Assignment #2

Assignment

C 언어로 개발된 실행 프로그램 (cal과 intruder)를 분석하고, 수정해보세요. (실행 프로그램은 ELF
64-bit 형태임)

Q1. intruder 프로그램을 분석하여 암호를 알아내세요 (50점)

- Intruder 프로그램의 main 함수의 어셈블리어를 분석하세요 (20점)
- 분석을 통해 확인한 로직을 프로그램으로 다시 개발해보세요 (10점)
- 바이너리 파일을 분석하여 암호(9자리)를 찾아내세요 (10점)
- 바이너리 파일을 수정하여 본인의 암호(9자리)를 만들어보세요 (10점)

```
$ ./intruder
passwd:*********
hello owner

$ ./intruder
passwd:*********
you're intruder
```

Q2 cal 프로그램을 분석하여 출력값이 12가 나오도록 프로그램으로 변조하세요 (40점)

- cal 프로그램의 main 함수의 어셈블리어를 분석하세요 (20점)
- 분석을 통해 확인한 로직을 프로그램으로 다시 개발해보세요 (10점)
- 바이너리 파일에서 프로그램을 변조하여 값이 12가 나오도록 해보세요 (10점)

```
$ ./cal
12
```

Hint

- 우분투에서 필요한 라이브러리 혹은 도구 설치를 위해서는 아래와 같이 사용하면 됩니다.

```
sudo apt install [필요한 도구/라이브러리 이름]
```

- 컴파일러는 gcc를 사용했습니다.
- objdump 사용하세요
    - ex) objdump -d -M intel intruder
- 바이너리 파일 수정시 ghex를 활용해보세요. 찾기 메뉴를 사용하면, 쉽게 바이너리 위치를 찾을 수 있습니다.