重庆大学大数据与软件学院

上 机 实 验 报 告

|  |  |
| --- | --- |
| 上机实践项目 | S-AES算法实现 |
| 课程名称 | 信息安全导论 |

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 | 路静雯 | 成绩 |  |
|  | 张梅璈 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 学号 | 20220856 | 教师 | **胡海波** |
|  | 20220568 |

|  |  |  |  |
| --- | --- | --- | --- |
| 班级 | 软工03班 | 日期 | 2024/10/28 |

**《计算机网络》上机实验报告**

**开课实验室： 2024 年 9月28 日**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 姓 名 | | 路静雯  张梅璈 | 年级、班级 | 2022级软工03班 | 学号 | **20220856**  **20220568** |
| 上机（项目）名称 | | | S-AES算法实现 | | 指导教师 | 胡海波 |
| 教师评语 | 教师签名：  **年 月 日** | | | | | |

1. **上机目的**

根据"信息安全导论"课程第8-9次课讲述的AES算法，在课外认真阅读教科书附录D的内容，学习了解S-AES算法，并使用你们自己最擅长的程序语言(C++/QT或Java+Swing、Python+QT等)来编程实现加、解密程序。

1. **基本原理**

参考教科书《密码编码学于网络安全—原理与实践(第8版)》，附录D：简化AES。请同学们认真阅读。

1. **使用的软件、硬件**

软件：jdk-21.0.2

Java+Swing

硬件：Windows-PC

1. **编程和测试要求**

**主界面（图4.0.1）**

图4.0.1

**4.1 第1关：基本测试**

**根据S-AES算法编写和调试程序，提供GUI解密支持用户交互。输入可以是16bit的数据和16bit的密钥，输出是16bit的密文。**

**加密**：输入明文密钥，点击加密，得到加密后的密文（图4.1.1），加密后的密文为1111101010100101

这里输入的是明文1110101011001001，密钥1111000000111101

图4.1.1

**解密**：输入密文1111101010100101，密钥1111000000111101，得到解密后的明文1110101011001001（图4.1.2）



图4.1.2

**4.2 第2关：交叉测试**

**考虑到是"算法标准"，所有人在编写程序的时候需要使用相同算法流程和转换单元(替换盒、列混淆矩阵等)，以保证算法和程序在异构的系统或平台上都可以正常运行。**

**设有A和B两组位同学(选择相同的密钥K)；则A、B组同学编写的程序对明文P进行加密得到相同的密文C；或者B组同学接收到A组程序加密的密文C，使用B组程序进行解密可得到与A相同的P。**

4.2.1 我组加密结果

明文：1011010111011001

密钥：1100111011101110

密文：1000101110001110

4.2.2 对方解密结果

密文：1000101110001110

密钥：1100111011101110

明文：1011010111011001

**4.3 第3关：扩展功能**

**考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为2 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)。**

**加密**：输入明文asdfghjklzxcvbnm,密钥1010101010101010，点击ASCLL加密按钮，得到加密后的密文（图4.3.1.1）

图4.3.1.1

解密：输入密文,密钥1010101010101010，点击ASCLL解密按钮，得到解密后的密文（图4.3.1.2）



图4.3.1.2

**4.4 第4关：多重加密**

**4.4.1 双重加密**

**将S-AES算法通过双重加密进行扩展，分组长度仍然是16 bits，但密钥长度为32 bits。**

**加密：**输入明文1100011010101100,密钥11100011101110001100100110011001，点击双重加密按钮，得到加密后的密文（图4.4.1.1）



图4.4.1.1

**解密：**输入密文1111110101101011,密钥11100011101110001100100110011001，点击双重解密按钮，得到解密后的明文（图4.4.1.2）



图4.4.1.2

**4.4.2 中间相遇攻击**

**假设你找到了使用相同密钥的明、密文对(一个或多个)，请尝试使用中间相遇攻击的方法找到正确的密钥Key(K1+K2)。**

输入明文1111110101101011,密文1010110000111100，点击中间相遇攻击按钮，得到可能的密钥对：K1: 0000100010011001, K2: 1111111111111111（图4.4.2.1）



图4.4.2.1

**4.4.3 三重加密**

**将S-AES算法通过三重加密进行扩展，下面两种模式选择一种完成：**

**(1)按照32 bits密钥Key(K1+K2)的模式进行三重加密解密，**

**(2)使用48bits(K1+K2+K3)的模式进行三重加解密。**

这里选择的是模式一

**加密：**输入明文0011100101000110,密钥11000001111010101100010111001010，点击三重加密按钮，得到三重加密后的密文1011010010100100。（如图4.4.3.1）



图4.4.3.1

**解密：**输入密文1011010010100100,密钥11000001111010101100010111001010，点击三重加密按钮，得到三重解密后的明文0011100101000110。（如图4.4.3.2）



图4.4.3.2

**4.5 第5关：工作模式**

**基于S-AES算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。注意初始向量(16 bits) 的生成，并需要加解密双方共享。**

**在CBC模式下进行加密，并尝试对密文分组进行替换或修改，然后进行解密，请对比篡改密文前后的解密结果。**

如图



图4.5

1. **过程原始记录(数据、图表、计算等)**

代码见附件