一.安装 gpg

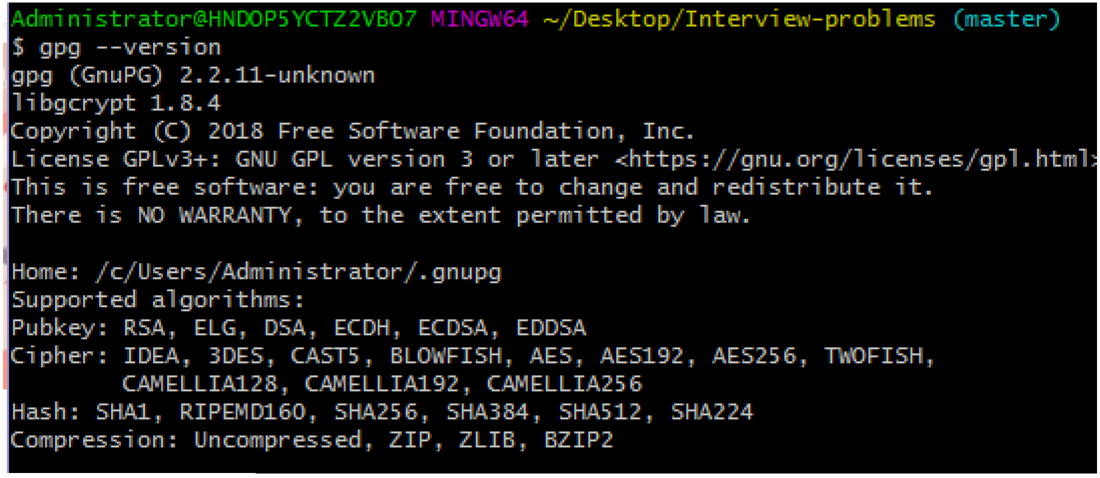
```
brew install gpg
```

也可以安装包下载安装:

```
http://www.ruanyifeng.com/blog/2013/07/gpg.html
```

二.查看gpg版本

gpg --version



```
Administrator@HNDOP5YCTZ2VBO7 MINGW64 ~/Desktop/Interview-problems (master)
$ gpg --version
gpg (GnuPG) 2.2.11-unknown
libgcrypt 1.8.4
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /c/Users/Administrator/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

三.创建gpg-ID

如果gpg版本在2.1.17以上，就用下面的命令:

```
gpg --full-generate-key
```

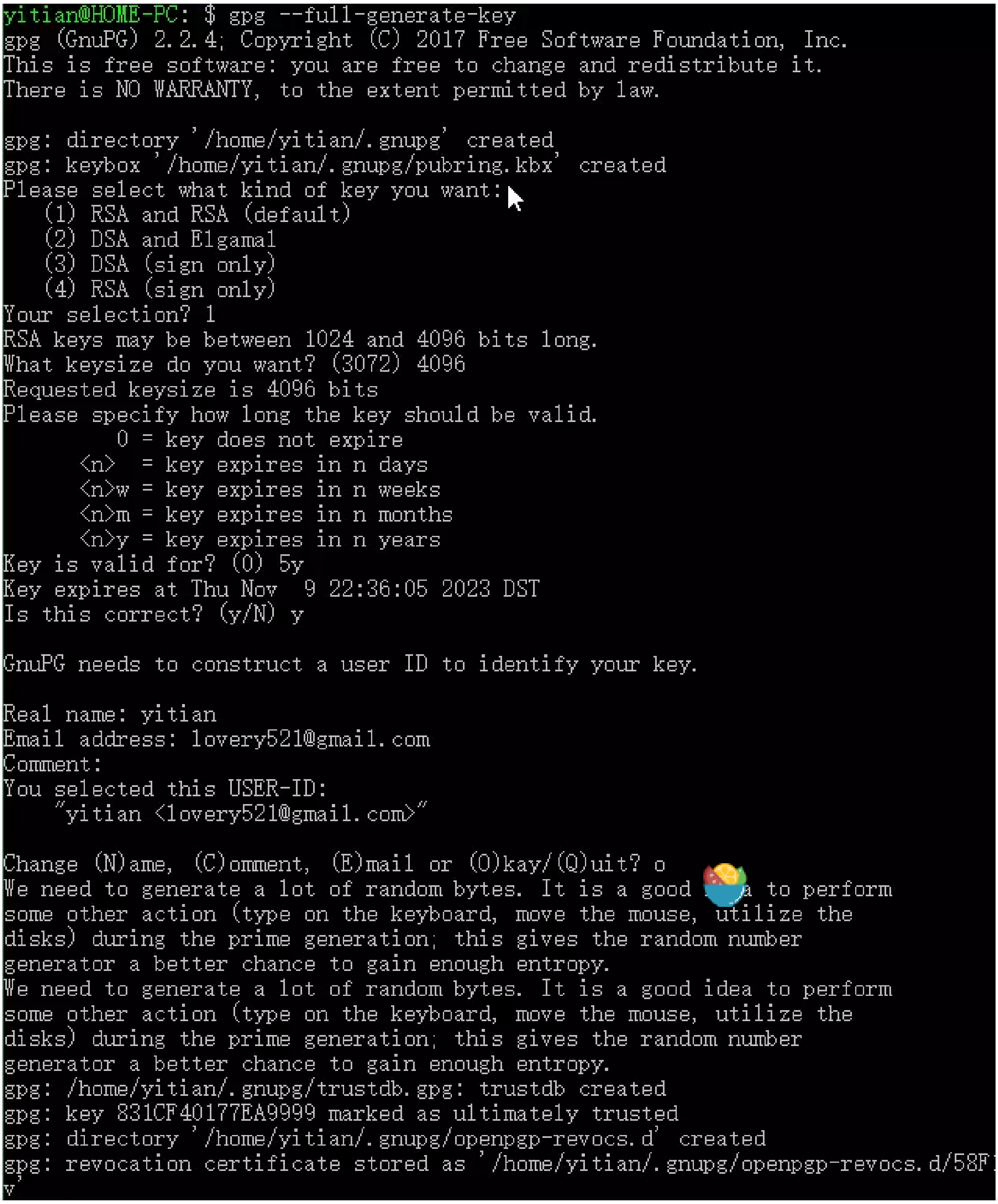
如果gpg版本在2.1.17以下，用下面的命令:

```
gpg --default-new-key-algo rsa4096 --gen-key
```

我们也可以输入:(默认使用这个)

```
gpg --gen-key
```

然后按照提示输入密钥类型、密钥长度、过期时间、用户名、密码等信息，其中密钥长度推荐4096，其他按需输入即可。



```
yitian@HOME-PC: $ gpg --full-generate-key
gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/yitian/.gnupg' created
gpg: keybox '/home/yitian/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 5y
Key expires at Thu Nov  9 22:36:05 2023 DST
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: yitian
Email address: lovery521@gmail.com
Comment:
You selected this USER-ID:
    "yitian <lovery521@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/yitian/.gnupg/trustdb.gpg: trustdb created
gpg: key 831CF40177EA9999 marked as ultimately trusted
gpg: directory '/home/yitian/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/yitian/.gnupg/openpgp-revocs.d/58F
```

四.查看公钥和秘钥

日后你可以使用该命令查看这些信息：

- 查看公钥

```
gpg --list-keys --keyid-format LONG
```

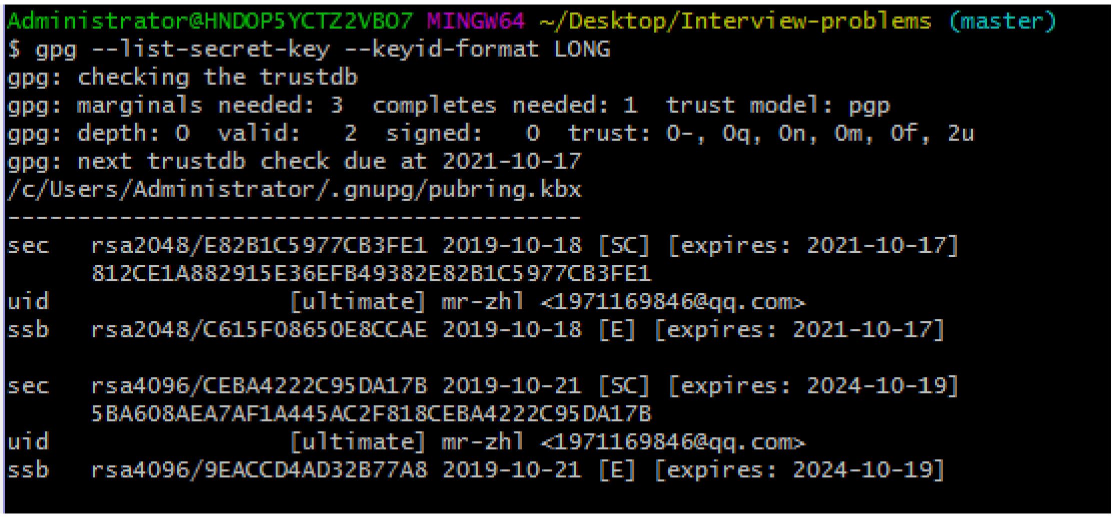
- 查看私钥

```
gpg --list-secret-keys --keyid-format LONG
```

最后会输出信息中最后三行，如下，

其中pub为公钥，C51F99A5 为公钥Key；sub为私钥768FFEAA为私钥Key，过期时间为2028年

```
pub 2048R/C51F99A5 2018-01-14 [expires: 2028-01-12]
 Key fingerprint = XXXX 3596 8DA0 616E 8E39 ABCD 5823 8C2F EFGN YYYY
uid realname (github) <xxxx@163.com>
sub 2048R/768FFEAA 2018-01-14 [expires: 2028-01-12]
```



```
Administrator@HNDOP5YCTZ2VBO7 MINGW64 ~/Desktop/Interview-problems (master)
$ gpg --list-secret-key --keyid-format LONG
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2021-10-17
/c/Users/Administrator/.gnupg/pubring.kbx
-----------------------------------------
sec   rsa2048/E82B1C5977CB3FE1 2019-10-18 [SC] [expires: 2021-10-17]
      812CE1A882915E36EFB49382E82B1C5977CB3FE1
uid                 [ultimate] mr-zhl <1971169846@qq.com>
ssb   rsa2048/C615F08650E8CCAE 2019-10-18 [E] [expires: 2021-10-17]

sec   rsa4096/CEBA4222C95DA17B 2019-10-21 [SC] [expires: 2024-10-19]
      5BA608AEA7AF1A445AC2F818CEBA4222C95DA17B
uid                 [ultimate] mr-zhl <1971169846@qq.com>
ssb   rsa4096/9EACCD4AD32B77A8 2019-10-21 [E] [expires: 2024-10-19]
```

如果要让当前git项目启用签名验证，使用下面的命令：

```
git config commit.gpgsign true
```

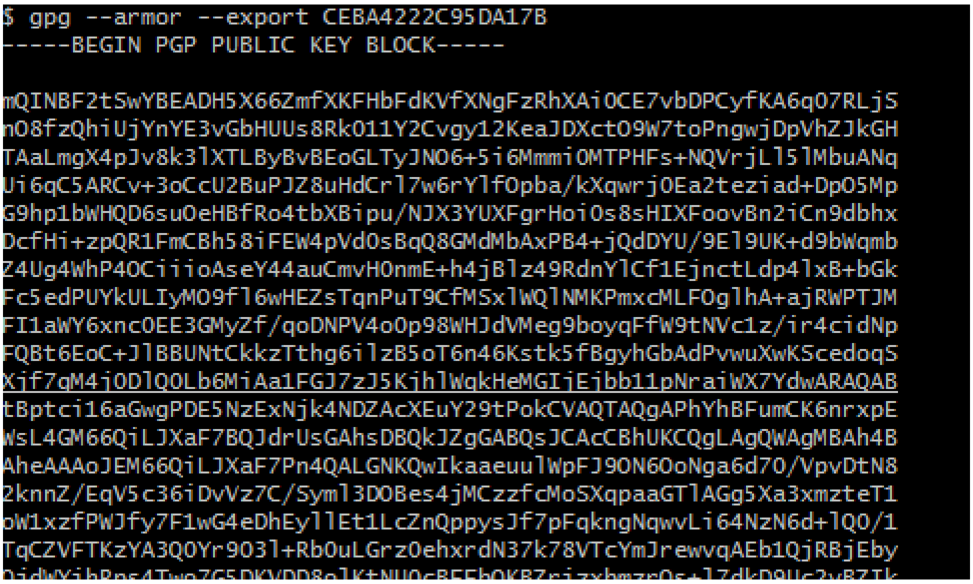
如果要让所有项目都启用签名验证：(一般选这项)

```
git config --global commit.gpgsign true
```

四.配置gitconfig,将gpg 秘钥添加在git仓库

1. 查看密钥内容了，你需要将ID替换为自己的：

```
gpg --armor --export <GPG key ID>
```

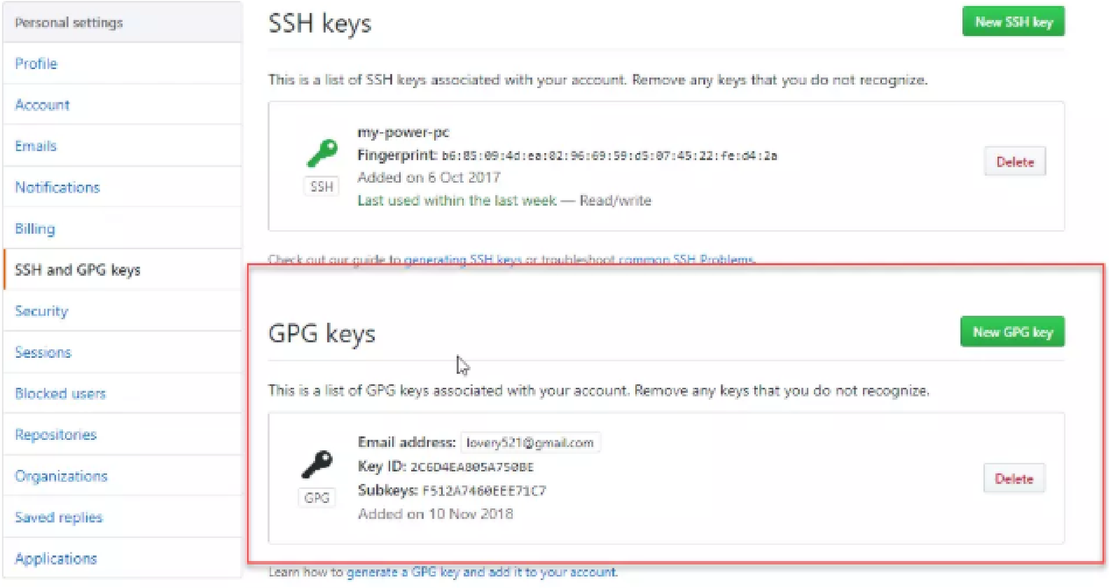


```
$ gpg --armor --export CEBA4222C95DA17B
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBF2tSwYBEADH5X66ZmfXKFHbFdKVfXNgFzRhXAiOCE7vbDPCyfKA6qO7RLjS
nO8fzQhiUjYnYE3vGbHUUs8RkO11Y2Cvgy12KeaJDXctO9W7toPngwjDpVhZJkGH
TAaLmgX4pJv8k3lXTLByBvBEoGLTyJNO6+5i6MmmiOMTPHFs+NQVrjLl5lMbuANq
Ui6qC5ARCv+3oCcU2BuPJZ8uHdCrl7w6rYlfOpba/kXqwrjOEa2teziad+DpO5Mp
G9hp1bWHQD6suOeHBfRo4tbXBipu/NJX3YUXFgrHoiOs8sHIXFoovBn2iCn9dbhx
DcfHi+zpQR1FmCBh58iFEW4pVdOsBqQ8GMdMbAxPB4+jQdDYU/9El9UK+d9bWqmb
Z4Ug4WhP4OCiiioAseY44auCmvHOnmE+h4jBlz49RdnYlCf1EjnctLdp4lxB+bGk
Fc5edPUYkULIyMO9fl6wHEZsTqnPuT9CfMSxlWQlNMKPmxcMLFOglhA+ajRWPTJM
FI1aWY6xnc0EE3GMyZf/qoDNPV4oOp98WHJdVMeg9boyqFfW9tNVc1z/ir4cidNp
FQBt6EoC+JlBBUNtCkkzTthg6ilzB5oT6n46Kstk5fBgyhGbAdPvwuXwKScedoqS
Xjf7qM4jODlQOLb6MiAa1FGJ7zJ5KjhlWqkHeMGIjEjbb11pNraiWX7YdwARAQAB
tBptci16aGwgPDE5NzExNjk4NDZAcXEuY29tPokCVAQTAQgAPhYhBFumCK6nrxpE
WsL4GM66QiLJXaF7BQJdrUsGAhsDBQkJZgGABQsJCAcCBhUKCQgLAgQWAgMBAh4B
AheAAAoJEM66QiLJXaF7Pn4QALGNKQwIkaaeuulWpFJ9ON6OoNga6d7O/VpvDtN8
2knnZ/EqV5c36iDvVz7C/Syml3DOBes4jMCzzfcMoSXqpaaGTlAGg5Xa3xmzteT1
oW1xzfPWJfy7F1wG4eDhEyllEt1LcZnQppysJf7pFqkngNqwvLi64NzN6d+lQO/1
TqCZVFTKzYA3QOYr9O3l+RbOuLGrzOehxrdN37k78VTcYmJrewvqAEb1QjRBjEby
```

GPG key ID为私钥ID或公钥ID都可以。输出的内容就是我们要的GPG Keys了。点开GitHub的GPG配置页面，粘贴该内容。

向github添加gpg密钥

首先打开github用户设置，然后在`SSH and GPG keys`中添加GPG密钥，然后将上面得到的包括`BEGIN`和`END`在内的东西复制进去并选择添加，这样就完成了GPG密钥的添加工作。



This is a list of SSH keys associated with your account. Remove any keys that you do not recognize.

my-power-pc
Fingerprint: b6:85:09:4d:ea:82:96:69:59:d5:07:45:22:fe:d4:2a
Added on 6 Oct 2017
Last used within the last week — Read/write

Check out our guide to generating SSH keys or troubleshoot common SSH Problems.

This is a list of GPG keys associated with your account. Remove any keys that you do not recognize.

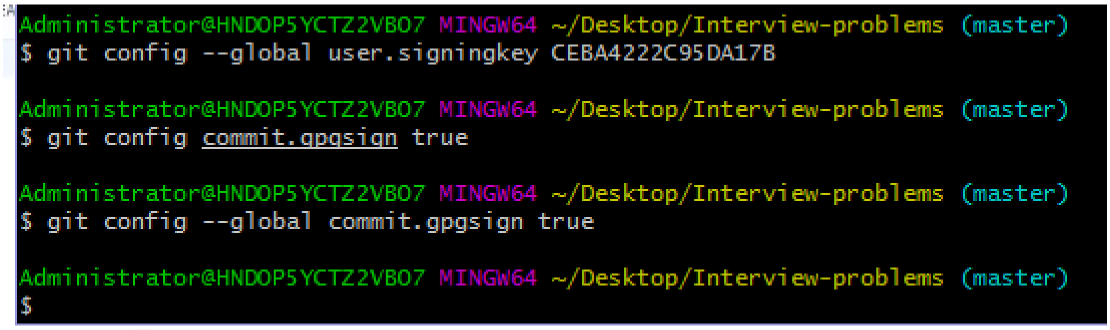
Email address: lovery521@gmail.com
Key ID: 2C6D4EA805A750BE
Subkeys: F512A7460EEE71C7
Added on 10 Nov 2018

Learn how to generate a GPG key and add it to your account.

添加gpg密钥

2.将密钥ID添加到git设置中：

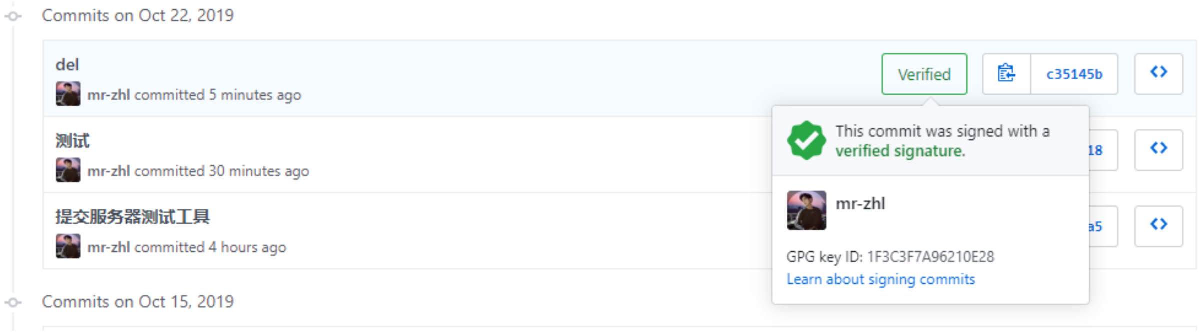
```
git config --global user.signingkey 831CF40177EA9999
```



```
Administrator@HNDOP5YCTZ2VBO7 MINGW64 ~/Desktop/Interview-problems (master)
$ git config --global user.signingkey CEBA4222C95DA17B

Administrator@HNDOP5YCTZ2VBO7 MINGW64 ~/Desktop/Interview-problems (master)
$ git config commit.gpgsign true

Administrator@HNDOP5YCTZ2VBO7 MINGW64 ~/Desktop/Interview-problems (master)
$ git config --global commit.gpgsign true

Administrator@HNDOP5YCTZ2VBO7 MINGW64 ~/Desktop/Interview-problems (master)
$
```

这样一来，在使用`git commit`命令提交的时候，就会用gpg来签名提交，当然也可以在提交的时候使用`git commit -S`参数来显式启用验证。

最后，当项目提交到Github之后，点击进入提交详情查看的时候，就可以看到一个绿色的Verified标志，表示这次提交已经经过验证，确认是作者本人的提交了。



Commits on Oct 22, 2019

del
mr-zhl committed 5 minutes ago

测试
mr-zhl committed 30 minutes ago

提交服务器测试工具
mr-zhl committed 4 hours ago

Commits on Oct 15, 2019

Verified

c35145b

This commit was signed with a verified signature.

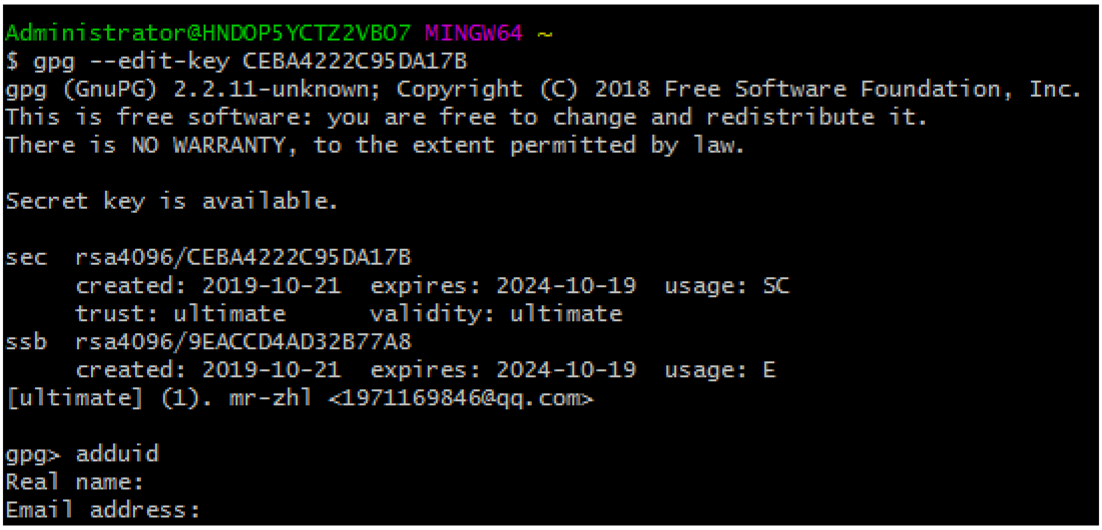
mr-zhl

GPG key ID: 1F3C3F7A96210E28
Learn about signing commits

3.我们可以通过以下命令查询本机所有的Key:

```
gpg --list-secret-keys
gpg --list-keys
```

五.如果想要修改邮件,也可以修改



```
Administrator@HNDOP5YCTZ2VBO7 MINGW64 ~
$ gpg --edit-key CEBA4222C95DA17B
gpg (GnuPG) 2.2.11-unknown; Copyright (C) 2018 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec  rsa4096/CEBA4222C95DA17B
     created: 2019-10-21  expires: 2024-10-19  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa4096/9EACCD4AD32B77A8
     created: 2019-10-21  expires: 2024-10-19  usage: E
[ultimate] (1). mr-zhl <1971169846@qq.com>

gpg> adduid
Real name:
Email address:
```

具体可以访问:

```
https://help.github.com/cn/github/authenticating-to-github/associating-an-email-with-your-gpg-key
```