**BƯỚC 1: PHÂN TÍCH BINARY**

**1.1 Sử dụng Ghidra để decompile**

**1.2 Hiểu luồng chương trình**

main() → verify\_password() → decrypt\_flag()

**Luồng logic:**

1. Nhập password
2. Verify password bằng XOR với 0x42
3. Nếu đúng → decrypt flag bằng XOR với key



**BƯỚC 2: REVERSE PASSWORD**

**2.1 Phân tích hàm verify\_password()**

*// Password được XOR với 0x42 và so sánh với:*

local\_38 = 0x673a257671212f28;

local\_30 = 0x3131122d140d2d2d;



**Tạo script reverse XOR**

*target = [0x28, 0x2f, 0x21, 0x71, 0x76, 0x25, 0x3a, 0x67,*

*0x2d, 0x2d, 0x0d, 0x14, 0x2d, 0x12, 0x31, 0x31]*

*# Reverse XOR với 0x42*

*password = ""*

*for byte\_val in target:*

*password += chr(byte\_val ^ 0x42)*

*print(f"Password: {password}")*

*# Kết quả: jmc34gx%ooOVoPss*

