多人联合授权加解密工具

核心原理： RSA 非对称加密，SHA256-HMAC 消息摘要，AES 对称加密

使用方法（以 3 人联合加密为例）

生成密钥对操作：

3人依次输入密码，3人互不知道对方输入的是什么

软件将返回两个密钥：

1、加密公钥：用于给文件加密，可以告诉任何人，比如具体操作文件加密的人

2、解密私钥：解密的时候需要填写

加密文件操作：

1、选择要加密的文件

2、填写加密公钥

3、生成加密文件

解密文件操作：

1、选择要解密的文件

2、填写解密私钥

3、三人在软件上依次输入但是生成密钥时输入的密码

4、得到解密文件

以上三种操作均能以命令行指令执行，供其他软件和程序调用。

技术细节

使用 `openssl` 生成秘钥对

```
openssl genrsa -out test.key 1024
openssl rsa -in test.key -pubout -out test_pub.key
```

可以分别得到原始的私钥和公钥如下:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC/WCMk355ft6ZGQ89XHiGRRm6CABvPORjG3Tdh7hzbBM9P0dxU
0kzhJfivoke3DKvzUGqiSoLg2AjxXHtsTt/3SMe1M6482HLyjaH/XvCKbuwdzsl/
QL88UIerlrAaiwp7IFalZCplSSwLX6mWFktNIrMIB93Jjzcs4GzOlgf5XwIDAQAB
```

```
AoGAa8FL0VkpTEgVGF7Zpfru9mwOkaFUB+fknyE3Liw1DdZwlUfe59mit+x1Vxtx
fZFiSFzSIGELwWmH57yoOP9WOmf3OIKofck0ck35zMxRg5sgVcalYW5jVyklbOpY
5KEMH/NJXKaiYWQIrdI419Ae0aEWMbpjqIH+MLF9Jlo5wXECQQDeF/4OOcFcirTh
0jOEl73cBcafPTQW5+beLh/sqmO52Pdx9/QO3KM+NWmWURuCv5mZkstM4n/K0/mN
npZ69eeXAkEA3I5gQMOGa9kRS94Jx6Two2+6xyz1t1LTJp1XT2SiyABAnhvh1tN4
SuqFqQgO+RNfBhXnQbCZJGqeHGCtXWb1eQJBANfN1mcN+GZOvVhkiPzA+ZJO5nYa
4X+UbOfdR9YOsD2yjpZmifba+6BaBDQOsZe1l4n7cqJNwEEVAntS6wOl6BcCQCD7
5ecrAj/UuaJ39Ux3HUnD5tHspl6hM1S+CRWlfjac2wOKLG8dNws1IYIS43JadEaL
tgb76xsoGrcxuhuSzzkCQQCrN7m8mJrmEr+dAJSDTUzCGKMZOnr9ZYIfKqhfLFVL
As84coN56qWwZ39m8JL5Y4i6S6fpGnvcDdld/YIH9QDK
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/WCMk355ft6ZGQ89XHiGRRm6C
ABvPORjG3Tdh7hzbBM9P0dxU0kzhJfivoke3DKvzUGqiSoLg2AjxXHtsTt/3SMe1
M6482HLyjaH/XvCKbuwdzsl/QL88UIerlrAaiwp7IFalZCplSSwLX6mWFktNIrMI
B93Jjzcs4Gz0lgf5XwIDAQAB
-----END PUBLIC KEY-----
```

利用三人分别输入的密码处理 `加密私钥`

上一步中生成的公钥可以直接在软件界面上显示给使用者

但是原始的私钥是不能直接告知使用者的，需要经过加密处理，如下：

1、依次对所有的输入密码使用 `SHA256-HMAC` 进行摘要处理，例如三人分别输入的是 `aaa` 、 `bbb` 、 `ccc`

算法为: `sha256_hamc(sha256_hamc('aaa', 'bbb'), 'ccc')`

摘要结果为: `6e063dc453a0646c762d80682b577f33abcb16a5a92a2b35929beee94380a39b`

2、将以上结果用作加密 `key`，对原始私钥进行 `AES` 加密，得到结果如下

```
b'c\xbf\xdc\xab\n\xfd\x1aH\x81\xaa\xe4\x88\x1b\x12\xb4\x03H\xfd\xe8z\x9d\xf3\xe1Rbq\x9aW\xe
c\xca\xcc\xa5\x14\x15\x04I\xf9\x9b\x99\xb8\xbeD\xec\xfd\x14o\xc8\xfe\x13D\x80\x86\xa4\xabQk
n9\xf6y0\x9c,\xc1W+\xb8\x8f\t\xf7%\x9b:\x02C/\x14\xb2{\xaa\x00m\xe3?"\x81\xb3\x06\xfcq\x1b\
xa5\xc3)T\x01f3\x92\tE\xae\xd1\xd8\xc2>\xb9\xe6]\xfc\x9e\xf1\x8d&\r\x95~i,2Y`\xd38\x80I\xe2
j\xea\xc3do\xbe\xd8N\xedT&\xeb_u\xe8\x1bC\x80*\xb5\x92\xe2\x85B\\&md\xbb\xa9\x83\xd0X\xccRd
\x11\x92T\xdf\xe2\x0fu\xf1\x7fu\xa0\xda\xcb\xddb4f\xde\x97\x83\xd3\xe1\x17r\x13\x8e\xff\xc2
\x12\x10(q\xd9]\xa9p\x01\x144k\xf8$y\xc7\x16\x89
\x18\xc8\xcb\xc5\x9e\x1d\xdb\xc2\x17\xd6\x7fe:\n\x16V\xd3\x90\x98\xdb\x99\x87\xc0\r\xddm\xb
9\x9f\x8a\xbf\xb6\x88\xc8\x869\xda\x90\r\xcb\xdfk\xcdH\xdfAE\xa6\xa9$\xf3\xae\x9e\xf2\xc0\x
1f+\x0f\xb9\xa9\xc4\x15'
```

3、将以上结果进行 base64 编码后就是解密私钥如下

```
Y7/cqwr9GkiBquSIGxK0A0j96Hqd8+FSYnGaV+zKzKUUFQRJ+ZuZuL5E7POUb8j+E0SAhqSrUWtuOfZ5MJwswVcruI8
J9yWbOgJDLxSye6oAbeM/IoGzBvxxG6XDKVQBZjOSCUWu0djCPrnmXfye8YOmDZV+aSwyWWDTOIBJ4mrqw2RvvthO7V
Qm61916BtDgCq1kuKFQlwmbWS7qYPQWMxSZBGSVN/iD3Xxf3Wg2svdYjRm3peDO+EXchOO/8ISEChx2V2pcAEUNGv4J
HnHFokgGMjLxZ4d28IX1n9lOgoWVtOQmNuZh8AN3W25n4q/tojIhjnakA3L32vNSN9BRaapJPOunvLAHysPuanEFQ==
```

以上是 `加密公钥` 和 `解密私钥` 生成的全部过程，最终展示给使用者的数据示例如下：

```
加密公钥:
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC/WCMk355ft6ZGQ89XHiGRRm6CABvPORjG3Tdh7hzbBM9POdxU
OkzhJfivoke3DKvzUGqiSoLg2AjxXHtsTt/3SMe1M6482HLyjaH/XvCKbuwdzsl/
QL88UIerlrAaiwp7IFalZCplSSwLX6mWFktNIrMIB93Jjzcs4GzOlgf5XwIDAQAB
AoGAa8FLOVkpTEgVGF7Zpfru9mwOkaFUB+fknyE3Liw1DdZwlUfe59mit+x1Vxtx
fZFiSFzSIGELwWmH57yoOP9WOmf3OIKofckOck35zMxRg5sgVcalYW5jVyklbOpY
5KEMH/NJXKaiYWQIrdI419Ae0aEWMbpjqIH+MLF9Jlo5wXECQQDeF/4OOcFcirTh
OjOEl73cBcafPTQW5+beLh/sqmO52Pdx9/QO3KM+NWmWURuCv5mZkstM4n/K0/mN
npZ69eeXAkEA3I5gQMOGa9kRS94Jx6Two2+6xyz1t1LTJp1XT2SiyABAnhvh1tN4
SuqFqQgO+RNfBhXnQbCZJGqeHGCtXWb1eQJBANfN1mcN+GZOvVhkiPzA+ZJO5nYa
4X+UbOfdR9YOsD2yjpZmifba+6BaBDQOsZe1l4n7cqJNwEEVAntS6wOl6BcCQCD7
5ecrAj/UuaJ39Ux3HUnD5tHspl6hM1S+CRWlfjac2wOKLG8dNws1IYIS43JadEaL
tgb76xsoGrcxuhuSzzkCQQCrN7m8mJrmEr+dAJSDTUzCGKMZOnr9ZYIfKqhfLFVL
As84coN56qWwZ39m8JL5Y4i6S6fpGnvcDdld/YIH9QDK
-----END RSA PRIVATE KEY-----

解密私钥:
Y7/cqwr9GkiBquSIGxKOAOj96Hqd8+FSYnGaV+zKzKUUFQRJ+ZuZuL5E7POUb8j+EOSAhqSrUWtuOfZ5MJwswVcruI8
J9yWbOgJDLxSye6oAbeM/IoGzBvxxG6XDKVQBZjOSCUWuOdjCPrnmXfye8YOmDZV+aSwyWWDTOIBJ4mrqw2RvvthO7V
Qm61916BtDgCq1kuKFQlwmbWS7qYPQWMxSZBGSVN/iD3Xxf3Wg2svdYjRm3peDO+EXchOO/8ISEChx2V2pcAEUNGv4J
HnHFokgGMjLxZ4d28IX1n9lOgoWVtOQmNuZh8AN3W25n4q/tojIhjnakA3L32vNSN9BRaapJPOunvLAHysPuanEFQ==
```

利用 `加密公钥` 加密文件

```
openssl rsautl -encrypt -in key -inkey test_pub.key -pubin -out secret_key
```

1、加密前生成一个随机字符串，作为 `key`，对 `文件a` 进行 `AES` 加密，生成 `文件b`

2、使用 `加密公钥` 对 `key` 进行 rsa 加密

3、将上一步上的加密结果添加到 `文件b` 的头部

4、最终 `文件b` 为加密后的文件

利用 `解密私钥` 以及三人密码解密文件

此例中 `解密私钥` 为:

```
Y7/cqwr9GkiBquSIGxKOAOj96Hqd8+FSYnGaV+zKzKUUFQRJ+ZuZuL5E7POUb8j+EOSAhqSrUWtuOfZ5MJwswVcruI8
J9yWbOgJDLxSye6oAbeM/IoGzBvxxG6XDKVQBZjOSCUWuOdjCPrnmXfye8YOmDZV+aSwyWWDTOIBJ4mrqw2RvvthO7V
Qm61916BtDgCq1kuKFQlwmbWS7qYPQWMxSZBGSVN/iD3Xxf3Wg2svdYjRm3peDO+EXchOO/8ISEChx2V2pcAEUNGv4J
HnHFokgGMjLxZ4d28IX1n9lOgoWVtOQmNuZh8AN3W25n4q/tojIhjnakA3L32vNSN9BRaapJPOunvLAHysPuanEFQ==
```

三人密码依次是: `aaa`、 `bbb`、 `ccc`

要解密的文件是: `文件b`

1、首先对 `解密私钥` 进行 base64 解码，得到如下字节数据:

```
b'c\xbf\xdc\xab\n\xfd\x1aH\x81\xaa\xe4\x88\x1b\x12\xb4\xO3H\xfd\xe8z\x9d\xf3\xe1Rbq\x9aW\xec
\xca\xcc\xa5\x14\x15\xO4I\xf9\x9b\x99\xb8\xbeD\xec\xfd\x14o\xc8\xfe\x13D\x8O\x86\xa4\xabQkn9
\xf6yO\x9c,\xc1W+\xb8\x8f\t\xf7%\x9b:\xO2C/\x14\xb2{\xaa\xOOm\xe3?"\x81\xb3\xO6\xfcq\x1b\xa5
\xc3)T\xO1f3\x92\tE\xae\xd1\xd8\xc2>\xb9\xe6]\xfc\x9e\xf1\x8d&\r\x95~i,2Y`\xd38\x8OI\xe2j\xe
a\xc3do\xbe\xd8N\xedT&\xeb_u\xe8\x1bC\x8O*\xb5\x92\xe2\x85B\\&md\xbb\xa9\x83\xdOX\xccRd\x11\
x92T\xdf\xe2\xOfu\xf1\x7fu\xaO\xda\xcb\xddb4f\xde\x97\x83\xd3\xe1\x17r\x13\x8e\xff\xc2\x12\x
1O(q\xd9]\xa9p\xO1\x144k\xf8$y\xc7\x16\x89
\x18\xc8\xcb\xc5\x9e\x1d\xdb\xc2\x17\xd6\x7fe:\n\x16V\xd3\x9O\x98\xdb\x99\x87\xcO\r\xddm\xb9
\x9f\x8a\xbf\xb6\x88\xc8\x869\xda\x9O\r\xcb\xdfk\xcdH\xdfAE\xa6\xa9$\xf3\xae\x9e\xf2\xcO\x1f
+\xOf\xb9\xa9\xc4\x15'
```

2、然后对三人密码进行摘要处理，方法同上述生成密钥环节中所述的 `SHA256-HMAC` 一致，得到摘要如下:

```
6eO63dc453aO646c762d8O682b577f33abcb16a5a92a2b35929beee9438Oa39b
```

3、以摘要结果作为 `key`，对文件内容进行 `AES` 解密，得到原始的私钥内容，如下:

```
-----BEGIN PUBLIC KEY-----
MIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/WCMk355ft6ZGQ89XHiGRRm6C
ABvPORjG3Tdh7hzbBM9POdxUOkzhJfivoke3DKvzUGqiSoLg2AjxXHtsTt/3SMe1
M6482HLyjaH/XvCKbuwdzsl/QL88UIerlrAaiwp7IFalZCplSSwLX6mWFktNIrMI
B93Jjzcs4GzOlgf5XwIDAQAB
-----END PUBLIC KEY-----
```

4、从 `文件b` 提取此前加密后的头部数据，利用原始私钥对其进行解密，得到 `key`

```
openssl rsautl -decrypt -in secret_key -inkey test.key -out key
```

5、利用上一步中得到的 `key`，对 `文件b` 进行 `AES` 解密，得到 `文件a`，完成整个解密流程