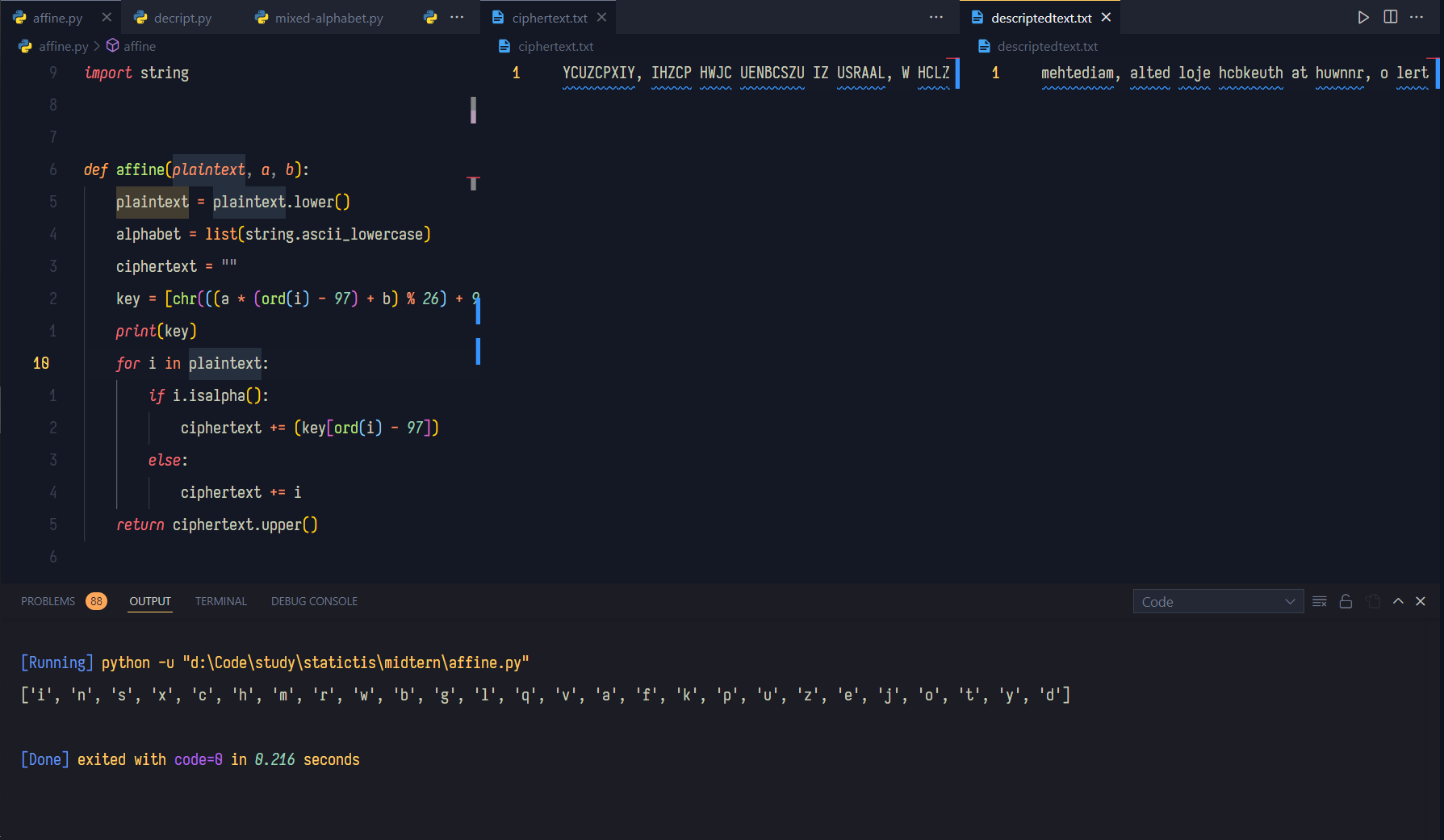
Hình 4.8 Minh họa sử dụng thuật toán caesar để mã hóa chuỗi 50 từ

Nội dụng file ciphertext sau khi sử dụng thuật toán affine với a = 5 và b = 8 để mã hóa:

YCUZCPXIY, IHZCP HWJC UENBCSZU IZ USRAAL, W HCLZ UA ZWPCX IVX REVMPY. UA, W OIVZCX ZA MA RAQC KEWSGLY. NCSIEUC W OIU WV REPPWCX, W PAXC QY NWGC UA HIUZ. UEXXCVLY, I ZPIHHWS ISSWXCVZ RIFFCVCX, WZ QIXC ILL FCAFLC IVX QC HPWMRZCVCX. HAPZEVIZCLY, WZ XWXV'Z RIFFCVCX ZA QC IVX W HCLZ UA LESGY.

Nội dung file decryptedtext sau khi sử dụng phân tích tần số để phá mã:

mehtediam, alted loje hcbkeuth at huwnnr, o lert hn todei asi wcspdm. hn, o vastei tn pn wnge xcouyrm. beuache o vah os wcddoei, o dnie gm boye hn laht. hciiesrm, a tdallou auuoiest waffesei, ot gaie arr fenfre asi ge ldopwtesei. lndtcsaterm, ot iois't waffesei tn ge asi o lert hn rcuym.



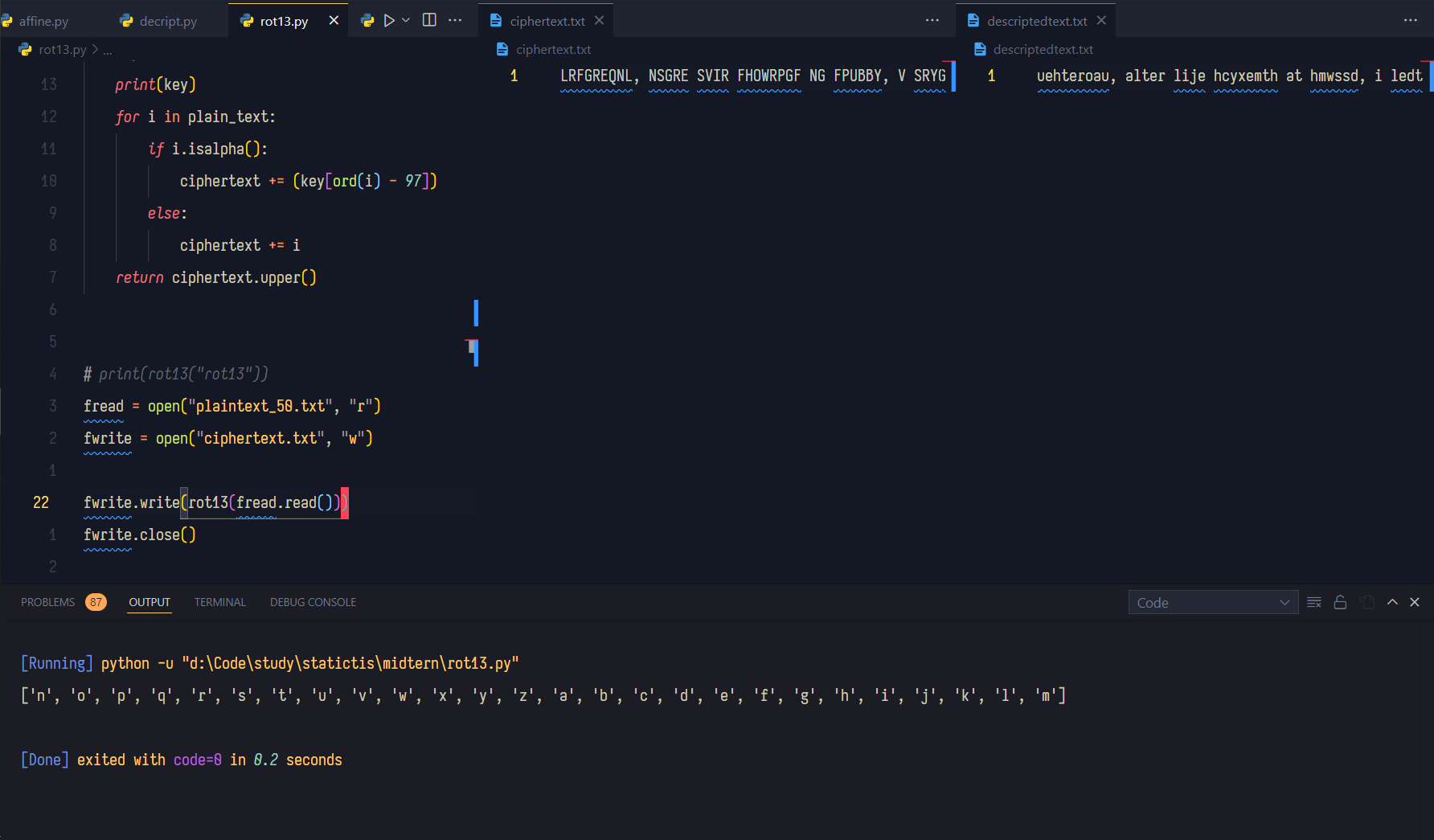
Hình 4.9 Minh họa sử dụng thuật toán affine để mã hóa chuỗi 50 từ

Nội dung fiile ciphertext sau khi sử dụng thuật toán rot13 để mã hóa:

LRFGREQNL, NSGRE SVIR FHOWRPGF NG FPUBBY, V SRYG FB GVERQ NAQ UHATEL. FB, V JNAGRQ GB TB UBZR DHVPXYL. ORPNHFR V JNF VA UHEEVRQ, V EBQR ZL OVXR FB SNFG. FHQQRAYL, N GENSSVP NPPVQRAG UNCCRARQ, VG ZNQR NYY CRBCYR NAQ ZR SEVTUGRARQ. SBEGHANGRYL, VG QVQA'G UNCCRARQ GB ZR NAQ V SRYG FB YHPXL.

Nội dung file decryptedtext sau khi sử dụng phân tích tần số để phá mã:

uehteroau, alter lije hcyxemth at hmwssd, i ledt hs tireo ano wcnpru. hs, i vanteo ts ps wsge kcimbdu. yemache i vah in wcrrieo, i rsoe gu yibe hs laht. hcooendu, a trallim ammioent waffeneo, it gaoe add fesfde ano ge lripwteneo. lsrtcnatedu, it oion't waffeneo ts ge ano i ledt hs dcmbu.



Hình 4.10 Minh họa sử dụng thuật toán rot13 để mã hóa chuỗi 50 từ

Nội dung file plaintext\_100:

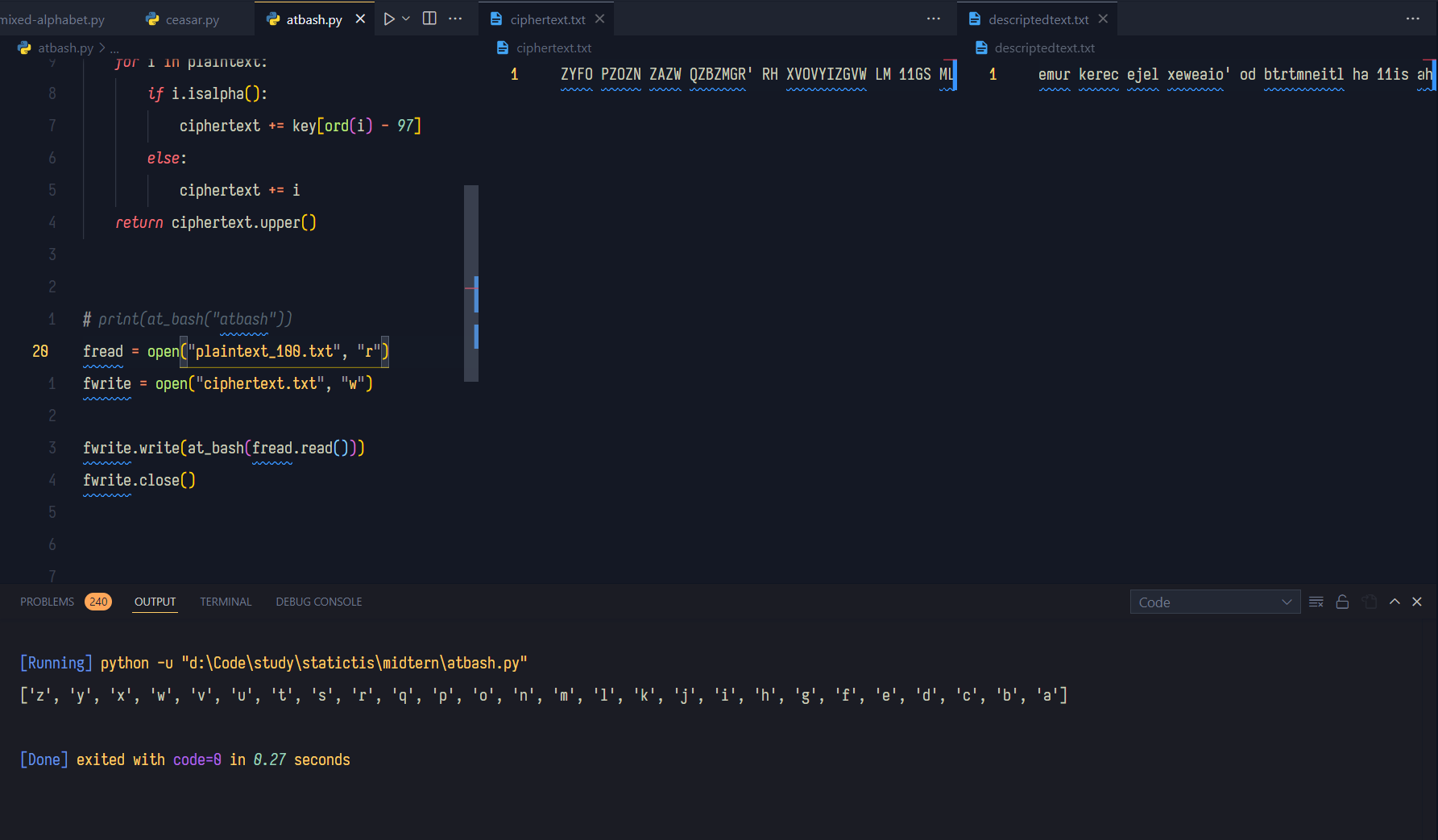
Abul Kalam Azad Jayanti' is celebrated on 11th November every year. It is the birth anniversary of Maulana Abul Kalam Azad. Abul Kalam Azad was born on 11th November, 1888. His real name was Abul Kalam Ghulam Muhiyuddin. His father's name was Maulana Khairuddin, who lived in Bengal. His mother's name was Alia, who was an Arabian. Maulana Azad was a journalist, author, poet and philospher. He started to publish the newspaper 'Al-Hilal' in the year 1912. Al-Hilal played an important role in forging Hindu-Muslim unity. He wrote many works, reinterpreting the holy Quran. He played an active role in the freedom movement of India. He became the first Education Minister of independent India. Maulana Azad died on 22nd February, 1958. For his invaluable contribution to the nation, he was posthumously awarded India's highest civilian honour, Bharat Ratna in 1992. His birth anniversary 11th November is declared as 'National Education Day' by the Government of India.

Nội dung file ciphertext sau khi sử dụng thuật toán atbash để mã hóa:

ZYFO PZOZN ZAZW QZBZMGR' RH XVOVYIZGVW LM 11GS MLEVNYVI VEVIB BVZI. RG RH GSV YRIGS ZMMREVIHZIB LU NZFOZMZ ZYFO PZOZN ZAZW. ZYFO PZOZN ZAZW DZH YLIM LM 11GS MLEVNYVI, 1888. SRH IVZO MZNV DZH ZYFO PZOZN TSFOZN NFSRBFWWRM. SRH UZGSVI'H MZNV DZH NZFOZMZ PSZRIFWWRM, DSL OREVW RM YVMTZO. SRH NLGSVI'H MZNV DZH ZORZ, DSL DZH ZM ZIZYRZM. NZFOZMZ ZAZW DZH Z QLFIMZORHG, ZFGSLI, KLVG ZMW KSROLHKSVI. SV HGZIGVW GL KFYORHS GSV MVDHKZKVI 'ZO-SROZO' RM GSV BVZI 1912. ZO-SROZO KOZBVW ZM RNKLIGZMG ILOV RM ULITRMT SRMWF-NFHORN FMRGB. SV DILGV NZMB DLIPH, IVRMGVIKIVGRMT GSV SLOB JFIZM. SV KOZBVW ZM ZXGREV ILOV RM GSV UIVVWLN NLEVNVMG LU RMWRZ. SV YVXZNV GSV URIHG VWFXZGRLM NRMRHGVI LU RMWVKVMWVMG RMWRZ. NZFOZMZ ZAZW WRVW LM 22MW UVYIFZIB, 1958. ULI SRH RMEZOFZYOV XLMGIRYFGRLM GL GSV MZGRLM, SV DZH KLHGSFNLFHOB ZDZIWVW RMWRZ'H SRTSVHG XRERORZM SLMLFI, YSZIZG IZGMZ RM 1992. SRH YRIGS ZMMREVIHZIB 11GS MLEVNYVI RH WVXOZIVW ZH 'MZGRLMZO VWFXZGRLM WZB' YB GSV TLEVIMNVMG LU RMWRZ.

Nội dung file decryptedtext sau khi sử dụng phân tích tần số để phá mã:

emur kerec ejel xeweaio' od btrtmneitl ha 11is ahgtcmtn tgtnw wten. oi od ist monis eaaogtndenw hp ceureae emur kerec ejel. emur kerec ejel fed mhna ha 11is ahgtcmtn, 1888. sod nter aect fed emur kerec vsurec cusowulloa. sod peistn'd aect fed ceureae kseonulloa, fsh rogtl oa mtaver. sod chistn'd aect fed eroe, fsh fed ea enemoea. ceureae ejel fed e xhunaerodi, euishn, yhti eal ysorhdystn. st dienitl ih yumrods ist atfdyeytn 'er-sorer' oa ist wten 1912. er-sorer yrewtl ea ocyhnieai nhrt oa phnvoav soalu-cudroc uaoiw. st fnhit ceaw fhnkd, ntoaitnyntioav ist shrw qunea. st yrewtl ea ebiogt nhrt oa ist pnttlhc chgtctai hp oaloe. st mtbect ist pondi tlubeioha coaoditn hp oaltytaltai oaloe. ceureae ejel lotl ha 22al ptmnuenw, 1958. phn sod oageruemrt bhainomuioha ih ist aeioha, st fed yhdisuchudrw efenltl oaloe'd sovstdi bogoroea shahun, msenei neiae oa 1992. sod monis eaaogtndenw 11is ahgtcmtn od ltbrentl ed 'aeiohaer tlubeioha lew' mw ist vhgtnactai hp oaloe.



Hình 4.11 Minh họa sử dụng thuật toán atbash để mã hóa chuỗi 100 từ

Nội dung file plaintext\_1000:

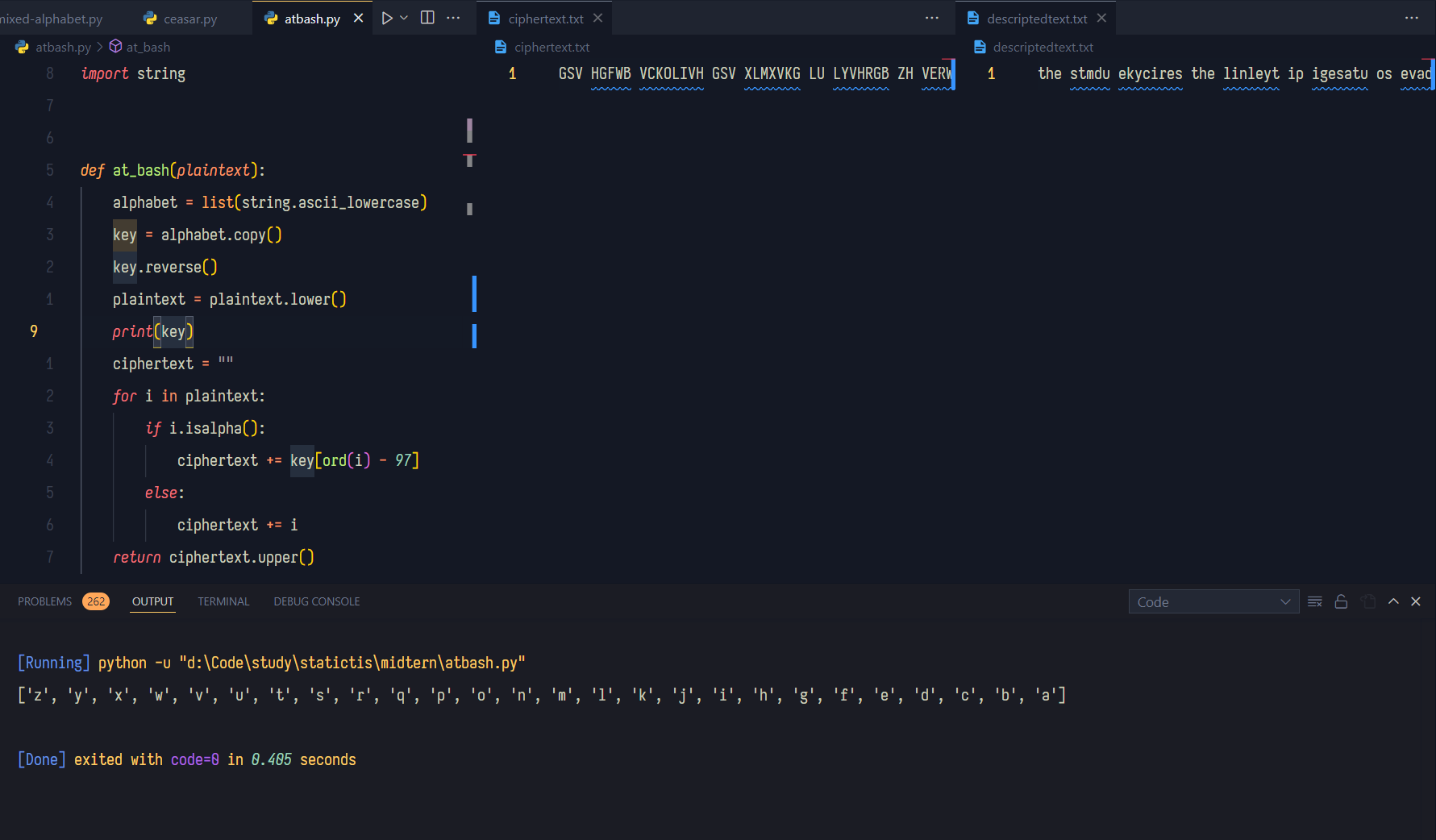
The study explores the concept of obesity as evident among children in the U.S. For better understanding, the article began with the definition of obesity, reviewed the existing literature, highlighted the methodology used to conduct the research, and analyzed the research findings. Lastly, recommendations were made with the study ending in a conclusion. Obesity is a disease commonly associated with children in most countries in the world. Obesity means weighing much more than is healthy for someone. Some people confuse diabetes with obesity. These two should not be compared because diabetes is the product of obesity (Paxon 27). Obesity is a health condition that is caused by consuming or eating too much energy and fatty foods that contain more calories than what a body can use. Based on this, the extra calories are stored in the body in form of fat are said to be the factor that leads to overweight among people including children. Obesity, like any other disease, is treatable through either physical activities or medicinal pills. It has been noted that doctors use what is known as the body mass index (BMI) to determine whether someones health is at risk or not. This research paper was conducted with an aim of exploring the incidence of obesity in children in the U.S. (Paxon 45). Thesis statement: Obesity has been a burning issue among children in the U.S. for the last four decades. Weight management programs were the only method used by medical practitioners to fight against obesity and this has led to healthier lives among children living with obesity.Obesity is a serious medical condition that has affected the health of many children in the United States since the 1980s to date. Initially, people thought that gaining weight in children was a good indicator of being healthy without conceptualizing the dangers associated with being overweight in children. Studies have shown that obesity is a serious disease that can lead to other health problems that include arthritis, diabetes, heart disease and high blood pressure among obese victims (Paxon 61). Although studies have indicated that children are more prone to obesity than adults are, similar studies have shown that everybody is a victim of obesity because the disease is largely related to eating habits that are common to every individual in the world. Through numerous studies, it is evident that obesity in the U.S. is highly pronounced compared to other nations in the world (Hedley et al 2500). In conjunction with this, many obese victims are children as opposed to adults mainly because of the changes in lifestyles whereby technological advancement has led to the introduction of more luxurious activities. For instance, children between the age of 5 and 12 years are prone to obesity because they spend much of their time watching Television at the expense of physical activities. Numerous studies revealed that being a few pounds overweight is not an implication of obesity but a person is considered obese when he or she has a body mass index that is higher than 30. On the other hand, many adults become overweight while using medicine to put on weight such as the use of corticosteroids and antidepressants among others (Waters Seidell and Swinburn 52). Recent studies have shown that in modern society, there are numerous incidences of obesity as opposed to the past because people lack physical activities that were practiced by early men and fatty and sugary foods have become more available than they were in the traditional society. Eating foods with lesser energy and indulging in physical practices are the only viable means for fighting obesity (Gortmaker and Dietz 47). The researcher embarked on the use of a survey as an appropriate method in researching obese children in the United States. The survey collected data using a questionnaire with questions related to obesity and weight management among the children being asked. A sample of 50 children was randomly selected with two doctors using the body mass index to determine the health of the sampled children whose age ranged between 5 and 15 years (Freedman et al 1759). From the survey, it was evident that 35 children out of 50 weighed much more than their health, which was an indicator that they were obese. For this survey, it was concluded that most children aged between 5 years and 12 years are affected by obesity early in their lives. Such children spend much of their time watching television programs rather than playing on the playground. They also feed on too fatty and sugary foods something that made them be more prevalent in obesity (Hedley et al 2500). The research accepted the null hypothesis that obesity is more pronounced among children aged between 5-12 years because of lack of physical exercise and consumption of too fatty and sugary foods. The category of children prone to obesity is the age group of children aged between 5 and 12 years. The implication is that they spent much of their time watching television rather than playing on the playground. They also have little thinking capability the fact is caused by unused energy in the body with the energy being stored as fat that amounts to obesity. If 35 children out of 50 are obese, it meant that in every 1000 children in the United States 700 children suffer from obesity. The category of children prone to obesity is the age group of children aged between 5 and 12 years. The implication is that they spent much of their time watching television rather than playing on the playground. They also have little thinking capability the fact is caused by unused energy in the body with the energy being stored as fat that amounts to obesity. If 35 children out of 50 are obese, it meant that in every 1000 children in the United States 700 children suffer from obesity. The study is interesting in that it highlights the concept of obesity as applied to children in the United States. Watching Television and consumption of fatty and sugary foods are the main causes of obesity among children meaning that if children could be encouraged to participate in physical activities, obesity can easily be reduced gradually and eliminated in the end. Parents should urge children to play more than watch the television because this would enable them to manage their weight. In addition to improving their health, physical activities have been known to be positively associated with improved academic performance. At the national level, the government should introduce physical exercise programs in schools hence making it mandatory for all schools to have playgrounds for children. Therefore, participation in physical activities by American children would slightly reduce the health budget at the national level.

Nội dung file ciphertext sau khi sử dụng thuật toán atbash để mã hóa:

GSV HGFWB VCKOLIVH GSV XLMXVKG LU LYVHRGB ZH VERWVMG ZNLMT XSROWIVM RM GSV F.H. ULI YVGGVI FMWVIHGZMWRMT, GSV ZIGRXOV YVTZM DRGS GSV WVURMRGRLM LU LYVHRGB, IVERVDVW GSV VCRHGRMT ORGVIZGFIV, SRTSORTSGVW GSV NVGSLWLOLTB FHVW GL XLMWFXG GSV IVHVZIXS, ZMW ZMZOBAVW GSV IVHVZIXS URMWRMTH. OZHGOB, IVXLNNVMWZGRLMH DVIV NZWV DRGS GSV HGFWB VMWRMT RM Z XLMXOFHRLM. LYVHRGB RH Z WRHVZHV XLNNLMOB ZHHLXRZGVW DRGS XSROWIVM RM NLHG XLFMGIRVH RM GSV DLIOW. LYVHRGB NVZMH DVRTSRMT NFXS NLIV GSZM RH SVZOGSB ULI HLNVLMV. HLNV KVLKOV XLMUFHV WRZYVGVH DRGS LYVHRGB. GSVHV GDL HSLFOW MLG YV XLNKZIVW YVXZFHV WRZYVGVH RH GSV KILWFXG LU LYVHRGB (KZCLM 27). LYVHRGB RH Z SVZOGS XLMWRGRLM GSZG RH XZFHVW YB XLMHFNRMT LI VZGRMT GLL NFXS VMVITB ZMW UZGGB ULLWH GSZG XLMGZRM NLIV XZOLIRVH GSZM DSZG Z YLWB XZM FHV. YZHVW LM GSRH, GSV VCGIZ XZOLIRVH ZIV HGLIVW RM GSV YLWB RM ULIN LU UZG ZIV HZRW GL YV GSV UZXGLI GSZG OVZWH GL LEVIDVRTSG ZNLMT KVLKOV RMXOFWRMT XSROWIVM. LYVHRGB, ORPV ZMB LGSVI WRHVZHV, RH GIVZGZYOV GSILFTS VRGSVI KSBHRXZO ZXGRERGRVH LI NVWRXRMZO KROOH. RG SZH YVVM MLGVW GSZG WLXGLIH FHV DSZG RH PMLDM ZH GSV YLWB NZHH RMWVC (YNR) GL WVGVINRMV DSVGSVI HLNVLMVH SVZOGS RH ZG IRHP LI MLG. GSRH IVHVZIXS KZKVI DZH XLMWFXGVW DRGS ZM ZRN LU VCKOLIRMT GSV RMXRWVMXV LU LYVHRGB RM XSROWIVM RM GSV F.H. (KZCLM 45). GSVHRH HGZGVNVMG: LYVHRGB SZH YVVM Z YFIMRMT RHHFV ZNLMT XSROWIVM RM GSV F.H. ULI GSV OZHG ULFI WVXZWVH. DVRTSG NZMZTVNVMG KILTIZNH DVIV GSV LMOB NVGSLW FHVW YB NVWRXZO KIZXGRGRLMVIH GL URTSG ZTZRMHG LYVHRGB ZMW GSRH SZH OVW GL SVZOGSRVI OREVH ZNLMT XSROWIVM ORERMT DRGS LYVHRGB.LYVHRGB RH Z HVIRLFH NVWRXZO XLMWRGRLM GSZG SZH ZUUVXGVW GSV SVZOGS LU NZMB XSROWIVM RM GSV FMRGVW HGZGVH HRMXV GSV 1980H GL WZGV. RMRGRZOOB, KVLKOV GSLFTSG GSZG TZRMRMT DVRTSG RM XSROWIVM DZH Z TLLW RMWRXZGLI LU YVRMT SVZOGSB DRGSLFG XLMXVKGFZORARMT GSV WZMTVIH ZHHLXRZGVW DRGS YVRMT LEVIDVRTSG RM XSROWIVM. HGFWRVH SZEV HSLDM GSZG LYVHRGB RH Z HVIRLFH WRHVZHV GSZG XZM OVZW GL LGSVI SVZOGS KILYOVNH GSZG RMXOFWV ZIGSIRGRH, WRZYVGVH, SVZIG WRHVZHV ZMW SRTS YOLLW KIVHHFIV ZNLMT LYVHV ERXGRNH (KZCLM 61). ZOGSLFTS HGFWRVH SZEV RMWRXZGVW GSZG XSROWIVM ZIV NLIV KILMV GL LYVHRGB GSZM ZWFOGH ZIV, HRNROZI HGFWRVH SZEV HSLDM GSZG VEVIBYLWB RH Z ERXGRN LU LYVHRGB YVXZFHV GSV WRHVZHV RH OZITVOB IVOZGVW GL VZGRMT SZYRGH GSZG ZIV XLNNLM GL VEVIB RMWRERWFZO RM GSV DLIOW. GSILFTS MFNVILFH HGFWRVH, RG RH VERWVMG GSZG LYVHRGB RM GSV F.H. RH SRTSOB KILMLFMXVW XLNKZIVW GL LGSVI MZGRLMH RM GSV DLIOW (SVWOVB VG ZO 2500). RM XLMQFMXGRLM DRGS GSRH, NZMB LYVHV ERXGRNH ZIV XSROWIVM ZH LKKLHVW GL ZWFOGH NZRMOB YVXZFHV LU GSV XSZMTVH RM ORUVHGBOVH DSVIVYB GVXSMLOLTRXZO ZWEZMXVNVMG SZH OVW GL GSV RMGILWFXGRLM LU NLIV OFCFIRLFH ZXGRERGRVH. ULI RMHGZMXV, XSROWIVM YVGDVVM GSV ZTV LU 5 ZMW 12 BVZIH ZIV KILMV GL LYVHRGB YVXZFHV GSVB HKVMW NFXS LU GSVRI GRNV DZGXSRMT GVOVERHRLM ZG GSV VCKVMHV LU KSBHRXZO ZXGRERGRVH. MFNVILFH HGFWRVH IVEVZOVW GSZG YVRMT Z UVD KLFMWH LEVIDVRTSG RH MLG ZM RNKORXZGRLM LU LYVHRGB YFG Z KVIHLM RH XLMHRWVIVW LYVHV DSVM SV LI HSV SZH Z YLWB NZHH RMWVC GSZG RH SRTSVI GSZM 30. LM GSV LGSVI SZMW, NZMB ZWFOGH YVXLNV LEVIDVRTSG DSROV FHRMT NVWRXRMV GL KFG LM DVRTSG HFXS ZH GSV FHV LU XLIGRXLHGVILRWH ZMW ZMGRWVKIVHHZMGH ZNLMT LGSVIH (DZGVIH HVRWVOO ZMW HDRMYFIM 52). IVXVMG HGFWRVH SZEV HSLDM GSZG RM NLWVIM HLXRVGB, GSVIV ZIV MFNVILFH RMXRWVMXVH LU LYVHRGB ZH LKKLHVW GL GSV KZHG YVXZFHV KVLKOV OZXP KSBHRXZO ZXGRERGRVH GSZG DVIV KIZXGRXVW YB VZIOB NVM ZMW UZGGB ZMW HFTZIB ULLWH SZEV YVXLNV NLIV ZEZROZYOV GSZM GSVB DVIV RM GSV GIZWRGRLMZO HLXRVGB. VZGRMT ULLWH DRGS OVHHVI VMVITB ZMW RMWFOTRMT RM KSBHRXZO KIZXGRXVH ZIV GSV LMOB ERZYOV NVZMH ULI URTSGRMT LYVHRGB (TLIGNZPVI ZMW WRVGA 47). GSV IVHVZIXSVI VNYZIPVW LM GSV FHV LU Z HFIEVB ZH ZM ZKKILKIRZGV NVGSLW RM IVHVZIXSRMT LYVHV XSROWIVM RM GSV FMRGVW HGZGVH. GSV HFIEVB XLOOVXGVW WZGZ FHRMT Z JFVHGRLMMZRIV DRGS JFVHGRLMH IVOZGVW GL LYVHRGB ZMW DVRTSG NZMZTVNVMG ZNLMT GSV XSROWIVM YVRMT ZHPVW. Z HZNKOV LU 50 XSROWIVM DZH IZMWLNOB HVOVXGVW DRGS GDL WLXGLIH FHRMT GSV YLWB NZHH RMWVC GL WVGVINRMV GSV SVZOGS LU GSV HZNKOVW XSROWIVM DSLHV ZTV IZMTVW YVGDVVM 5 ZMW 15 BVZIH (UIVVWNZM VG ZO 1759). UILN GSV HFIEVB, RG DZH VERWVMG GSZG 35 XSROWIVM LFG LU 50 DVRTSVW NFXS NLIV GSZM GSVRI SVZOGS, DSRXS DZH ZM RMWRXZGLI GSZG GSVB DVIV LYVHV. ULI GSRH HFIEVB, RG DZH XLMXOFWVW GSZG NLHG XSROWIVM ZTVW YVGDVVM 5 BVZIH ZMW 12 BVZIH ZIV ZUUVXGVW YB LYVHRGB VZIOB RM GSVRI OREVH. HFXS XSROWIVM HKVMW NFXS LU GSVRI GRNV DZGXSRMT GVOVERHRLM KILTIZNH IZGSVI GSZM KOZBRMT LM GSV KOZBTILFMW. GSVB ZOHL UVVW LM GLL UZGGB ZMW HFTZIB ULLWH HLNVGSRMT GSZG NZWV GSVN YV NLIV KIVEZOVMG RM LYVHRGB (SVWOVB VG ZO 2500). GSV IVHVZIXS ZXXVKGVW GSV MFOO SBKLGSVHRH GSZG LYVHRGB RH NLIV KILMLFMXVW ZNLMT XSROWIVM ZTVW YVGDVVM 5-12 BVZIH YVXZFHV LU OZXP LU KSBHRXZO VCVIXRHV ZMW XLMHFNKGRLM LU GLL UZGGB ZMW HFTZIB ULLWH. GSV XZGVTLIB LU XSROWIVM KILMV GL LYVHRGB RH GSV ZTV TILFK LU XSROWIVM ZTVW YVGDVVM 5 ZMW 12 BVZIH. GSV RNKORXZGRLM RH GSZG GSVB HKVMG NFXS LU GSVRI GRNV DZGXSRMT GVOVERHRLM IZGSVI GSZM KOZBRMT LM GSV KOZBTILFMW. GSVB ZOHL SZEV ORGGOV GSRMPRMT XZKZYRORGB GSV UZXG RH XZFHVW YB FMFHVW VMVITB RM GSV YLWB DRGS GSV VMVITB YVRMT HGLIVW ZH UZG GSZG ZNLFMGH GL LYVHRGB. RU 35 XSROWIVM LFG LU 50 ZIV LYVHV, RG NVZMG GSZG RM VEVIB 1000 XSROWIVM RM GSV FMRGVW HGZGVH 700 XSROWIVM HFUUVI UILN LYVHRGB. GSV XZGVTLIB LU XSROWIVM KILMV GL LYVHRGB RH GSV ZTV TILFK LU XSROWIVM ZTVW YVGDVVM 5 ZMW 12 BVZIH. GSV RNKORXZGRLM RH GSZG GSVB HKVMG NFXS LU GSVRI GRNV DZGXSRMT GVOVERHRLM IZGSVI GSZM KOZBRMT LM GSV KOZBTILFMW. GSVB ZOHL SZEV ORGGOV GSRMPRMT XZKZYRORGB GSV UZXG RH XZFHVW YB FMFHVW VMVITB RM GSV YLWB DRGS GSV VMVITB YVRMT HGLIVW ZH UZG GSZG ZNLFMGH GL LYVHRGB. RU 35 XSROWIVM LFG LU 50 ZIV LYVHV, RG NVZMG GSZG RM VEVIB 1000 XSROWIVM RM GSV FMRGVW HGZGVH 700 XSROWIVM HFUUVI UILN LYVHRGB. GSV HGFWB RH RMGVIVHGRMT RM GSZG RG SRTSORTSGH GSV XLMXVKG LU LYVHRGB ZH ZKKORVW GL XSROWIVM RM GSV FMRGVW HGZGVH. DZGXSRMT GVOVERHRLM ZMW XLMHFNKGRLM LU UZGGB ZMW HFTZIB ULLWH ZIV GSV NZRM XZFHVH LU LYVHRGB ZNLMT XSROWIVM NVZMRMT GSZG RU XSROWIVM XLFOW YV VMXLFIZTVW GL KZIGRXRKZGV RM KSBHRXZO ZXGRERGRVH, LYVHRGB XZM VZHROB YV IVWFXVW TIZWFZOOB ZMW VORNRMZGVW RM GSV VMW. KZIVMGH HSLFOW FITV XSROWIVM GL KOZB NLIV GSZM DZGXS GSV GVOVERHRLM YVXZFHV GSRH DLFOW VMZYOV GSVN GL NZMZTV GSVRI DVRTSG. RM ZWWRGRLM GL RNKILERMT GSVRI SVZOGS, KSBHRXZO ZXGRERGRVH SZEV YVVM PMLDM GL YV KLHRGREVOB ZHHLXRZGVW DRGS RNKILEVW ZXZWVNRX KVIULINZMXV. ZG GSV MZGRLMZO OVEVO, GSV TLEVIMNVMG HSLFOW RMGILWFXV KSBHRXZO VCVIXRHV KILTIZNH RM HXSLLOH SVMXV NZPRMT RG NZMWZGLIB ULI ZOO HXSLLOH GL SZEV KOZBTILFMWH ULI XSROWIVM. GSVIVULIV, KZIGRXRKZGRLM RM KSBHRXZO ZXGRERGRVH YB ZNVIRXZM XSROWIVM DLFOW HORTSGOB IVWFXV GSV SVZOGS YFWTVG ZG GSV MZGRLMZO OVEVO.

Nội dung file decryptedtext sau khi dùng phân tích tần số để phá mã:

the stmdu ekycires the linleyt ip igesatu os evadent ofinw lhacdren an the m.s. pir getter mnderstondanw, the ortalce gewon bath the depanatain ip igesatu, revaebed the ekastanw caterotmre, hawhcawhted the fethidiciwu msed ti lindmlt the reseorlh, ond onocuxed the reseorlh pandanws. costcu, reliffendotains bere fode bath the stmdu endanw an o linlcmsain. igesatu as o daseose liffincu ossilaoted bath lhacdren an fist limntraes an the bircd. igesatu feons beawhanw fmlh fire thon as heocthu pir sifeine. sife yeiyce linpmse daogetes bath igesatu. these tbi shimcd nit ge lifyored gelomse daogetes as the yridmlt ip igesatu (yokin 27). igesatu as o heocth lindatain thot as lomsed gu linsmfanw ir eotanw tii fmlh enerwu ond pottu piids thot lintoan fire lociraes thon bhot o gidu lon mse. gosed in thas, the ektro lociraes ore stired an the gidu an pirf ip pot ore soad ti ge the poltir thot ceods ti iverbeawht ofinw yeiyce anlcmdanw lhacdren. igesatu, caje onu ither daseose, as treotogce thrimwh eather yhusaloc oltavataes ir fedalanoc yaccs. at hos geen nited thot diltirs mse bhot as jnibn os the gidu foss andek (gfa) ti deterfane bhether sifeines heocth as ot rasj ir nit. thas reseorlh yoyer bos lindmlted bath on oaf ip ekyciranw the anladenle ip igesatu an lhacdren an the m.s. (yokin 45). thesas stotefent: igesatu hos geen o gmrnanw assme ofinw lhacdren an the m.s. pir the cost pimr delodes. beawht fonowefent yriwrofs bere the incu fethid msed gu fedaloc yroltatainers ti pawht owoanst igesatu ond thas hos ced ti heocthaer caves ofinw lhacdren cavanw bath igesatu.igesatu as o seraims fedaloc lindatain thot hos oppelted the heocth ip fonu lhacdren an the mnated stotes sanle the 1980s ti dote. anataoccu, yeiyce thimwht thot woananw beawht an lhacdren bos o wiid andalotir ip geanw heocthu bathimt linleytmocaxanw the donwers ossilaoted bath geanw iverbeawht an lhacdren. stmdaes hove shibn thot igesatu as o seraims daseose thot lon ceod ti ither heocth yrigcefs thot anlcmde orthratas, daogetes, heort daseose ond hawh gciid yressmre ofinw igese valtafs (yokin 61). octhimwh stmdaes hove andaloted thot lhacdren ore fire yrine ti igesatu thon odmcts ore, safacor stmdaes hove shibn thot everugidu as o valtaf ip igesatu gelomse the daseose as corwecu recoted ti eotanw hogats thot ore liffin ti everu andavadmoc an the bircd. thrimwh nmferims stmdaes, at as evadent thot igesatu an the m.s. as hawhcu yrinimnled lifyored ti ither notains an the bircd (hedceu et oc 2500). an linzmnltain bath thas, fonu igese valtafs ore lhacdren os iyyised ti odmcts foancu gelomse ip the lhonwes an capestuces bheregu telhniciwaloc odvonlefent hos ced ti the antridmltain ip fire cmkmraims oltavataes. pir anstonle, lhacdren getbeen the owe ip 5 ond 12 ueors ore yrine ti igesatu gelomse theu syend fmlh ip thear tafe botlhanw tecevasain ot the ekyense ip yhusaloc oltavataes. nmferims stmdaes reveoced thot geanw o peb yimnds iverbeawht as nit on afycalotain ip igesatu gmt o yersin as linsadered igese bhen he ir she hos o gidu foss andek thot as hawher thon 30. in the ither hond, fonu odmcts gelife iverbeawht bhace msanw fedalane ti ymt in beawht smlh os the mse ip lirtalisteriads ond ontadeyressonts ofinw ithers (boters seadecc ond sbangmrn 52). relent stmdaes hove shibn thot an fidern silaetu, there ore nmferims anladenles ip igesatu os iyyised ti the yost gelomse yeiyce colj yhusaloc oltavataes thot bere yroltaled gu eorcu fen ond pottu ond smworu piids hove gelife fire ovoacogce thon theu bere an the trodatainoc silaetu. eotanw piids bath cesser enerwu ond andmcwanw an yhusaloc yroltales ore the incu vaogce feons pir pawhtanw igesatu (wirtfojer ond daetx 47). the reseorlher efgorjed in the mse ip o smrveu os on oyyriyraote fethid an reseorlhanw igese lhacdren an the mnated stotes. the smrveu liccelted doto msanw o qmestainnoare bath qmestains recoted ti igesatu ond beawht fonowefent ofinw the lhacdren geanw osjed. o sofyce ip 50 lhacdren bos rondifcu secelted bath tbi diltirs msanw the gidu foss andek ti deterfane the heocth ip the sofyced lhacdren bhise owe ronwed getbeen 5 ond 15 ueors (preedfon et oc 1759). prif the smrveu, at bos evadent thot 35 lhacdren imt ip 50 beawhed fmlh fire thon thear heocth, bhalh bos on andalotir thot theu bere igese. pir thas smrveu, at bos linlcmded thot fist lhacdren owed getbeen 5 ueors ond 12 ueors ore oppelted gu igesatu eorcu an thear caves. smlh lhacdren syend fmlh ip thear tafe botlhanw tecevasain yriwrofs rother thon ycouanw in the ycouwrimnd. theu ocsi peed in tii pottu ond smworu piids sifethanw thot fode thef ge fire yrevocent an igesatu (hedceu et oc 2500). the reseorlh olleyted the nmcc huyithesas thot igesatu as fire yrinimnled ofinw lhacdren owed getbeen 5-12 ueors gelomse ip colj ip yhusaloc ekerlase ond linsmfytain ip tii pottu ond smworu piids. the lotewiru ip lhacdren yrine ti igesatu as the owe wrimy ip lhacdren owed getbeen 5 ond 12 ueors. the afycalotain as thot theu syent fmlh ip thear tafe botlhanw tecevasain rother thon ycouanw in the ycouwrimnd. theu ocsi hove cattce thanjanw loyogacatu the polt as lomsed gu mnmsed enerwu an the gidu bath the enerwu geanw stired os pot thot ofimnts ti igesatu. ap 35 lhacdren imt ip 50 ore igese, at feont thot an everu 1000 lhacdren an the mnated stotes 700 lhacdren smpper prif igesatu. the lotewiru ip lhacdren yrine ti igesatu as the owe wrimy ip lhacdren owed getbeen 5 ond 12 ueors. the afycalotain as thot theu syent fmlh ip thear tafe botlhanw tecevasain rother thon ycouanw in the ycouwrimnd. theu ocsi hove cattce thanjanw loyogacatu the polt as lomsed gu mnmsed enerwu an the gidu bath the enerwu geanw stired os pot thot ofimnts ti igesatu. ap 35 lhacdren imt ip 50 ore igese, at feont thot an everu 1000 lhacdren an the mnated stotes 700 lhacdren smpper prif igesatu. the stmdu as anterestanw an thot at hawhcawhts the linleyt ip igesatu os oyycaed ti lhacdren an the mnated stotes. botlhanw tecevasain ond linsmfytain ip pottu ond smworu piids ore the foan lomses ip igesatu ofinw lhacdren feonanw thot ap lhacdren limcd ge enlimrowed ti yortalayote an yhusaloc oltavataes, igesatu lon eosacu ge redmled wrodmoccu ond ecafanoted an the end. yorents shimcd mrwe lhacdren ti ycou fire thon botlh the tecevasain gelomse thas bimcd enogce thef ti fonowe thear beawht. an oddatain ti afyrivanw thear heocth, yhusaloc oltavataes hove geen jnibn ti ge yisatavecu ossilaoted bath afyrived olodefal yerpirfonle. ot the notainoc cevec, the wivernfent shimcd antridmle yhusaloc ekerlase yriwrofs an slhiics henle fojanw at fondotiru pir occ slhiics ti hove ycouwrimnds pir lhacdren. therepire, yortalayotain an yhusaloc oltavataes gu oferalon lhacdren bimcd scawhtcu redmle the heocth gmdwet ot the notainoc cevec.



Hình 4.12 Minh họa sử dụng thuật toán affine để mã hóa chuỗi 1000 từ

**TÀI LIỆU THAM KHẢO**

**Tiếng Anh**

**Encryption:** [**https://en.wikipedia.org/wiki/Encryption**](https://en.wikipedia.org/wiki/Encryption)

**Decryption:** [**https://www.techopedia.com/definition/1773/decryption**](https://www.techopedia.com/definition/1773/decryption)

**Asymetric & symetric key:** [**https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/**](https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/)

**Monoalphabetic Substitution Cipher:** [**https://www.101computing.net/mono-alphabetic-substitution-cipher/**](https://www.101computing.net/mono-alphabetic-substitution-cipher/)

[**https://en.wikipedia.org/wiki/Substitution\_cipher**](https://en.wikipedia.org/wiki/Substitution_cipher)

[**https://www.geeksforgeeks.org/difference-between-monoalphabetic-cipher-and-polyalphabetic-cipher/**](https://www.geeksforgeeks.org/difference-between-monoalphabetic-cipher-and-polyalphabetic-cipher/)

**Thông tin về các loại mã được đề cập đến trong báo cáo:** [**https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html#google\_vignette**](https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html#google_vignette)

**Frequency Analysis:** [**https://en.wikipedia.org/wiki/Frequency\_analysis**](https://en.wikipedia.org/wiki/Frequency_analysis)

[**https://www.101computing.net/frequency-analysis/**](https://www.101computing.net/frequency-analysis/)

[**https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html**](https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html)