**《网络空间安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | | **张梓健** | | **年级** | | **2021** |
| **学号** | | **20214578** | | **专业、班级** | | **计算机科学与技术05班** |
| **实验名称** | **实验二 DES加解密算法的实现** | | | | | |
| **实验时间** | **2024.4.27** | | **实验地点** | | **DS3402** | |
| **实验成绩** |  | | **实验性质** | | **□验证性 □设计性 □综合性** | |
| 教师评价：  □算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  评语：  评价教师签名（电子签名）： | | | | | | |
| 一、实验目的   1. 掌握DES加密算法的加解密过程。 | | | | | | |
| 二、实验内容  利用编程语言实现DES加解密算法。  1、 编程：包含的功能函数有：  static void DES(char Out[8], char In[8], const SUBKEY\_P pskey, bool Type);//标准DES 加/解密  static void SETKEY(const char\* Key, int len);// 设置密钥  static void Set\_SubKey(SUBKEY\_P pskey, const char Key[8]);// 设置子密钥  static void F\_FUNCTION(bool In[32], const bool Ki[48]);// f 函数完成扩展置换、S-盒代替和P 盒置换  static void S\_BOXF(bool Out[32], const bool In[48]);// S-盒代替函数  static void TRANSFORM(bool \*Out, bool \*In, const char \*Table, int len);// 变换函数  static void XOR(bool \*InA, const bool \*InB, int len);//异或函数  static void CYCLELEFT(bool \*In, int len, int loop);// 循环左移函数  static void ByteToBit(bool \*Out, const char \*In, int bits);// 字节组转换成位组函数  static void BitToByte(char \*Out, const bool \*In, int bits);// 位组转换成字节组函数  2、 调试  3、 运行结果  4、 存盘 | | | | | | |
| 三、实验过程或算法（源程序）  （1）DES算法流程：  DES( Data DES( Data Encryption Standard)算法，于1977年得到美国政府的正式许可，是一种用56位密钥来加密64位数据的方法。DES算法以被应用于许多需要安全加密的场合。  (一)、密钥生成  1、变换密钥  取得64位的密钥，每个第8位作为奇偶校验位。  2、变换密钥。  (1)、舍弃64位密钥中的奇偶校验位，根据下表（PC-1）进行密钥变换得到56位的密钥，在变换中，奇偶校验位以被舍弃。  (2)、将变换后的密钥分为两个部分，开始的28位称为C[0]，最后的28位称为D[0]。  (3)生成16个子密钥，初始I=1。  (i)、同时将C[I]、D[I]左移1位或2位，根据I值决定左移的位数。  (ii)、将C[I]D[I]作为一个整体按下表（PC-2）变换，得到48位的K[I]  (iii)、从1-2-3-1处循环执行，直到K[16]被计算完成。  (二)、处理64位的数据  1、取得64位的数据，如果数据长度不足64位，应该将其扩展为64位（例如补零）  2、将64位数据按下表变换（IP）  3、将变换后的数据分为两部分，开始的32位称为L[0]，最后的32位称为R[0]。  4、用16个子密钥加密数据，初始I=1。  (1)、将32位的R[I-1]按下表（E）扩展为48位的E[I-1]  (2)、异或E[I-1]和K[I]，即E[I-1] XOR K[I]  (3)、将异或后的结果分为8个6位长的部分，第1位到第6位称为B[1]，第7位到第12位称为B[2]，依此类推，第43位到第48位称为B[8]。  (4)、按S表变换所有的B[J]，初始J=1。所有在S表的值都被当作4位长度处理。  (i)将B[J]的第1位和第6位组合为一个2位长度的变量M，M作为在S[J]中的行号。  (ii)、将B[J]的第2位到第5位组合，作为一个4位长度的变量N，N作为在S[J]中的列号。  (iii)、用S[J][M][N]来取代B[J]。  (iv)、从(i)处循环执行，直到B[8]被替代完成。  (5)、将B[1]到B[8]组合，按下表（P）变换，得到P。  (6)、异或P和L[I-1]结果放在R[I]，即R[I]=P XOR L[I-1]。  (7)、L[I]=R[I-1]  (8)、从2-4-1处开始循环执行，直到K[16]被变换完成。  5、、组合变换后的R[16]L[16]（注意：R作为开始的32位），按下表（IP-1）变换得到最后的结果。  （2）DES算法实现（仅展示实验文档要求的部分函数）  1. 标准DES 加/解密       1. 生成子密钥      1. f 函数完成扩展置换、S-盒代替和P 盒置换      1. 扩展置换函数      1. S-盒代替函数      1. P盒置换函数      1. 异或函数      1. 循环左移函数      1. 字节组转换成位组函数      1. 位组转换成字节组函数      1. 主程序 | | | | | | |
| 四、实验结果及分析和（或）源程序调试过程  1. 加密    2. 解密    3. 未支持功能 | | | | | | |