

**实 验 报 告**

**（2019 / 2020 学年 第 二 学期）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | 算法分析与设计 | | | | | |
| 实验名称 | 完成简单的RSA公开密钥系统的构造 | | | | | |
| 实验时间 | 2020 | 年 | 5 | 月 | 20 | 日 |
| 指导单位 | 计算机学院软件工程系 | | | | | |
| 指导教师 | 毛毅 | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 学生姓名 | 梁佩欣 | 班级学号 | B18030409 |
| 学院(系) | 计算机学院 | 专 业 | 计算机科学与技术 |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **实验名称** | 完成简单的密钥系统的构造 | | | **指导教师** | 毛毅 |
| **实验类型** | **课内实验** | **实验学时** | **2** | **实验时间** | 2020.05.20 |
| 1. **实验目的和要求**   内容：自学并完成一个简单的RSA公开密钥系统的构造。 要求：1. 了解密码学中的加/解密原理，掌握数论的基本知识，理解非对称密码体制RSA加密算法的工作原理和流程。   1. 能够设计并实现一个简单的RSA公开密钥系统。 | | | | | |
| 二、**实验环境(实验设备)**  硬件：微型计算机  软件：Windows 操作系统、Microsoft Visual C++6.0 | | | | | |
| **三、实验原理及内容**  原理：RSA算法的公开密钥和私人蜜月是一对大素数的函数。  产生密钥的过程：   1. 选择两个大素数P和q,p≠q; 2. 计算乘积n=pq,得到Φ（n）=(p-1)(q-1); 3. 选择随机整数e，0<e<Φ(n)，使得gcd(e,Φ(n))=1; 4. Jisuan d=modΦ(n); 5. 公开密钥为{e,n}，私人密钥为{d,n}.   加密公式：；  解密公式：。  （明文分组M是一个小于n的数。）  源代码：  #include <iostream>  #include <stdio.h>  #define p 43  #define q 59  #define e 13  int candp(int a,int b,int c); //数据处理函数，实现幂的取余运算  int fun(int x,int y); //公钥e 与 t的互素判断  int main()  {  int d, m, n, t, c, r;  int m\_t = 0, m\_i = 0, m\_j = 0;  int ciphertext[100]; //存放密文的数组  int proclaimedtext[100]; //存放明文的数组  n = p \* q;  t = (p - 1) \* (q - 1); //求n的欧拉数  d = 1;  while(((e \* d) % t) != 1) d++;//由公钥e求出私钥d  while(1)  {  printf("加密请输入 1 解密请输入 2\n"); //加密或解密选择  scanf("%d",&r);  switch(r)  {  case 1:  printf("请输入密文 m: ");  scanf("%d",&m);  while(m / 100)  {  m\_t = m % 100;  ciphertext[m\_i] = m\_t;  proclaimedtext[m\_i] = candp(m\_t, e, n);  m /= 100;  m\_i++;  }  ciphertext[m\_i] = m;  proclaimedtext[m\_i] = candp(m, e, n);  printf("明文为: \n");  for(int i = 0 ; i <= m\_i ;i++)  {  printf("%d",proclaimedtext[i]);  }  printf("\n");  break;  case 2:  printf("明文为 c: ");  for(int i = 0 ; i <= m\_i ;i++)  {  printf("%d",proclaimedtext[i]);  }  printf("\n");  while(m\_i--)  {  ciphertext[m\_j] = candp(proclaimedtext[m\_j], d, n);  m\_j++;  }  printf("密文为: \n");  for(int i = m\_j ; i >= 0 ;i--)  {  printf("%d",ciphertext[i]);  }  printf("\n");  break;  }  }  }  int candp(int a, int b, int c) //数据处理函数，实现幂的取余运算  {  int r = 1;  while(b-- != 0)  r = (r \* a) % c;  return r;  }  int fun(int x, int y) //公钥e 与t 的互素判断  {  int t;  while(y)  {  t = x;  x = y;  y = t % y;  }  return x == 1 ? 0: 1;  } | | | | | |

**实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **四、实验小结**（包括问题和解决方法、心得体会、意见与建议等）  (一)实验中遇到的主要问题及解决方法  在实验时，设计恢复明文的部分比较难，有时候会出错，n比较大就不大存在需要分组的问题。  （二）实验心得  要充分理解RSA产生密钥的过程，在计算e时，要注意是一个与Φ（n）互为素数的数。  （三）意见与建议（没有可省略） | | | | | |
| 1. **支撑毕业要求指标点**   （1）3-2-M能够根据用户需求，选取适当的研究方法和技术手段，确定复杂工程问题的解决方案。  （2）3-3-H能综合利用专业知识对解决方案进行优化，体现创新意识，并考虑健康、安全以及环境等因素。  （3）7-2-M正确理解和评价计算机及应用领域复杂工程问题实施对环境保护及社会可持续发展等的影响，评价产品周期中可能对人类和环境造成的损害和隐患。 | | | | | |
| **六、指导教师评语**   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **评 分 细 则** | **评分项** | **优秀** | **良好** | **中等** | **合格** | **不合格** | | **遵守实验室规章制度** |  |  |  |  |  | | **学习态度** |  |  |  |  |  | | **算法思想准备情况** |  |  |  |  |  | | **程序设计能力** |  |  |  |  |  | | **解决问题能力** |  |  |  |  |  | | **课题功能实现情况** |  |  |  |  |  | | **算法设计合理性** |  |  |  |  |  | | **算法效能评价** |  |  |  |  |  | | **回答问题准确度** |  |  |  |  |  | | **报告书写认真程度** |  |  |  |  |  | | **内容详实程度** |  |  |  |  |  | | **文字表达熟练程度** |  |  |  |  |  | | **其它评价意见** |  | | | | | | **本次实验能力达成评价（总成绩）** |  |  |  |  |  | | | | | | |
| **成 绩** |  | **批阅人** |  | **日 期** |  |