**密钥加解密实验**

**一、实验描述**

本实验的学习目的是让学生熟悉加密的概念，熟悉和了解加密算法(cipher)、加密模式(encryption mode)、以及初始向量(IV)的定义与作用。此外，学生还可以通过使用工具来编写基于Openssl库的C语言程序来实现消息的加密/解密。可以参见实验楼课程：<https://www.shiyanlou.com/courses/241>。

**二、实验环境**

1. 本实验中，将使用 openssl 命令行工具及其库。实验环境中已自带命令行工具，需安装 openssl 开发库。

2. 具体实验环境：linux加载Openssl库或者使用windows平台的MinGW加载OpenSSL库（BB平台可以下载编译好的MinGW和相关使用文档），两种平台上都可以进行实验，任选其一。

3. Linux平台可以使用虚拟机软件VM或者VirtualBox来加载Ubuntu或者CentOS镜像。如果不了解虚拟机相关安装方法可以参见：<http://www.cis.syr.edu/~wedu/seed/lab_env.html>，网页上有较详细的VirtualBox下的Ubuntu镜像（两种版本建议选择Ubuntu16.04）和详细的安装方法(User Manual)，安装方法百度也可。

4. Linux下Openssl库的加载方法：

$ sudo apt-get update

$ sudo apt-get install libssl-dev

5. 另外本实验还需要十六进制编辑器。Windows平台下，可以使用winhex或其他编辑器（第一次作业已用到）。linux平台可以使用 bless 十六进制编辑器，可以使用命令：$ sudo apt-get install bless

**三、实验内容**

**3.1 使用 openssl enc 命令来加密／解密一个文件。**

命令基本格式如下：

$ openssl enc ciphertype -e -in plain.txt -out cipher.bin -K 00112233445566778899aabbccddeeff

-iv 0102030405060708

请将上述命令代码中的 ciphertype 替换成指定的加密类型，比如-aes-128-cbc, -aes-128-cfb, -bf-cbc 等,在本实验中你至少需要使用三种不同的密码(cypher)与加密模式(encryption mode)可以通过输入man enc命令了解到各选项的含义以及 openssl 所支持的所有加密类型。

**在实验报告中回答下面问题：**

1. 配置好实验环境，并截图。

2. 创建一个文本文件，并任意输入内容，保存后作为输入文件，执行上面的命令行中的加密命令，给出实验结果截图。然后使用对应的解密命令，解密加密文件，并对比解密后的输出和原始输入文件是否相似。

3. 找一张bmp图片（可以使用bb平台提供的bmp图片，也可以使用其他任意bmp图片），作为输入文件，分别采用aes-128-ecb方式和aes-128-cbc方式加密并输出为图像文件。如果图像文件不能正常显示为图像，可以使用bless（linux平台）或winhex（windows平台）打开该图像文件，修改其前缀为标准的图像文件前缀，并保存。

打开加密后的图片，对比cbc方式ecb方式加密结果的异同，并给出两种方式下加密后的图片截图。

**3.2 使用 Openssl 加密库进行编程**

在本实验中，将学习如何使用 openssl 的加密库来加密／解密信息，openssl 提供一个叫作 EVP 的高级接口，已封装底层函数，尽管 openssl 也为每一个单独的加密算法提供接口，但使用 evp 会更方便一些。

以下地址给出样例代码，先自行熟悉 EVP 接口，再继续接下来的实验。

<https://blog.csdn.net/substitute_coder/article/details/53072100>

<http://www.cnblogs.com/cocoajin/p/6121706.html>

实验已给出明文和密文，如下所示，并且已知加密方法为 aes-128-cbc，IV 全由 0 组成，以及 key 的长度小于 16 个字母，该单词可以从一般的英文词典中得到。由于该单词小于 16 个字母（128bits）所以在其后追加了空格字符（对应 0x20）以达到 128bit 的长度。本例中词典已给出，文件名为word.txt.

**任务**：写一个程序找到加密密钥key。鼓励自己写程序，也可以使用实验楼中的代码，本实验即文件key.c，请调通key.c，给程序中每条语句添加注释，并画出程序的流程图。

明文 (21 个字符): This is a top secret.

密文 (十六进制形式): 8d20 e505 6a8d 24d0 462c e74e 4904 c1b5 13e1 0d1d f4a2 ef2a d454 0fae 1ca0 aaf9

注1: 明、密文对都直接放在了程序中。如果你打算将明文存储在文件中读取，可能会有一些麻烦。

注2: 为了编译代码，可以在linux平台需要写 makefile，如下。

INC=/usr/local/ssl/include/

LIB=/usr/local/ssl/lib/

all:

gcc -I\$(INC) -L$(LIB) -o enc yourcode.c -lcrypto –ldl

也可以直接在linux平台下直接运行带有相关参数的gcc命令。

如果使用另一种情形在windows平台下，可以使用codeblocks来作为编辑器，并加载已编译好的带有OpenSSL的MinGW编译器来编译你写的代码，编译的过程和普通的C程序是一样的。

注3：编写的程序代码可以参考实验楼平台的《密钥加解密实验 下》，本实验中给出该程序key.c，作为参考。但程序运行中可能会出现语法错误，需调试。Linux平台上key.c的错误可能少些，windows平台错误可能多些。此类错误均为由于不同平台下的C的语法稍有不同产生的语法错，而不是程序的逻辑错误。

关于codeblocks加载MinGW的方法见：提供的word文档《openssl+MinGW+ codeblocks》。

Windows codeblocks编译程序时，需要修改源文件key.c中的语法错误，该类错误为linux平台下和windows平台下编译器语法稍有不同。

提交实验报告到BB平台。实验报告命名：学号+姓名+Lab1。实验报告内容：回答3个问题和编程任务的答案以及运行结果截图。

备注：1. 寻找密钥的实验也可以使用python编程实现，给定明文和密文输出，通过穷举密码字典来找到加密密钥。也鼓励使用python编写类似key.py程序，找到密钥。

2. 实验楼还提供后续的随机数及熵的小任务，请酌情自己动手试试。不做实验报告要求。