**《信息安全概论》实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **姓名** | **陈鹏宇** | | **年级** | | **2020级** |
| **学号** | **20204227** | | **专业、班级** | | **计算机科学与技术01班** |
| **实验名称** | **加解密算法的实现** | | | | |
| **实验时间** | **2023.10.13** | **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**  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文本，并写出替换表   UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ   1. 编程实现Feistel加密/解密   CQUINFORMATIONSECURITYEXP | | | | | |
| **三、实验设计**  **1. 频度分析原理**  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，如下图所示：  表格  描述已自动生成  在上表中，不少字母出现的概率近乎相等。为了应用方便，常将英文字母表按字母出现的概率大小分类，分类情况见下表：  --------------------------  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 ionhis sth ers ver  特别，the出现的频率几乎为ing的3倍。 | | | | | |
| 1. **实验过程或算法** 2. **频度分析法解密** 3. **统计词频**     P: 0.1333  Z: 0.1167  U: 0.0833  S: 0.0833  O: 0.0750  M: 0.0667  H: 0.0583  E: 0.0500  D: 0.0500  V: 0.0417  X: 0.0417  W: 0.0333  F: 0.0333  Q: 0.0250  T: 0.0250  G: 0.0167  B: 0.0167  A: 0.0167  Y: 0.0167  I: 0.0083  J: 0.0083   1. **先将最高词频字母和次高词频字母替换，即P替换成e，Z替换为t**      1. **发现单词tWe，结合三字母的最高词频the，猜测将W替换为h**      1. **观察到thSt，猜测为that**      1. **观察到haFe，猜测为have**      1. **观察到QUth，猜测为with**      1. **观察到waO，猜测为was**      1. **观察到AeeD，猜测为been**      1. **观察到TaVe，猜测为made**      1. **观察到seveEaX，猜测为several**      1. **观察到direHt，猜测为direct**      1. **观察到cMntacts，猜测为contacts**      1. **观察到inBormal，猜测为informal**      1. **观察到GesterdaG，猜测为yesterday**      1. **观察到bIt，猜测为but**      1. **观察到Yolitical，猜测为political**      1. **观察到conJ，猜测为cong**      1. **Feistel网络加密解密** 2. **基础函数实现**      1. **验证字符串和二进制数转换的正确性**      1. **设置密钥**      1. **加密**      1. **解密验证** | | | | | |
| 1. **实验过程中遇到的问题及解决情况** 2. 频度分析法一些单词很生僻，比如Viet cong，无法通过经验尝试出来；不仅要通过频度和语法判断，还需要结合语境进行分析。 3. 频度分析法不经过人工分析的结果不理想，完全看不懂，所以抛弃机器分析结果，根据语法和频度人工修正，才能正确解密。 4. feistel网络在解密过程中，需要逆置密钥，否则解密会失败 5. feistel网络中的轮函数F为非线性函数，查询资料后发现通常为伪随机置换PRF或者为随机函数PRF，这里为了简便就直接采用异或函数。 | | | | | |
| 1. **实验结果及分析和（或）源程序调试过程** 2. 频度分析法解密 3. 解密结果   it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow   1. 替换表  |  |  | | --- | --- | | 密文字母 | 明文字母 | | A | b | | B | f | | C | \* | | D | n | | E | r | | F | v | | G | y | | H | c | | I | u | | J | g | | K | \* | | L | \* | | M | o | | N | \* | | O | s | | P | e | | Q | w | | R | \* | | S | a | | T | m | | U | i | | V | d | | W | h | | X | l | | Y | p | | Z | t |   “\*”表示字符串中没有出现的字母   1. Feistel网络加密解密 2. 加密  * 密文：cÆ¬âÎÉî¨vÖÇòÅq"áHeõáa * 二进制：01000011010100010101010101001001010011100100011001001111010100100100110101000001010101000100100101001111010011100101001101000101010000110101010101010010010010010101010001011001010001010101100001010000  1. 解密  * 结果：CQUINFORMATIONSECURITYEXP * 二进制：01000011010100010101010101001001010011100100011001001111010100100100110101000001010101000100100101001111010011100101001101000101010000110101010101010010010010010101010001011001010001010101100001010000 | | | | | |