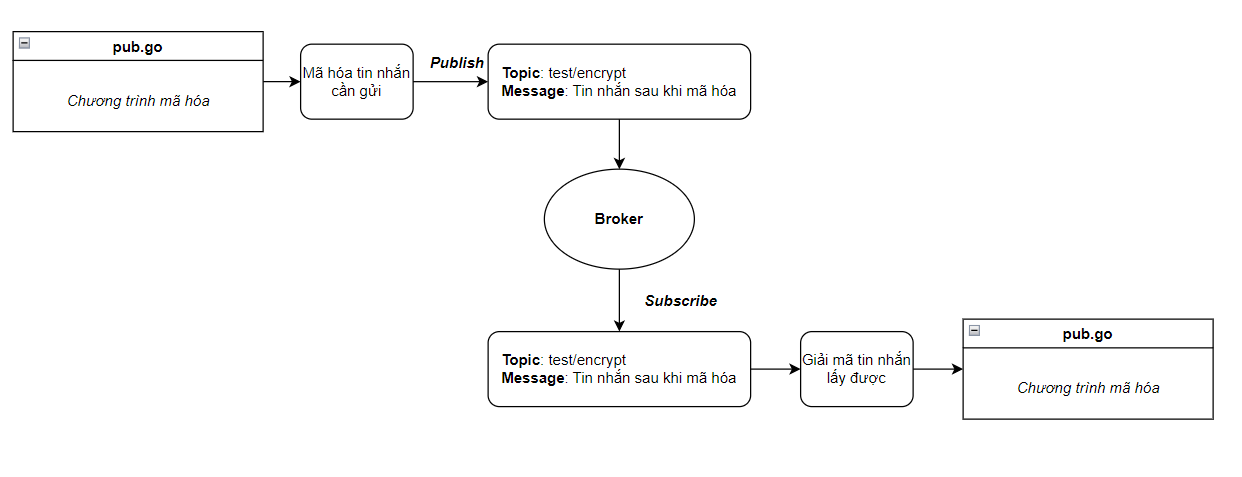
4, Demo symmetric encryption trong MQTT

- Sử dụng thuật toán mã hóa khóa đối xứng AES

- Sử dụng ngôn ngữ Golang để xây dựng chương trình mã hóa và chương trình mã hóa

- Xây dựng ý tưởng:



- Chương trình mã hóa:

+ Khởi tạo mqttBegin() kết nối với broker (cụ thể broker ở đây là mosquitto mqtt)

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Thực hiện tạo thông tin cần mã hóa và khóa chỉ định hay có thể hiểu là mật khẩu cho thông tin cần mã hóa

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Thực hiện mã hóa tin nhắn theo thuật toán AES, sau đó thực hiện cứ 2s sẽ public dữ liệu vừa được mã hóa lên broker:

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Chương trình giải mã:

+ Thực hiện khởi tạo mqttBegin() và thực hiện subscribe topic của chương trình mã hóa bên trên để thực hiện lấy tin nhắn.

Ảnh có chứa văn bản

Mô tả được tạo tự động

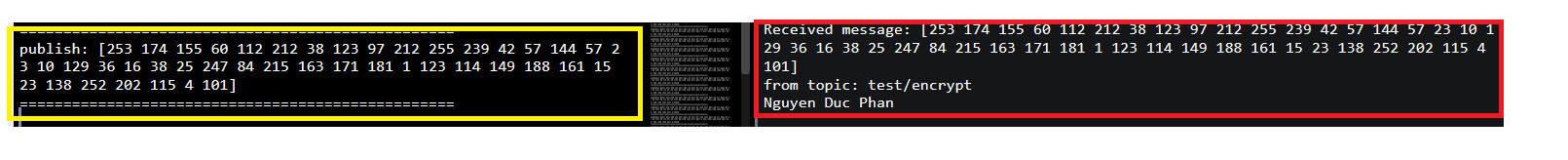
+ Thực hiện giải mã sau khi subscriber được dữ liệu trong hàm callback sau:

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ key của chương trình giải mã phải trùng hợp với key của chương trình mã hóa thì tin nhắn mới được giải mã thành công.

- Kết quả:



+ Khung màu vàng là tin nhắn sau khi mã hóa được biểu diễn dưới mảng dữ liệu kiểu byte

+ Khung mà đỏ là dữ liệu nhận được chính là dữ liệu trước đó đã mã hóa, dòng cuối cùng là “Nguyen Duc Phan” là tin nhắn giải mã thành công