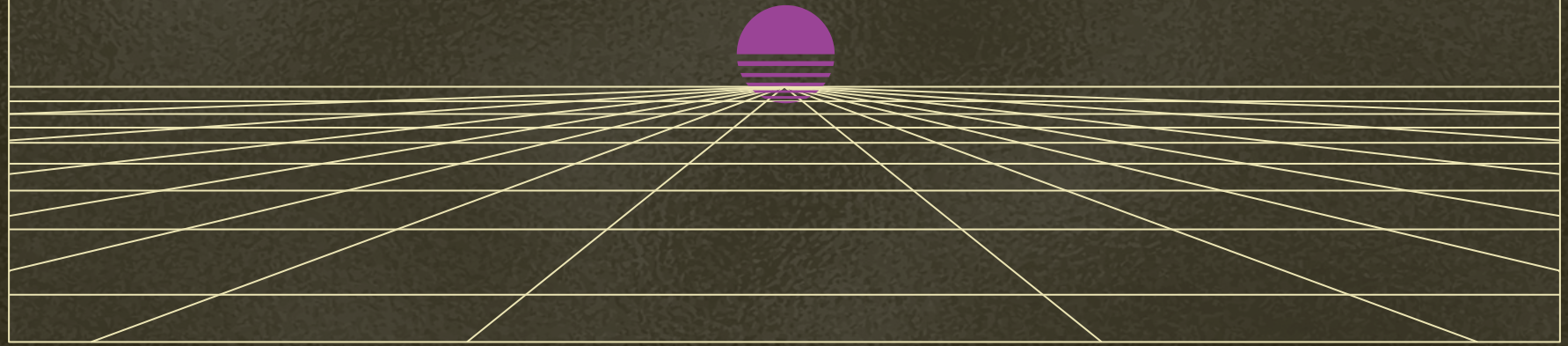
GNU PRIVACY GUARD

Um guia prático



$whoami

Wilgnne Riann

Graduado em Defesa Cibernética e Sistemas para Internet. Atualmente representa Alagoas nas Olimpíadas do Senai em Cybersecurity. CTF-player, entusiasta da segurança da informação e simpatizante do movimento Software Livre.

01

Conceitos Iniciais

Contexto atual de vigilância e criptografia

02

GnuPG

Entendendo o GPG

03

GPG Pair-Keys

Gerando e exportando chaves públicas e privadas

04

Criptografando comunicações

Encrypt/Decrypt de mensagens e arquivos

05

Compartilhando chaves públicas

Como compartilhar chaves públicas com outros usuários

06

Conclusão

Referências e links para acesso

Quem interessa?

Ativistas

Jornalistas

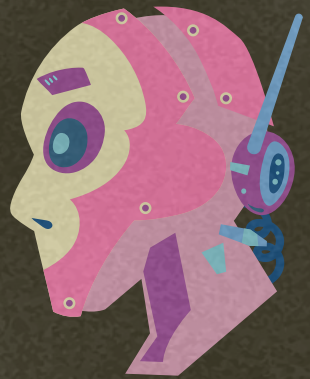
Denunciantes

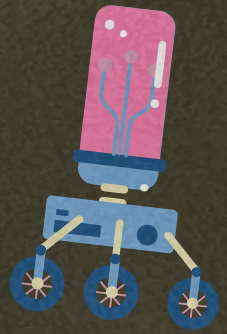
Pessoas preocupadas com a privacidade

Conceitos Iniciais

Vigilância Cibernética

A coleta sistemática de dados sobre uma população sem o seu consentimento

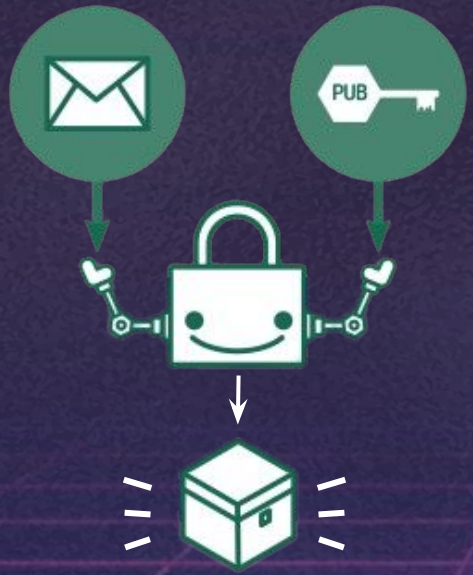


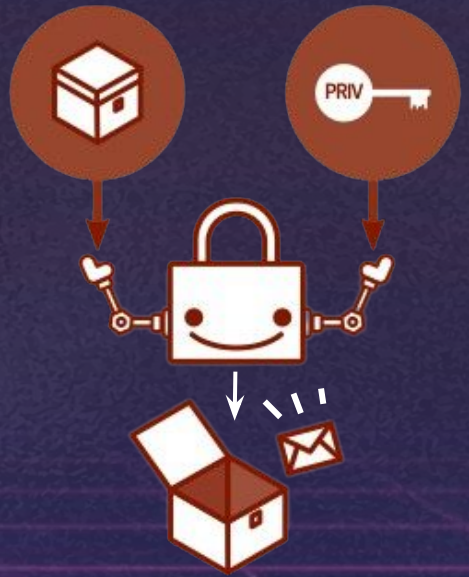


Criptografia

Prática de proteger a comunicação, tornando-a indecifrável para quem não tenha as chaves

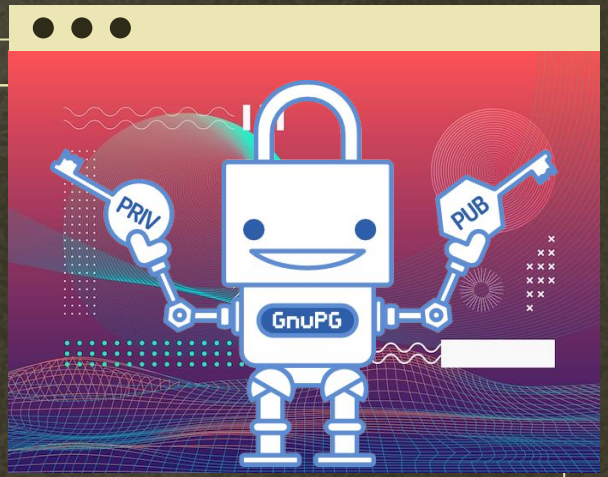
A chave pública e chave privada





Entendendo GNU Privacy Guard

Software Livre que fornece criptografia de e-mail e arquivos. É uma implementação do OpenPGP, que é um padrão de criptografia de dados.



Gerando o par de chaves

```
exiled@cyberia:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; 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.

gpg: directory '/home/exiled/.gnupg' created
gpg: keybox '/home/exiled/.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)
  (14) Existing key from card
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) 1w
Key expires at Wed 10 May 2023 08:36:39 PM -03
Is this correct? (y/N) y
```

512 bits

Em 1999, levou-se 6 meses com hardware avançado da época, hoje pode ser quebrado em 4h

2048 bits

Um computador clássico levaria cerca de ~300 trilhões de anos para quebrar a chave

Informações do par de chaves

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

Real name: Wilgnne Riann
Email address: exiled_contact@proton.me
Comment:
You selected this USER-ID:
    "Wilgnne Riann <exiled_contact@proton.me>"

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/exiled/.gnupg/trustdb.gpg: trustdb created
gpg: key 582AE89F35165EF7 marked as ultimately trusted
gpg: directory '/home/exiled/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/exiled/.gnupg/openpgp-
revocs.d/D6D16DF844592D2D22C74698582AE89F35165EF7.rev' public and secret key created and signed.

pub   rsa4096 2023-05-03 [SC] [expires: 2023-05-10]
      D6D16DF844592D2D22C74698582AE89F35165EF7
uid                      Wilgnne Riann <exiled_contact@proton.me>
sub   rsa4096 2023-05-03 [E] [expires: 2023-05-10]

exiled@cyberia:~$
```

Exportando a chave privada

```
exiled@cyberia:~$ gpg --list-keys exiled_contact@proton.me
pub   rsa4096 2023-05-03 [SC] [expires: 2023-05-10]
      D6D16DF844592D2D22C74698582AE89F35165EF7
uid           [ultimate] Wilgnne Riann <exiled_contact@proton.me>
sub   rsa4096 2023-05-03 [E] [expires: 2023-05-10]

exiled@cyberia:~$ gpg --export-secret-keys -a D6D16DF844592D2D22C74698582AE89F35165EF7 > secret_key.asc


┌──────────────────────────────────────────────────┐
| Please enter the passphrase to export the OpenPGP secret key:  |
| "Wilgnne Riann <exiled_contact@proton.me>"       |
| 4096-bit RSA key, ID 582AE89F35165EF7,           |
| created 2023-05-03.                              |
|                                                  |
|                                                  |
| Passphrase: _____________________________________ |
|                                                  |
|         <OK>                          <Cancel>   |
└──────────────────────────────────────────────────┘

exiled@cyberia:~$ ls -la secret_key.asc
-rw-r--r-- 1 exiled exiled 6781 May  4 00:34 secret_key.asc

exiled@cyberia:~$
```

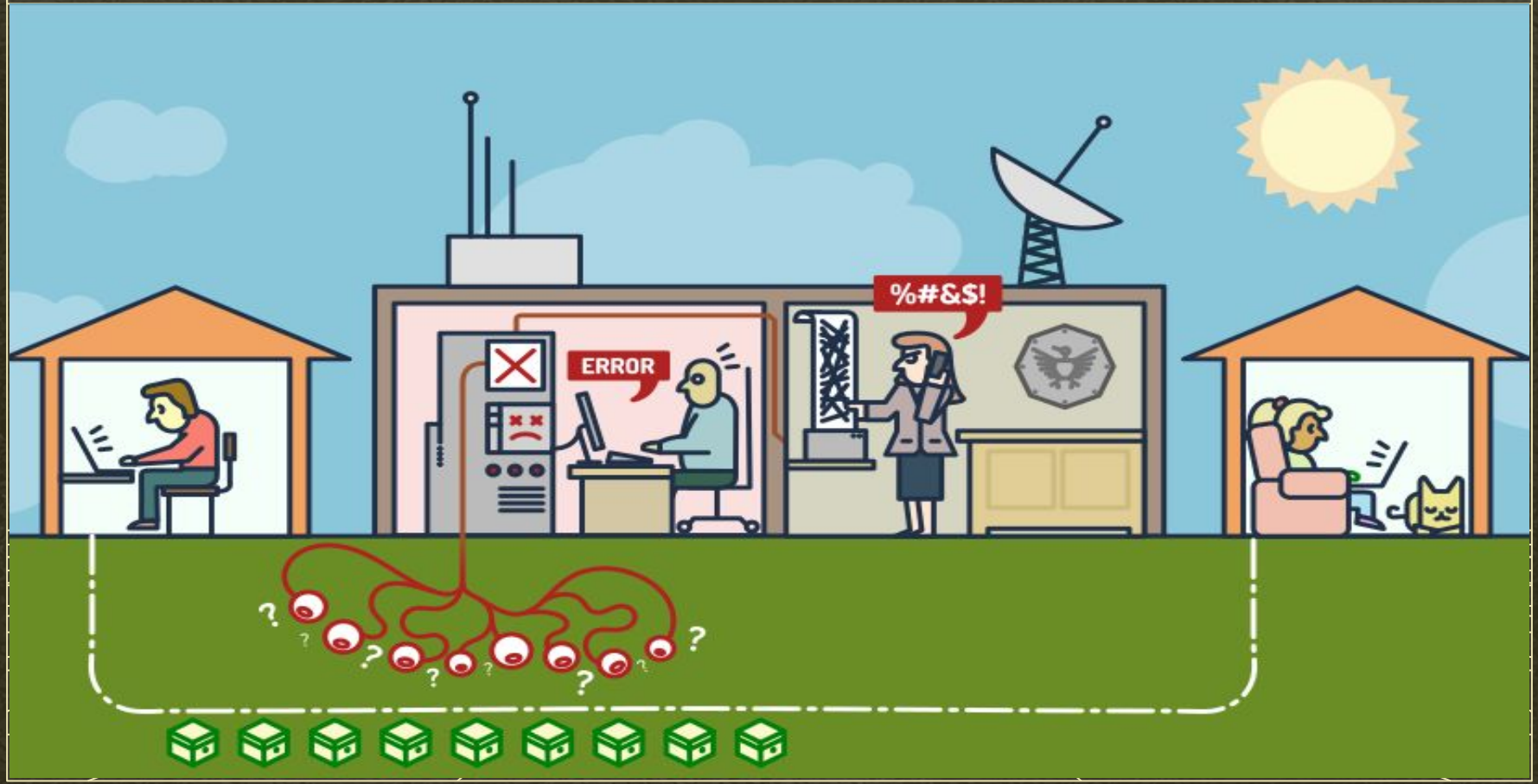
Como se parecem as chaves

```
gpg --export -a exiled_contact@proton.me > public_key.asc
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGRS8WIBEACkwFORykGMurmX3U6gstKlmNuyTOjEqQv8GGOjFiYofIxxusmg
MLROVQJdKzZ9CyQJ5e5F81yA0l5LoruWURCE3x5W0+W2I80fGSy9tl/R7HyAMOH5
yJ1/olGRFQqOb0C8en8Ycl/1bKhKtQnzE536EPE7EHF+ltbdo7T0QB6kqv3AO2hh
3yNPS6U+O90rp2oy+koYnf3s5FMCfeQw9uR/OhFKDzgFAJvQr8SP7wMHj7Gu3OOc
diCKycv+fi190A4q3fqQ9Tc+AsiXrOr7I7nrsJsG2ZIO++21gGzYWTSdlNCfdTvb
7Zdwbz3iyje/CHnvKnkxbXu/7sDkp6wQB2AMq+QHfs0JT0DtXm6AUuNjgmrzhAAS
                          [...]
w1Y7QCMALzhemZd8LZIsGHY20dSKACbLTnZBpSt5PodL0SpDbr5CZxIidBSUcyBp
CZm0TwwAQAPOGpoyq9fpphh9CJCEmTBlIx7aJ8RcvTXV7KO4fzxlWwL8nG3ilzru
h9m1/2sdO8ZQQ+t8tA9qaFXyzXWljXyd6EFNkfpXFjiVEfzkAHpFa/Asa6jeSB0X
ZgqxOumRZicM/NrPtDZFXjik7a26uzESvesqTIUG99hJTtxZm0NchN7pxVbvWQlt
IPTuMITO3ppxXiV0i58YN1EcqSLu4AiLobrmeQo04+cnzEEIlwctgU1ZYS4XODm6
g559PCRZLmRPGNBOnQCskxP5RSpyeablO+tJBk6TgwHITqu5umx8aREuKXlEKkIf
JKmfa8+L5Eenp5rYwT6h9JyjHdunprQS/GBwmvwCli5/OrbLmooifEUPgLJTZp55
Kkf9jPLQPe3QxTprXXbP33HA73ZrSQOxIIvzmy5gpBqYUkZxQuk0A/wgdjLEmQfy
y0uHk0ZWleHy0HQZKTW85/bpGpaOIvGM7GtdyEqntP/o7hN7ov4D0VlotPSyhb8+
/HhDkrH1Cq1tJRq7hSHWSg==
=kDta
-----END PGP PUBLIC KEY BLOCK-----
```

```
gpg --export-secret-keys -a key_id > secret_key.asc
```

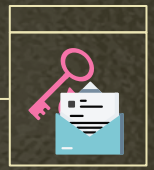
```
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQdGBGRS8WIBEACkwFORykGMurmX3U6gstKlmNuyTOjEqQv8GGOjFiYofIxxusmg
MLROVQJdKzZ9CyQJ5e5F81yA0l5LoruWURCE3x5W0+W2I80fGSy9tl/R7HyAMOH5
yJ1/olGRFQqOb0C8en8Ycl/1bKhKtQnzE536EPE7EHF+ltbdo7T0QB6kqv3AO2hh
3yNPS6U+O90rp2oy+koYnf3s5FMCfeQw9uR/OhFKDzgFAJvQr8SP7wMHj7Gu3OOc
diCKycv+fi190A4q3fqQ9Tc+AsiXrOr7I7nrsJsG2ZIO++21gGzYWTSdlNCfdTvb
7Zdwbz3iyje/CHnvKnkxbXu/7sDkp6wQB2AMq+QHfs0JT0DtXm6AUuNjgmrzhAAS
                          [...]
LBh2NtHUigAmy052QaUreT6HS9EqQ26+QmcSInQUlHMgaQmZtE8MAEADzhqaMqvX
6aYYfQiQhJkwZSMe2ifEXL011eyjuH88ZVsC/Jxt4pc67ofZtf9rHTvGUEPrfLQP
amhV8s11pY18nehBTZH6VxY4lRH85AB6RWvwLGuo3kgdF2YKsTrpkWYnDPzaz7Q2
RV44pO2tursxEr3rKkyFBvfYSU7cWZtDXITe6cVW71kJbSD07jCEzt6acV4ldIuf
GDdRHKki7uAIi6G65nkKNOPnJ8xBCJcHLYFNWWEuFzg5uoOefTwkWS5kTxjQTp0A
rJMT+UUqcnmm5TvrSQZOk4MByE6rubpsfGkRLil5RCpCHySpn2vPi+RHp6ea2ME+
ofScox3bp6a0EvxgcJr8ApYufzq2y5qKInxFD4CyU2aeeSpH/Yzy0D3t0MU6a112
z99xwO92a0kDsSCL85suYKQamFJGcULpNAP8IHYyxJkH8stLh5NGVpXh8tB0GSk1
vOf26RqWjiLxjOxrXchKp7T/6O4Te6L+A9FZaLT0soW/Pvx4Q5Kx9QqtbSUau4Uh
1ko=
=XdSq
-----END PGP PRIVATE KEY BLOCK-----
```


ERROR
%#&$!

Recapitulando sobre chaves e certificados

Secret Key

Usada para **decriptar** um e-mail e deve ser protegida com atenção



Public Key

Para **encriptar** e-mails e é compartilhada publicamente

Certificado de Revogação

Se a chave privada for **comprometida ou perdida**, a chave é revogada

Encriptando arquivos

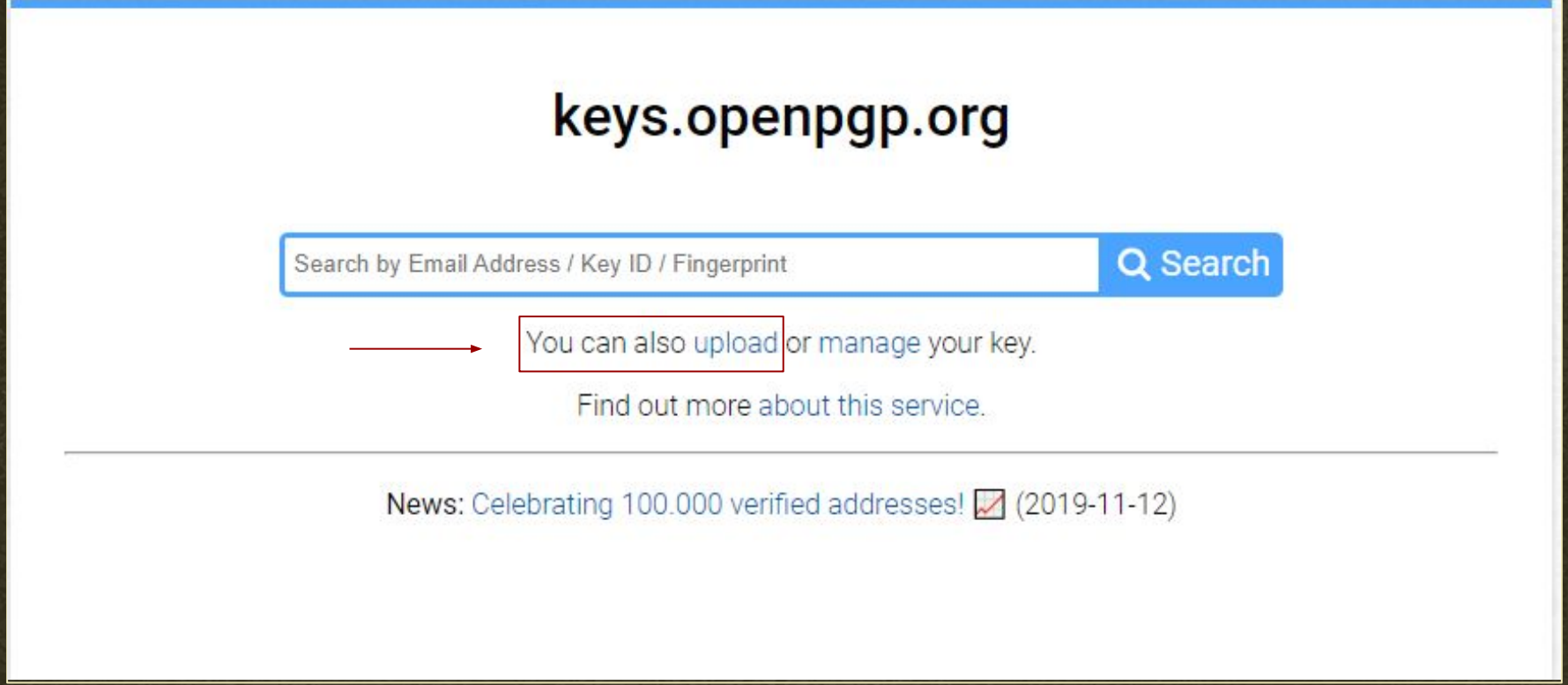
```
exiled@cyberia:~$ echo "Essa mensagem será encriptada" > message.txt
exiled@cyberia:~$ cat message.txt
Essa mensagem será encriptada

# Encriptando com criptografia assimétrica
exiled@cyberia:~$ gpg --encrypt --recipient exiled_contact@proton.me message.txt
exiled@cyberia:~$ ls -la message.txt.gpg
-rw-r--r-- 1 exiled exiled 627 May  4 12:39 message.txt.gpg

# Encriptando com criptografia simétrica
exiled@cyberia:~$ gpg --symmetric message.txt
```


```
File 'message.txt.gpg' exists. Overwrite? (y/N) N
Enter new filename: message_with_symmetric
exiled@cyberia:~$ ls
message.txt  message.txt.gpg  message_with_symmetric
```

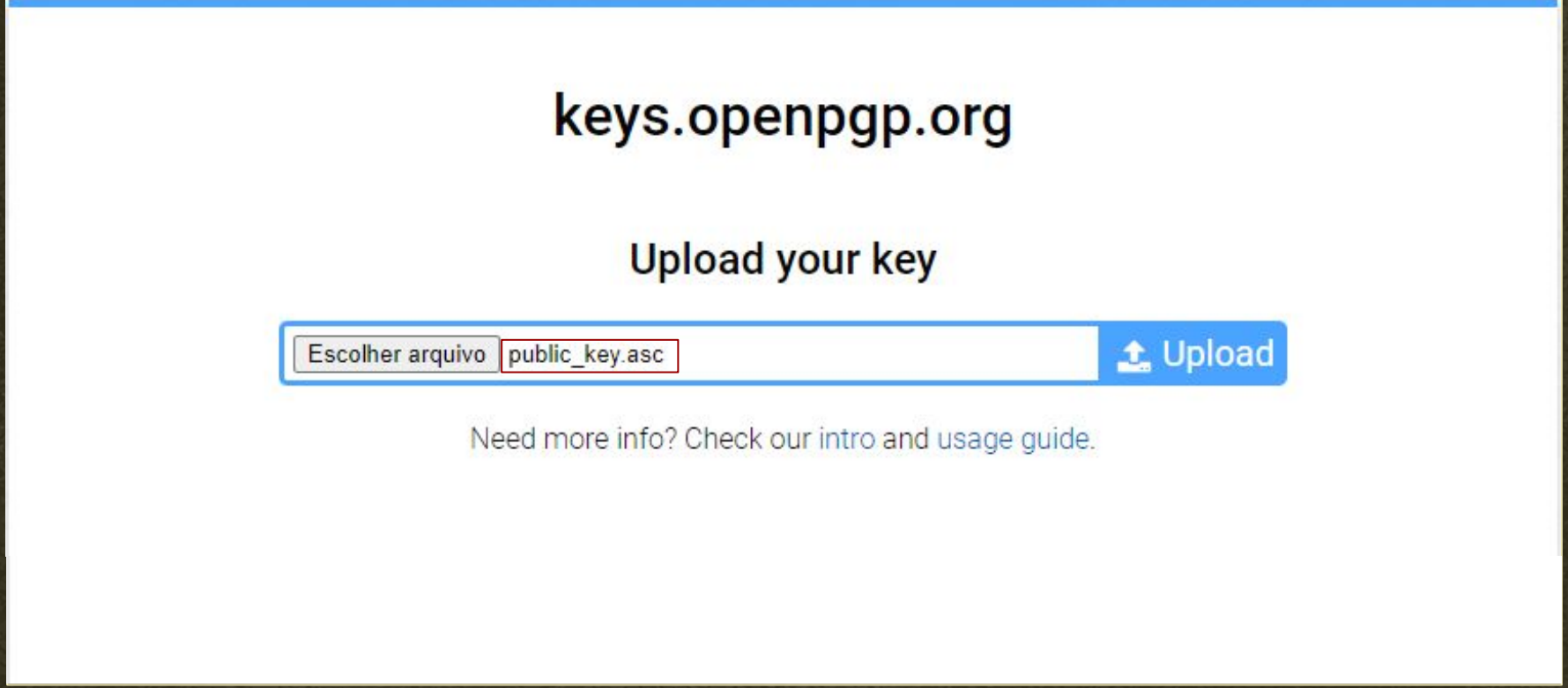
Decrypt em arquivos

```
exiled@cyberia:~$ gpg --decrypt message.txt.gpg
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:
│ "Wilgnne Riann <exiled_contact@proton.me>"
│ 4096-bit RSA key, ID EAD5C42A7AE861EF,
│ created 2023-05-03 (main key ID 582AE89F35165EF7).
│
│
│ Passphrase: _____________________________________________
│
│         <OK>                                  <Cancel>
└──────────────────────────────────────────────────────┘
gpg: encrypted with 4096-bit RSA key, ID EAD5C42A7AE861EF, created 2023-05-03
    "Wilgnne Riann <exiled_contact@proton.me>"
Essa mensagem será encriptada

exiled@cyberia:~$ gpg --decrypt message_with_symmetric
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
Essa mensagem será encriptada
```

Compartilhando chaves públicas



Compartilhando chaves públicas



Compartilhando chaves públicas

keys.openpgp.org

You uploaded the key D6D16DF844592D2D22C74698582AE89F35165EF7.

This key is now published with only non-identity information. (What does this mean?)

To make the key available for search by email address, you can verify it belongs to you:

exiled_contact@proton.me → Send Verification Email

Note: Some providers delay emails for up to 15 minutes to prevent spam. Please be patient.

Verificando a chave pública

Verify exiled_contact@proton.me for your key on keys.openpgp.org

De keyserver@keys.openpgp.org
Para exiled_contact@proton.me

Hi,

This is an automated message from keys.openpgp.org. If you didn't request this message, please ignore it.

OpenPGP key: D6D16DF844592D2D22C74698582AE89F35165EF7

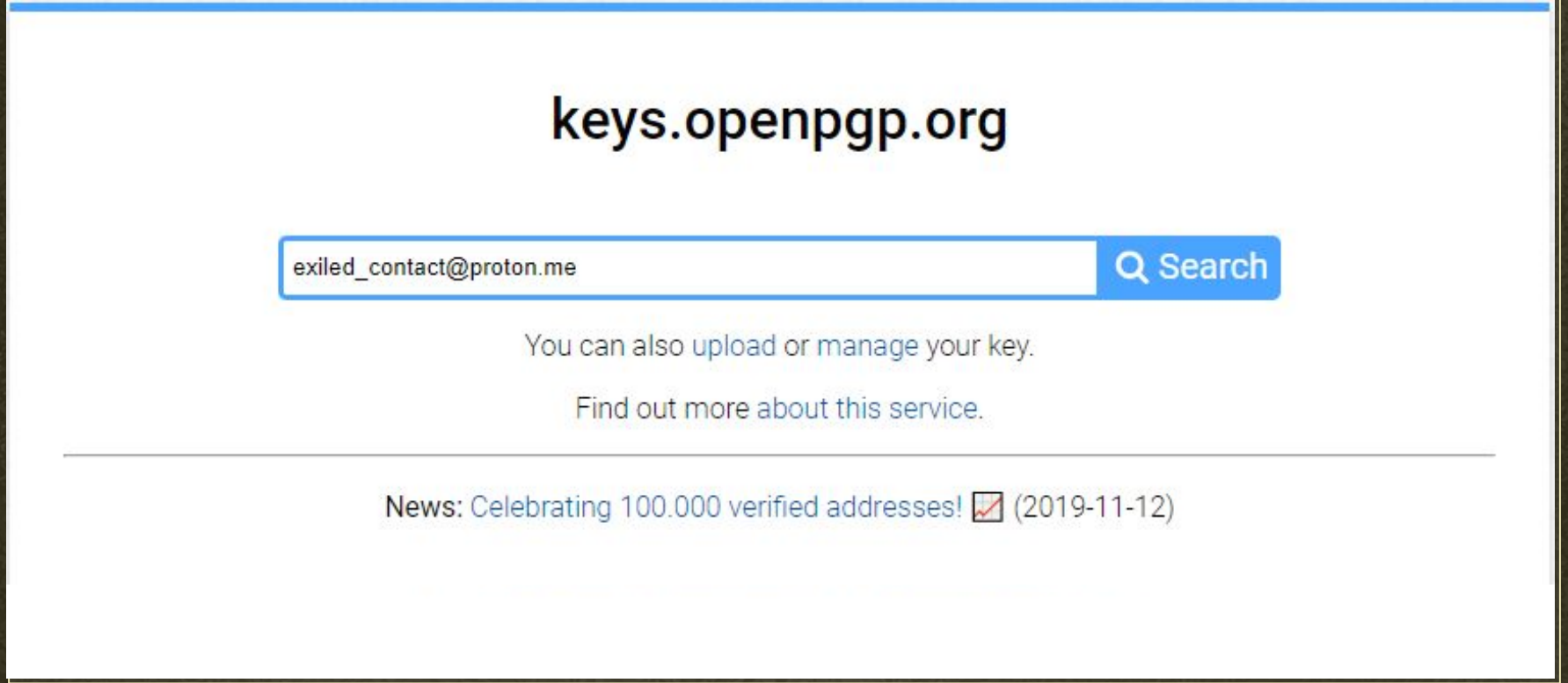
To let others find this key from your email address "exiled_contact@proton.me", please click the link below:

https://keys.openpgp.org/verify/fStz8ZxxbIPeyYQhlXIB1LDwKngjBptk21wIZQrDcRj

You can find more info at keys.openpgp.org/about.

https://keys.openpgp.org
distributing OpenPGP keys since 2019

Procurando por chaves públicas



Encontrando chaves públicas

keys.openpgp.org

We found an entry for `exiled_contact@proton.me`.

https://keys.openpgp.org/vks/v1/by-fingerprint/D6D16DF844592D2D22C74698582AE89F35165EF7

Hint: It's more convenient to use `keys.openpgp.org` from your OpenPGP software.

Take a look at our usage guide for details.

Referências

Electronic Frontier Foundation

https://ssd.eff.org/

Free Software Foundation

https://emailselfdefense.fsf.org/

Auto Defesa Org

https://autodefesa.fluxo.info/

OBRIGADO!

Alguma dúvida?

exiled_contact@proton.me
https://linkedin.com/in/wilgnneriann
https://github.com/will-exiled