密码学与网络安全 实验报告
实验二 DES 密码

学号：15336061　姓名：胡梦秋　专业：网络工程　实验日期：2017.11.27

【实验目的】

(1) 熟悉对称密钥体制 DES 的加密解密方法；
(2) 掌握 ECB、CBC、CFB、OFB、CTR 五种密码模式。

【实验内容与要求】

(1) 实现对任意字符（英文、中文、符号）进行编码并使用 DES 加密解密；
(2) 实现 ECB、CBC、CFB、OFB、CTR 五种模式的加密解密。

【实验环境】

(1) 操作系统：Windows 10
(2) IDE：QT Creator 4.4.1
(3) 编程语言：C++

【实验重点和难点】

实验重点：

1. 掌握 DES 的加密和解密原理，并且用编程语言实现加密和解密。
2. 掌握 ECB、CBC、CFB、OFB、CTR 五种密码模式的原理，并且用编程语言实现。

实验难点：

1. 实现将任意字符编码成二进制比特

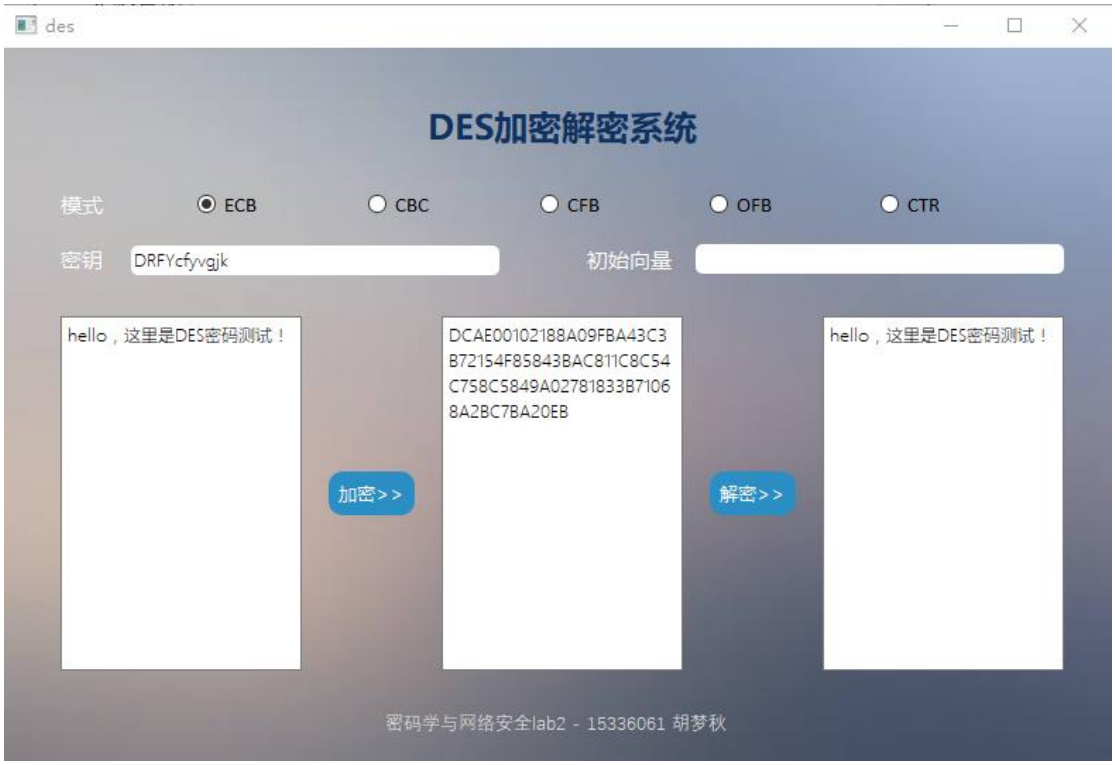
【实验原理与实现思路】

1. 首先需要实现 DES 密码，将固定 64 位比特加密和解密。DES 主要分成加密和轮密钥的生成两部分。
   加密部分在初始置换后需要进行 16 轮，每一轮中的 DES 函数是加密的关键部分。DES 函数要经过扩展置换盒、异或、换字盒、直接置换等步骤，最终经过最终置换盒得到密文。
   轮密钥的生成需要先进行压缩置换去除奇偶校验位，然后进行 16 轮，每一轮根据左移位表进行左移然后进行压缩置换得到 16 个 48 位的轮密钥。
   加密和解密的过程实际是一样的，只是轮密钥的顺序要反过来。
2. 然后需要实现将任意的字符转成二进制的比特串。这里我使用了将输入的任意字符按照 char 字符的 ASCII 码将字节转成对应的比特的方法。对于密文的输出，我使用了 16 进制来表示。

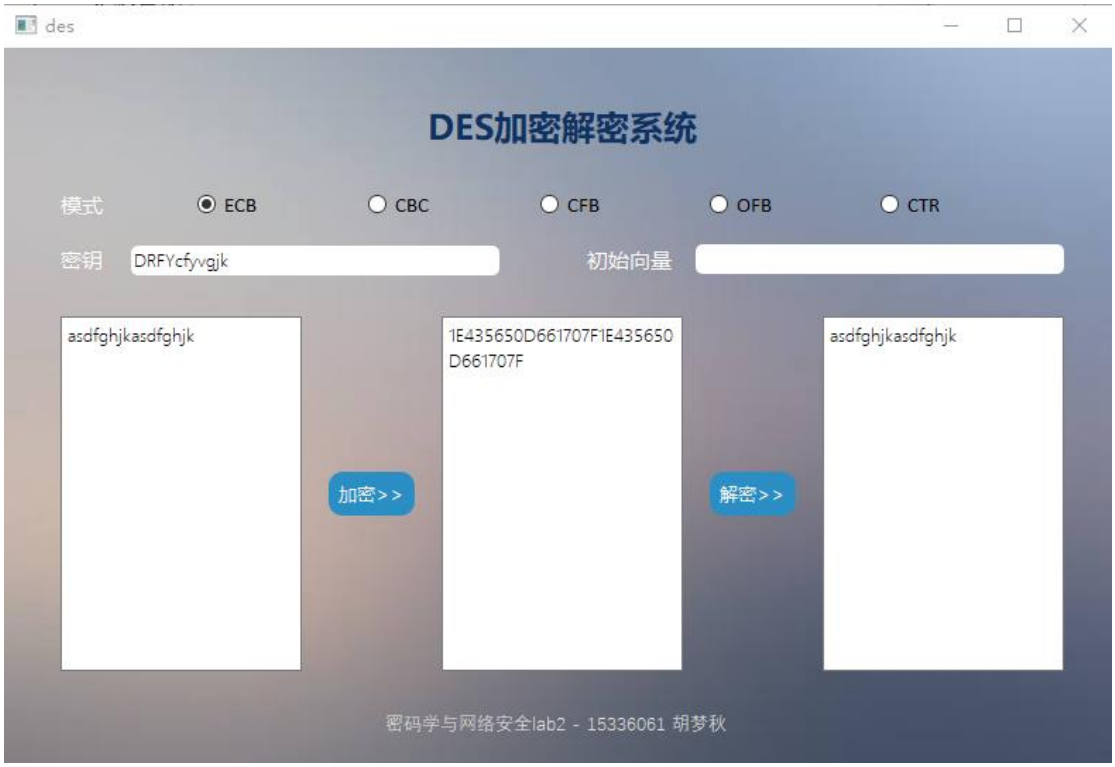
3. 对于 ECB、CBC、CFB、OFB、CTR 五种模式，可以实现任意长度的加密解密，前两种模式如果明文的长度不是 64 的倍数需要在后面补 0。CFB、OFB 的 r 取了 8，是一个字节的长度。密钥和初始向量 IV 不足 64 位补 0，超过 64 位只取前 64 位。五种模式按照书上的原理实现难度不大，而且还有很多代码其实是差不多的。最开始可以用 ECB 模式来检验相同的 64 比特的密文是否一样以验证 DES 加密解密是否正确。

【实验结果】

（1） ECB

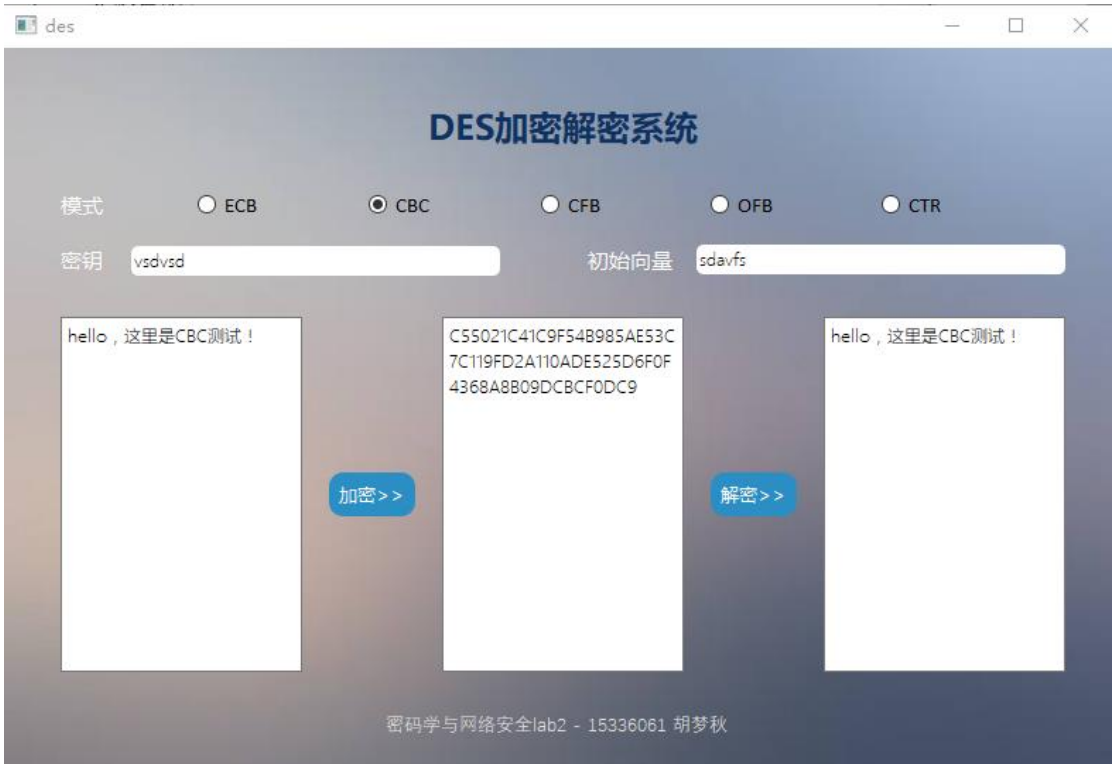


ECB 模式不需要初始向量，因此不用填入。

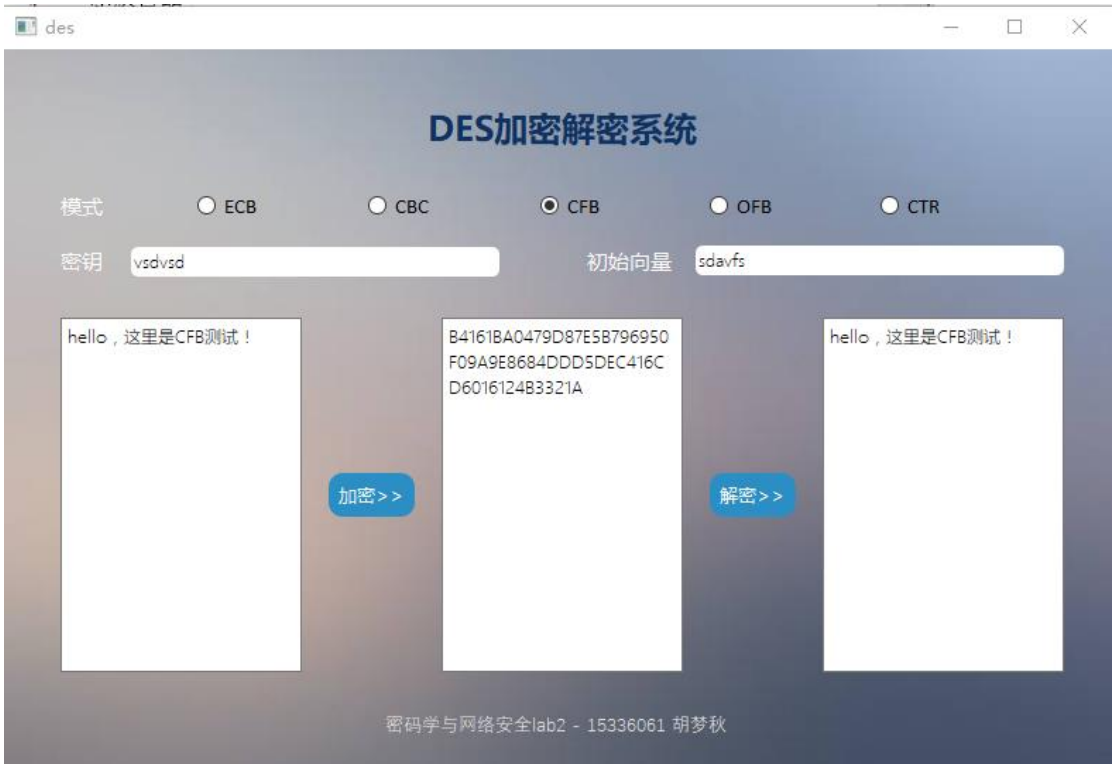


可以看出，前 8 个字母（64 比特）和后 8 个字母（64 比特）是一样的，因此加密后的密文也一样。

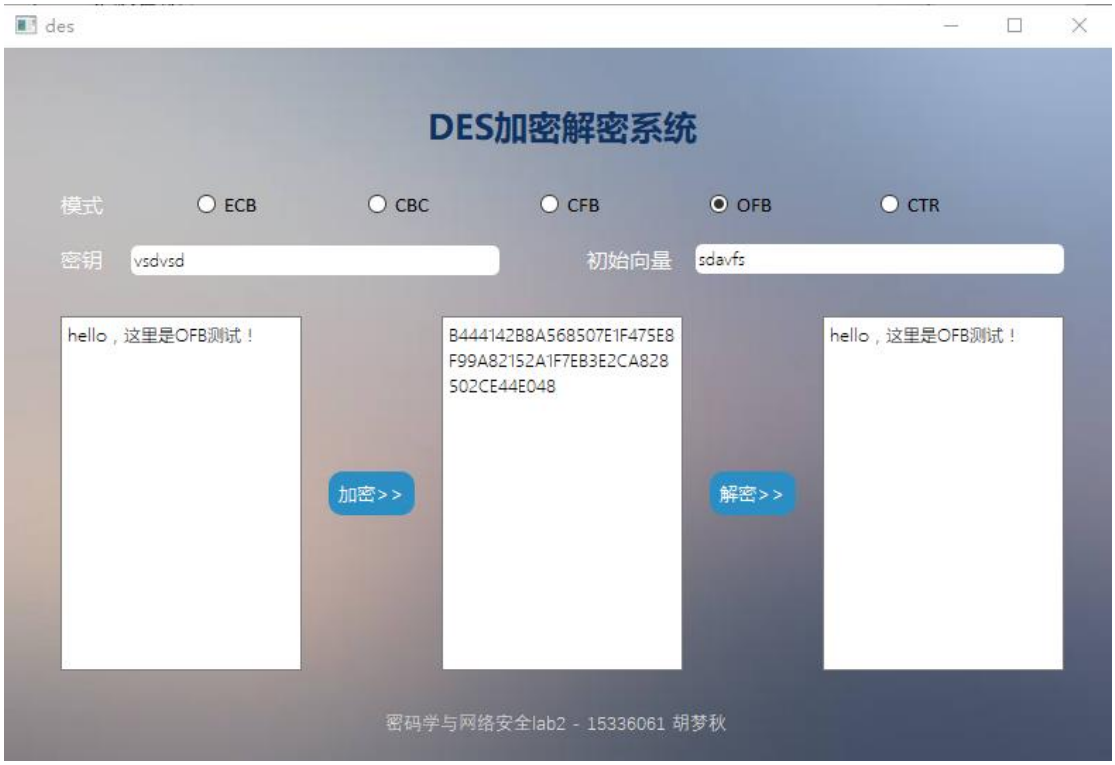
(2) CBC



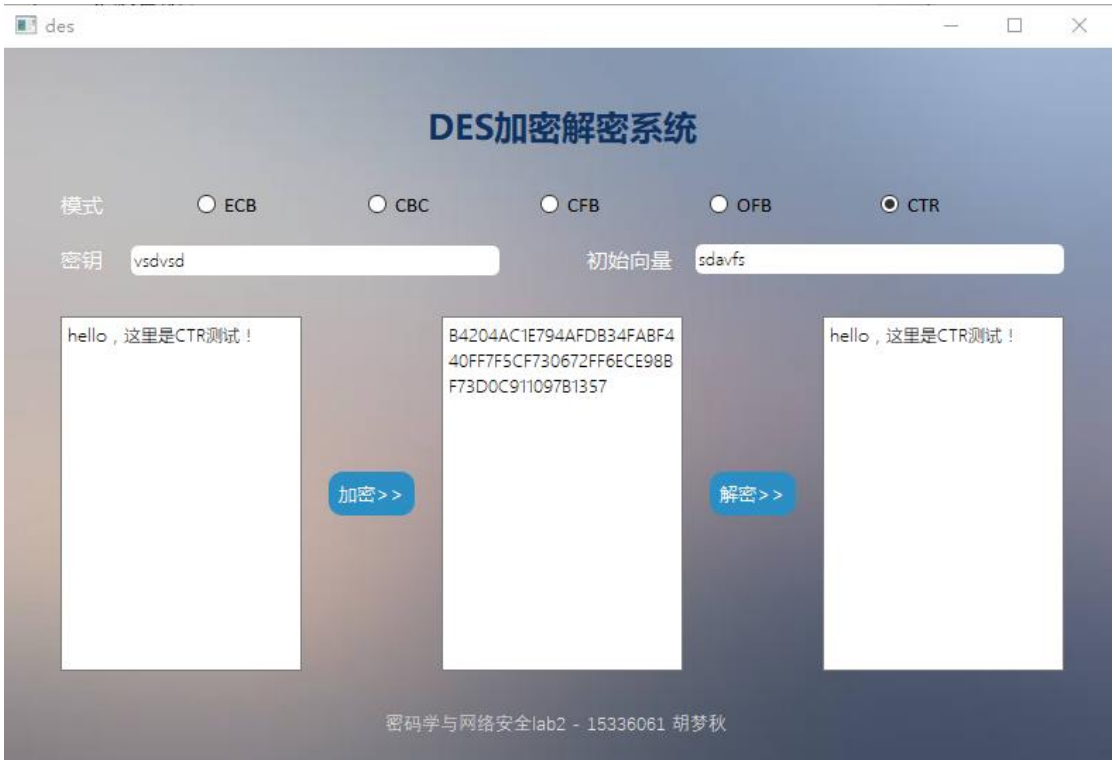
(3) CFB


des
DES加密解密系统
模式
ECB
CBC
CFB
OFB
CTR
密钥
vsdvsd
初始向量
sdavfs
hello，这里是CFB测试！
加密>>
B4161BA0479D87E5B796950
F09A9E8684DDD5DEC416C
D6016124B3321A
解密>>
hello，这里是CFB测试！
密码学与网络安全lab2 - 15336061 胡梦秋

(4) OFB


des
DES加密解密系统
模式
ECB
CBC
CFB
OFB
CTR
密钥
vsdvsd
初始向量
sdavfs
hello，这里是OFB测试！
加密>>
B444142B8A568507E1F475E8
F99A82152A1F7EB3E2CA828
502CE44E048
解密>>
hello，这里是OFB测试！
密码学与网络安全lab2 - 15336061 胡梦秋

(5) CTR



【实验心得】

1. DES 由于书上都给出了伪代码，所以实现起来也不是很难，主要的思考放在了字符转比特的问题上。一开始知道英文和常见的符号可以通过 ASCII 码表示，但不知道怎么解决中文的问题。后来发现，即使是中文也有对应的 ASCII 码，只不过是负数，还是能够转成比特的。
2. 过程中还遇到了一个比较蠢的问题是，不知道怎么把密文表示出来，以为要把比特再转成字符，这样转过来之后全都是乱码，再读取之后的比特会改变，就无法解密了。后来发现其实根本不需要显示出字符，一般的做法是将比特流转成十六进制输出。
3. 在控制台程序里中文是两个字节，转到 QT 里之后也没太注意这个问题，给老师演示的时候才发现 4 个中文并不是 64 比特，反而要 8 个中文才能使得 ECB 模式相同的两组 8 个中文能够加密成相同的密文。那时候以为 8 个中文是 64 比特，但是回来之后又多尝试了几次，并且查了一下资料发现其实一个中文是 3 个字节即 24 比特，这和 QT 界面控件的文本的编码方式有关。因此要 8 个中文，即 192 比特才是最小的能够整除 64 的数。
4. 总的来说，通过此次实验，我对 DES 以及五种加密模式的原理理解的更透彻了，受益匪浅。