

**实 验 报 告**

**EXPERIMENT REPORT**

姓名

学号

专业

教师 徐士伟

科目 信息安全

**信 息 学 院**

**COLLEGE OF INFORMATIC**

**CBC模式的DES加解密**

**一、实验内容**

编程实现DES加密和解密算法，并使用DES加解密算法实现3DES加解密算法

3DES的加解密的工作模式，采用密码分组链接（CBC）模式

选择一种填充方式，对需要加密的文件进行填充（解密要去掉填充部分），填充方法采用ANSI X9.23请参考：https://www.jianshu.com/p/16e1cbc0b7a9

读取/写入被加密/解密文件时，采用字节流的形式进行文件读取/写入（字节流文件的查看，可以使用UltraEdit的十六进制查看模式，可以轻松查看十六进制）

完成实验后，需要交实验报告（包括：重要函数的功能分析和流程图）

**二、实验原理**

**2.1 DES加解密原理**

**2.2 3DES加解密原理**

**2.3 分组密码CBC加解密模式原理**

**2.4 填充原理**

三、**实验过程**

**3.1 变量说明**

**3.1.1 主函数变量说明**

**3.1.2 其他重要变量说明（以下为举例）**

static TABLE IP\_Table[64]//初始置换IP表

static TABLE IP1\_Table[64]//逆初始置换IP1表

**3.2 函数功能说明**

**3.2.1主函数说明**

**3.2.2 其他重要函数说明（以下为举例）**

1）string bit2byte(string bit)

作用：比特串转字符串

参数：需要转换成字符串的比特串

返回：转换后的字符串

2）string function(string R, string K)

作用：f函数

参数：需要进行运算的字符串R,密钥K

返回：f函数运算后的结果

3）string iterative(string L, string R, string\* K, MODE mode)

作用：16轮迭代

参数：需要运算的左右字符串L，R，子密钥集K，加或解密模式mode

返回：迭代运算以后的结果

**3.3 流程图**

**3.3.1 主函数流程图**

**3.3.2 其他重要函数流程图（可自行增加小节）**

**四、实验结果与截图**

**五、实验总结**