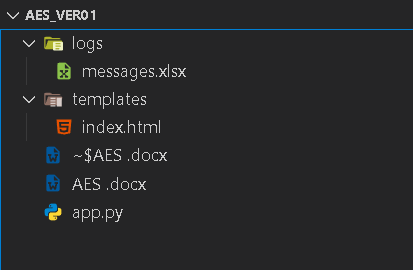
AES

# Cấu trúc dự án



# Tìm hiểu IV

IV là một khối dữ liệu có kích thước bằng với kích thước khối của thuật toán mã hóa (8 bytes cho DES, 16 bytes cho AES). Đây là một giá trị đầu vào được sử dụng cùng với khóa mã hóa, nhưng không phải là một khóa bí mật.

IV Giúp:

Tạo tính ngẫu nhiên:

IV giúp đảm bảo rằng cùng một plaintext khi được mã hóa nhiều lần với cùng một khóa sẽ cho ra các ciphertext khác nhau

Điều này ngăn chặn việc hacker có thể nhận ra các mẫu lặp lại trong dữ liệu mã hóa

· Ngăn chặn các cuộc tấn công mẫu:

Nếu không có IV (hoặc sử dụng IV giống nhau), hai thông điệp giống nhau sẽ tạo ra cùng một ciphertext

Điều này cho phép kẻ tấn công nhận biết khi nào cùng một thông điệp được gửi đi nhiều lần

· Xử lý khối đầu tiên:

Trong chế độ CBC, mỗi khối plaintext được XOR với khối ciphertext trước đó trước khi mã hóa

Đối với khối đầu tiên, không có khối ciphertext nào trước đó, nên IV được sử dụng thay thế

# Giải thích hàm mã hóa AES

- Sử dụng chế độ CBC

