과제: OpenSSL을 사용한 암호화

1. openssl을 사용할 수 있는 환경을 구축하시오.

- Windows에 openssl을 설치해서 사용할 수 있으나 Linux에서는 기본적으로 설치되어 있으므로 Linux를 사용하는 것이 편리하다.
- 자신의 리눅스 머신이 없는 경우에 Windows에서 **Oracle Virtualbox**를 설치한 후에 여기에 Linux 가상머신을 설치하여 사용한다.
- Virtualbox를 실행한 후 다음과 같이 주어진 Linux 가상머신을 설치한다.
  1) [새로 만들기] 메뉴 선택
  2) 가상머신 만들기 상자에서
     이름: "security" 로 입력하고, 종류: Linux, 버전: Linux 2.6/...(32-bit)를 선택
  3) 다음을 선택하여 계속 진행한 후 하드디스크에서
     [기존 가상하드디스크 파일 사용]을 선택하고 주어진 "**Boxes2.vmdk**" 파일 선택
- Virtualbox에서 설치한 가상머신 security을 더블클릭하여 실행시킴
- 가상머신의 터미널 창에서 **login: user, Password: user**를 입력하여 로그인
- 다음과 같이 openssl 명령어가 실행되는 지 확인해본다.

```
$ openssl
OpenSSL> quit
```

- 가상머신을 종료하려면 [파일-닫기]를 선택함. 현재 시스템 상태 저장하기를 하면 다음에 가상머신의 현재 상태를 빠르게 복원할 수 있다.

2. 대칭키 암호화 실행

암호화를 위한 기본 사용 방법은 다음과 같다. (-d는 복호화용)

openssl enc *–cipher_type* [–d] -in file –out file

(1) 다음과 같이 처음 64바이트와 둘째 64바이트가 같은 텍스트 파일을 만드시오.

0123456789012345678901234567890123456789012345678901234567890123456789012

0123456789012345678901234567890123456789012345678901234567890123456789012

- vi 편집기를 사용하거나 다음 명령어를 사용하여 생성함

$ cat > testin

1줄입력

2줄입력

^D

(2) 이 파일을 des-ecb와 des-cbc 방법(cipher_type으로 des-ecb와 des-cbc를 사용)으로 암호화하여 저장하시오. 그리고 다음 명령어를 실행시켜서 암호화파일을 16진수 형식으로 내용을 확인하고 (첫째 줄의 내용과 마지막 줄의 내용은 암호화 내용이 아님) 차이점을 말하시오.

```
$ xxd –g1 암호화파일
```

(3) 암호화파일을 다시 복호화하여 저장한 후 원본파일과 비교하시오. 비교할 때에는 내용을 읽어서 비교하거나 다음 명령어를 사용할 수 있다.

```
$ diff 원본 복호화파일
```

3. 공개키 암호화 실행

(1) 1024bit 길이의 개인키를 생성하시오.

```
$ openssl genrsa -out private.pem 1024
```

(2) 생성한 개인키에 대한 공개키를 생성하시오.

```
$ openssl rsa -in private.pem -out public.pem -outform PEM -pubout
```

(3) 공개키를 가지고 파일을 암호화 함.

```
$ openssl rsautl -encrypt -inkey public.pem -pubin -in 원본파일 -out 암호화파일
```

(4) 개인키를 사용하여 암호화 파일을 복호화하시오.

```
$ openssl rsautl -decrypt -inkey private.pem -in 암호화파일 -out 원본파일
```

(5) 복호한 파일을 원본 파일과 비교하시오.