**《网络空间安全概论》实验报告**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **姓名** | |  | | **年级** | | **2021级** |
| **学号** | |  | | **专业、班级** | | **计算机科学与技术01班** |
| **实验名称** | **实验一 加解密算法的实现** | | | | | |
| **实验时间** | **2024.3.30** | | **实验地点** | | **DS3304** | |
| **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  掌握频度分析法原理和Feistel加解密原理。 | | | | | | |
| 二、实验项目内容  1.使用频度分析法解密以下文本，并给出替换表：  UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ  2.编程实现Feistel加密解密以下文本：  CQUINFORMATIONSECURITYEXP | | | | | | |
| 三、实验设计  **1.频度分析法**  对于任何一种书面语言而言，不同的字母或字母组合出现的频率各不相同。如果以这种语言书写足够长的文本，都呈现出大致相同的特征字母分布规律，虽然不少字母出现的概率近乎相等，但也有极少数字母出现的概率有较大差异。  为了分析密文信息方便，常将英文字母表按字母出现的概率大小分类，分类情况如下：极高频 E，次高频 T A O I N S H R，中等频 D L，低频 C U M W F G Y P B，甚低频 V K J X Q Z  语言的单字母统计特性没有反映出英文双字母和多字母的特征，在双字母中统计出概率最大的30对字母按概率大小排列为：th he in er an re ed on es st en at to nt ha nd ou ea ng as or ti is et it ar te se hi of  类似的，我们还可以考察英文课文中三字母出现的频率。按Beker在1982年统计的结果(样本总数100 360)得到概率最大的20组三字母按概率大小排列为：the ing and her ere ent tha nth was eth for dth hat she ion his sth ers ver，特别地，the出现的频率几乎为ing的3倍。  可通过统计密文中字母出现频率来模拟整个英文体系的字母频率分布，即将密文视为样本，以样本的参数估计整体参数，将密文中频率分布的字母与整体的频率分布字母进行替换。当然，这种估计是有误差存在的，但是基于英文书写的特点（常用单词、语法特征、短语搭配等）与英文单词构成，我们可以在估计的基础上进一步猜测和修正，进而破解出整个密文段。  **2. Feistel加密解密算法**    **·初始置换**  利用初始置换IP对64位明文X进行换位重新组合处理，打乱原来的次序，并把乱序后的明文组分为、两部分，每部分各长32位。  **·子密钥生成**  加密者输入的密钥为64 bit，其中只有56 bit是有用的位数（因为有8位为奇偶校验位）。但是加密过程有16轮循环函数，其中需要用到16个密钥，所以要将这56 bit密钥扩展生成16个48 bit 的子密钥。步骤如下：  1.用PC\_1表置换  PC\_1置换的主要步骤和初始IP置换一样，PC\_1置换的目的是为了去掉64 bit密钥k中的8个奇偶校验位，并对其余56位打乱排列。置换完成后，同样将密钥分成左右两部分各28 bit，左边为, 右边为。  2.创建16个块和  对于，在第n轮分别对和进行循环左移，所移的位数为1位或者2位，取决于n的值，当n=1,2,9,16时左移1位，其它左移2位。进行移位后得到到，到。  3. 得到16个子密钥K  = PC\_2()，PC\_2为固定置换，用于从 中选取48 bit作为子密钥， 表示从左到右将 排在 的后面，的长度为56 bit。至此，子密钥全部生成，进入轮函数。  **·轮函数**  轮函数的设计：首先用位选择表将32位的扩展为48位的；再用与48位的子密钥 进行异或运算；接着将得到的48位数分成8个6位数，将每个6位子块输入函数（盒代换），输出8个4位二进制块（）；最后合成32位二进制块之后，用换位表进行置换（盒代换），结果即为轮函数的32位输出。  **·逆置换**  轮函数最后一步的左边32 bit和右边32 bit合成64 bit，再进行逆初始置换，得到最终密文。  **算法描述：**  1.输入64位明文数据，并进行初始置换IP；  2.在初始置换IP后，明文数据再被分为左右两部分，每部分32位，以，表示；  3.在密钥的控制下，经过16轮运算；  4.16轮后，左、右两部分交换，并连接在一起，再进行逆置换；  5.最后输出64位密文。  加密和解密使用相同的算法。加密和解密唯一不同的是密钥的次序是相反的。就是说如果每一轮的加密密钥分别是,,,，那么解密密钥就是,,,。  **·加密处理**  令为轮函数，并令,,,,分别为轮的子密钥。  基本操作如下：  将明文块拆分为两个等长的块，对每轮 ，计算  则密文为。  **·解密处理**  解密密文为则通过计算  则为明文。 | | | | | | |
| 四、实验过程或算法  **（一）频度分析法**  密文：UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ  1.统计密文中各字母出现的频率，按照从高到低进行排序    2.由于密文中字母P和Z出现频率远高于其他字母，根据频度分析法的原理，将密文中出现频率最高的字母P替换为极高频字母e，接着将密文中出现频率第二高的字母Z替换为次高频字母t    3.由于其余字母出现频率区别不大，接下来根据英语单词的词法和语法特性结合字母出现频率统计规律，分析可能的密文字母替换表  3.1根据替换后的密文中“tWe”单词组合，结合统计规律，推测该单词为“the”，故将密文中字母W替换为h；接着根据密文中“tWSt”单词组合，推测为“that”，故将密文中字母S替换为a    3.2根据替换后的密文中“haFe”单词组合，结合统计规律，推测该单词为“have”，故将密文中字母F替换为v；接着根据密文中“Ut”单词组合并且该单词位于句首，推测为“it”，故将密文中字母U替换为i    3.3根据替换后的密文中“Qith”单词组合，结合统计规律，推测该单词为“with”，故将密文中字母Q替换为w    3.4根据替换后的密文中“waO”单词组合，结合统计规律以及位于主语it之后的语法规则，推测该单词为“was”，故将密文中字母O替换为s    3.5根据替换后的密文中“seveEaX”单词组合，结合统计规律以及用词习惯，推测该单词为“several”，故将密文中字母E替换为r，字母X替换为l    3.6根据替换后的密文中“reYreseDtatives”单词组合，结合统计规律以及用词习惯，推测该单词为“representatives”，故将密文中字母Y替换为p，字母D替换为n    3.7根据替换后的密文中“VireHt”单词组合，结合统计规律以及用词习惯，推测该单词为“direct”，故将密文中字母V替换为d，字母H替换为c    3.8根据替换后的密文中“GesterdaG”单词组合，结合统计规律，且开头和结尾的字母一致，根据用词习惯推测该单词为“yesterday”，故将密文中字母G替换为y；接着根据密文中“cMntacts”和“pMlitical”单词组合，推测为“contacts”和“political”，故将密文中字母M替换为o    3.9根据替换后的密文中“Aeen”单词组合，结合统计规律，并且位于单词“have”之后，根据用词习惯和语法规则推测该单词为“been”，故将密文中字母A替换为b；接着根据密文中“oB”单词组合，结合统计规律，推测为 “of”，故将密文中字母B替换为f    3.10根据替换后的密文中“inforTal”单词组合，根据用词习惯推测该单词为“informal”，故将密文中字母T替换为m；接着根据密文中“bIt”单词组合，结合统计规律，推测为 “but”，故将密文中字母I替换为u    3.11根据替换后的密文中“conJ”单词组合，根据前后语义结合用词习惯推测该单词为“cong”，故将密文中字母J替换为g    **（二）Feistel加密解密算法**  加解密文本：CQUINFORMATIONSECURITYEXP  1.初始置换  将输入的64位明文plainText按照初始置换表IP进行置换。  2. 逆初始置换  将输入的64位密文cipherText按照逆初始置换表IP\_inverse进行置换。    3.子密钥生成  根据输入的64位密钥生成16轮的子密钥。在实现过程中，首先将64位密钥按照PC1置换表进行置换，然后将得到的56位结果分为左右两部分，并根据移位表moveKey进行左移操作，然后将左右部分合并，并根据PC2置换表生成48位子密钥。    4.轮函数  首先对右半部分进行扩展，然后与子密钥进行异或操作，接着将结果分为8组，每组6位，通过S盒代换得到4位结果，最后经过P盒置换得到32位输出。    5.Feistel加密  首先对明文进行初始置换，然后将置换后的结果分为左右两部分，经过16轮Feistel加密后，进行逆初始置换得到密文。    6.Feistel解密  首先对密文进行初始置换，然后将置换后的结果分为左右两部分，经过16轮Feistel解密后，进行逆初始置换得到明文。    7.字符串格式转换  加密：首先需要将输入的明文和密钥由字符串类型转换为二进制字符串，接着再对二进制明文串用子密钥进行分组加密处理，最后再将加密后的密文串由二进制字符串转换为十六进制字符串，向用户展示密文。  解密：首先需要将输入的密文由十六进制字符串转换为二进制字符串以及将密钥由字符串类型转换为二进制字符串，接着再对二进制密文串用子密钥进行分组解密处理，最后再将解密后的明文串由二进制字符串转换为字符串类型，向用户展示明文。 | | | | | | |
| 五、实验过程中遇到的问题及解决情况  **1.问题：**无法直接通过字母出现频率统计规律对密文进行破译  **解决方案：**将密文中频率分布特殊的部分字母与整体的频率分布字母进行替换。然后基于英文书写的特点（常用单词、语法特征、短语搭配等）与英文单词构成，在估计的基础上进一步猜测和修正，进而破解出整个密文段。  **2.问题：**Feistel加密解密算法安全性保证  **解决方案：**  分组长度：分组长度越长意味着安全性越高，但是会降低加、解密的速度。这种安全性的增加来自更好的扩散性。传统上，64位的分组长度比较合理，在分组密码设计里很常用。  密钥长度：密钥较长同样意味着安全性较高，但会降低加、解密的速度。这种安全性的增加来自更好的抗穷尽攻击能力和更好的混淆性。通常使用的密钥长度是64位。  迭代轮数：Feistel密码的本质在于单轮不能提供足够的安全性而多轮加密可取得很高的安全性。迭代轮数的典型值是16。  子密钥产生算法：子密钥产生越复杂，密码分析就越困难。  轮函数F：同样，轮函数越复杂，抗攻击的能力就越强。  DES算法是基于Feistel 算法发展的，是目前最为流行的加密算法之一，其安全性以及运行效率通过长期实践得以证明。故采取DES算法思路实现Feistel加密解密算法。  **3.问题：**Feistel加密的明文字符数不满足8的整数倍，即最后一个分组不足8个字符（64位），无法进行加密操作  **解决方案：**对明文末尾进行空格填充，将明文字符数填充至8的整数倍，对加密后的密文进行解密操作，由于填充的字符为空格，不影响解密后的明文内容。 | | | | | | |
| 六、实验结果及分析和（或）源程序调试过程  **（一）频度分析法**  ·密文：UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ  1.解密结果：  2.替换表（部分明文字母由于密文的有限导致无法推断，故为空）：    **（二）Feistel加密解密算法**  **1. Feistel加密**  明文：CQUINFORMATIONSECURITYEXP  密钥：HelloCQU    Feistel加密后的密文：42D2864841F0AFA1CEA2A84FD3E7B08A01AAA1C548748BA7A31018D3642E3350  ·密钥不同，相同明文Feistel加密后的密文不同  明文：CQUINFORMATIONSECURITYEXP  密钥：12345678    Feistel加密后的密文：01A2AA8521C68C200C528842B354A20AC22A89459CBE8AA6615020D848041090  **2. Feistel解密**  密文：42D2864841F0AFA1CEA2A84FD3E7B08A01AAA1C548748BA7A31018D3642E3350  密钥：HelloCQU    Feistel解密后的明文：CQUINFORMATIONSECURITYEXP  ·密钥不同，相同密文Feistel解密后的明文不同  密文：42D2864841F0AFA1CEA2A84FD3E7B08A01AAA1C548748BA7A31018D3642E3350  密钥：12345678    Feistel解密后的明文：GF\_R峇d峴蕇D礦乨qWX亦,?c | | | | | | |