UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**Báo cáo**

Môn: Mật mã học

Cuối kì I (2023 – 2024)

**ENCRYPTION AUDIO DATA ON MULTIMEDIA**

**PRODUCT SERVICE PLATFORM**

Student: Mai Nguyễn Nam Phương

Student ID Number: 22521164

Student: Nguyễn Nhật Quang

Student ID Number: 22521203  
Student: Cao Quốc Thịnh

Student ID Number: 18521436

Class: NT219.O21

University of Information Technology

Lecturer: PhD. Nguyễn Ngọc Tự

**Lời cảm ơn**

Lời đầu tiên, cho phép tập thể Nhóm 22 đến từ lớp NT219.O21 xin gửi lời cảm ơn và tri ân sâu sắc đến thầy Nguyễn Ngọc Tự - giảng viên môn Mật Mã Học, vì sự tận tâm giúp đỡ, chỉ bảo và hướng dẫn trong quá trình thực hiện dự án. Những buổi thảo luận và sự hướng dẫn của thầy đóng vai trò quan trọng trong việc hoàn thiện đề tài này. Chúng em chân thành cảm ơn thầy vì kiến thức và kinh nghiệm mà thầy đã chia sẻ với chúng em.

Chúng em cũng muốn gửi lời cảm ơn đến tất cả các thành viên trong nhóm đồ án. Sự đóng góp và nỗ lực của mỗi người trong việc tìm kiếm tài liệu, đưa ra ý tưởng và hoàn thiện đề tài đã tạo nên thành công của cuộc . Mặc dù kiến thức của chúng em còn hạn chế và không tránh khỏi những sai sót, nhưng sự đóng góp ý kiến của mọi người đã giúp chúng em hoàn thiện và cải thiện đề tài một cách tốt nhất.

Cuối cùng, vì thời gian và năng lực có hạn nên không thể tránh khỏi sai sót trong khi thực hiện đồ án học tập của chúng em. Rất mong sự góp ý và bổ sung của thầy và các bạn để đề tài chúng em trở nên hoàn thiện hơn. Một lần nữa, chân thành cảm ơn tất cả mọi người đã tham gia và ủng hộ cuộc dự án này.

Contents

[I. Tổng quan đề tài: 4](#_Toc155562174)

[1. Chủ đề: 4](#_Toc155562175)

[2. Ngữ cảnh vấn đề: 4](#_Toc155562176)

[2.1. Lí do chọn đề tài: 4](#_Toc155562177)

[2.2. Mục tiêu: 4](#_Toc155562178)

[3. Vai trò của các bên liên quan: 5](#_Toc155562179)

[4. Giải pháp: 5](#_Toc155562180)

[II. Bối cảnh: 5](#_Toc155562181)

[1. Double DNA encoding: 5](#_Toc155562182)

[2. Chaotic map: 6](#_Toc155562183)

[III. Hướng giải quyết và code: 7](#_Toc155562184)

[1. Solution Architecture: 7](#_Toc155562185)

[2. Encryption: 8](#_Toc155562186)

[3. Decryption: 13](#_Toc155562187)

[IV. Thực nghiệm và kết quả: 18](#_Toc155562188)

[V. Tổng kết và công việc tương lai: 18](#_Toc155562189)

[1. Tổng kết: 18](#_Toc155562190)

[2. Công việc tương lai: 18](#_Toc155562191)

# I. Tổng quan đề tài:

## 1. Chủ đề:

- Project topic: Mã hóa âm thanh

- Project title: Mã hóa dữ liệu âm thanh trên nền tảng dịch vụ sản phẩm đa phương tiện

## 2. Ngữ cảnh vấn đề:

- Lượng dữ liệu âm thanh đang ngày càng tăng lớn, bao gồm các nội dung như phim ảnh, video, podcast, âm nhạc trực tuyến... Điều quan trọng là cần có các giải pháp mã hóa hiệu quả để lưu trữ, truyền tải và bảo mật dữ liệu âm thanh.

- Nhiều dịch vụ số ngày nay cung cấp nội dung đa phương tiện kết hợp video, hình ảnh và âm thanh. Việc xử lý và mã hóa dữ liệu âm thanh trên các nền tảng này là rất cần thiết.

- Nghiên cứu về mã hóa dữ liệu âm thanh giúp cải thiện chất lượng trải nghiệm nghe nhạc, xem phim của người dùng trên các thiết bị di động và internet.

### 2.1. Lí do chọn đề tài:

- Âm thanh là một phần quan trọng của dịch vụ sản phẩm đa phương tiện. Việc mã hóa dữ liệu âm thanh đảm bảo rằng người dùng có thể truy cập và tận hưởng âm thanh một cách chất lượng và liền mạch trên nền tảng này.

- Mã hóa dữ liệu âm thanh có thể cung cấp cơ chế bảo mật để đảm bảo rằng dữ liệu âm thanh không bị truy cập trái phép hoặc biến đổi trong quá trình truyền tải.

### 2.2. Mục tiêu:

- Từ những điều đó, ta cần phải xây dựng một hệ thống mã hoá và giải mã để có thể bảo đảm về tính bảo mật, tính toàn vẹn và tính khả dụng của âm thanh khi được phát trực tuyến

### 3. Vai trò của các bên liên quan:

- Nhà cung cấp dịch vụ (Service Provider): Thực hiện các biện pháp bảo mật, cung cấp cơ chế mã hóa và đảm bảo tính khả dụng và chất lượng âm thanh cho người dùng.

- Tác giả (Author): Đăng tải các bản nhạc, file âm thanh.

- Người dùng (User): Những người đăng kí/ đăng nhập, mua bản quyền và sử dụng dịch vụ để có thể nghe các nội dung được phát.

- Hạ tầng (Infrastructure): Cung cấp nền tích cho dịch vụ lưu trữ, truyền tải dữ liệu mã hóa âm thanh an toàn, ổn định.

- Kẻ tấn công (Attacker): Cố gắng xâm phạm hệ thống để truy cập trái phép vào nội dung bản quyền.

## 4. Giải pháp:

- Xây dựng nền tảng cung cấp dịch vụ nghe nhạc trực tuyến cho người dùng

- Mã hoá dữ liệu và lưu trữ

- Giải mã và cung cấp cho nền tảng giúp cung cấp đến người dùng

# II. Bối cảnh:

## 1. Double DNA encoding:

- Double DNA encoding là quá trình mã hóa đôi sử dụng phép cộng DNA.

- Trong quá trình này, dữ liệu nhị phân được chuyển đổi thành dạng mã DNA theo một quy tắc nhất định, thông thường là chuyển mã 02 bit thành một trong 4 nucleic acid A, C, G, T.

- Sau khi chuyển đổi sang dạng mã DNA, phép cộng DNA được áp dụng giữa chuỗi DNA của dữ liệu và hai chuỗi mã DNA khác.

- Phép cộng DNA tuân theo bảng phép cộng DNA, trong đó quy định kết quả của phép cộng giữa các cặp nucleic acid.

- Kết quả sau cùng của double DNA encoding là một chuỗi DNA thu được sau phép cộng DNA thứ hai.

- Chuỗi kết quả này sau đó được chuyển đổi trở lại dạng nhị phân để áp dụng các bước tiếp theo trong thuật toán mã hóa.

## 2. Chaotic map:

- Chaotic map là bản đồ hỗn loạn, được sử dụng để tạo ra các chuỗi ngẫu nhiên nhưng mang tính hỗn loạn cao.

- Chaotic map cung cấp tính phi tuyến và nhạy cảm với điều kiện ban đầu. Chúng thường được sử dụng trong các thuật toán mã hóa để tạo ra sự lẫn lộn và lan truyền.

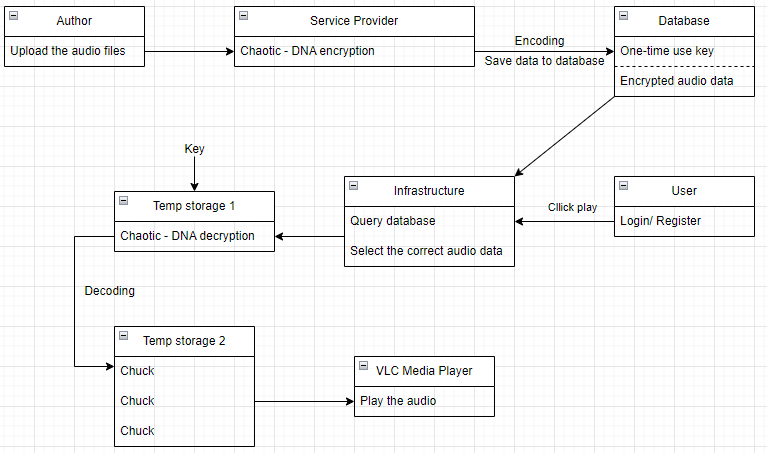
- Các chaotic map phổ biến bao gồm Logistic map, Sine map, Tent map. Tuy nhiên chúng có một số nhược điểm như khoảng hỗn loạn nhỏ, cửa sổ ổn định.

- Sử dụng hai loại chaotic map là Sine-Cosine map (SC map) và Logistic Sine Cosine map (LSC map). Đây là hai bản đồ một chiều kết hợp, có khoảng hỗn loạn lớn và khắc phục các nhược điểm của các bản đồ truyền thống.

- Chaotic map được sử dụng trong thuật toán để tạo ra các chuỗi ngẫu nhiên phục vụ các bước pha truy xuất, lan truyền dữ liệu.

# III. Hướng giải quyết và code:

## 1. Solution Architecture:



- Tác giả tải file bài nhạc lên hệ thống.

- Hệ thống sẽ mã hóa file âm thanh đó, đồng thời lúc này xuất ra hai file “One-time use key” và file âm thanh đã được mã hóa được lưu vào database.

- Khi người dùng muốn nghe nhạc phải đăng nhập vào trang web với thông tin cá nhân đã được đăng kí.

- Người dùng nhấn chọn bài hát muốn nghe.

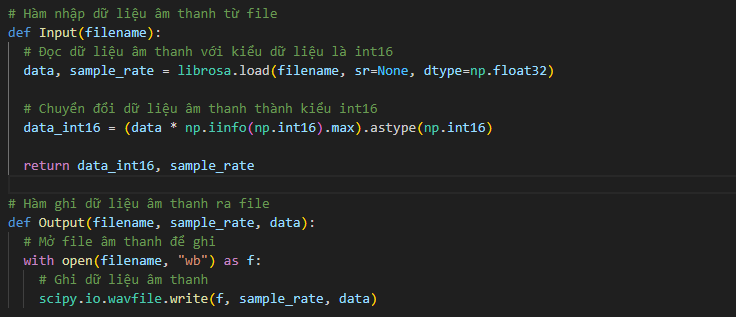
- Hệ thống sẽ truy vấn và chọn dữ liệu bài hát đã được mã hóa đúng với yêu cầu của người dùng từ cơ sở dữ liệu, đưa ra bộ nhớ tạm 1.

- File bài hát này sẽ kết hợp với “One-time use key” để được giải mã theo từng chuck âm thanh và đưa vào bộ nhớ tạm 2.

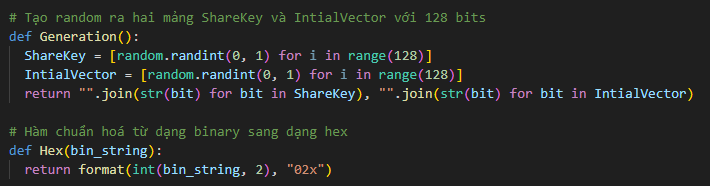
- Giao diện VLC media player sẽ được hiển thị làm giao diện chính để phát nhạc cho người dùng theo từng chuck âm thanh được tải lên.

## 2. Encryption:

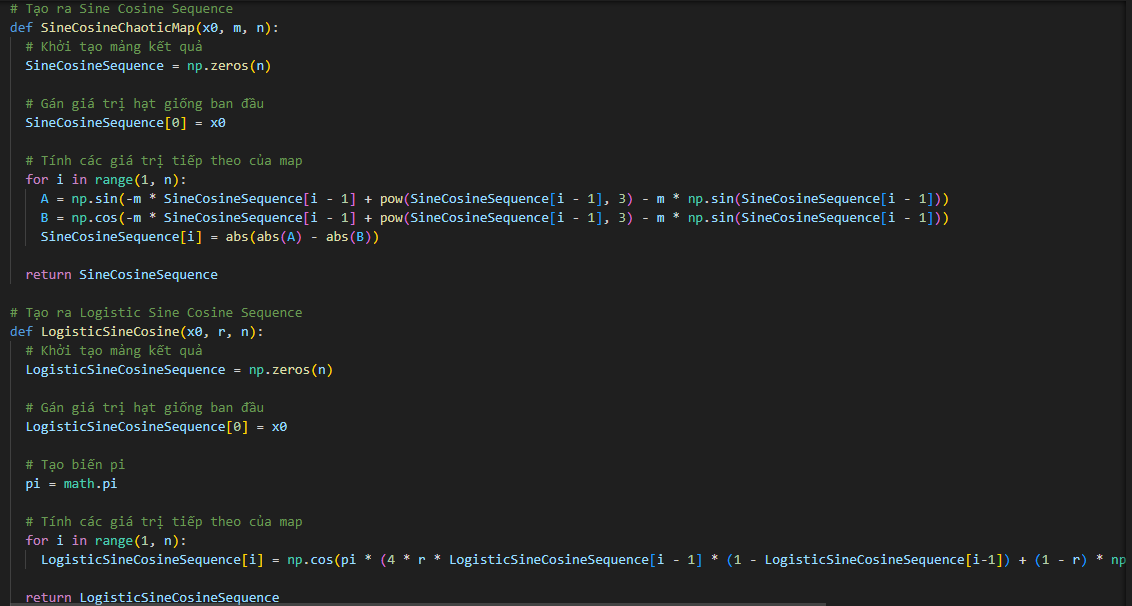
**- Nhập và ghi dữ liệu âm thanh:**



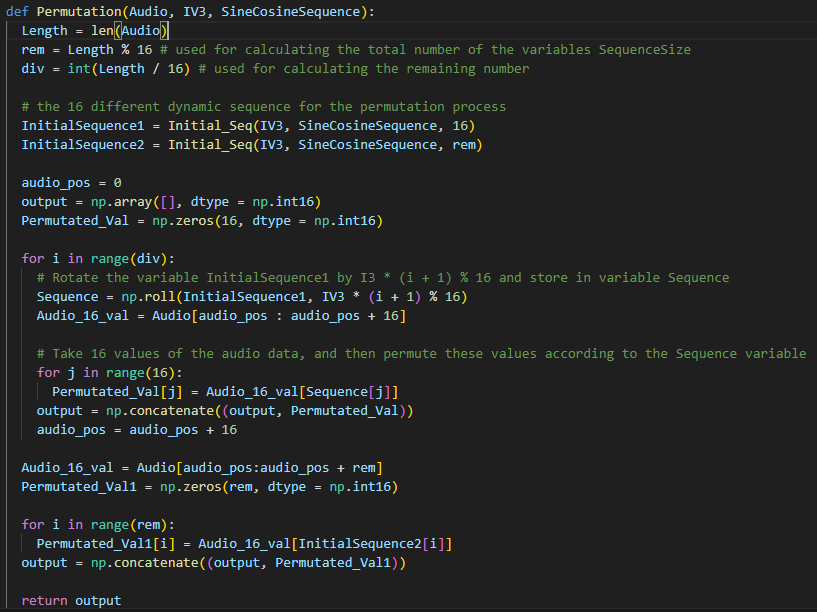
**- Khởi tạo khóa và Vector:**



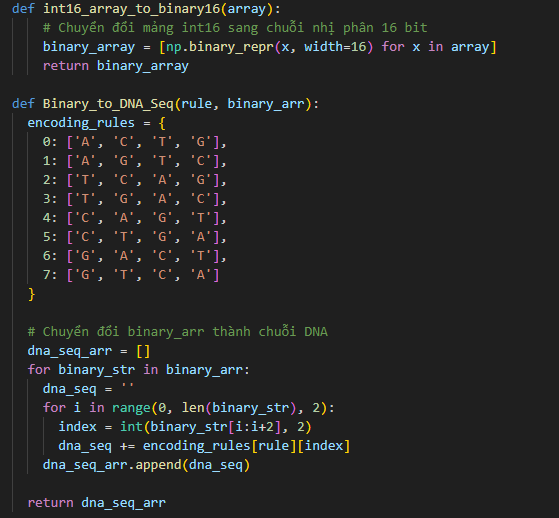
**- Tạo ra chuỗi ngẫu nhiên bằng chaotic map:**

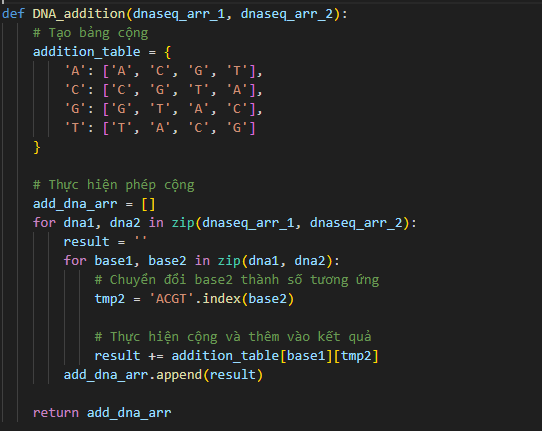


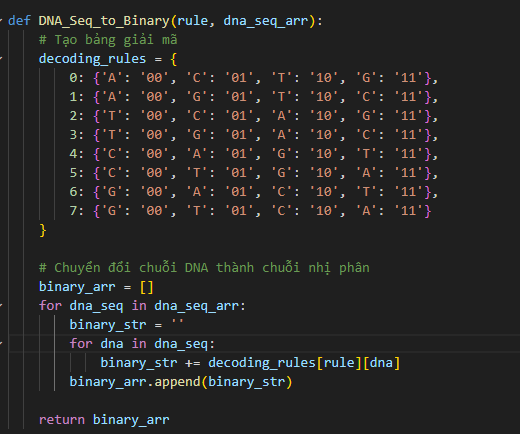
**- Permutation:**

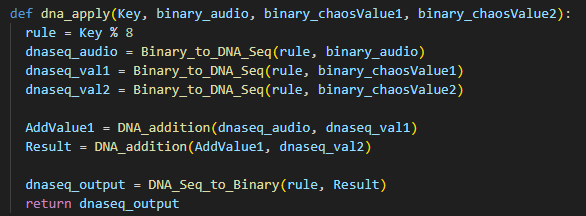


**- Diffusion:**

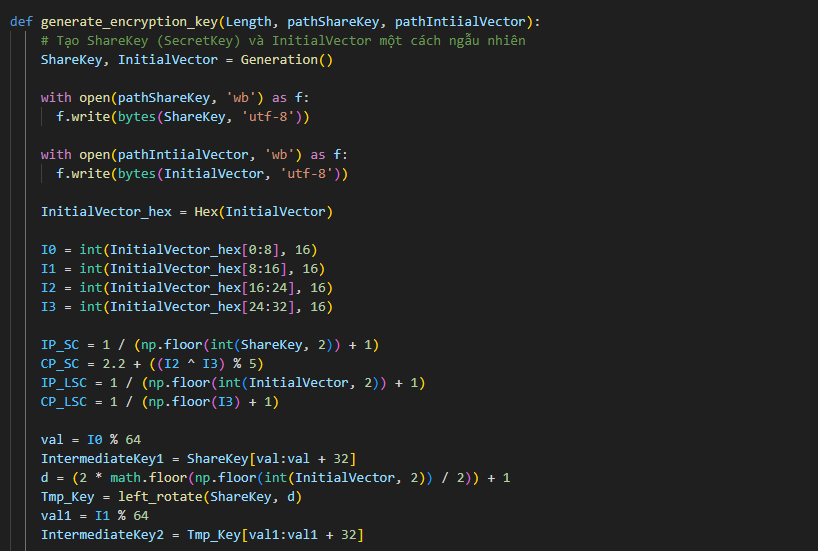








**- Tạo SecretKey và InitialVector:**

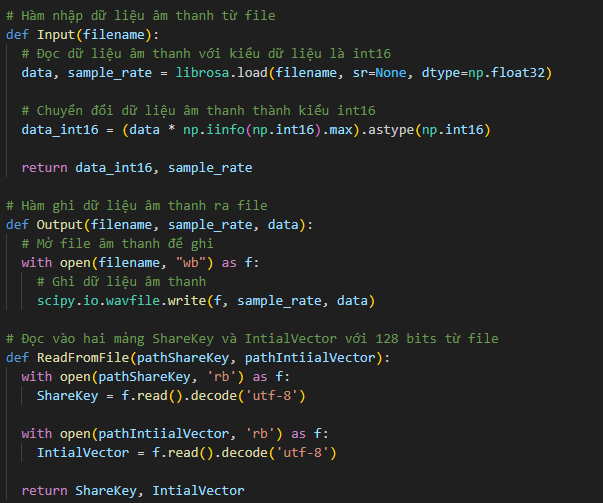
****

**- Encryption:**

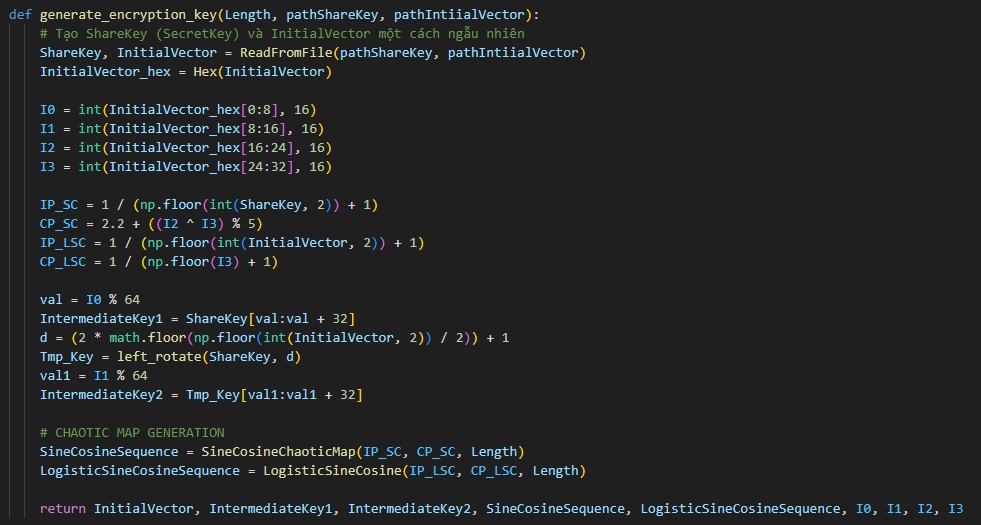
****

## 3. Decryption:

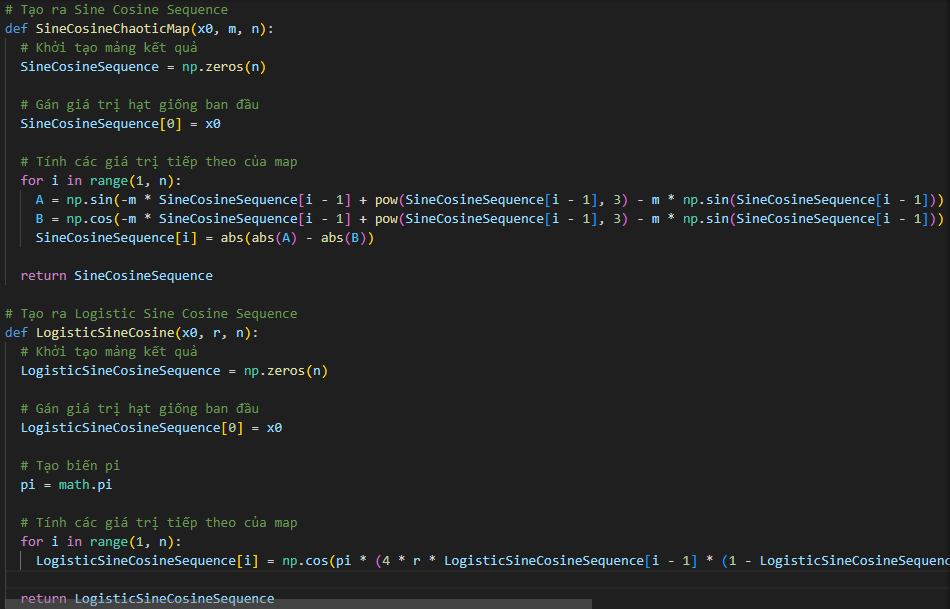
**- Đọc dữ liệu đầu vào:**

****

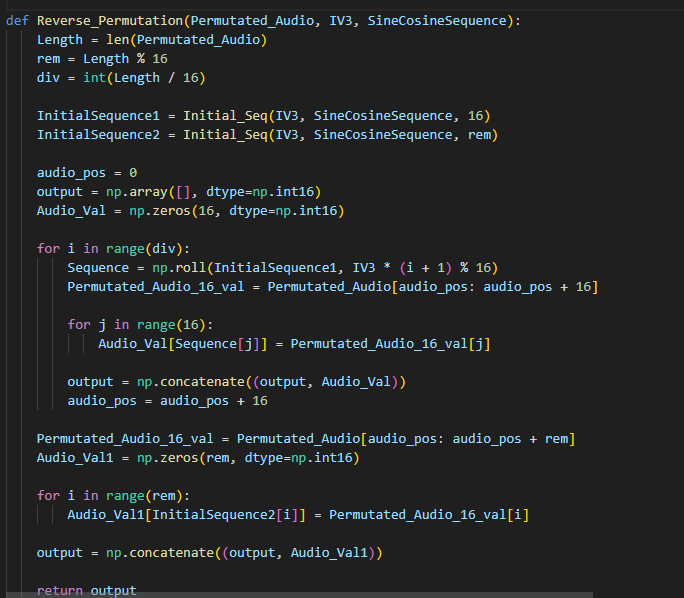
**- Thuật toán khởi tạo:**

****

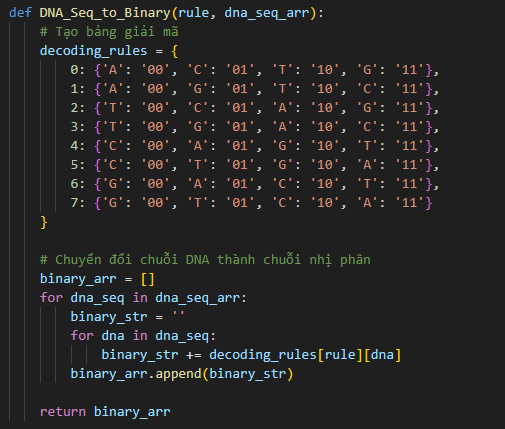
**- Tạo ra chuỗi ngẫu nhiên bằng Chaotis map:**

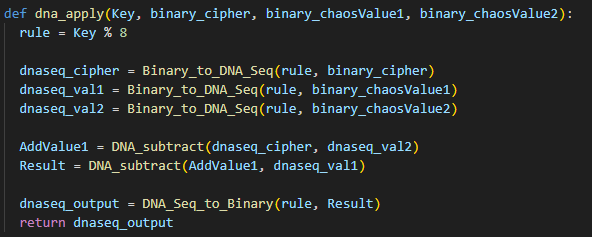
****

**- Reverse\_Permutation:**

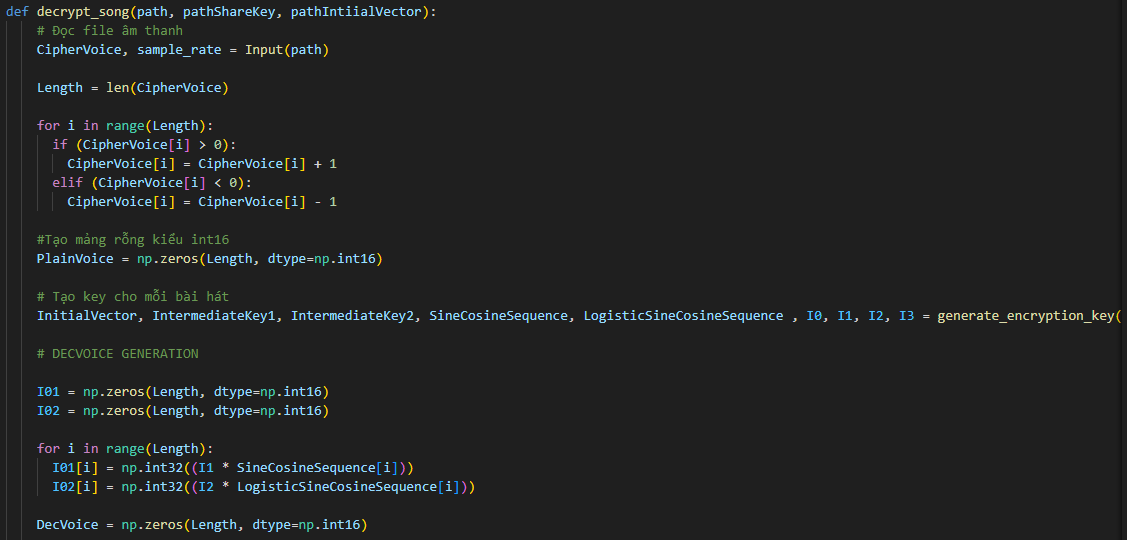
****

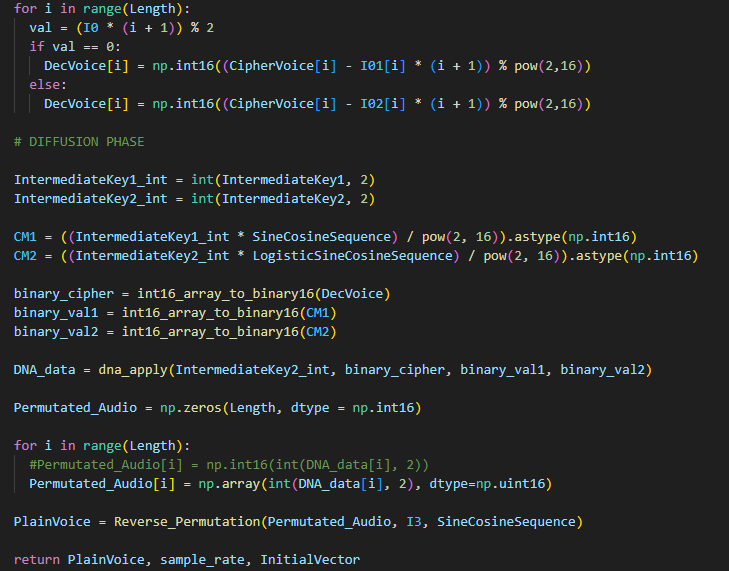
**- Diffusion:**

****

****

**- Decryption:**

****

****

# IV. Thực nghiệm và kết quả:

- Video demo trong file zip

# V. Tổng kết và công việc tương lai:

## 1. Tổng kết:

- Tạo ra nền tảng đơn giản cung cấp dịch vụ nghe nhạc cho người dùng

- Mã hóa và giải mã thành công, thu về biểu đồ như mong đợi

- Đảm bảo dữ liệu được đưa đến người dùng như mong muốn, không thể bị đánh cắp bởi attacker

- Toàn bộ dữ liệu trước khi được đưa vào lưu trữ đều được mã hoá

## 2. Công việc tương lai:

- Nghiên cứu và ứng dụng các thuật toán mã hóa mới như mã hóa không mất dữ liệu, mã hóa trích xuất đặc trưng và nhận diện giọng nói để nâng cao chất lượng và độ an toàn.

- Phát triển các giải pháp mã hóa dữ liệu âm thanh phù hợp với các định dạng file khác nhau như mp3, wav, m4a.

- Tích hợp mã hóa âm thanh vào các nền tảng phổ biến như YouTube, Spotify, SoundCloud để tối ưu hóa trải nghiệm người dùng.

- Nghiên cứu các giải pháp mã hóa âm thanh trực tuyến và trên thiết bị di động nhằm bảo vệ quyền riêng tư và bản quyền.

- Xây dự hệ thống mang tính trực tuyến

- Cung cấp thêm các dịch vụ cần thiết cho các bên liên quan

- Nâng cấp thuật toán để tối ưu thời gian thực thi