



实验报告

姓名 班级 学号 实验日期

课程名称 数字内容安全

指导教师

成绩

实验名称：RSA 加密算法

一、实验目的

了解数据加密的原理，掌握公钥加密算法

二、实验内容

使用 matlab 编程实现 RSA 加密

三、实验过程

题目：RSA 算法

内容：

rsa_pq.m 文件代码如下：

本代码主要作用如下：

- 1、随机选定两个互异的大素数 p, q
- 2、计算 $n=p*q$
- 3、计算 n 的欧拉函数 $Q=(p-1)*(q-1)$
- 4、选定一个正整数 e ，使 $1<e<Q$ ，且 e 与 Q 互质
- 5、求出正数 d ，使其满足 $d*e \equiv 1 \pmod{Q}$ ，则将 (n, d) 作为私钥

```
function [p, q, n, Q, e, d]=rsa_pq()
n1=101;%我随便给的
n2=167;
p=ceil(n1.*rand(1,1));%产生两个随机数
q=ceil(n2.*rand(1,1));%产生两个随机数
n=q*p; %计算n
Q=(p-1)*(q-1); %欧拉函数fi
%循环用于随机生成一个e
for j=1:1:100
    k=0;
    E=ceil(30*rand); %随机生成E
    if E<Q %判断这个E是否小于Q
        for i=2:1:(Q-1) %i:除了1和Q本身
            if rem(Q,i)==0&&rem(E,i)==0 %如果Q、E不是质数,break
                k=1;
                break;
            end
        end
        if k==0 %Q、E互质
            e=E;
            break;
        end
    end
end
end
```



实验报告

姓名 班级 学号 实验日期

课程名称 数字内容安全

指导教师

成绩

```
%循环用于随机生成一个d
for j=1:1:100
    d=ceil(((Q*j)+1)/e); %d=e*j倍的Q加1
    if mod(e*d,Q*j)==1 %如果mod(e*d,Q*j)等于1
        d=ceil(((Q*j)+1)/e); %上述d值可用
        break;
    end
end
disp('-----RSA算法开始执行-----');
disp(' 正在随机生成p,q,n,Q,e,d');
Y = ['p=', num2str(p), ' ', 'q=', num2str(q), ' ', 'n=', num2str(n), ' ', 'Q=', num2str(Q), ' ', 'e=', num2str(e), ' ', 'd=', num2str(d)];
disp(Y)
```

rsa_encrypt.m 文件代码如下:

本代码主要实现的是将明文采用 RSA 算法进行加密。

```
1 %RSA加密算法, key1明文-->key2密文
2 function rsal=rsa_encrypt(key1, e, n)
3     length_key=length(key1);
4     bin_e=dec2bin(e);
5     length_e=length(bin_e);
6     for j=1:1:length_key%加密
7         x=0;
8         c=1;
9         for i=1:1:length_e
10            x=2*x;
11            c=mod(c*c, n); %这部分为自定义设置
12            if bin_e(i)=='1'
13                x=x+1;
14                c=mod(c*key1(j), n); %RSA核心算法
15            end
16        end
17        key2(j)=c; %加mod后c最终的值赋给key2
18    end
19    disp(' 李家兴的RSA加密算法:');
20    disp(' 明文为: ');
21    disp(key1);
22    disp(' 密文为: ');
23    disp(key2);
24    rsal=key2;
```



上海工程技术大学

实验报告

姓名 班级 学号 实验日期

课程名称 数字内容安全

指导教师

成绩

my_RSAoutput.m 文件代码如下:

```
新建 打开 保存 比较 转至 注释 % % % 断点 运行
打印 查找 缩进 编辑 断点
文件 导航 编辑 断点
my_RSAoutput.m
1 %%RSA算法加密
2 function my_RSAoutput(key1)
3 disp('您输入的明文字符串如下:');
4 disp(key1);
5 length_key1=length(key1);%求字符串长度
6 key=[];%用于放置分割后的明文
7 m=1;
8 j=1;
9 for i=1:j:length_key1%分割明文, 拆分成单个字符
10 key(m)=abs(key1(i));%明文的字母换成ASCII的十进制数
11 m=m+1;
12 end
13 [p,q,n,Q,e,d]=rsa_pq();
14 rsal=rsa_encrypt(key,e,n);
15 end
```

运行结果:

```
>> my_RSAoutput('lijiaxing')
您输入的明文字符串如下:
lijiaxing
-----RSA算法开始执行-----
正在随机生成p,q,n,Q,e,d
p=71 q=53 n=3763 Q=3640 e=29 d=3389
李家兴的RSA加密算法:
明文为:
    108    105    106    105    97    120    105    110    103

密文为:
列 1 至 6

    1741         105        2279         105        1020        2503

列 7 至 9

    105        1601        2730
```



上海工程技术大学

实 验 报 告

姓名 班级 学号 实验日期

课程名称 数字内容安全 指导教师 成绩

四、实验总结/心得

(1)、通过本次实验，我掌握了 RSA 加密算法，其主要过程是：

- 1、随机选定两个互异的大素数 p, q
- 2、计算公共模数 $n = p \times q$
- 3、计算模数 n 的欧拉函数 $\phi(n) = (p-1) \times (q-1)$
- 4、选定一个正整数 e ，使 $e \in (1, \phi(n))$ ，且 e 与 $\phi(n)$ 互质
- 5、求出正数 d ，使其满足 $d \times e = 1 \bmod \phi(n)$ ，则将 (n, d) 作为私钥，最后，对于明文 M ，由 $C = M^e \bmod n$ ，得到密文 C 。

(2)、RSA 加密算法对字节数是有一定要求的。(网上查是不能超过 117 字节)

(3)、对于输入的明文字符串首先要进行拆分，并将拆分后的单个字符转换成 ASCII 码。最好加入判断是否存在无效字符的代码。

(4)、RSA 加密算法中往往具有用户自定义设置部分，解密时 also 需要注意相应部分的转化。