

《密码学》课程设计实验报告

实验序号：07

实验项目名称：公钥密码

| | | | | | |
|------|-----------------|------|-----|------|-------------|
| 学 号 | | 姓 名 | | 专业、班 | 18 信安 3-4 班 |
| 实验地点 | 网安基地新珈楼 B308 | 指导教师 | 王张宜 | 时间 | 2020.11.24 |

一、 实验目的及要求

实验目的：

- (1) 掌握公钥密码的概念和基本工作方式；
- (2) 掌握 RSA 密码、ElGamal 密码和椭圆曲线密码的原理与算法；
- (3) 了解 RSA 密码、ElGamal 密码和椭圆曲线密码的安全性；
- (4) 了解 RSA 密码、ElGamal 密码和椭圆曲线密码的应用。

实验要求：

- (1) 掌握 RSA 密码的实现方案；
- (2) 掌握 ElGamal 密码的实现方案；
- (3) 掌握椭圆曲线密码的实现方案；
- (4) 了解公钥算法实现中的相关优化算法。

二、实验设备（环境）及要求

Windows 操作系统，高级语言开发环境

三、实验内容与步骤

1. RSA 密码

(1) RSA 加解密算法

- ①随机地选择两个大素数 p 和 q ，而且保密；
- ②计算 $n=pq$ ，将 n 公开；
- ③计算 $\varphi(n)=(p-1)(q-1)$ ，对 $\varphi(n)$ 保密；
- ④随机地选取一个正整数 e ， $1 < e < \varphi(n)$ 且 $(e, \varphi(n)) = 1$ ，将 e 公开；
- ⑤根据 $ed \equiv 1 \pmod{\varphi(n)}$ ，求出 d ，并对 d 保密；
- ⑥加密运算：

$$C = M^e \pmod{n} \quad (7-4)$$

- ⑦解密运算：

$$M = C^d \pmod{n} \quad (7-5)$$

(2) 求逆算法:

欧几里得迭代求逆算法

求 $a^{-1} \bmod p, (0 < a < p)$

令 $R_1 = p, R_2 = a$, 计算:

$$R_1 = R_2 \square Q_2 + R_3$$

$$R_2 = R_3 \square Q_3 + R_4$$

.....

$$R_{n-1} = R_n \square Q_n + 1$$

其中每步中的商 Q_i 为整数, 余数满足 $0 \leq R_i < R_{i-1}$

令 $S_0 = 0, S_1 = 1$, 计算:

$$S_i = S_{i-2} - S_{i-1} \square Q_i$$

$$S_n \text{ 即为 } a^{-1} \bmod p$$

参考实现 (伪码)

算法 1 利用扩展 Euclidean 算法求 \mathbb{F}_p 上的逆

输入: 素数 p 和 $a \in [0, P-1]$;

输出: $a^{-1} \bmod p$;

1、 $u \leftarrow a, b \leftarrow p$;

2、 $x_1 \leftarrow 1, x_2 \leftarrow 0$;

3、 当 $u \neq 1$ 重复进行

3.1 $q \leftarrow \lfloor v/u \rfloor$ //商

3.2 $r \leftarrow v - qu$ //余数

3.3 $x \leftarrow x_2 - qx_1$; // $S[i] = S[i-2] - S[i-1] * Q_i$

3.4 $v \leftarrow u$ //把除数作为新的被除数

3.5 $u \leftarrow r$ //把余数作为新的除数

3.6 $x_2 \leftarrow x_1$ //更新 $S[i-2]$

3.7 $x_1 \leftarrow x$; //更新 $S[i-1]$

4、 返回 $(x_1 \bmod p)$ 。 //返回 $x_1 \bmod p$

(3) 快速乘方运算

反复平方乘算法（教材 p221）

设要计算 $c=a^b \bmod n$ 。

```
c ← 0; f ← 1
for i ← k downto 0
  do c ← 2 × c
    f ← (f × f) mod n
  if bi = 1
    then c ← c + 1
      f ← (f × a) mod n
return f
```

注：整数 b 表示为二进制 $b_kb_{k-1}\dots b_0$ 。

例如：

表 9.4 计算 $a^b \bmod n$ 的快速模幂算法, 其中 $a=7, b=560=100110000, n=561$

| i | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|-------|---|----|-----|-----|-----|-----|-----|-----|-----|-----|
| b_i | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| c | 1 | 2 | 4 | 8 | 17 | 35 | 70 | 140 | 280 | 560 |
| d | 7 | 49 | 157 | 526 | 160 | 241 | 298 | 166 | 67 | 1 |

算法 2 计算点乘的从右向左的二进制方法

输入: $k=(k_{t-1}, \dots, k_2, k_1, k_0)_2, P \in E(\mathbb{F}_q)$;

输出: kP ;

- 1、 $Q \leftarrow \infty$;
- 2、对于 i 从 0 到 $t-1$ 重复执行
 - 2.1 如果 $k_i=1$ 则 $Q \leftarrow Q+P$;
 - 2.2 $P \leftarrow 2P$;
- 3、返回 (Q) 。

算法 3 计算点乘的从左向右的二进制方法

输入: $k=(k_{t-1}, \dots, k_2, k_1, k_0)_2, P \in E(\mathbb{F}_q)$;

输出: kP ;

- 1、 $Q \leftarrow \infty$;
- 2、对于 i 从 $t-1$ 到 0 重复执行
 - 2.1 $Q \leftarrow 2Q$;
 - 2.2 如果 $k_i=1$ 则 $Q \leftarrow Q+P$;
- 3、返回 (Q) 。

实验（1） 令 $p=3, q=11, d=7, m=5$, 手工或编程计算密文 C 。

实验（2） 设 RSA 密码的 $e=3, n=33, C=9$, 手工或编程计算明文 M 。

实验（3） 令 $p=17, q=11, e=7$, 试计算 RSA 密码其余参数。

进一步对于 $m=88$, 计算密文 C 。

2. ELGamal 密码（参见教材 p219）

例： 设 $p=19, m=17$, 构造一个 ELGamal 密码，并用它对 m 加密。

对于 $p=19$, 原根有 $\{2, 3, 10, 13, 14, 15\}$, 任选其中之一作为模 19 的本原元（生成元），如选择 $\alpha = 10$

步骤 1: 密钥生成

用户随机地选择一个整数 d 作为自己的秘密的解密密钥， $1 < d < p-1$, 计算 $y \equiv \alpha^d \pmod{p}$, 取 y 为自己的公开的加密钥。例如选择 $d = 5$, $y = \alpha^d \pmod{p} = 10^5 \pmod{19} = 3$, 即私钥为 5, 公钥为 3.

步骤 2: 加密过程

将明文消息 M ($0 \leq M \leq p-1$) 加密成密文的过程如下:

① 随机地选取一个整数 k , $1 \leq k \leq p-1$. 例如随机选择 $k = 6$

② 计算

$$U = y^k \pmod{p} = 3^6 \pmod{19} = 729 \pmod{19} = 7 \quad (7-8)$$

$$C_1 = \alpha^k \pmod{p} = 10^6 \pmod{19} = 11 \quad (7-9)$$

$$C_2 = UM \pmod{p} = 7 \times 17 \pmod{19} = 5 \quad (7-10)$$

③ 取 $(C_1, C_2) = (11, 5)$ 作为的密文。

步骤 3: 解密过程

将密文 (C_1, C_2) 解密的过程如下:

① 计算

$$V = C_1^d \pmod{p} = 11^5 \pmod{19} = 161051 \pmod{19} = 7 \quad (7-11)$$

② 计算

$$M = C_2 V^{-1} \pmod{p} = 5 \times 11 \pmod{19} = 55 \pmod{19} = 17 \quad (7-12)$$

实验（4） 设 $p=5, m=3$, 构造一个 ELGamal 密码，并用它对 m 加密。

3.椭圆曲线密码（选作）

（1）GF(p)上的椭圆曲线

实验（5） 取 $p=23$, 求出椭圆曲线 $y^2=x^3+x+1$ 的全部解点。（选作）

表 10.1 椭圆曲线 $E_{23}(1,1)$ 上的点

| | | |
|--------|---------|---------|
| (0,1) | (6,4) | (12,19) |
| (0,22) | (6,19) | (13,7) |
| (1,7) | (7,11) | (13,16) |
| (1,16) | (7,12) | (17,3) |
| (3,10) | (9,7) | (17,20) |
| (3,13) | (9,16) | (18,3) |
| (4,0) | (11,3) | (18,20) |
| (5,4) | (11,20) | (19,5) |
| (5,19) | (12,4) | (19,18) |

（2）椭圆曲线密码

理解并实现 SM2 算法加解密过程。（教材 p239）

四、实验结果与数据处理

五、分析与讨论

六、教师评语

签名：
日期：

成绩

(必做) 实验 (1) 令 $p=3, q=11, d=7, m=5$, 手工或编程计算密文 C 。(表格数据均为 10 进制)

| 姓名 | 密钥参数组 | | | | | | 明文 | 密文 |
|-------------------|-------|------|---------|---------------|------|----------|--------|------|
| | 素数 P | 素数 Q | $N=P*Q$ | $(P-1)*(Q-1)$ | 公钥 e | 私钥 d | 明文 M | 密文 C |
| 2017301510027 李兆恒 | 1979 | 3719 | | | | 2609921 | 965579 | |
| 2016301500207 肖亦晓 | 3023 | 2857 | | | | 8492599 | 617267 | |
| 2016301500241 杨燚锂 | 3547 | 2531 | | | | 5673067 | 852979 | |
| 2017301500191 吴润泽 | 1237 | 1231 | | | | 872827 | 251819 | |
| 2017301500330 陈 磊 | 2029 | 3137 | | | | 1762939 | 299889 | |
| 2018302060248 张培铭 | 2083 | 1709 | | | | 239353 | 536865 | |
| 2018302070001 沈思源 | 1831 | 1607 | | | | 1582283 | 676155 | |
| 2018302070131 湛金垚 | 3623 | 3517 | | | | 9661301 | 307714 | |
| 2018302080167 王智超 | 1871 | 2939 | | | | 3457967 | 617721 | |
| 2018302110381 李江旭 | 1741 | 3307 | | | | 2789137 | 540810 | |
| 2018302180056 鲁震豪 | 2143 | 2143 | | | | 945367 | 898236 | |
| 2018302180057 王晨旭 | 2551 | 1669 | | | | 131201 | 369282 | |
| 2018302180059 梅润元 | 2087 | 4019 | | | | 8205145 | 593438 | |
| 2018302180060 吴逸豪 | 3571 | 1373 | | | | 4641817 | 307301 | |
| 2018302180062 翁 斌 | 3221 | 3631 | | | | 4803107 | 182861 | |
| 2018302180063 袁浩天 | 3319 | 3631 | | | | 770873 | 952769 | |
| 2018302180064 张展鹏 | 1873 | 2657 | | | | 2752177 | 483387 | |
| 2018302180067 李星辰 | 1151 | 1103 | | | | 1182901 | 687865 | |
| 2018302180068 陈亚楠 | 1789 | 2857 | | | | 2929607 | 559175 | |
| 2018302180069 郭点点 | 3373 | 1999 | | | | 1086487 | 146995 | |
| 2018302180070 程昊天 | 1637 | 3779 | | | | 1125151 | 2511 | |
| 2018302180073 郭梦卓 | 2707 | 4013 | | | | 10513457 | 471666 | |
| 2018302180077 郑津哲 | 2087 | 4129 | | | | 8284459 | 230084 | |
| 2018302180079 王怡静 | 2141 | 1543 | | | | 870211 | 621810 | |
| 2018302180083 王丹君 | 1669 | 4003 | | | | 1413587 | 689252 | |
| 2018302180084 倪迩畅 | 1307 | 3331 | | | | 3617219 | 263108 | |
| 2018302180085 张思远 | 2237 | 2851 | | | | 3100727 | 118797 | |
| 2018302180086 严诚逸 | 2539 | 3533 | | | | 3177487 | 999823 | |
| 2018302180087 李宁馨 | 1031 | 4049 | | | | 953951 | 258728 | |
| 2018302180088 周渴一 | 3511 | 1021 | | | | 911771 | 972699 | |
| 2018302180091 盛威龙 | 1277 | 3499 | | | | 4233809 | 653643 | |
| 2018302180097 易子嘉 | 3137 | 3259 | | | | 8046511 | 91422 | |
| 2018302180098 陈映江 | 1493 | 1163 | | | | 840355 | 444194 | |
| 2018302180099 郭瑞华 | 2711 | 3089 | | | | 5862031 | 421217 | |

| | | | | | | | | |
|-------------------|------|------|--|--|--|----------|--------|--|
| 2018302180151 邱振芳 | 2423 | 4093 | | | | 5892583 | 291178 | |
| 2018302180154 许 可 | 1621 | 1847 | | | | 987917 | 493070 | |
| 2018302180160 唐炜钦 | 3251 | 4049 | | | | 1263519 | 826789 | |
| 2018302180163 李金峰 | 2339 | 2663 | | | | 5389 | 557142 | |
| 2018302180166 梅荣新 | 2339 | 2389 | | | | 1710061 | 277565 | |
| 2018302180168 徐搏鸿 | 1489 | 2293 | | | | 2506577 | 48881 | |
| 2018302180169 叶嘉昕 | 1489 | 2699 | | | | 1112657 | 153553 | |
| 2018302180174 汪 毓 | 1301 | 3821 | | | | 2999541 | 787378 | |
| 2018302180176 蔡文颂 | 1201 | 1291 | | | | 917923 | 148237 | |
| 2018302180179 陈思涵 | 1091 | 1187 | | | | 988239 | 675486 | |
| 2018302180181 潘昱霏 | 3347 | 1999 | | | | 1659695 | 643737 | |
| 2018302180183 曾一帆 | 1487 | 1489 | | | | 1202227 | 921251 | |
| 2018302180184 林玉龙 | 2207 | 2423 | | | | 4482129 | 465844 | |
| | | | | | | | | |
| | 1367 | 3109 | | | | 1797139 | 934952 | |
| | 3467 | 1997 | | | | 510349 | 545863 | |
| | 3593 | 3457 | | | | 11249423 | 733564 | |
| | 1619 | 1567 | | | | 2037383 | 636922 | |
| | 2309 | 3851 | | | | 15473 | 466969 | |
| | 1999 | 2377 | | | | 432787 | 439362 | |
| | 3541 | 2687 | | | | 5875841 | 637989 | |
| | 1097 | 2131 | | | | 28523 | 582968 | |
| | 3461 | 1063 | | | | 3653767 | 324080 | |
| | | | | | | | | |

| | | | | | | | | |
|----|------|------|----------|----------|-------|---------|--------|----------|
| 例题 | 3637 | 2593 | 9430741 | 9424512 | 11083 | 3556195 | 636199 | 379840 |
| | 3943 | 2741 | 10807763 | 10801080 | 11087 | 9864863 | 203814 | 3554314 |
| | 1663 | 1367 | 2273321 | 2270292 | 10091 | 86843 | 904653 | 1743554 |
| | 2777 | 2309 | 6412093 | 6407008 | 10559 | 669887 | 561373 | 196331 |
| | 3251 | 2039 | 6628789 | 6623500 | 10799 | 5396199 | 245758 | 1443563 |
| | 2693 | 3637 | 9794441 | 9788112 | 11447 | 3030407 | 917572 | 5600009 |
| | 2351 | 2273 | 5343823 | 5339200 | 11897 | 5234633 | 107708 | 2372442 |
| | 2441 | 2789 | 6807949 | 6802720 | 10711 | 2071111 | 71232 | 3179726 |
| | 1013 | 3121 | 3161573 | 3157440 | 11801 | 685481 | 758720 | 2752692 |
| | 3923 | 2003 | 7857769 | 7851844 | 11083 | 5606031 | 158414 | 7805049 |
| | 1907 | 1867 | 3560369 | 3556596 | 11549 | 2143997 | 47072 | 1127299 |
| | 3989 | 2207 | 8803723 | 8797528 | 11831 | 8308983 | 953986 | 7338595 |
| | 1913 | 1459 | 2791067 | 2787696 | 10501 | 1771213 | 190490 | 1919001 |
| | 3307 | 3637 | 12027559 | 12020616 | 10141 | 8909077 | 126383 | 10977697 |

实验（2）设 RSA 密码的 $e=3, n=33, C=9$ ，手工或编程计算明文 M 。

| 姓名 | 密钥参数组 | | | | | | 明文 | 密文 |
|-------------------|---------|---------|----------|---------------|-----------|--------|------|----------|
| | 素数 P | 素数 Q | $N=P*Q$ | $(P-1)*(Q-1)$ | 公钥 e | 私钥 d | 明文 M | 密文 C |
| 2017301510027 李兆恒 | | | 7651307 | | 10627 | | | 1551242 |
| 2016301500207 肖亦晓 | | | 3869339 | | 11887 | | | 842001 |
| 2016301500241 杨燊锂 | | | 2180609 | | 10391 | | | 1516068 |
| 2017301500191 吴润泽 | | | 6604259 | | 10891 | | | 6270152 |
| 2017301500330 陈 磊 | | | 10047497 | | 11113 | | | 5291065 |
| 2018302060248 张培铭 | | | 4811143 | | 10099 | | | 2607825 |
| 2018302070001 沈思源 | | | 2529629 | | 10861 | | | 2346717 |
| 2018302070131 湛金垚 | | | 3482863 | | 10847 | | | 2419589 |
| 2018302080167 王智超 | | | 5812817 | | 10589 | | | 1965023 |
| 2018302110381 李江旭 | | | 6088391 | | 11003 | | | 4477076 |
| 2018302180056 鲁震豪 | | | 3896771 | | 10009 | | | 1846991 |
| 2018302180057 王晨旭 | | | 2471789 | | 10301 | | | 1675691 |
| 2018302180059 梅润元 | | | 4730113 | | 11833 | | | 1965990 |
| 2018302180060 吴逸豪 | | | 6210293 | | 11393 | | | 3881554 |
| 2018302180062 翁 斌 | | | 3605177 | | 10337 | | | 243839 |
| 2018302180063 袁浩天 | | | 9026009 | | 11287 | | | 4899462 |
| 2018302180064 张展鹏 | | | 5584547 | | 11821 | | | 1942584 |
| 2018302180067 李星辰 | | | 2972657 | | 10639 | | | 1990651 |
| 2018302180068 陈亚楠 | | | 2159161 | | 11519 | | | 1648892 |
| 2018302180069 郭点点 | | | 3781787 | | 11279 | | | 1049161 |
| 2018302180070 程昊天 | | | 3659377 | | 11399 | | | 3258522 |
| 2018302180073 郭梦卓 | | | 5620921 | | 11447 | | | 1935755 |
| 2018302180077 郑津哲 | | | 14378579 | | 10909 | | | 12508006 |
| 2018302180079 王怡静 | | | 8208029 | | 10559 | | | 3338520 |
| 2018302180083 王丹君 | | | 1322353 | | 11779 | | | 551036 |
| 2018302180084 倪迹畅 | | | 6316991 | | 10729 | | | 4671414 |
| 2018302180085 张思远 | | | 8170429 | | 11149 | | | 6409320 |
| 2018302180086 严诚逸 | | | 11229487 | | 10433 | | | 3345397 |
| 2018302180087 李宁馨 | | | 7373437 | | 11273 | | | 5291971 |
| 2018302180088 周渴一 | | | 4711643 | | 11311 | | | 979814 |
| 2018302180091 盛威龙 | | | 3135149 | | 11087 | | | 307677 |
| 2018302180097 易子嘉 | | | 9565973 | | 11329 | | | 4385268 |
| 2018302180098 陈映江 | | | 6553627 | | 10627 | | | 2479710 |

| | | | | | | | | |
|-------------------|--|--|----------|--|-------|--|--|---------|
| 2018302180099 郭瑞华 | | | 10177841 | | 10303 | | | 8143046 |
| 2018302180151 邱振芳 | | | 3457379 | | 11159 | | | 642530 |
| 2018302180154 许 可 | | | 6507013 | | 11321 | | | 4962433 |
| 2018302180160 唐炜钦 | | | 2839423 | | 10631 | | | 1881046 |
| 2018302180163 李金峰 | | | 4145563 | | 10253 | | | 623813 |
| 2018302180166 梅荣新 | | | 6626449 | | 10141 | | | 5830220 |
| 2018302180168 徐搏鸿 | | | 5649929 | | 10369 | | | 4641677 |
| 2018302180169 叶嘉昕 | | | 1728401 | | 10259 | | | 834397 |
| 2018302180174 汪 毓 | | | 5349559 | | 10709 | | | 353593 |
| 2018302180176 蔡文颂 | | | 6234961 | | 10267 | | | 2488229 |
| 2018302180179 陈思涵 | | | 4769483 | | 11329 | | | 1303258 |
| 2018302180181 潘昱霏 | | | 4338149 | | 11287 | | | 3408129 |
| 2018302180183 曾一帆 | | | 1393429 | | 11113 | | | 82176 |
| 2018302180184 林玉龙 | | | 2734073 | | 10169 | | | 208794 |
| | | | | | | | | |
| | | | 6151487 | | 10487 | | | 5433845 |
| | | | 6600967 | | 10861 | | | 3325838 |
| | | | 9789763 | | 11447 | | | 3334724 |
| | | | 3840553 | | 11273 | | | 3137384 |
| | | | 4686391 | | 10079 | | | 1020672 |
| | | | 5929519 | | 11467 | | | 4847568 |
| | | | 6682271 | | 10009 | | | 4628089 |
| | | | 4609961 | | 10331 | | | 2074434 |
| | | | 2577277 | | 11717 | | | 1868939 |
| | | | | | | | | |

| | | | | | | | | |
|----|------|------|----------|----------|-------|---------|--------|----------|
| 例题 | 2909 | 3847 | 11190923 | 11184168 | 11833 | 344041 | 431790 | 2283161 |
| | 3779 | 2689 | 10161731 | 10155264 | 10093 | 7101541 | 575678 | 10056465 |
| | 2953 | 3083 | 9104099 | 9098064 | 10039 | 8261575 | 257668 | 5102872 |
| | 3643 | 3823 | 13927189 | 13919724 | 10321 | 1954237 | 797086 | 11611366 |
| | 1237 | 2749 | 3400513 | 3396528 | 10979 | 1980251 | 195040 | 2754682 |
| | 1621 | 3539 | 5736719 | 5731560 | 11057 | 4985633 | 942830 | 1294555 |
| | 1907 | 1879 | 3583253 | 3579468 | 11447 | 643535 | 296209 | 1309838 |
| | 3863 | 2243 | 8664709 | 8658604 | 10159 | 6756251 | 671662 | 6381782 |
| | 2999 | 2593 | 7776407 | 7770816 | 11833 | 1464457 | 91360 | 5861731 |
| | 2161 | 3433 | 7418713 | 7413120 | 10771 | 5090971 | 280224 | 6383798 |
| | 2237 | 3881 | 8681797 | 8675680 | 10427 | 7069843 | 101523 | 2167066 |
| | 3019 | 3433 | 10364227 | 10357776 | 10391 | 7539815 | 506695 | 6398397 |