

密码学

平时实验报告

（ 2020 / 2021 学年 第 二 学期）

题 目： RSA

|  |  |
| --- | --- |
| **专 业** | 信息安全 |
| **组 长 姓 名** | 茹兴奥 |
| **组 员 姓 名** |  |
| **班 级 学 号** | B19030824 |
| **指 导 教 师** | 李琦 |
| **指 导 单 位** | 信息安全系 |
| **日 期** | 2021年6月1日 |

|  |  |
| --- | --- |
| **成员分工** | |
| 组长（1） | 姓名茹兴奥学号B19030824 具体分工全部 |
| 组员（1） | 姓名 学号 具体分工 |
| 组员（2） | 姓名 学号 具体分工 |
| **简短评语：**  **指导教师： 李琦 年 月 日** | |

**Windows系统环境下的口令破解实验**

1. **课题内容和要求**

**1.实验环境**

实验主机操作系统为Windows 10 Dev-C++

**2.实验内容**

学习RSA

**二、课题需求分析**

运用C语言写代码

**三、测试数据及其结果分析**

#include<cstring>

#include<iostream>

using namespace std;

const int p=3, q=11, e=7;

int gcd(int e, int phi){

for(int d=2; ;d++){

if(d\*e%phi == 1)

return d;

}

}

// pow(a,b,c) = a^b % c

int pow(int a,int b,int c){

int res=1;

for(int i=0;i<b;i++){

res\*=a;

}

return res%c;

}

int main(){

char ch;

// 1、计算 n = p×q，φ(n) = (p-1)×(q-1)

// 2、计算 d，满足 d\*e ≡ 1mod φ(n)

// 3、得到：公钥为 {e,n}, 私钥为 {d,n}

int n = p\*q;

int phi = (p-1)\*(q-1);

int d = gcd(e,phi);

// 4、加密用公钥，密文：C = M^e (mod n)

printf("发送方公钥(e,n)为:(%d,%d)\n",e,n);

freopen("RSA1.txt","r",stdin);

freopen("RSA2.txt","w",stdout);

while(scanf("%c",&ch)==1){

int t = pow(ch-'A',e,n);

printf("%c",t+'A');

}

fclose(stdin);

fclose(stdout);

// 5、解密用私钥，明文：M = C^d (mod n)

printf("接收方秘钥(d,n)为:(%d,%d)\n",d,n);

freopen("RSA2.txt","r",stdin);

freopen("RSA3.txt","w",stdout);

while(scanf("%c",&ch)==1){

int t = pow(ch-'A',d,n);

printf("%c",t+'A');

}

fclose(stdin);

fclose(stdout);

return 0;

}

**四、课题完成过程中遇到的问题及解决方法**

(1) 代码不熟练，多看看以前的书就好点了

**五、总结**

经过本次实验，我明白了基本的RSA加解密的方法，对密码学有了更加深入的了解