同济大学
计算机科学与技术系

密码学课程设计实验报告

学　　号 **1751237**

姓　　名 张天然

专　　业 信息安全

授课老师 杨礼珍

日　　期 **2019.09.01**

一、 软件设计说明书

1） 程序构成：

各部分所需函数在头文件中进行声明和定义，主函数只负责调用函数完成相应的功能。

2） 功能模块说明：

RSA.h	//随机生成512bit的大素数p和q
	void get_p_q(ZZ& p, ZZ& q) {
	//完成Alice的操作：发送信息并进行数字签名
	void Alice(ZZ p, ZZ q, ZZ & n, ZZ & a, ZZ & b, ZZ & x, ZZ & y)
	//选择是否改变Alice信息中的内容
	void Oscar(ZZ & x, ZZ & y)
	//验证签名
	void Bob(ZZ n, ZZ b, ZZ x, ZZ y)

ElGamal.h	//生成大素数p、本原元aa和私钥a
	void createkeys(ZZ& p, ZZ& aa, ZZ& bb, ZZ& a)
	//完成Alice的操作：发送信息并进行数字签名
	void Alice(ZZ p, ZZ q, ZZ & n, ZZ & a, ZZ & b, ZZ & x, ZZ & y)
	//选择是否改变Alice信息中的内容
	void Oscar(ZZ & x, ZZ & y)
	
	//bob判断两次签名是否相同
	void Bob(ZZ & x, ZZ & r, ZZ & o, ZZ & p, ZZ & aa, ZZ & bb)

Verification.h	//将a扩展至b的位数，并取b的最高位
	ZZ zzcat(ZZ a, ZZ b)
	//生成两个大素数pq
	void get_p_q_3(ZZ & p, ZZ & q, int b = 0)
	//生成验证签名
	void create_sig_ver(ZZ p, ZZ q, ZZ & n, ZZ & a, ZZ & b, int bb = 0)
	//生成rsa验证需要的公钥和密钥
	void Rsa(ZZ & r_p, ZZ & r_q, ZZ & r_n, ZZ & r_a, ZZ & r_b, int b = 0)
	//生成elgamal签名需要的公钥密钥
	void ELGamal(ZZ & e_p, ZZ & e_aa, ZZ & e_bb, ZZ & e_a)
	//Alice发出消息并选择一种方式颁发证书
	void Alice(ZZ n, ZZ b, ZZ & r_p, ZZ & r_q, ZZ & r_n, ZZ & r_a, ZZ & r_b, ZZ & e_p, ZZ & e_aa, ZZ & e_bb, ZZ & e_a)

	//rsa验证
	bool Rsa_ver(ZZ r_x, ZZ r_y, ZZ r_n, ZZ r_b)
	//elgamal验证
	bool ELGamal_ver(ZZ & x, ZZ & r, ZZ & o, ZZ & p, ZZ & aa, ZZ & bb)
	//bob验证Alice的证书
	void Bob(ZZ & r_n, ZZ & r_b, ZZ & e_p, ZZ & e_aa, ZZ & e_bb)

PKI.h	未完成

二、 软件使用说明书

在main.cpp中运行程序，按照提示输入。

RSA：

不改变Alice发送的消息及签名：


C:\Users\zhang\source\repos\CryptoCourseDesign\Debug\CryptoCourseDesign.exe
RSA TEST
Alice
input news=10086
signature=876740702324576164740796544015123968347402645760911705460920246065752223078781667853626387
024794807008659705054639913080394091041850788032989185165248061813131652025129007902106124222596703 3
916345995791794144397515210636538919785093774456627440709240612281375692214133261856578504822756464 3
903381987693961437

Oscar
change news or signature(press 0 to give up)
news=0
signature=0

Bob
Bob get News=10086
signature=876740702324576164740796544015123968347402645760911705460920246065752223078781667853626387
024794807008659705054639913080394091041850788032989185165248061813131652025129007902106124222596703 3
916345995791794144397515210636538919785093774456627440709240612281375692214133261856578504822756464 3
903381987693961437
verification result:SUCCESS

改变Alice发送的消息：


C:\Users\zhang\source\repos\CryptoCourseDesign\Debug\CryptoCourseDesign.exe
RSA TEST
Alice
input news=10086
signature=137475082420538199200347605350339083618788527378911101087424423447736970476427176163288112
126784322883419977152740374450948801767222317708623454383122086336155669809332167652283345463626477 5
072077072851639177457837087979217588386010492911064315455774233630960320711960415946968100133978642 4
0725210579102543012

Oscar
change news or signature(press 0 to give up)
news=10001
signature=0

Bob
Bob get News=10001
signature=137475082420538199200347605350339083618788527378911101087424423447736970476427176163288112
126784322883419977152740374450948801767222317708623454383122086336155669809332167652283345463626477 5
072077072851639177457837087979217588386010492911064315455774233630960320711960415946968100133978642 4
0725210579102543012
verification result:FAILURE

ElGamal：

不改变Alice发送的消息和签名：

```
ElGamal TEST
_Alice_
Please input news=10086
result:
k:756139
r:1216508
o:202864

_Oscar_
chang News or Signature(press 0 to give up)
News=0
Signature_r=0
Signature_o=0

_Bob_
SUCCESS
```

改变Alice发送的消息：

```
ElGamal TEST
_Alice_
Please input news=10086
result:
k:1055571
r:407823
o:365205

_Oscar_
chang News or Signature(press 0 to give up)
News=10001
Signature_r=0
Signature_o=0

_Bob_
FAILURE
```

Verification：

Certification的内容由txt文件输入，Alice的id在程序中已设定。

RSA验证：

```
_Alice_
Rsa(press 0) Or ELGamal(press 1) To Make Your Certificate=0
Alice's id:43
Alice's ver_:43143103
Alice's s:116059393733752118712636026799
Alice's Certification:43143103-116059393733752118712636026799

_Bob_
Bob get the cert:43143103-116059393733752118712636026799
Bob's validation:SUCCESS
```

Elgamal验证：

（这一部分不完全正确所以并未显示完整）

```
_Alice_
Rsa(press 0) Or ELGamal(press 1) To Make Your Certificate=1
Alice's id:43
Alice's ver_:43143103
Alice's s:1446308_837711
Alice's Certification:43143103-1446308_837711
```