**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 5 月9 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** | 公钥密码实验—RSA算法 | | | | | **指导**  **老师** | 李树栋 |

1. 实验目的
2. 实现RSA加解密
3. 实现费马因子分解
4. 练习小指数迭代攻击方法（选做）
5. 实验内容
6. 使用python实现RSA加解密算法，根据参数p=61,q=53,m=’hello world’随机选取e生成公私钥对和密文c，再对密文解密还原
7. 使用费马因子分解法分解整数：476714679652321667
8. 使用小指数迭代攻击法破解以下密文

e = 3

c =

358367237930161611287553617821502821834060085243898907996647845293765170791369942269257353667444037801340579758680509083796235778230457983351909760841969489695686448841352419071149675085236615042625125

n =

16503642207789401613904637446670329919611766947715053323104219193209988406515756550342556551087269744552311616952010203456790322170970296166677505605996894842559532450550835236993676533810157091757910377447156599161839816759569000052558651907868440945641567209771534186995020539019344287451849086813001914316093471981888660658969896738024934729735528534566540708968896374055591535315302278504854219775669117057573452687716997892400605761254842309025919547236250830974219452915644544246195460317093268045928951431217025117317053023012828445449507248638685265783199196296512529426531595699588709043560235664398614480367

1. 实验过程及结果

3.1 同学们把你们的实验过程及结果写在下面

3.2

3.3

1. 实验总结

4.1 同学们把你们的实验过程及结果写在下面

4.2

4.3