**《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** | **实验一　单表替代的分析** | | | | | |
| **实验时间** | **2024.3.30** | | **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. 熟悉单表替换加密的概念 2. 学会单表替代加密的分析方法 3. 手工实现单表替换的密码分析 | | | | | | |
| 1. 实验项目内容 2. 单表替代加密的破解 3. 破解task.txt的内容 | | | | | | |
| 三、实验过程或算法（源程序）  （1）原理  单表代替是密码学中最基础的一种加密方式。在加密时用一张自制字母表上的字母来代替明文上的字母（比如说A——Z，B——D）来达到加密。移位密码也属于单表代替，只不过比较有规律，相当于集体向前或向后。这种加密方法最容易被破解。破解方法为统计法。在英语中，最常用的字母为E，所以在密文中代替E 的字母出现的频率也最高，由此便可破解。  （2）实现过程  1. 首先编写了一段代码，统计密文中每个字母的出现频率，并按从大到小排序，以便后续破译时参考，代码和结果如下：         |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **E** | **T** | **A** | **O** | **I** | **N** | **S** | **R** | **H** | | **0.1268** | **0.0978** | **0.0788** | **0.0776** | **0.0707** | **0.0706** | **0.0634** | **0.0594** | **0.0573** | | **L** | **D** | **U** | **C** | **F** | **M** | **W** | **Y** | **G** | | **0.0394** | **0.0389** | **0.028** | **0.0268** | **0.0256** | **0.0244** | **0.0214** | **0.0202** | **0.0187** | | **P** | **B** | **V** | **K** | **X** | **J** | **Q** | **Z** |  | | **0.0186** | **0.0156** | **0.0102** | **0.006** | **0.0016** | **0.001** | **0.0009** | **0.0006** |  |  1. 对照正常英文字母的频率表进行破译，首先确定频率最高的字母k，基本可以肯定其对应e，然后是t，大概率就是对应t，接下来就不好猜测了，因为A，O，I，N四个频率相近，对应密文的o，q，p，e频率也很相近，不好确定，经过多种组合的尝试都没能成功，破解陷入僵局。 2. 从单个字母没法继续推进，尝试换个角度，从单词入手，由于k的推理大概率是正确的，所以我尝试搜索所有的k，然后观察有没有重复出现的包含k的组合。这一看，还真让我发现了一个经常出现的组合：“TOK”，整整出现了10次，并且这10次其前后跟着的字母基本都不相同，所以基本可以确定这是个单独的单词。此外，k已知对应e，而t大概率对应e，o的出现频率很高，并且tok这个单词很常用，那么经过一一比对，锁定了目标：h！tok对应the！这是个非常重要的发现，因为h的频率在正常字母中不在前面几个，所以之前猜测时完全没有考虑h，如果不是通过tok推理出来这个，估计是永远想不到了…… 3. 之后又从单词的角度推理出几个：tqfk -> take，tok skpsxk -> the people，kqeto -> earth…… 然后再通过比对频率表依次填词尝试，最终把出现过的字母所对应的正确字母都推理出来了。 | | | | | | |
| 四、实验结果及分析和（或）源程序调试过程  字母对应表    明文  it is rather for us to be here dedicated to the great task remaining before us that from these honored dead we take increased devotion to that cause for which they gave the last full measure of devotion that we here highly resolve that these dead shall not have died in vain that this nation under god shall have a new birth of freedom and that government of the people by the people for the pk shall not perish from the earth | | | | | | |