密码学与网络安全实验：DES

第二次试验

姓名：王跃辉	学号：15336182	专业：网络工程
课程：密码学与网络安全	指导老师：龙东阳	完成时间：2017.11.24

实验准备：

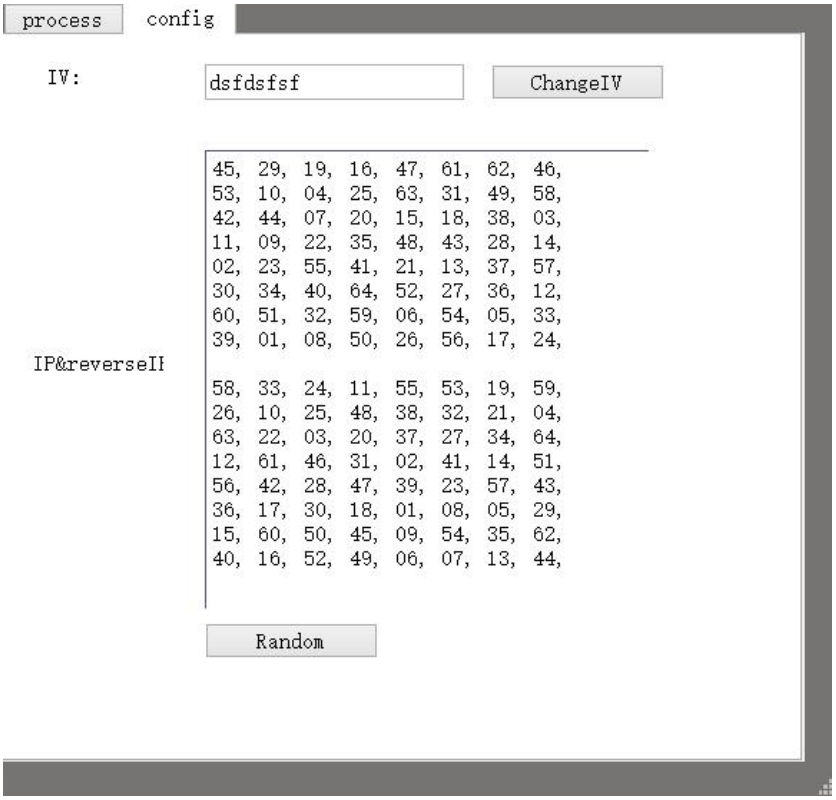
实验题目	DES 加密算法的实现（及其五种模式）
实验内容	使用 DES 加密算法加密和解密字符串（包括中文）
实验环境	Linux，QT，C++编写代码；windows 下发布

实验结果：

本次实验实现了 DES 加密算法以及 ECB,CBC,CFB,OFB,CTR 五种模式；五种模式均支持键盘上所有输入输出的加密解密；支持初始置换和逆初始置换的随机生成；IV 的任意设置；及时对 16 组子秘钥的查看。

Process 界面：

Configure 界面：



实验原理：

加密/解密模式	密码类型	分析介绍
ECB	分组密码	简介：最基础的分块加密，将明文分成相等长度的小段，逐段加密 优点：操作简单，易于实现；分组独立，易于并行；误差不会被传送。 缺点：掩盖不了明文结构信息，难以抵抗统计分析攻击。
CBC	分组密码	简介：先将明文切分成若干小段，然后每一小段与初始块或者上一段的密文段进行异或运算后，再与密钥进行加密。 优点：能掩盖明文结构信息，保证相同密文可得不同明文。 缺点：不利于并行计算；（2）传递误差——前一个出错则后续全错。
CFB	流密码	简介：密码算法的密码会反馈到密码算法的输入中，CFB 模式通过将明文分组和密码算法的密文进行 XOR 来产生密文分组。 优点：隐藏了明文模式；结合了分组加密和流密码（分组密码转化为流模式）； 缺点：不利于并行计算；需要生成秘钥流
OFB	流密码	简介：密码算法的输出（指密码 key 而不是密文）会反馈到密码算法的输入中，OFB 模式并不是通过密码算法对明文直接加密，而是通过将明文分组和密码算法的输出进行 XOR 来产生密文分组。 优点：类似于 CFB 缺点：类似于 CFB
CTR	流密码	简介：完全的流模式。将瞬时值与计数器连接起来，然后对此进行加密产生密钥流的一个密钥块，再进行 XOR 操作 优点：不泄露明文；仅需实现加密函数；无需填充；可并行计算。

		缺点：需要瞬时值 IV，难以保证 IV 的唯一性。

程序说明：

Process 界面：	说明
模式选择	五种模式的选择，任意选择一种时会清空所有文本框。
输入输出 支持键盘上所有输入输出，包括中文，英文，数字，符号等	Plain 为明文输入（支持中文），key 为秘钥，encode 为密文输出（01 比特流），decode 为解密输出。
子秘钥查看	每行代表一组 48bit 的子秘钥。
Configure 界面：	
IV 设置	支持任意 46bit 的 IV 设置。
IP 及 RIP 随机生成	随机生成初始置换即对应的逆置换。

实验总结：

本次试验难度尚可，主要是基于 DES 的加密以及解密的算法实现，唯一的难点是考虑键盘上的任意输入输出。

Windows 系统下默认为 GBK 编码，而 Linux 下默认为 UTF-8，并且中文在程序设计语言（C++）中默认占两个字节而一个字符占一个字节，这样一来中文输入势必会乱码。幸好 C++中有<bitset>类，这个类就是专门用来处理 01 比特流的一个类，在各种类型转换的时候，用它本身的成员函数就不会产生乱码了。

除了这个问题以外，算法实现的问题基本与老师在课堂上讲解的没什么出入，按照 PPT 的思路做也可行，本次试验我们接触了真正运用在实际当中的加密解密算法，印象还是很深刻。希望下一次实验，我能做得更好。