《密码学》课程设计实验报告

实验序号：08　　实验项目名称：数字签名

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) 掌握数字签名的概念；

(2) 掌握基于RSA密码、ElGamal密码和椭圆曲线密码的数字签名方法；

(3) 了解基于RSA密码、ElGamal密码和椭圆曲线密码的数字签名的安全性；

(4) 熟悉盲签名的原理，了解盲签名的应用。

实验要求：

(1) 掌握RSA数字签名的实现方案；

(2) 掌握ElGamal数字签名的实现方案；

(3) 掌握SM2椭圆曲线数字签名的实现方案；

(4) 了解数字签名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. 编程实现RSA数字签名方案

参数准备阶段：同实验07中的RSA密码算法

签名运算：

$$S = M^d \mod n \qquad (8\text{-}5)$$

验证签名运算（判断式）：

$$M = S^e \mod n \qquad (8\text{-}6)$$

实验1：采用实验06中的RSA密码算法的相关参数，对于M进行签名及验证。

思考1：RSA数字签名方案的几种攻击方法

思考2：基于RSA数字签名的盲签名方案的实现

2. 编程实现ELGamal数字签名方案

复习数论的一个结论。对于素数q，如果α是q的原根，则有：$\alpha,\alpha^2,...,\alpha^{q-1}$ 取模(mod q)后各不相同。因此如果α是q的原根，进一步有：

1. 对于任意整数m，$\alpha^m \equiv 1(\mathrm{mod}\, q)$当且仅当$m \equiv 0(\mathrm{mod}\, q-1)$

2. 对于任意整数i，j，$\alpha^i \equiv \alpha^j(\mathrm{mod}\, q)$当且仅当$i \equiv j(\mathrm{mod}\, q-1)$

同ELGamal加密方案一样，ELGamal数字签名方案的基本元素是素数p和α，其中α是p的原根。用户A通过如下步骤产生公钥/私钥对：

1. 生成随机整数X_A，使得$1 < X_A < p-1$。

2. 计算$Y_A = \alpha^{X_A} \bmod p$。

A的私钥是X_A；A的公钥是$\{p,\alpha,Y_A\}$。

例：设p=19，m=14,构造一个ELGamal数字签名方案，并用它对m签名。

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x作为自己的秘密的解密钥，1<x<p-1，计算$y \equiv \alpha^x \bmod p$，取y为自己的公开的加密钥。例如选择$x = 16$，$y = \alpha^d \bmod p = 10^5 \bmod 19 = 4$，即私钥为16，公钥为4.

步骤2：**签名过程**

将明文消息M（0≤M≤p-1)加密成密文的过程如下：

① 随机地选取一个整数k，k与p-1互素且1≤k≤p-1。例如随机选择$k = 5$

② 计算$r = \alpha^k \bmod p = 10^5 \bmod 19 = 3$

$$s = (m - xr)k^{-1} \bmod p - 1 = (14 - 16 \times 3) \times 5^{-1} \bmod 18 = 2 \times 11 \bmod 18 = 4$$

③ 取（r，s）=（3,4）作为m=14的签名。

步骤3：**验证过程**

对签名（r，s）验证的过程如下：

① 计算$V_1 = \alpha^m \bmod p = 10^{14} \bmod 19 = 16$

② 计算$V_2 = y^r r^s \bmod p = 4^3 \times 3^4 \bmod 19 = 7 \times 5 \bmod 19 = 16$

由于$V_1 = V_2$，所以签名是合法的。

实验2：采用实验07中的ELGamal密码算法的相关参数，对于M进行签名及

验证。

实验 3：任意选作教材 p254 表 8-1 中的数字签名的变形算法，对于 M 进行签名及验证。

实验 4：设 $r=\alpha^k \bmod p$，根据签名算法的一般形式 $Ak=B+Cx \bmod p-1$，以及对应的验证算法的一般形式 $r^A=\alpha^C y^B \bmod p$，自己尝试设计新的基于离散对数的数字签名方案，并对于 M 进行签名及验证。（选作）

3. 编程实现 SM2 椭圆曲线数字签名方案（选作）

思考 1：椭圆曲线加密、签名的快速实现；

提示 1：模参数、曲线参数的选取优化；

提示 2：点加和倍点运算的快速实现；

思考 2：k=15 时，kP 运算次数

反复平方乘 31P=$[11111]_2$P=2(2（2（2P+P）+P）+P)+P，共 4 次加法、4 次倍加

改进编码 31P=（25-1）P=2(2(2(2(2P))))-P，需要 5 次倍加，1 次加法（减法）

四、实验结果与数据处理

五、分析与讨论

六、教师评语	成绩
签名： 日期：	

椭圆曲线参数 $y^2=x^3+3x+2 \bmod 2017$ （即 p=2017，a=3，b=2）

姓名	点加运算			多倍点（标量）运算		
	点 P	点 Q	P+Q	点 P	倍数 k	kP
2017301510027 李兆恒	(746,90)	(2001,500)		(26,479)	1487	
2016301500207 肖亦晓	(1898,217)	(1280,354)		(322,1557)	1589	
2016301500241 杨燏锂	(1938,138)	(1916,713)		(438,94)	1603	
2017301500191 吴润泽	(516,1844)	(220,1786)		(752,814)	142	
2017301500330 陈 磊	(1144,1888)	(361,21)		(1637,1910)	228	
2018302060248 张培铭	(136,113)	(1042,435)		(1424,660)	1614	
2018302070001 沈思源	(781,1583)	(1863,518)		(1291,1442)	856	
2018302070131 谌金垚	(1379,366)	(204,756)		(1332,504)	123	
2018302080167 王智超	(1303,1362)	(341,331)		(759,255)	315	
2018302110381 李江旭	(1561,84)	(901,1217)		(1614,881)	413	
2018302180056 鲁震豪	(1474,1964)	(724,1175)		(1623,1415)	1191	
2018302180057 王晨旭	(1238,1514)	(286,1673)		(118,320)	660	
2018302180059 梅润元	(581,1844)	(326,1367)		(1079,1536)	1161	
2018302180060 吴逸豪	(1975,925)	(917,505)		(29,318)	450	
2018302180062 翁 斌	(932,776)	(589,986)		(1657,827)	1643	
2018302180063 袁浩天	(1677,1160)	(494,279)		(1646,22)	569	
2018302180064 张展鹏	(100,1608)	(513,1182)		(795,97)	1664	
2018302180067 李星辰	(22,1677)	(569,785)		(274,1801)	286	
2018302180068 陈亚楠	(49,1386)	(1102,1422)		(1432,1972)	112	
2018302180069 郭点点	(761,1512)	(538,258)		(49,631)	346	
2018302180070 程昊天	(1071,174)	(831,1788)		(662,1969)	1646	
2018302180073 郭梦卓	(1362,1704)	(67,221)		(632,651)	113	
2018302180077 郑津哲	(872,1441)	(1106,999)		(1651,402)	1801	
2018302180079 王怡静	(1662,1983)	(665,1933)		(303,937)	119	
2018302180083 王丹君	(1881,116)	(1172,622)		(405,140)	295	
2018302180084 倪迩畅	(1328,333)	(290,1037)		(964,1413)	1505	
2018302180085 张思远	(118,320)	(1206,962)		(37,1062)	820	
2018302180086 严诚逸	(1910,1417)	(1744,1663)		(585,458)	431	
2018302180087 李宁馨	(205,293)	(1082,1952)		(1954,1513)	728	
2018302180088 周渴一	(2001,500)	(1837,1358)		(1830,37)	363	
2018302180091 盛威龙	(972,911)	(184,1224)		(831,1788)	859	
2018302180097 易子嘉	(30,1162)	(539,1358)		(1297,210)	782	
2018302180098 陈映江	(1021,849)	(688,63)		(1209,1437)	1410	
2018302180099 郭瑞华	(1162,1757)	(1415,359)		(942,741)	428	
2018302180151 邱振芳	(1720,1336)	(1431,1615)		(834,1922)	928	

2018302180154 许 可	(543,1749)	(1547,113)		(262,394)	995	
2018302180160 唐炜钦	(208,1566)	(1554,102)		(321,136)	1812	
2018302180163 李金峰	(427,60)	(1766,1944)		(1655,1045)	1742	
2018302180166 梅荣新	(734,520)	(1289,160)		(470,116)	1921	
2018302180168 徐搏鸿	(1827,1146)	(1840,576)		(345,1064)	342	
2018302180169 叶嘉昕	(406,1993)	(1681,1128)		(887,1046)	1006	
2018302180174 汪 毓	(1293,32)	(1209,580)		(1543,1293)	1571	
2018302180176 蔡文颂	(395,638)	(1830,1980)		(1740,49)	544	
2018302180179 陈思涵	(119,633)	(1552,1828)		(1695,522)	1529	
2018302180181 潘昱霏	(197,98)	(1242,737)		(576,1172)	360	
2018302180183 曾一帆	(1455,1478)	(650,1454)		(226,856)	686	
2018302180184 林玉龙	(65,81)	(2004,675)		(1130,1961)	9	
	(632,651)	(1743,604)		(1864,1416)	469	
	(333,991)	(733,996)		(1608,479)	1728	
	(428,1262)	(51,451)		(106,1685)	1847	
	(21,1266)	(1662,34)		(1359,722)	867	
	(520,1787)	(953,868)		(381,1845)	1354	
	(777,2012)	(590,42)		(1465,1071)	740	
	(1538,1291)	(879,1275)		(362,380)	1659	
	(802,753)	(1306,155)		(1662,1983)	1039	
	(50,851)	(405,1877)		(1334,437)	1834	
	(876,424)	(1354,1033)		(1916,1304)	1098	
	(1842,1885)	(1536,1028)		(51,451)	1479	
例题	(85,682)	(105,778)	(1608,479)	(1438,1542)	1147	(1752,1996)
	(1951,1197)	(706,1868)	(472,1549)	(1138,2008)	529	(795,97)
	(365,1535)	(1329,1456)	(949,873)	(534,617)	647	(1623,1415)
	(1620,178)	(852,298)	(1954,1513)	(1199,1410)	708	(536,543)
	(626,405)	(1714,140)	(1481,428)	(1414,414)	1942	(809,377)