**广州大学学生实验报告**

**开课学院及实验室：**网络空间安全学院 **2023年4月11日**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **学院** | 网络空间安全学院 | **年级/专业/班** | 网安211 | **姓名** |  | **学号** |  |
| **实验课程名称** | 密码技术及应用 | | | | | **成绩** |  |
| **实验项目名称** | 维吉尼亚密码破译 | | | | | **指导**  **老师** | 李树栋 |

1. 实验目的

（1）了解维吉尼亚密码的简单历史和数学原理，通过加密解密过程，包括如何使用密钥来生成密文以及如何对密文进行解密操作。

（2）通过该实验可以学习维吉尼亚系统的弱点，并使用频率分析和Kasiski测试来破解维吉尼亚密码。

1. 实验内容

（1）对于维吉尼亚密码，练习使用密钥对明文进行加密生成密文；

明文：ATTACKATDAWN，密钥：LEMONLEMONLE，密文：LXFOPVEFRNHR。

（2）对于维吉尼亚密码，练习使用密钥对密文进行解密得到明文的操作；

例：对于下面是一段经过维吉尼亚加密的密文，请你找出它的密钥并解密出原文。

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBWRVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAKLXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELXVRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHRZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBIPEWEVKAKOEWADREMXMTBHHCHRTKDNVRZ

（3）练习针对维吉尼亚密码，使用Kasiski测试确定密钥长度；

（4）频率分析和Kasiski测试来破解维吉尼亚密码

（5）练习使用拟重合指数法确定密钥内容。

1. 实验过程及结果
2. 实验总结