# Báo Cáo: Chương Trình Mã Hóa - Giải Mã File Dữ Liệu Sử Dụng Thuật Toán AES

## 1. Giới Thiệu

Mục tiêu của chương trình là cung cấp công cụ mã hóa và giải mã file dữ liệu một cách an toàn và tiện dụng trên nền web, đồng thời có hỗ trợ phiên bản Python để sử dụng offline. Thuật toán được lựa chọn là AES (Advanced Encryption Standard) với chế độ AES-CBC, đảm bảo bảo mật và hiệu năng cao.

## 2. Phân Tích Ý Tưởng

- \*\*Thuật Toán AES:\*\* Thuật toán mã hóa đối xứng, sử dụng cùng một khóa cho cả mã hóa và giải mã.

- \*\*Khóa động, độ dài tự do:\*\* Người dùng nhập khóa với độ dài tùy ý. Khóa này được xử lý bằng hàm băm SHA-256 để cho ra khóa AES chuẩn 256-bit cố định.

- \*\*Vector Khởi Tạo (IV):\*\* Mỗi lần mã hóa, IV ngẫu nhiên 16 bytes được tạo để đảm bảo an toàn và bảo mật cho mỗi phiên mã hóa. IV được lưu lại ở đầu file mã hóa để dùng cho việc giải mã.

- \*\*File dữ liệu:\*\* Được đọc dưới dạng nhị phân (ArrayBuffer trong web, bytes trong Python) và áp dụng mã hóa hoặc giải mã trực tiếp.

3. Phân Tích Sơ Đồ Hoạt Động

1. Nhận file và khóa: Người dùng chọn file cần xử lý và nhập khóa (độ dài tự do).

2. Mã hóa hoặc giải mã:

- Mã hóa: Tạo IV ngẫu nhiên, mã hóa file bằng AES-CBC với khóa tạo từ SHA-256 của mật khẩu. Gộp IV và ciphertext rồi trả về file mã hóa.

- Giải mã: Tách IV từ file, sử dụng khóa đã tạo để giải mã phần ciphertext, trả về file gốc.

3. Giao diện:

- Trên Web: Giao diện hiện đại, đẹp, có chức năng upload file, nhập khóa, nút mã hóa/giải mã và tự động tải file kết quả về máy.

- Python: Script cho phép chạy lệnh mã hóa/giải mã trên máy với các tham số input/output và khóa.

4. Mô Tả Ứng Dụng Web

- Giao diện: Trang Web với background ảnh đẹp, form nằm giữa màn hình, bố cục dễ dùng và responsive.

- Chức năng:

- Upload file cần mã hóa hoặc giải mã.

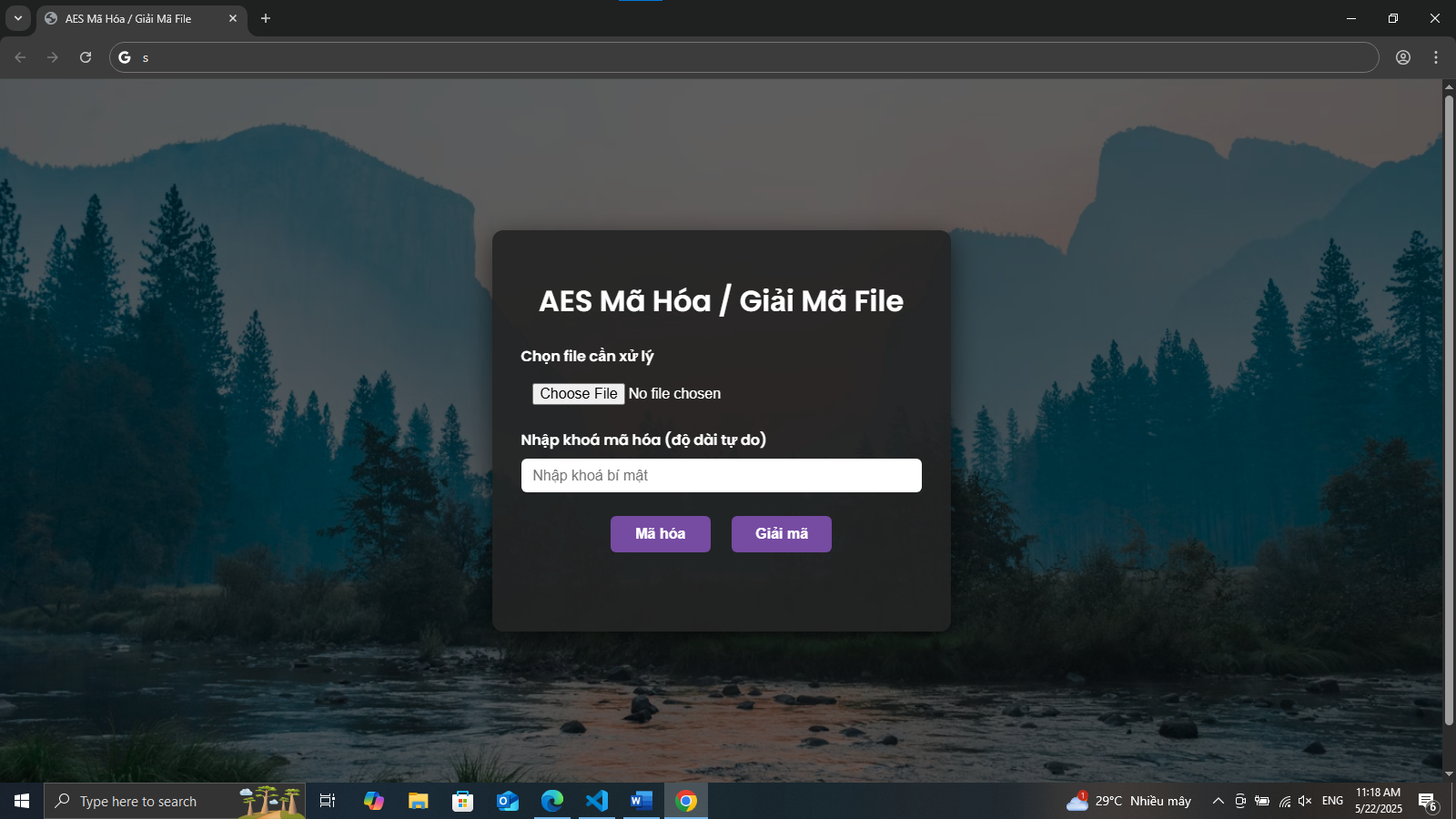
- Nhập khóa mật khẩu bất kỳ.

- Nút Mã hóa / Giải mã với hiệu ứng tải khi xử lý.

- Tự động tải file kết quả với tên hợp lý.

- Thông báo trạng thái rõ ràng cho người dùng.

- Công nghệ: Sử dụng Web Crypto API để mã hóa, giải mã trực tiếp trên trình duyệt, không tải file lên server nên bảo mật tốt.



5. Mô Tả Script Python

- File `aes\_file\_crypto.py` sử dụng thư viện `cryptography` để thực thi mã hóa và giải mã AES-CBC.

- Khóa được tạo từ mật khẩu bằng hàm SHA-256.

- IV ngẫu nhiên, được lưu ở đầu file mã hóa.

- Module tích hợp argparse cho giao diện dòng lệnh, hỗ trợ truyền tham số đầu vào, đầu ra và khóa.

- Có kiểm tra lỗi, xử lý padding PKCS7.