一、软件设计说明

1. 数据结构说明

下面列举所有数据类型，并说明其中的数据组成。简单起见，所有的类中，对成员函数和数据成员没有区分 Public、Private、Protected 权限。但是考虑实际情况，部分数据成员是不可以外部访问的，例如私钥、秘密指数等。

```
struct R_key
struct E_key
```

RSA / ElGamal 密钥组。其中包括：私钥组、私钥（私钥组元素拼接而成）、公钥组、公钥（公钥组元素拼接而成）。

```
class RSA
class ElGamal
```

RSA / ElGamal 类。包括：RSA / ElGamal 密钥组、密钥生成函数 void GenKey()、签名函数 void RSA_sig(ZZ x, ZZ &y) / void ElGamal_sig(ZZ x, ZZ &gamma, ZZ &delta)、签名验证函数 bool RSA_ver(ZZ x, ZZ y) / bool ElGamal_ver(ZZ x, ZZ gamma, ZZ delta)。

所有函数依照 RSA / ElGamal 签名协议编写，RSA 默认密钥长度 512 位，ElGamal 默认密钥长度 1024 位。

```
class user
```

用户类。包括：姓名、ID、签名方法选择、随机挑战选择、秘密指数及其公开值、证书（RSA 证书或 ElGamal 证书，由 TA 决定）、RSA 类、ElGamal 类。特别的，为了便于证书验证，证书中包含以下内容：ID || ver || s、ID || ver、s、秘密指数公开值。

```
class ta
```

可信权威机构类。包括：签名方法选择、RSA 类、ElGamal 类、生成用户 ID 函数 void GenID(user &p)、为用户颁布证书函数 void GenCert(user &p)、生成证书文件函数 void GenCertFile(user p)、为其他用户验证某一用户证书函数 bool Cert_ver(user p)。

用户 ID 中只包含姓名信息，为用户生成 ID 时，将其姓名转为大整数即可。

实际运用本类时，由于 PowerMod 函数的参数限制，可信权威机构的密钥长度应当长于用户的密钥长度，源代码中，可信权威机构的密钥长度是用户密钥长度的 4 倍。

颁布证书和验证证书完全依照协议 9.5 编写。

2. 功能模块说明

下面列举所有功能型函数和测试型函数，并具体说明功能和数据传输过程。

`bool is_prime(ZZ p, int n = 50)`

判断 p 是否是素数，利用 Miller-Rabin 算法测试，默认测试次数为 50 次，可以在调用时自行更改。

`void get_pri_root(ZZ &a, ZZ p,ZZ p0)`

获取 Zp*的原根，赋值到 a，其中，p=2*q0+1，依据定理：

定理 1.1: 如果$p>2$是素数，且$\alpha \in \mathbb{Z}_p^*$。那么$\alpha$是模$p$的本原元当且仅当

$$\alpha^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}, \text{对所有素数} q|p-1$$

`ZZ connect(ZZ a, ZZ b)`

拼接两个大整数，例如 connect(1234, 56789) 得到 123456789。

通过循环寻找到比大整数 b 大的一个最小的大整数 n，且这个大整数 n 必须是 10 的整数次幂，函数返回 a*n+b 即可。

`ZZ str_to_zz(string s)`

将字符串 s 转化为一个大整数。

将字符串视为一个 256 进制数，每一个字符所代表的十进制数值为该字符的 ASCII 码，用进制转换方法转成十进制即可。

（以下涉及到数据传输内容均为模拟，代码中没有具体体现数据传输）

`void RSA_test()`

RSA 测试函数。定义一个用户 Alice，其签名方法选择自动为 1（RSA 签名方案）。首先调用用户 Alice 的 RSA 密钥生成函数，这样 Alice 的 RSA 密钥组变量被赋值，之后调用 Alice 的 RSA 签名函数，利用密钥组的私钥为消息 x 签名得到 y。

`void ElGamal_test()`

ElGamal 测试函数。定义一个用户 Alice，其签名方法选择自动为 2（ElGamal 签名方案）。首先调用用户 Alice 的 ElGamal 密钥生成函数，这样 Alice 的 ElGamal 密钥组变量被赋值，

之后调用Alice的ElGamal签名函数,利用密钥组的私钥为消息x签名得到y,y中包括gamma和delta，共同构成签名。

void Cert_test()

证书颁布与验证测试函数。定义用户 Alice 和 Bob，定义可信权威机构 TA，让用户来选择 Alice 的签名方案，根据选择来生成 Alice 的密钥组。由用户选择 TA 的签名方案，根据选择来生成 TA 的密钥组。

由 TA 生成 Alice 的 ID，这样 Alice 中的 ID 元素被赋值，可以使用。由 TA 生成 Alice 的证书，颁布给 Alice，保存在 Alice 中，由 TA 来生成 Alice 的证书文件。

模拟数据传输,Bob获得了Alice的证书,实际代码中没有体现,只是Bob可以访问Alice中的证书数据,当然也可以是Bob可以打开TA生成的Alice的证书文件以获取Alice证书,我的代码中使用的方法是前者。Bob 向 TA 发出请求，利用 TA 提供的公钥和证书验证方法来验证 Alice 的证书。

void Interact_Cert_test()

交互认证测试函数。定义用户 Alice 和 Bob,定义可信权威机构 TA,让用户来选择 Alice 和 Bob 的签名方案，根据选择来生成 Alice 和 Bob 的密钥组。由用户选择 TA 的签名方案，根据选择来生成 TA 的密钥组。

首先，Bob 的相关操作：随机生成挑战 r1，让 TA 为其生成证书（包括生成 ID，生成证书）。随机挑战和证书均传给 Alice。

接下来，Alice 的相关操作：随机生成挑战 r2，让 TA 为其生成证书（包括生成 ID，生成证书），计算 y1。随机挑战、证书和 y1 均传给 Bob。

然后，又是 Bob 的相关操作：验证 Alice 的证书，验证 Alice 传来的 y1，选择接受与否，自己也计算 y2，将 y2 传给 Alice。

最后，又是 Alice 的相关操作：验证 Bob 的证书，验证 Bob 传来的 y2，选择接受与否。

void MTI_A0_test()

MTI/A0 密钥协商方案测试函数。为整个问题生成素数 p，和本原元 a，并得到常数 n。定义用户 U 和 V，定义可信权威机构 TA，让用户来选择 U 和 V 的签名方案，根据选择来生成 U 和 V 的密钥组。由用户选择 TA 的签名方案，根据选择来生成 TA 的密钥组。

首先，U 和 V 要生成各自的秘密指数，计算公开值，让 TA 为他们生成各自的证书（公开值加入证书），传输给对方，即二者均可访问到对方的证书和其中的公开值。

然后，U 和 V 选择各自的随机数 r，计算对应值 s，将 s 值传输给对方。

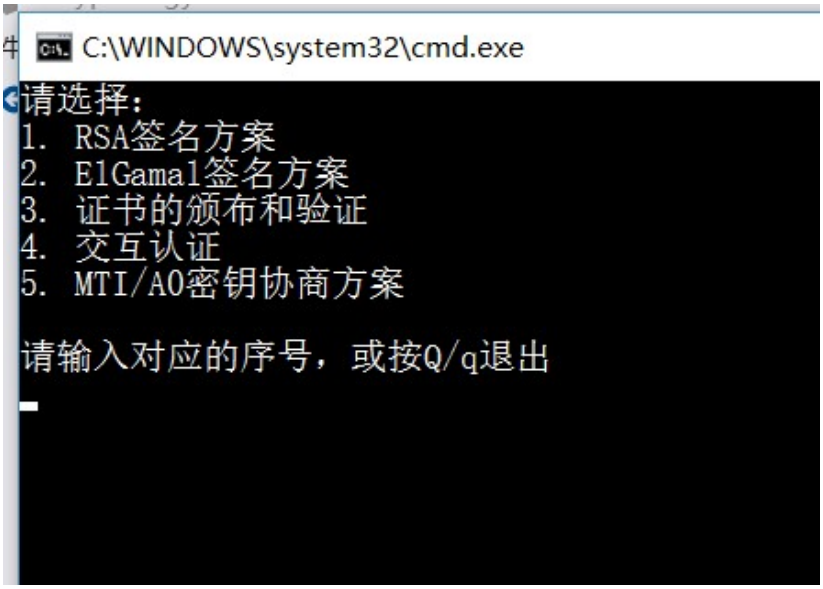
最后，U 和 V，利用所获得的对方的 s 值和证书中的公开值，计算会话密钥值，比对双

方各自算出的会话密钥是否相同。

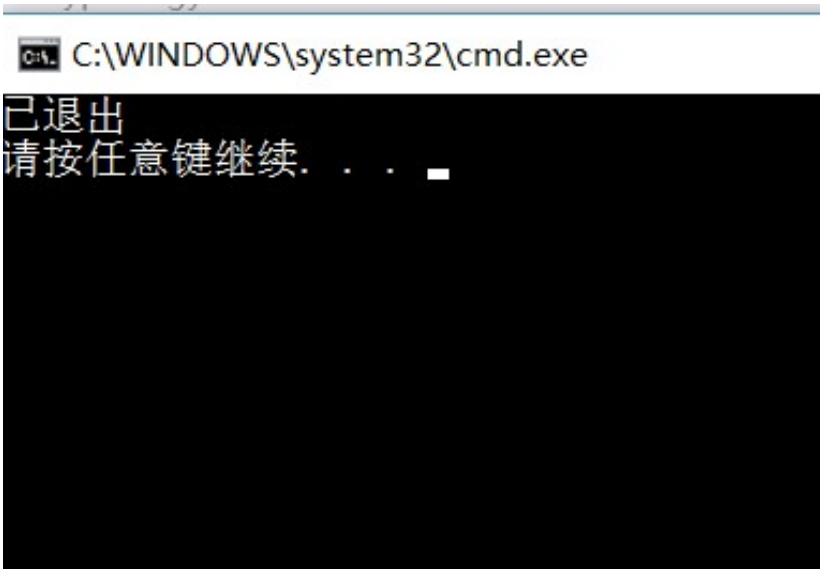
二、软件使用说明

输入格式及举例。为了方便调试，截图中的运行结果是在已经适当调整过密钥长度的条件下得到的，因为设置的密钥长度过长，会导致密钥生成和证书颁布的时间耗费极长，请耐心等待。

进入程序，界面如下；

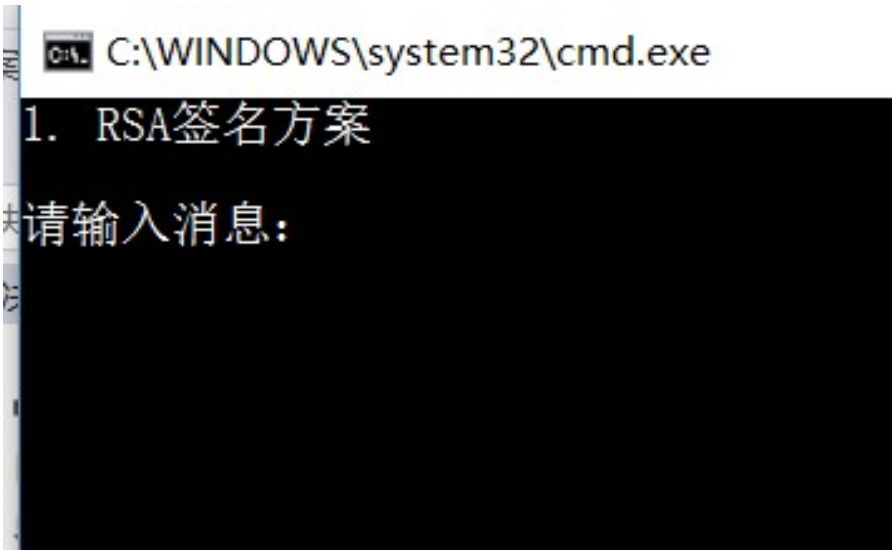


根据菜单栏指示，输入对应的序号进入对应的测试。如果不想继续，输入 Q 或 q 来退出。例如输入 q 后退出；

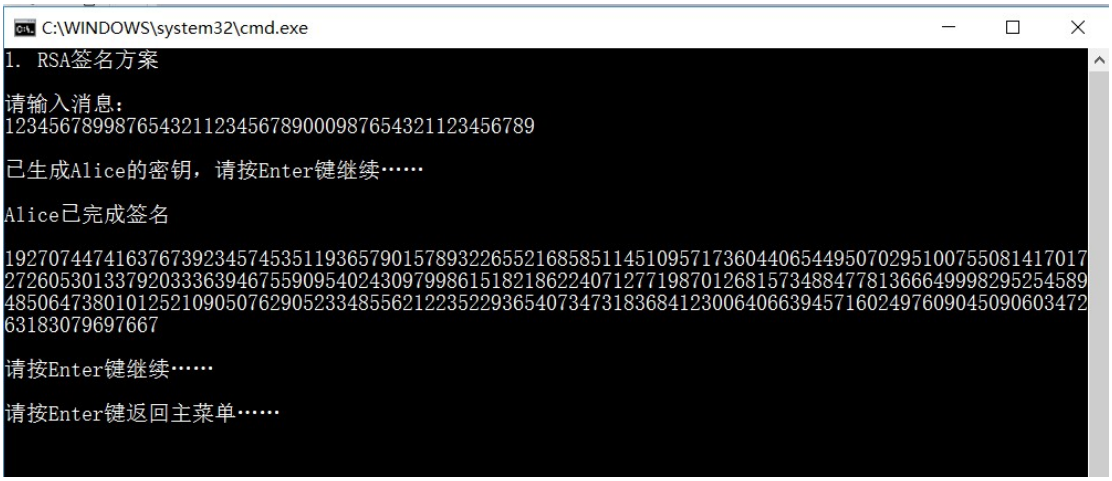


1. 当输入 1 后，进入 RSA 签名测试；

默认密钥长度：512 位



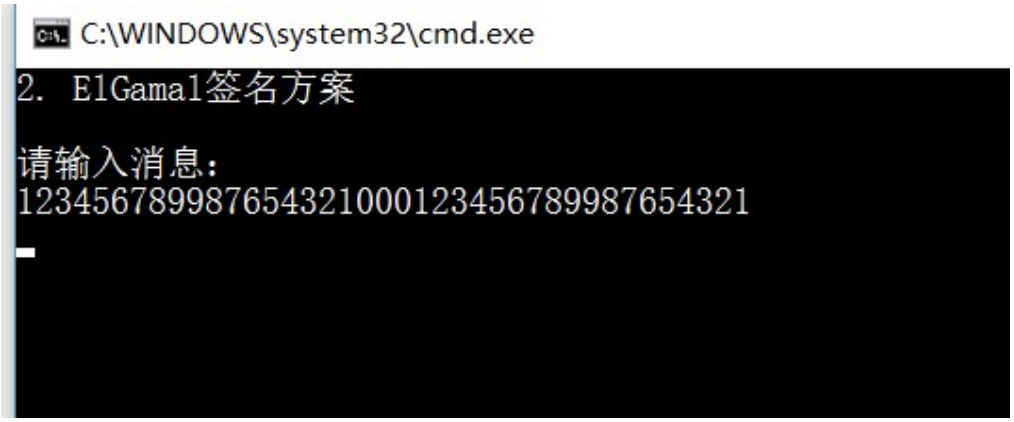
按照提示输入消息，格式：数字即可；



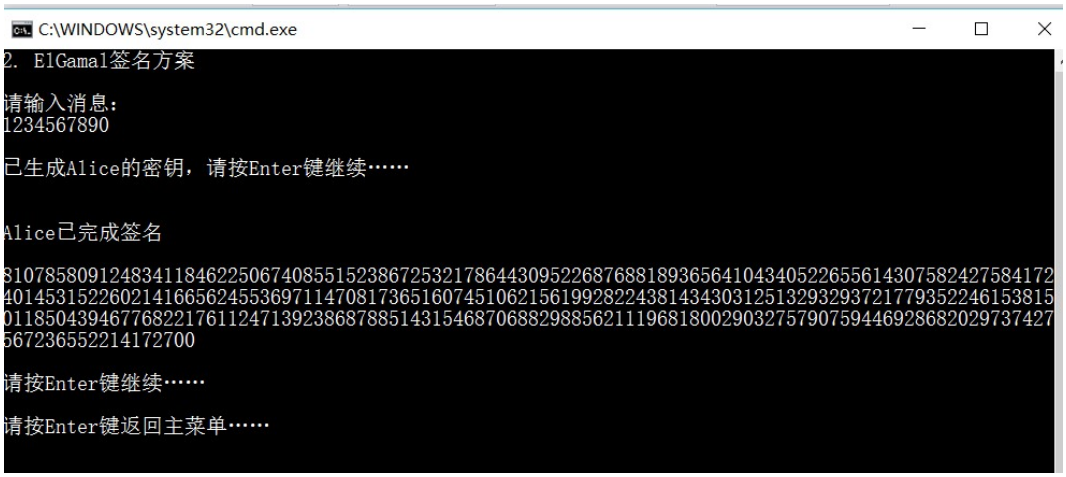
输入后按照提示，按 Enter 键继续程序的运行，适当的暂停可以为用户提供一定的方便。程序运行过程可能需要一段时间，请耐心等待，最后按 Enter 键回到主菜单。

2. 当输入 2 后，进入 ElGamal 签名测试；

默认密钥长度：1024 位



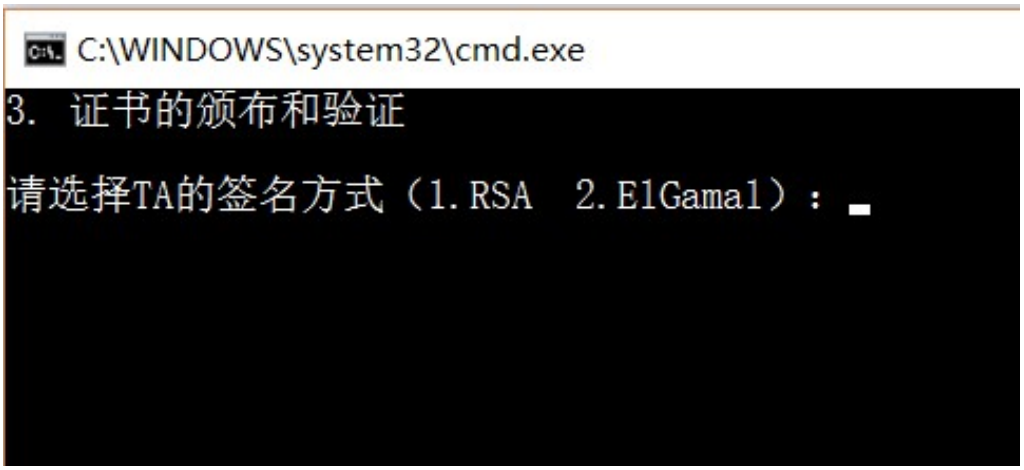
按照提示输入消息，格式：数字即可；



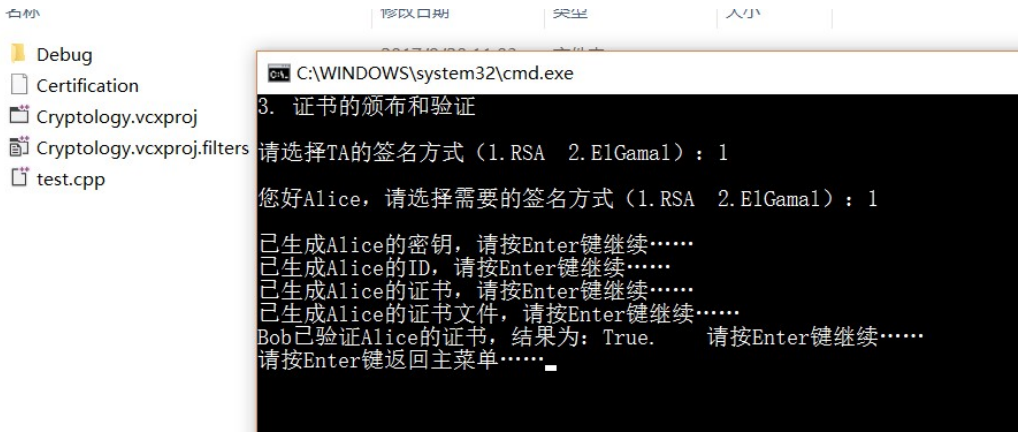
输入后按照提示，按 Enter 键继续程序的运行，适当的暂停可以为用户提供一定的方便。程序运行过程可能需要非常长的一段时间，请耐心等待，最后按 Enter 键回到主菜单。

3. 当输入 3 后，进入证书的颁布和验证测试；

默认的用户密钥长度：64 位，可在源代码中调整；可信权威机构密钥的默认长度长度是用户的 4 倍。



按照提示输入你的选择即可，输入 1 代表选择 RSA，输入 2 代表选择 ElGamal



按照提示按 Enter 键继续，如图所示当前目录下产生的名为“Certification”文件为生成的证书文件。

4. 当输入 4 后，进入交互认证测试；

默认的用户密钥长度为 64 位，可在源代码中进行调整；可信权威机构的默认密钥长度是用户密钥长度的 4 倍，随机挑战的默认长度是用户密钥长度的八分之一。

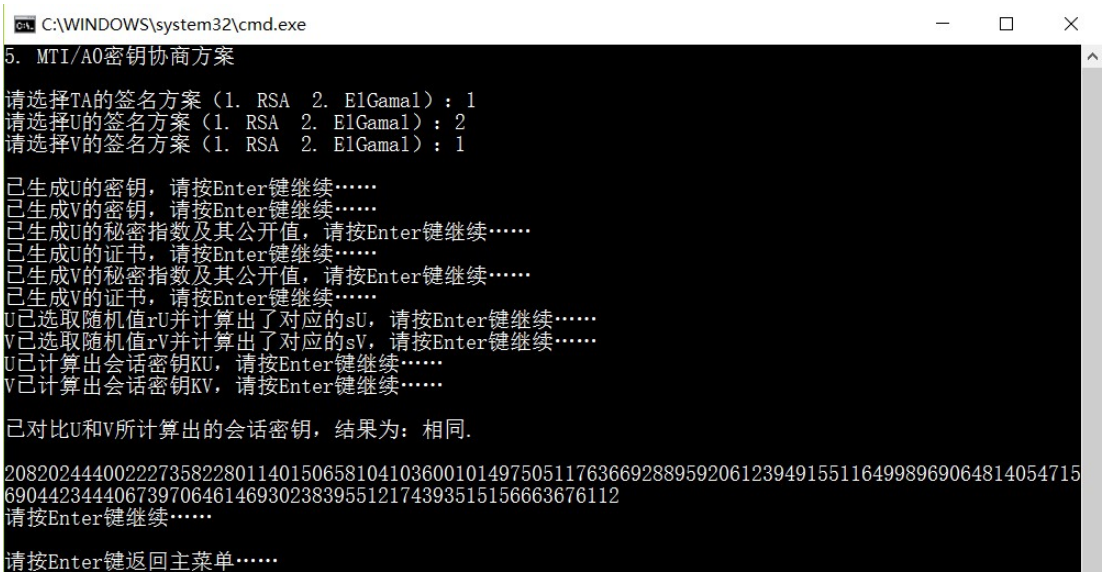
按照提示输入你的选择即可，输入 1 代表选择 RSA，输入 2 代表选择 ElGamal

按照提示，按 Enter 键继续，中间的验证结果会有显示。

5. 当输入 5 后，进入 MTI/A0 密钥协商方案测试；

默认的素数 p 的长度是 1024 位，可在源代码中调整，用户密钥长度是其八分之一，可信权威机构的密钥长度是其二分之一。

按照提示输入你的选择即可，输入 1 代表选择 RSA，输入 2 代表选择 ElGamal



按照提示按 Enter 键继续，最后比对会话密钥如果相同，会将会话密钥的值打印出来。