Invsub

Chức năng InvSubBytes là thực hiện thay thế từng byte của ma trận trạng thái, bằng một giá trị đã quy định trong chuẩn AES. Bảng quy định giá trị thay thế cho InvSubBytes gọi là S-box đảo (Inverse S-box)

Hàm InvSubBytes làm như sau:

Nhận đầu vào là một chuỗi hex (ví dụ: "2B7E1516").

Tách chuỗi hex thành các cặp ký tự (ví dụ: "2B", "7E", "15", "16").

Đối với mỗi cặp ký tự, chuyển đổi chúng thành các chỉ số tương ứng trong bảng tra cứu invSbox (bảng tra cứu ngược) và lấy giá trị tại vị trí đó.

Ghép kết quả các giá trị được thay thế thành một chuỗi hex mới, chính là kết quả của việc giải mã.

