Trabalho 3

Nome: Renan Rocha Souto dos Santos

Servidor utilizado: https://keyserver.ubuntu.com/

1) Criar certificado PGP.

renan.rocha@grad.ufsc.br: link.
ID: 006351923ceeb9cc

```
❯ gpg --gen-key
gpg (GnuPG) 2.2.32; Copyright (C) 2021 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.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: Renan Rocha
Email address: renan.rocha@grad.ufsc.br
You selected this USER-ID:
    "Renan Rocha <renan.rocha@grad.ufsc.br>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit?
Change (N)ame, (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: key 006351923CEEB9CC marked as ultimately trusted
gpg: directory '/home/effectrenan/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/effectrenan/.gnupg/openpgp-revocs.d/36B5D68E8433CD54C4BF5566006351923CEEB9CC.rev'
public and secret key created and signed.

pub   rsa3072 2022-02-05 [SC] [expires: 2024-02-05]
      36B5D68E8433CD54C4BF5566006351923CEEB9CC
uid                      Renan Rocha <renan.rocha@grad.ufsc.br>
sub   rsa3072 2022-02-05 [E] [expires: 2024-02-05]
```

Referência:
https://help.ubuntu.com/community/GnuPrivacyGuardHowto#Generating_an_OpenPGP_Key

2) Crie um novo certificado GPG para este trabalho individual (Não use o teu certificado pois este novo será revogado). Coloque esse certificado de testes no servidor GPG. Depois verifique seu status. Então, crie um certificado de revogação e revogue o certificado de testes.

renan.rocha+2@grad.ufsc.br: link.
ID: 8F04A22A769ECF4A.

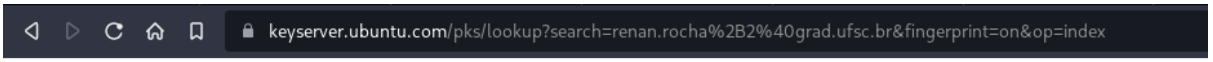
```
gpg (GnuPG) 2.2.32; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: Renan Rocha 2
Email address: renan.rocha+2@grad.ufsc.br
You selected this USER-ID:
    "Renan Rocha 2 <renan.rocha+2@grad.ufsc.br>"

Change (N)ame, (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: key 8F04A22A769ECF4A marked as ultimately trusted
gpg: revocation certificate stored as '/home/effectrenan/.gnupg/openpgp-revocs.d/3ED9592CEFC48B30B0B703CE8F04A22A769ECF4A.rev'
public and secret key created and signed.

pub   rsa3072 2022-02-05 [SC] [expires: 2024-02-05]
      3ED9592CEFC48B30B0B703CE8F04A22A769ECF4A
uid                      Renan Rocha 2 <renan.rocha+2@grad.ufsc.br>
sub   rsa3072 2022-02-05 [E] [expires: 2024-02-05]
```

Exportando certificado de revogação de renan.rocha+2@grad.ufsc.br (8F04A22A769ECF4A) :

```
❯ gpg --output revoke2.asc --gen-revoke 8F04A22A769ECF4A

sec  rsa3072/8F04A22A769ECF4A 2022-02-05 Renan Rocha 2 <renan.rocha+2@grad.ufsc.br>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? test revocation ufsc 2
Invalid selection.
Your decision? 0
Enter an optional description; end it with an empty line:
> test revocation ufsc 2
>
Reason for revocation: No reason specified
test revocation ufsc 2
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!
```

Enviando para o servidor:

```
❯ gpg --keyserver keyserver.ubuntu.com --send-keys 8F04A22A769ECF4A
gpg: sending key 8F04A22A769ECF4A to hkp://keyserver.ubuntu.com
```



Search results for 'renan.rocha+2@grad.ufsc.br'

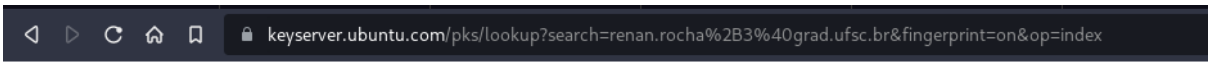
```
Type bits/keyID            cr. time   exp time   key expir
```

```
pub rsa3072/3ed9592cefc48b30b0b703ce8f04a22a769ecf4a 2022-02-05T18:35:30Z
        Hash=cfc3fe47657caf0708176e593220089a
sig revok 8f04a22a769ecf4a 2022-02-05T20:11:17Z ____________________ ____________________ [selfsig]

uid Renan Rocha 2 <renan.rocha+2@grad.ufsc.br>
sig  sig  8f04a22a769ecf4a 2022-02-05T18:35:30Z 2024-02-05T18:35:30Z ____________________ [selfsig]

sub rsa3072/c7452c0b537bf35b527f2bef72a114dd1f2b269d 2022-02-05T18:35:30Z
sig sbind 8f04a22a769ecf4a 2022-02-05T18:35:30Z ____________________ 2024-02-05T18:35:30Z []
```

3) Pratique a revogação de assinaturas e certificados GPG. Assine um certificado qualquer GPG (de outra pessoa). E envie esse certificado para o servidor GPG. Depois verifique o status do certificado. E então, revogue a assinatura que você fez. Confira o resultado no servidor GPG.

renan.rocha+3@grad.ufsc.br: link.
ID: 20f603be29382e2b.

Status do certificado criado para renan.rocha+3@grad.ufsc.br (20f603be29382e2b):



Search results for 'renan.rocha+3@grad.ufsc.br'

```
Type bits/keyID            cr. time   exp time   key expir
```

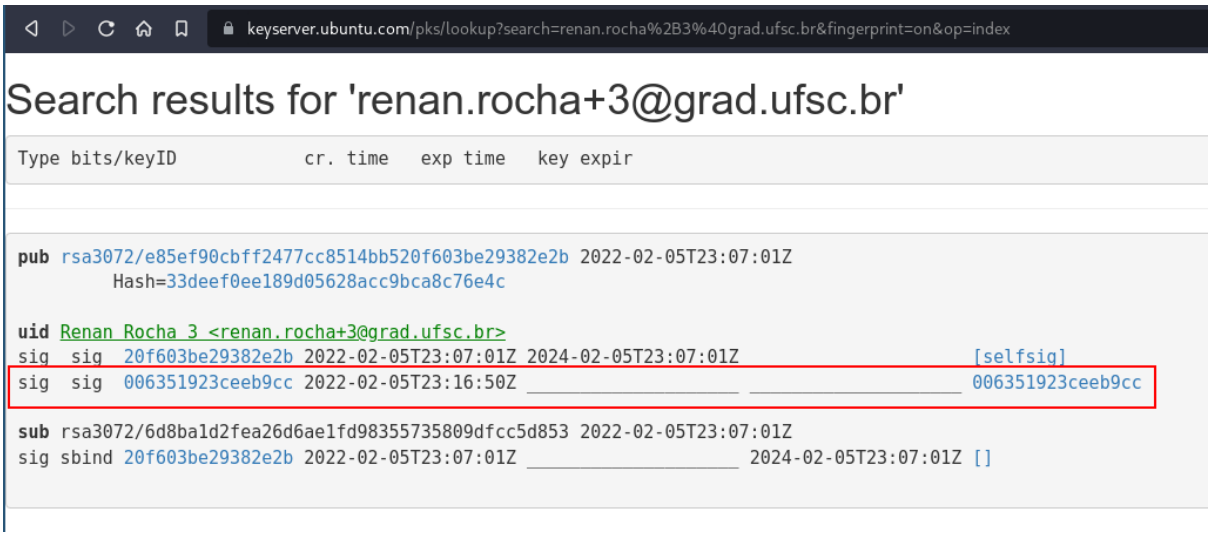
```
pub rsa3072/e85ef90cbff2477cc8514bb520f603be29382e2b 2022-02-05T23:07:01Z
        Hash=1433d28940b0bf78e05b7b19194594a8

uid Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>
sig  sig  20f603be29382e2b 2022-02-05T23:07:01Z 2024-02-05T23:07:01Z ____________________ [selfsig]

sub rsa3072/6d8ba1d2fea26d6ae1fd98355735809dfcc5d853 2022-02-05T23:07:01Z
sig sbind 20f603be29382e2b 2022-02-05T23:07:01Z ____________________ 2024-02-05T23:07:01Z []
```

Assinando renan.rocha+3@grad.ufsc.br (20f603be29382e2b) com renan.rocha@grad.ufsc.br (006351923ceeb9cc):

```
❯ gpg --sign-key "renan.rocha+3@grad.ufsc.br"

gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   3  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 3u
gpg: next trustdb check due at 2024-02-05
sec  rsa3072/20F603BE29382E2B
     created: 2022-02-05  expires: 2024-02-05  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/5735809DFCC5D853
     created: 2022-02-05  expires: 2024-02-05  usage: E
[ultimate] (1). Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>


sec  rsa3072/20F603BE29382E2B
     created: 2022-02-05  expires: 2024-02-05  usage: SC
     trust: ultimate      validity: ultimate
 Primary key fingerprint: E85E F90C BFF2 477C C851  4BB5 20F6 03BE 2938 2E2B

     Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>

This key is due to expire on 2024-02-05.
Are you sure that you want to sign this key with your
key "Renan Rocha <renan.rocha@grad.ufsc.br>" (006351923CEEB9CC)

Really sign? (y/N) y
```

Enviando para o servidor:

```
❯ gpg --send-keys --keyserver keyserver.ubuntu.com 20F603BE29382E2B
gpg: sending key 20F603BE29382E2B to hkp://keyserver.ubuntu.com
```



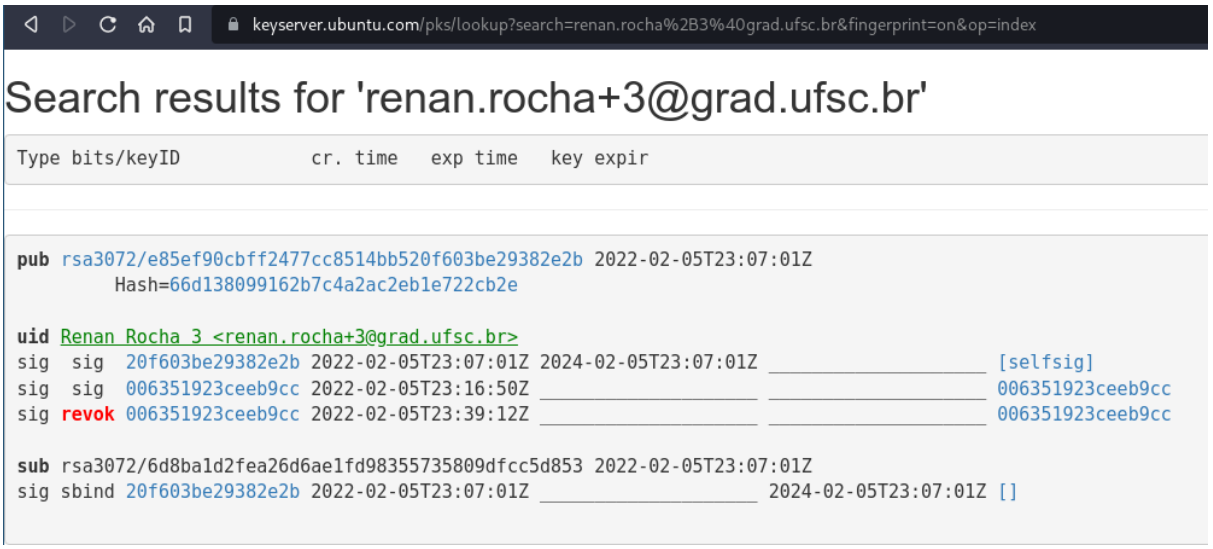
Revogação de renan.rocha@grad.ufsc.br (006351923ceeb9cc) por renan.rocha+3@grad.ufsc.br (20f603be29382e2b):

```
❯ gpg --edit-key 20F603BE29382E2B
gpg (GnuPG) 2.2.32; Copyright (C) 2021 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  rsa3072/20F603BE29382E2B
     created: 2022-02-05  expires: 2024-02-05  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/5735809DFCC5D853
     created: 2022-02-05  expires: 2024-02-05  usage: E
[ultimate] (1). Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>

gpg> revsig
You have signed these user IDs on key 20F603BE29382E2B:
     Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>
   signed by your key 20F603BE29382E2B on 2022-02-05
   signed by your key 006351923CEEB9CC on 2022-02-05

user ID: "Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>"
signed by your key 20F603BE29382E2B on 2022-02-05
Create a revocation certificate for this signature? (y/N) n
user ID: "Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>"
signed by your key 006351923CEEB9CC on 2022-02-05
Create a revocation certificate for this signature? (y/N) y
You are about to revoke these signatures:
     Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>
   signed by your key 006351923CEEB9CC on 2022-02-05
Really create the revocation certificates? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  4 = User ID is no longer valid
  Q = Cancel
Your decision? 0
Enter an optional description; end it with an empty line:
> test revocate ufsc
>
Reason for revocation: No reason specified
test revocate ufsc
Is this okay? (y/N) y
```

```
sec  rsa3072/20F603BE29382E2B
     created: 2022-02-05  expires: 2024-02-05  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/5735809DFCC5D853
     created: 2022-02-05  expires: 2024-02-05  usage: E
[ultimate] (1). Renan Rocha 3 <renan.rocha+3@grad.ufsc.br>

gpg> save
```

Enviando para o servidor:

```
❯ gpg --send-keys --keyserver keyserver.ubuntu.com 20F603BE29382E2B
gpg: sending key 20F603BE29382E2B to hkp://keyserver.ubuntu.com
```



Referência:
https://www.digitalocean.com/community/tutorials/how-to-use-gpg-to-encrypt-and-sign-messages

4) O que é o anel de chaves privadas? Como está estruturado? Na sua aplicação GPG onde este anel de chaves é armazenado? Quem pode ter acesso a esse porta chaves?

O PGP armazena as chaves em dois arquivos em disco, um para as chaves públicas e outro para as chaves privadas. Assim, o anel de chaves representa o arquivo que contém as chaves. Para o anel de chaves privadas, somente são salvas as chaves privadas nesse arquivo. Somente o proprietário deve ter acesso ao anel de chaves privadas, já que são essas chaves são responsáveis por decifrar as mensagens e o arquivo é protegido por uma senha criada pelo proprietário. Consequentemente, caso um anel de chaves privadas for perdido, não é possível decifrar as mensagens para esse anel. A estrutura consiste em:

- Timestamp: A data/hora em que o par de chaves foi gerado.
- Key ID: Identificador formado pelos 64 bits menos significativos da chave pública.
- Public key: A parte de chave pública.
- Private key: A parte de chave privada do par (campo criptografado).
- User ID: Identificador do usuário. Normalmente usa-se o e-mail do usuário.

Referência: Livro Cryptography and Network Security, página 643.

5) Qual a diferença entre assinar uma chave local e assinar no servidor?

Quando uma chave é assinada no servidor, a mudança se torna pública. Portanto, qualquer usuário que fizer uma consulta no servidor poderá ver as assinaturas,

assim tornando um processo sincronizado. Quando a assinatura acontece somente de forma local, os outros usuários só conseguem validar a assinatura se a chave assinalada for exportada e enviada.

6) O que é e como é organizado o banco de dados de confiabilidade?

O PGP fornece o banco e dados de confiança para associar a confiança das chaves públicas e explorar informações de confiança, representado pelo arquivo *trustdb.gpg*. Por exemplo, é possível um usuário confiar nas assinaturas de outros usuários a partir do comando *trust* no gpg, que irá então atualizar o *trustdb*. Em relação à estrutura, cada entrada no anel de chave pública é um certificado de chave pública. Associado a cada uma dessas entradas está um campo chave de legitimidade que indica até que ponto o PGP confiará que esta é uma chave pública válida para este usuário; quanto mais alto o nível de confiança, mais forte é a ligação desse ID de usuário a essa chave. Por sua vez, cada assinatura tem associado a ela um campo de confiança de assinatura que indica a grau em que este usuário PGP confia no signatário para certificar chaves públicas. O campo de legitimidade chave é derivado da coleção de campos de confiança de assinatura na entrada. Assim, cada entrada define uma chave pública associada a um proprietário específico, e um campo de confiança do proprietário, que indica o grau em que essa chave pública é confiável para assinar outros certificados de chaves públicas; este nível de confiança é atribuído pelo do utilizador.

Referência: Livro Cryptography and Network Security, página 649.

7) O que são e para que servem as sub-chaves?

As sub-chaves servem como uma cópia das chaves primárias. Assim, elas possuem as mesma veracidade, entretanto podem proporcionar algumas vantagens, tais como:

- Poder armazenar a chave primária offline ou em um dispositivo mais seguro. Se uma máquina com uma sub-chave for danificada, pode-se facilmente revogar a sub-chave sem todas as dificuldades de revogar sua chave primária (compartilhar uma nova chave, obter novas assinaturas, ...).
- Ter diferentes sub-chaves em diferentes máquinas.
- Usar uma chave primária com maior vida útil longa e sub-chaves com menos, porém mais rápidas, para uso diário.

Referências:

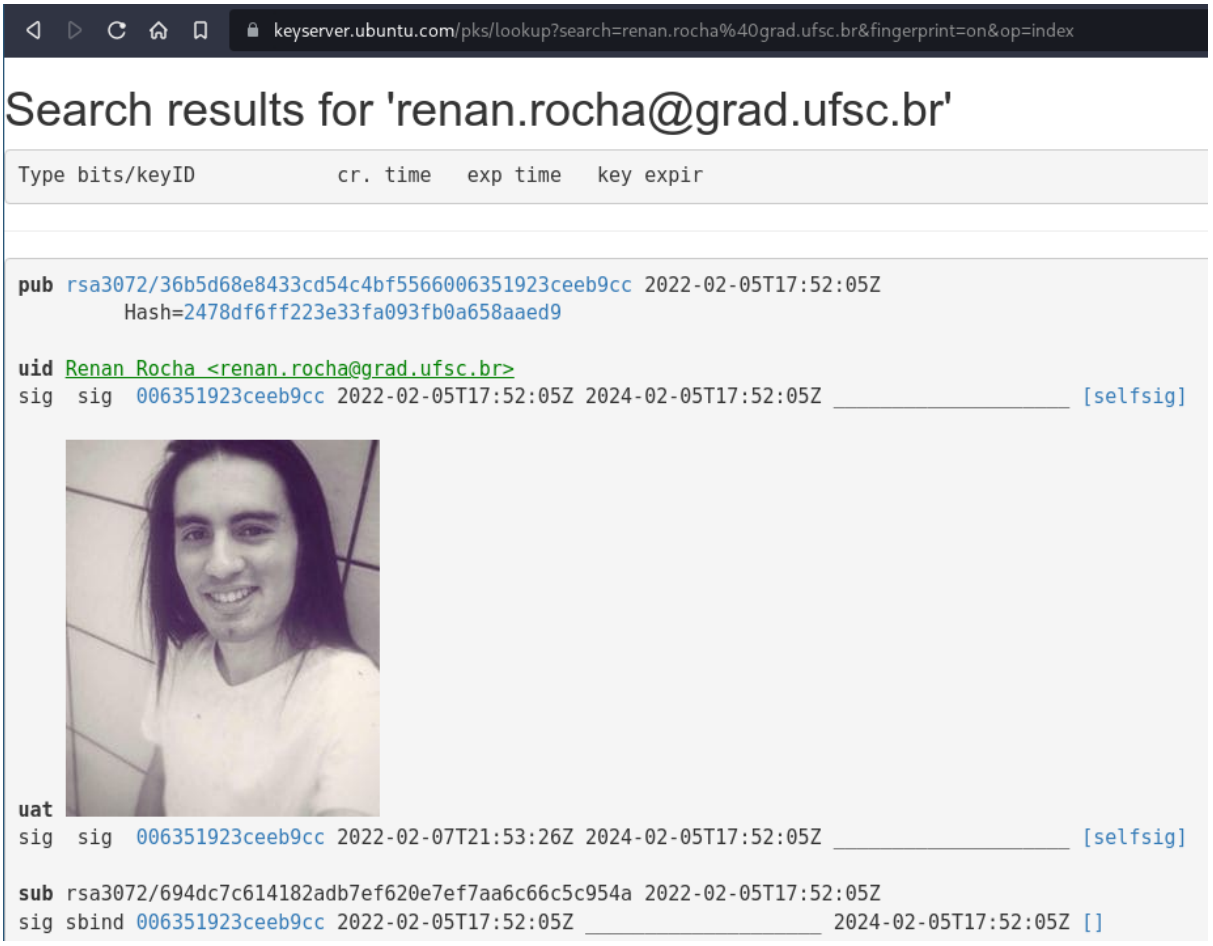
- https://wiki.debian.org/Subkeys
- https://security.stackexchange.com/questions/76940/what-exactly-is-a-subkey

8) Coloque sua foto (ou uma figura qualquer) que represente você em seu certificado GPG.

Certificado: renan.rocha@grad.ufsc.br (006351923CEEB9CC).

Comandos executados:

```
gpg --edit-key 006351923CEEB9CC
   addphoto
   /path/file
   save

gpg --send-keys --keyserver keyserver.ubuntu.com 006351923CEEB9CC
```



Referência: Livro PGP & GPG, Autor Michael W. Lucas, páginas 126-127.

9) O que é preciso para criar e manter um servidor de chaves GPG, sincronizado com os demais servidores existentes?

É necessário possuir espaço de armazenamento suficiente para suportar a estrutura. Possuir um servidor DNS para poder definir um endereço para o servidor. E manter o servidor sincronizado através do protocolo SKS.

Referências:

- https://www.researchgate.net/publication/338479605_BlockPGP_A_Blockchain-based_Framework_for_PGP_Key_Servers
- https://roll.urown.net/server/pgp-keyserver.html

10) Dê um exemplo de como tornar sigiloso um arquivo usando o GPG. Envie esse arquivo para um colega. Você deve decifrar e recuperar o conteúdo original.

Remetente: renan.rocha@grad.ufsc.br (006351923ceeb9cc).
Destinatário: renan.rocha+3@grad.ufsc.br (20f603be29382e2b).
Arquivo: file.txt.

Conteúdo do arquivo *file.txt*:

```
this is renan.rocha@grad.ufsc.br
```

Cifrando o arquivo *file.txt*:

```
gpg --output file.gpg --encrypt --default-key "renan.rocha@grad.ufsc.br" --recipient "renan.rocha+3@grad.ufsc.br" file.txt
```

Leitura do conteúdo do arquivo cifrado:

```
gpg --output output.txt --decrypt --default-key "renan.rocha+3@grad.ufsc.br" file.gpg
```

Conteúdo da saída output.txt:

```
❯ cat output.txt
this is renan.rocha@grad.ufsc.br
```

Referência: https://www.gnupg.org/gph/en/manual/x110.html

11) Mostre um exemplo de como assinar um arquivo (assinatura anexada e outro com assinatura separada), usando o GPG. Envie uma mensagem assinada para um colega. Esse colega deve enviar para você outra mensagem assinada. Verifique se a assinatura está correta.

Assinador: renan.rocha@grad.ufsc.br (006351923ceeb9cc).
Verificador: renan.rocha+3@grad.ufsc.br (20f603be29382e2b).

Conteúdo do arquivo file.txt:

```
this is renan.rocha@grad.ufsc.br
```

Assinando com assinatura anexada o arquivo *file.txt* com renan.rocha@grad.ufsc.br. Comando:

```
gpg --output file.sig  --default-key "renan.rocha@grad.ufsc.br" --sign file.txt
```

Lendo arquivo com renan.rocha+3@grad.ufsc.br. Comando:

```
gpg --default-key "renan.rocha+3@grad.ufsc.br" --output doc --decrypt file.sig
```

```
gpg: Signature made Mon 07 Feb 2022 10:39:07 PM -03
gpg:                using RSA key 36B5D68E8433CD54C4BF5566006351923CEEB9CC
gpg:                issuer "renan.rocha@grad.ufsc.br"
gpg: Good signature from "Renan Rocha <renan.rocha@grad.ufsc.br>" [ultimate]
gpg:                 aka "[jpeg image of size 6814]" [ultimate]
❯ cat doc
this is renan.rocha@grad.ufsc.br
```

Assinando com assinatura separada o arquivo *file.txt* com renan.rocha@grad.ufsc.br. Comando:

```
gpg --output file.sig  --default-key "renan.rocha@grad.ufsc.br" --detach-sign file.txt
```

Verificando assinatura com o renan.rocha+3@grad.ufsc.br. Comando:

```
gpg --default-key "renan.rocha+3@grad.ufsc.br" --verify file.sig file.txt
```

```
gpg: Signature made Mon 07 Feb 2022 10:25:44 PM -03
gpg:                using RSA key 36B5D68E8433CD54C4BF5566006351923CEEB9CC
gpg:                issuer "renan.rocha@grad.ufsc.br"
gpg: Good signature from "Renan Rocha <renan.rocha@grad.ufsc.br>" [ultimate]
gpg:                 aka "[jpeg image of size 6814]" [ultimate]
```

Referência: https://www.gnupg.org/gph/en/manual/x135.html