

OpenPGP

使用手册

2023 年 4 月 18 日

目 录

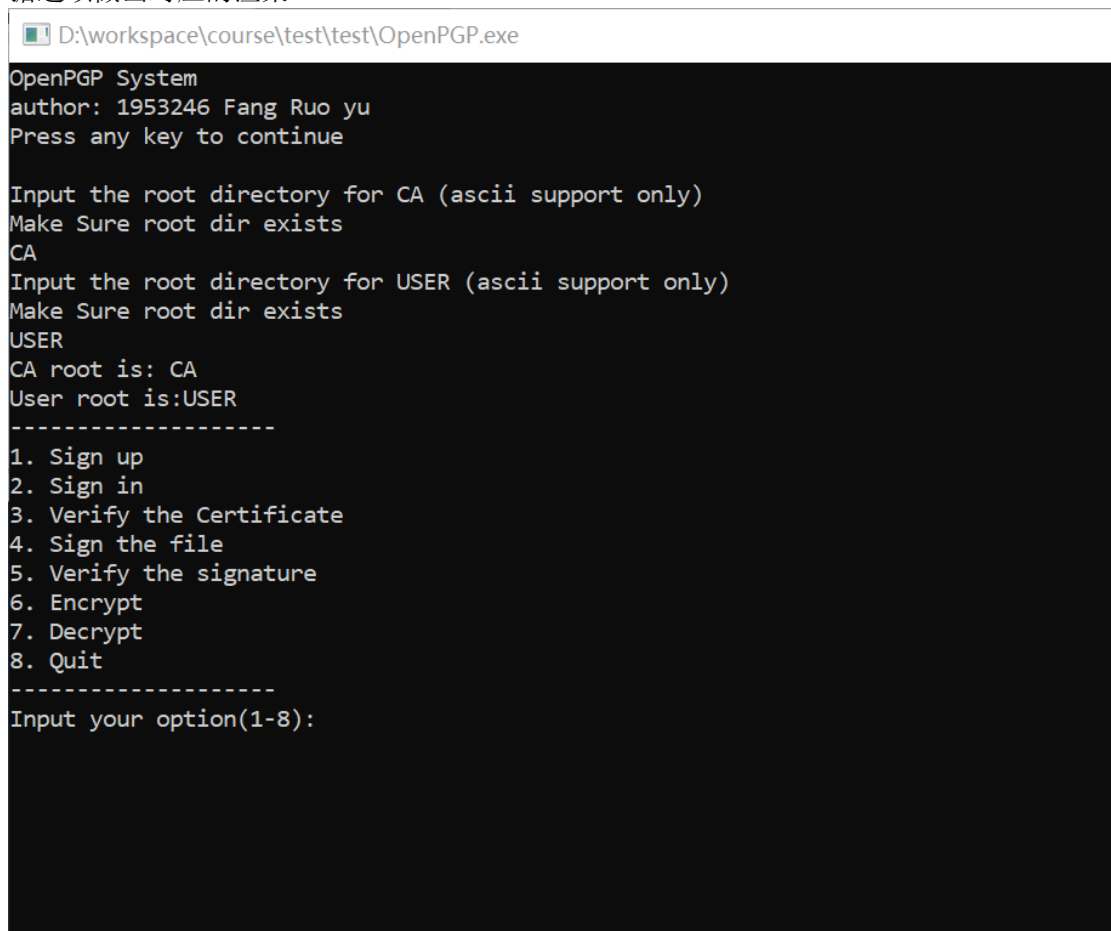
第 1 章	系统介绍	1
1.1	系统界面介绍	1
第 2 章	系统使用	1
2.1	系统初始化	1
2.1.1	系统启动	1
2.1.2	系统初始化	2
2.2	用户系统	3
2.2.1	用户注册	3
2.2.2	用户登录	4
2.3	安全系统	5
2.3.1	证书验证	5
2.3.2	证书签名	7
2.3.3	文件加密	8
2.3.4	文件解密	9
2.3.5	签名验证	11

第1章 系统介绍

该系统假定 CA 机构和 USER 系统是在云端部署的。除了用户获取自己的公钥和私钥以外，用户无法访问 CA 和 USER 的工作目录。该假定是基于攻击者无法修改服务器数据库的内容，攻击者只能修改本地的数据。

1.1 系统界面介绍

系统运行时是如下界面，包含一个菜单和一个等待用户输入选项的提示。然后系统会根据选项做出对应的渲染。



```
D:\workspace\course\test\test\OpenPGP.exe
OpenPGP System
author: 1953246 Fang Ruo yu
Press any key to continue

Input the root directory for CA (ascii support only)
Make Sure root dir exists
CA
Input the root directory for USER (ascii support only)
Make Sure root dir exists
USER
CA root is: CA
User root is:USER
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
-----
Input your option(1-8):
```

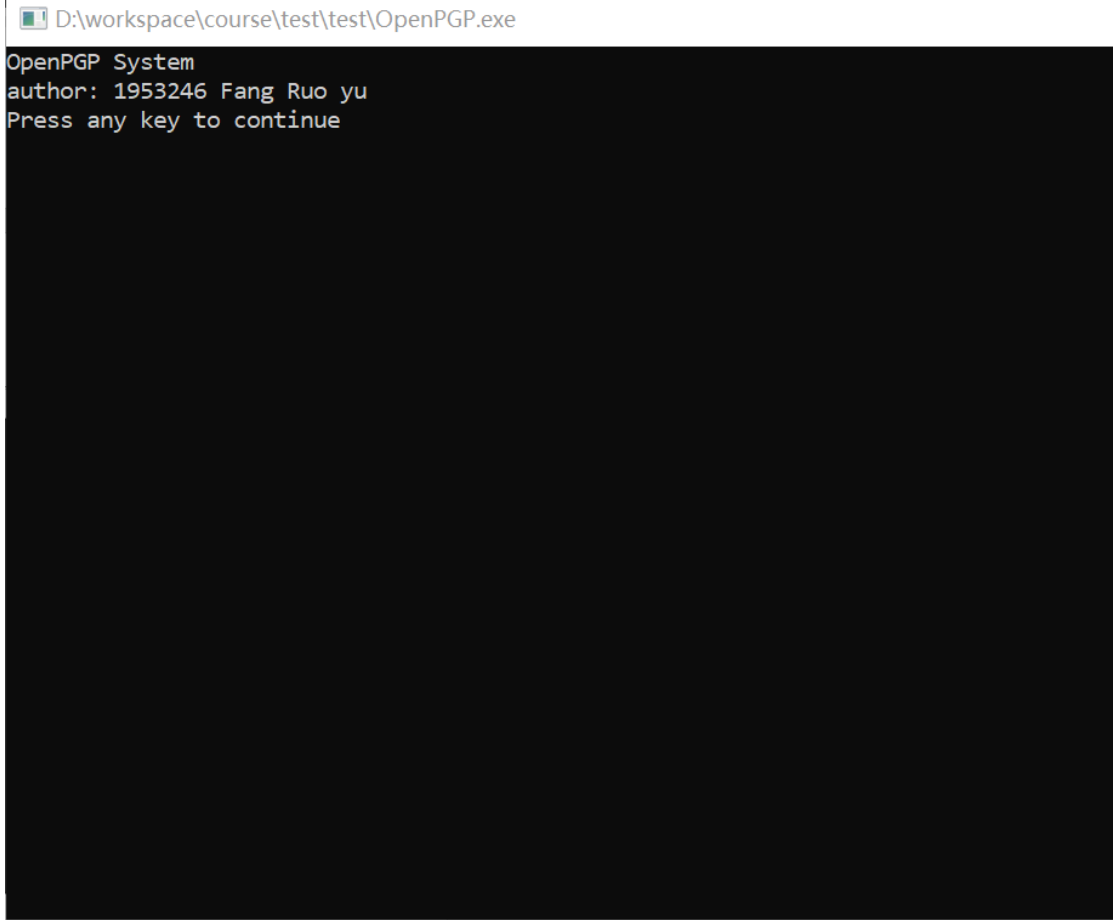
第2章 系统使用

2.1 系统初始化

2.1.1 系统启动

点击可执行文件，然后进入系统的启动界面。启动界面如下图。

点击任意键继续，即可进入系统的初始化过程。

A screenshot of a Windows command prompt window titled "D:\workspace\course\test\test\OpenPGP.exe". The window has a black background with white text. The text displayed is: "OpenPGP System", "author: 1953246 Fang Ruo yu", and "Press any key to continue".

```
D:\workspace\course\test\test\OpenPGP.exe
OpenPGP System
author: 1953246 Fang Ruo yu
Press any key to continue
```

2.1.2 系统初始化

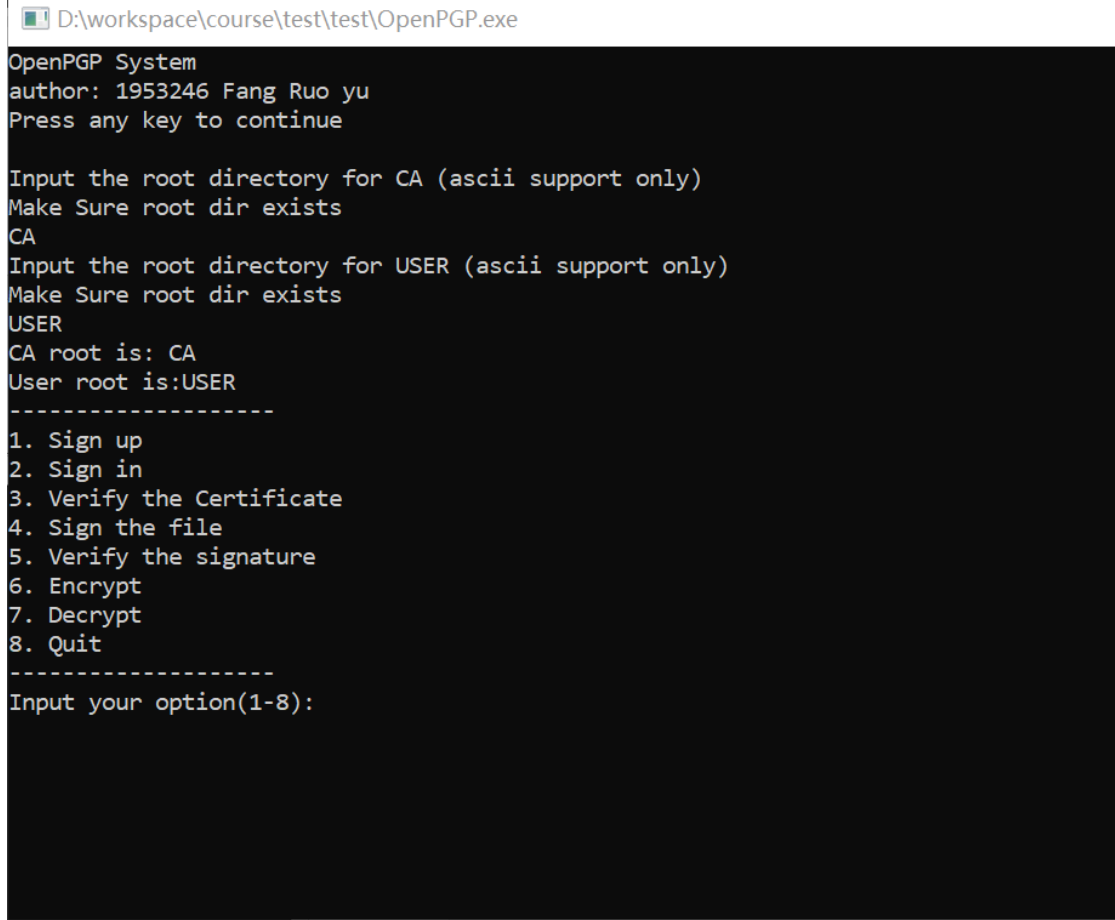
系统的初始化主要是对系统内部的 CA 和 User 数据库设置工作的根目录。

用户输入时，需要保证输入的目录是存在的。

输入目录的方式有两种：

- 输入绝对路径：该方式输入的路径不能以 ‘/’ 或 ‘\’ 结束
- 输入相对路径（推荐）：该方式，只需要在可执行文件的目录下创建一个目录，并输入该目录名即可，同样的，输入的路径不能以 ‘/’ 或 ‘\’ 结束

初始化成功后，会有如下界面。此后只需要根据界面上的输入提示操作即可。



```
D:\workspace\course\test\test\OpenPGP.exe
OpenPGP System
author: 1953246 Fang Ruo yu
Press any key to continue

Input the root directory for CA (ascii support only)
Make Sure root dir exists
CA
Input the root directory for USER (ascii support only)
Make Sure root dir exists
USER
CA root is: CA
User root is:USER
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
-----
Input your option(1-8):
```


当系统已经初始化后，下一次进入系统，则会自动读取根目录的数据文件。

2.2 用户系统

2.2.1 用户注册

选择 1，则进入系统的注册功能。首先用户需要根据提示输入用户名和密码，然后系统会在 USER 的根目录下创建用户的密码文件。

比如我注册两个用户，账号密码对分别是(1953246, 123456)和(1953245, 012345)。注册界面如下：



 D:\workspace\course\test\test\OpenPGP.exe

```
8. Quit
-----
Input your option(1-8):1

Input your id
1953246
Input the password
123456
REG: Success
Press any key to continue
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
-----
Input your option(1-8):1

Input your id
1953245
Input the password
012345
REG: Success
Press any key to continue
-----
1. Sign up
```

如果重复注册，系统会提示 **USER EXISTS**。注册成功后，可以在 **USER** 的工作根目录看到对应的密码文件夹，可以看到密码不是以明文的形式存储的。

 1953246.pwd X
D: > workspace > course > test > test > USER >  1953246.pwd
1 7c4a8d09ca3762af61e59520943dc26494f8941b

2.2.2 用户登录

选择 2，系统会启用登录功能，此时会进入系统的登录验证模块。登录验证模块需要先获取用户的私钥和公钥文件。输入路径后，先尝试错误的密码，用户名输入 1953246，密码输入 012345。可以看到系统会提示用户名和密码是不匹配的，并提示重新输入。

```
D:\workspace\course\test\test\OpenPGP.exe
8. Quit
-----
Input your option(1-8):2

Input the path for Private Key (ASCII only)
1953246.priv
Input the path for Public Key (ASCII only)
1953246.pub
Loading....
Input your ID:
1953246
Input your password:
012345
ID and Password not matched
Input your ID:
1953246
Input your password:
123456
Log in: Success
Done
Press any key to continue
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
```

此时输入正确的用户和密码即可登陆成功。

2.3 安全系统

该部分提供用户的基本操作，包括验证其他用户的证书，验证其他用户的签名。对文件进行签名、加密和解密。

2.3.1 证书验证

输入 3 即可进入证书验证模块，此时我们验证 CA 服务器上的 1953245.cert 是否是安全的证书。根据输入提示，我们需要输入待验证证书的用户 ID，这里是 1953245

D:\workspace\course\test\test\OpenPGP.exe

Input the path for Public Key (ASCII only)

1953246.pub

Loading....

Input your ID:

1953246

Input your password:

012345

ID and Password not matched

Input your ID:

1953246

Input your password:

123456

Log in: Success

Done

Press any key to continue

1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit

Input your option(1-8):3

Input the ID needs verified: 1953245

Verify: Success

可以看到验证通过，但是如果证书内容被修改后，比如被修改为 1953247，此时证书无法验证通过。

 D:\workspace\course\test\test\OpenPGP.exe

```
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
```

```
-----
```

```
Input your option(1-8):3
```

```
Input the ID needs verified: 1953245
```

```
Verify: Success
```

```
Press any key to continue
```

```
-----
```

```
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
```

```
-----
```

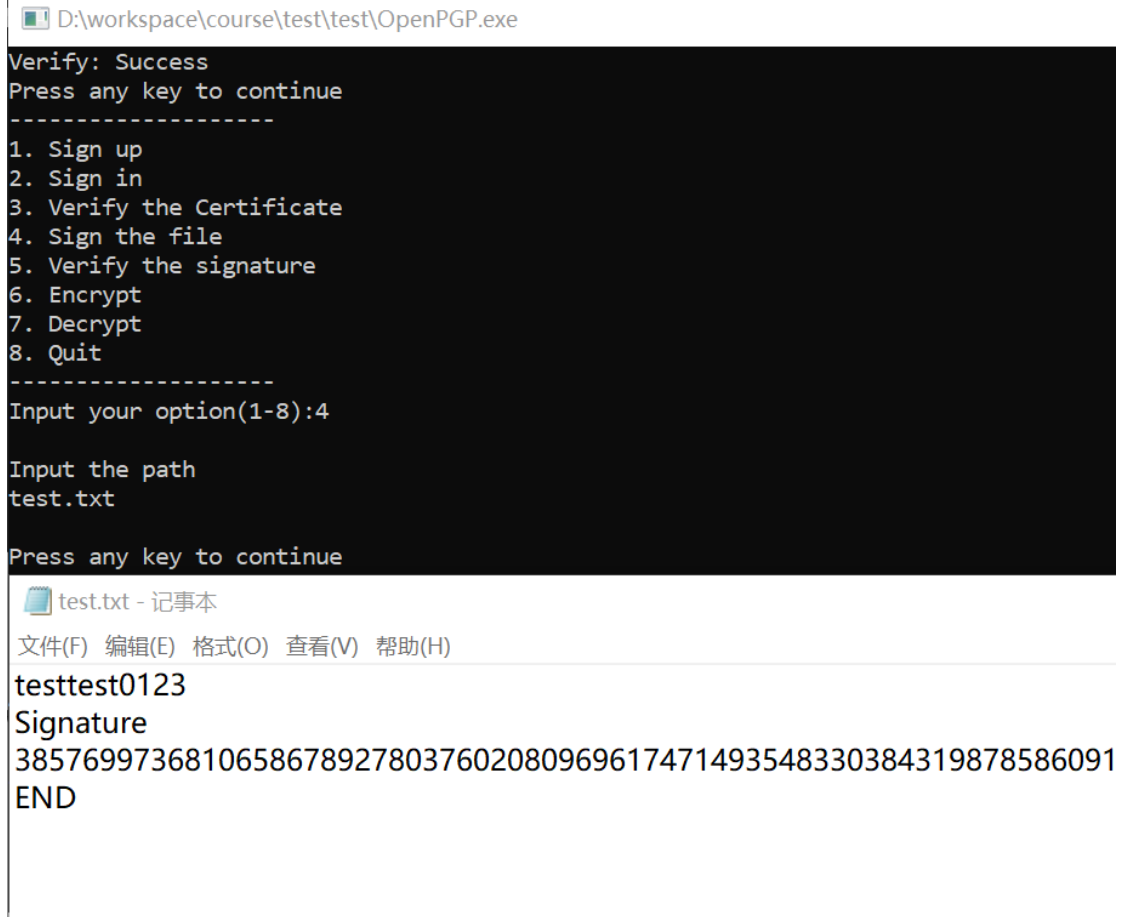
```
Input your option(1-8):3
```

```
Input the ID needs verified: 1953245
```

```
Verify: Fail
```

2.3.2 证书签名

输入 4 即可进入证书的签名页面。此时系统会提示用户输入待签名文件的路径。我们在可执行文件所在目录创建一个测试文件 test.txt，内容为 testtest0123，然后在系统中输入 test.txt，签名后，文件如下



The screenshot shows two windows. The top window is a command prompt titled 'D:\workspace\course\test\test\OpenPGP.exe'. It displays the following text: 'Verify: Success', 'Press any key to continue', a list of 8 options (1. Sign up, 2. Sign in, 3. Verify the Certificate, 4. Sign the file, 5. Verify the signature, 6. Encrypt, 7. Decrypt, 8. Quit), 'Input your option(1-8):4', 'Input the path', 'test.txt', and 'Press any key to continue'. The bottom window is a notepad titled 'test.txt - 记事本'. It contains the text: 'testtest0123', 'Signature', '38576997368106586789278037602080969617471493548330384319878586091', and 'END'.

```
D:\workspace\course\test\test\OpenPGP.exe
Verify: Success
Press any key to continue
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
-----
Input your option(1-8):4

Input the path
test.txt

Press any key to continue

test.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
testtest0123
Signature
38576997368106586789278037602080969617471493548330384319878586091
END
```

2.3.3 文件加密

现在我们对刚生成的签名后的文件进行加密。输入 6 进入加密模块：

1. 根据提示输入待加密文件的路径。此处输入的是 `test.txt`；
2. 然后输入用于加密的密钥，该密钥的长度需要为 8 字节，即该密钥由 8 个英文字符组成。我此处选择的密钥是 `key888888`；
3. 最后输入收件人的用户 ID 我输入的是 `1953245`

此时加密后的文件已经是不可阅读的乱码状态了



The screenshot shows a Windows desktop with two open applications. The top application is a terminal window titled "D:\workspace\course\test\test\OpenPGP.exe". It displays the following text:

```

8. Quit
-----
Input your option(1-8):
6

Input the path
test.txt

Input the key for encryption:key88888

Input the ID of receiver:1953245

Press any key to continue

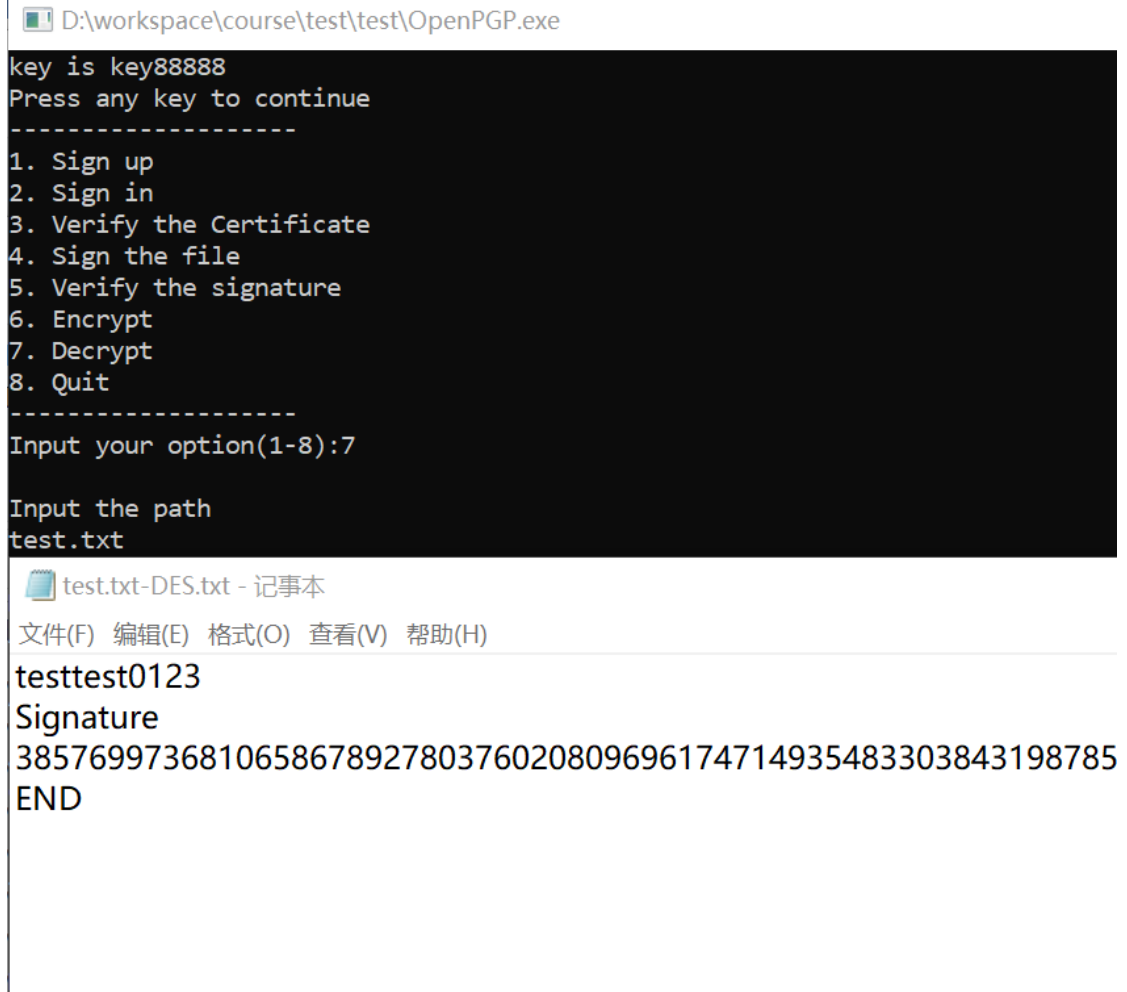
```

Below the terminal window is a Notepad window titled "test.txt - 记事本". Its menu bar includes "文件(F)", "编辑(E)", "格式(O)", "查看(V)", and "帮助(H)". The text area contains a single line of garbled characters: "J적錄喰苦殞순첼A △머韵鉞뵚口漳湫臉蔦 灑뵚岾 ㅅㅅ뵚n/薺荳鰾뵚 裊薹 ϕ 뵚ㅡ108靑".

2.3.4 文件解密

现在我们登录用户 1953245，然后选择 7 进入解密模块。输入文件路径。此处输入的是 test.txt。

可以看到，被成功解密了



```
D:\workspace\course\test\test\OpenPGP.exe
key is key88888
Press any key to continue
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
-----
Input your option(1-8):7

Input the path
test.txt

test.txt-DES.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
testtest0123
Signature
385769973681065867892780376020809696174714935483303843198785
END
```

此时我们再创建一个攻击者用户 1953247，密码为 234567，该用户用于测试系统是否能为非目标用户解密。因为解密时需要读取用户 ID 命名的 PGP 文件，现在我们拷贝假定用户截取了 1953246 用户发给 1953245 用户的 PGP 文件，并改名为 1953247.PGP，此时我们登录该用户，尝试解密。

可以看到解密出来是错误的结果。

```

D:\workspace\course\test\test\OpenPGP.exe
1953247
Input your password:
234567
Log in: Success
Done
Press any key to continue
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
-----
Input your option(1-8):7

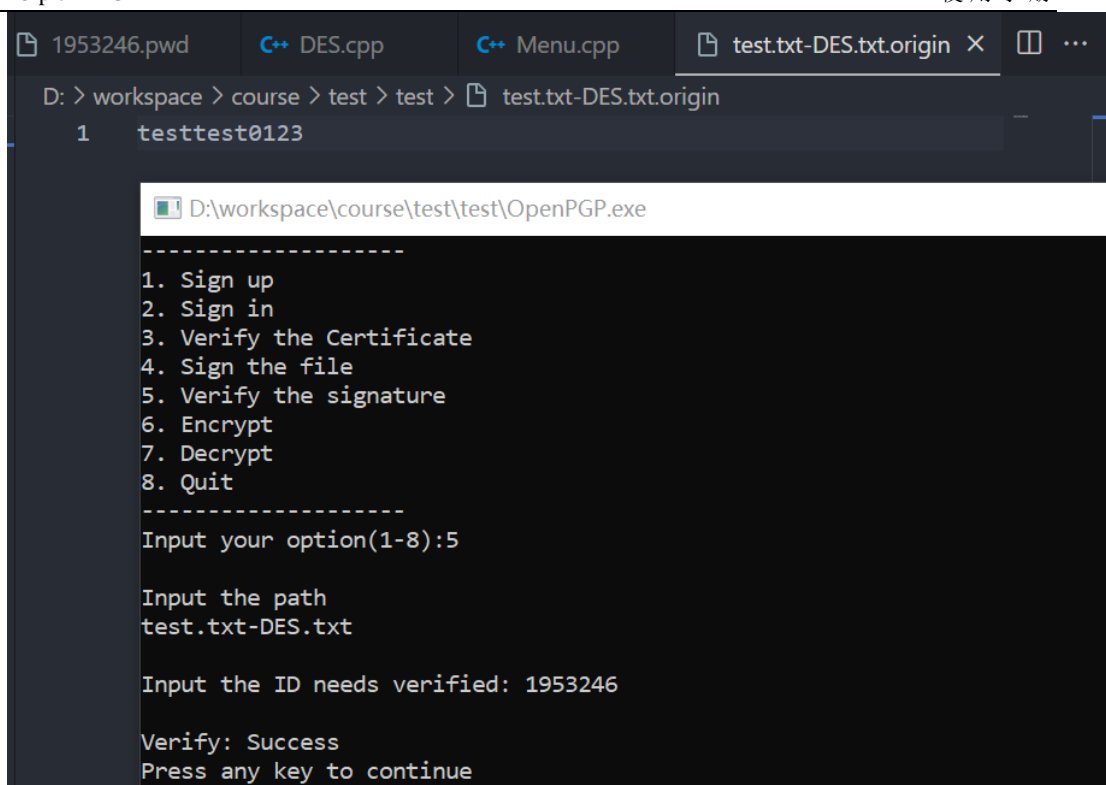
Input the path
test.txt

```

2.3.5 签名验证

选择 5，对文件的签名进行验证。根据提示输入文件路径即可开始验证

可以看到验证通过，且生成的.origin 文件已经还原到最开始的文件状态了



The screenshot shows a C++ IDE with a file named `test.txt-DES.txt.origin` open. The file content is `testtest0123`. A terminal window is open, showing the execution of `D:\workspace\course\test\test\OpenPGP.exe`. The terminal displays a menu with 8 options: 1. Sign up, 2. Sign in, 3. Verify the Certificate, 4. Sign the file, 5. Verify the signature, 6. Encrypt, 7. Decrypt, and 8. Quit. The user has selected option 5. The terminal then prompts for the path, which is `test.txt-DES.txt`, and the ID needs verified, which is `1953246`. The verification is successful, and the user is prompted to press any key to continue.

```
D:\workspace\course\test\test\OpenPGP.exe
-----
1. Sign up
2. Sign in
3. Verify the Certificate
4. Sign the file
5. Verify the signature
6. Encrypt
7. Decrypt
8. Quit
-----
Input your option(1-8):5

Input the path
test.txt-DES.txt

Input the ID needs verified: 1953246

Verify: Success
Press any key to continue
```