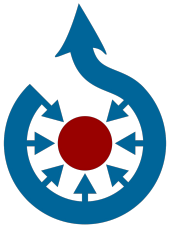
GPG para todos

Bricolabs-OSHWDem "Entre Tuxes"
12 xullo 2019

http://bit.ly/**gpg-para-todos**

Obxectivos

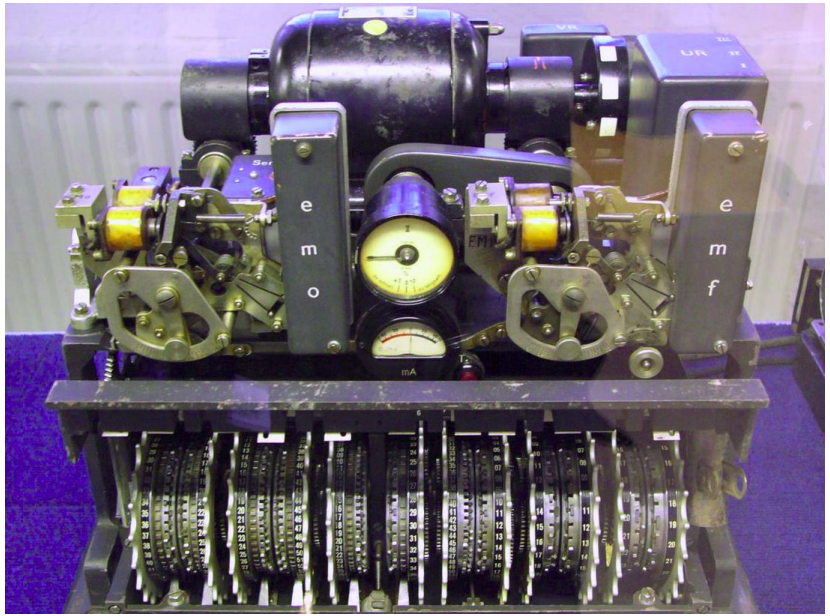
Conceptos + Obradoiro práctico



- Cifrado de mensaxes
- Criptografía asimétrica
- GNU Privacy Guard
- Intercambio de chaves

Criptografía

Necesidade de ocultar mensaxes a personas non autorizadas.



Seguro que tes necesidade de ocultar algo?

Dereitos!

- Artigos 12 e 17 de DUDH
- Artigo 18 da CE

!!

GNU Privacy Guard (GPG) a ferramenta libre

- Implementación **SwL** do estándar **OpenPGP** (RFC4880)
- `apt get install` **`gnupg`**
- Librería libgcrypt usada por outros programas

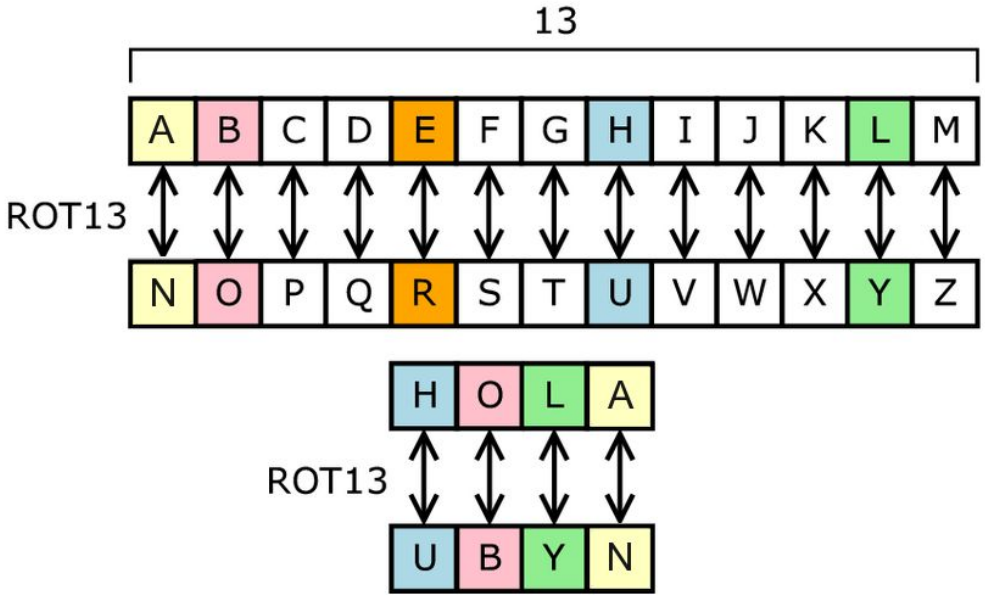
Comando na liña de texto **gpg**

```
caligari@tux-tux:~$ gpg --version
gpg (GnuPG) 2.2.12
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: /home/caligari/.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
```

Xogando aos segredos

Codificación: algoritmo usado para transformar unha mensaxe de texto



Operación lóxica XOR (a reversible!)

Táboa da verdade porta XOR

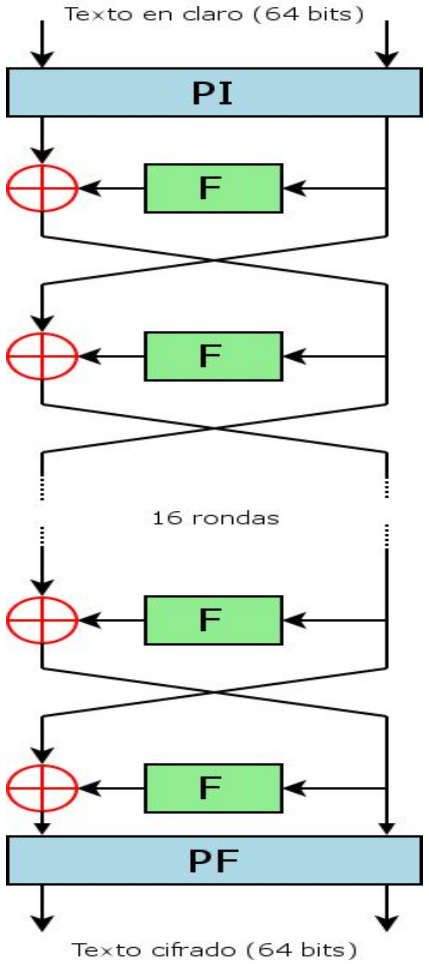
Entrada A	Entrada B	Saída $A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

```
  01010111 01101001 01101011 01101001
⊕ 11110011 11110011 11110011 11110011
= 10100100 10011010 10011000 10011010

  10100100 10011010 10011000 10011010
⊕ 11110011 11110011 11110011 11110011
= 01010111 01101001 01101011 01101001
```

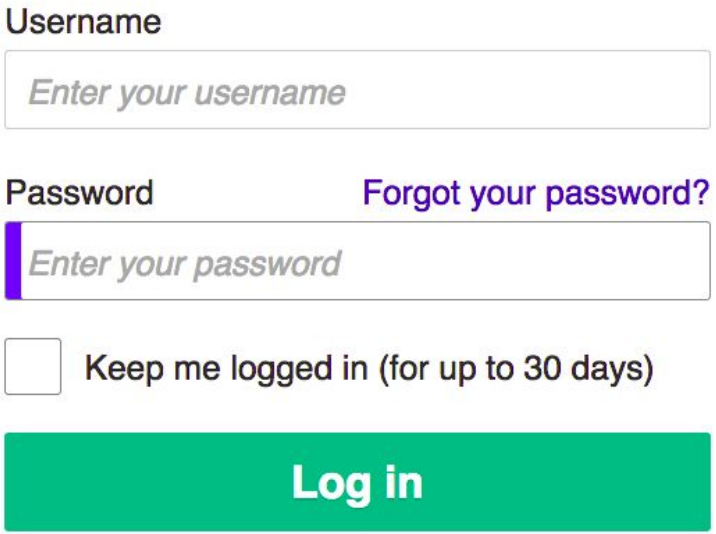
Cifrado simétrico

- DES: Data Encryption Standard (2^{56})
- 3DES: Triple-DES (2^{128})
- **AES: Advanced Encryption Standard (Rijndael, 2^{256})**

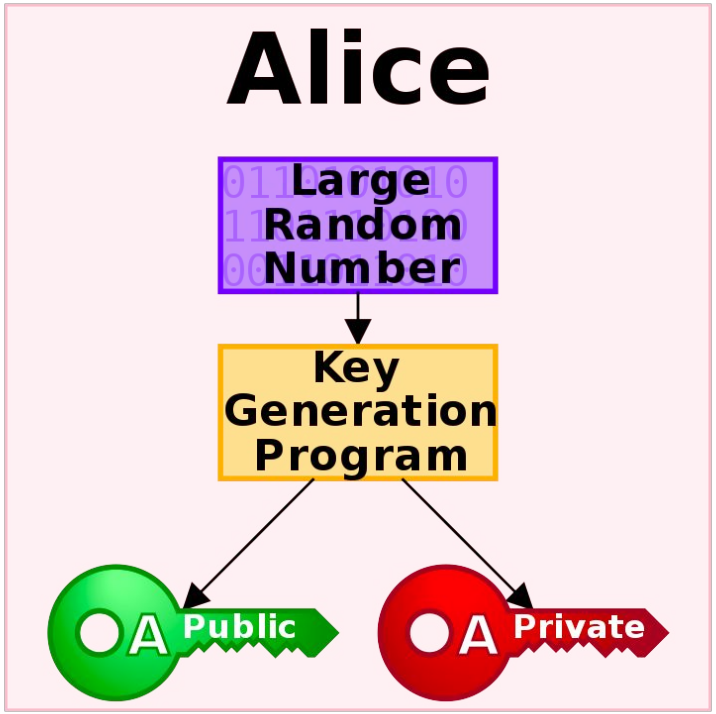


Problema coa distribución de claves

- Un contrasinal e moitas persoas?
- Quen pode cambiala?
- Como se retransmite a nova?
- Quen é realmente o que a usa?



Cifrado asimétrico (dobre chave)



- Xeneración de **par de chaves**
- Unha **pública** distribuida
- Outra **privada** NON distribuida

Xenerando o par de chaves (+ rápido co DNI)

gpg --gen-key

gpg **--full-gen-key**

Nota: vai pedir unha **contrasinal de usuario** para acceder á chave privada no futuro (non a esquezas!)

O *fingerprint* do teu par GPG

gpg **--list-secret-keys**

```
sec   dsa1024 2004-11-22 [SCA]
      86EC1582774F07BA443A1AE00C9C49B0D76ABDEC
uid           [ unknown] Rafa Couto <rafacouto@gmail.com>
uid           [ unknown] Rafa Couto <caligari@galpon.org>
uid           [ unknown] Rafa Couto <caligari@treboada.net>
uid           [ unknown] Rafa Couto <rafa@aplicacionesyredes.com>
uid           [ unknown] Rafa Couto (http://caligari.treboada.net) <rafacouto@gmail.com>
ssb   elg1024 2004-11-22 [E]
```

86EC1582774F07BA443A1AE00C9C49B0**D76ABDEC**

D76ABDEC

O directorio que usa GPG (salvagárdao!)

~/.gnupg

parametro: **--homedir**=/mnt/pen-drive/.gnupg

variable contorna: export **GNUPGHOME**=~/.gnupg

Exportar a chave pública (si, distribuible)

gpg --armor --export D76ABDEC > D76ABDEC.asc

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

liñas de texto ASCII inintelixibeis...

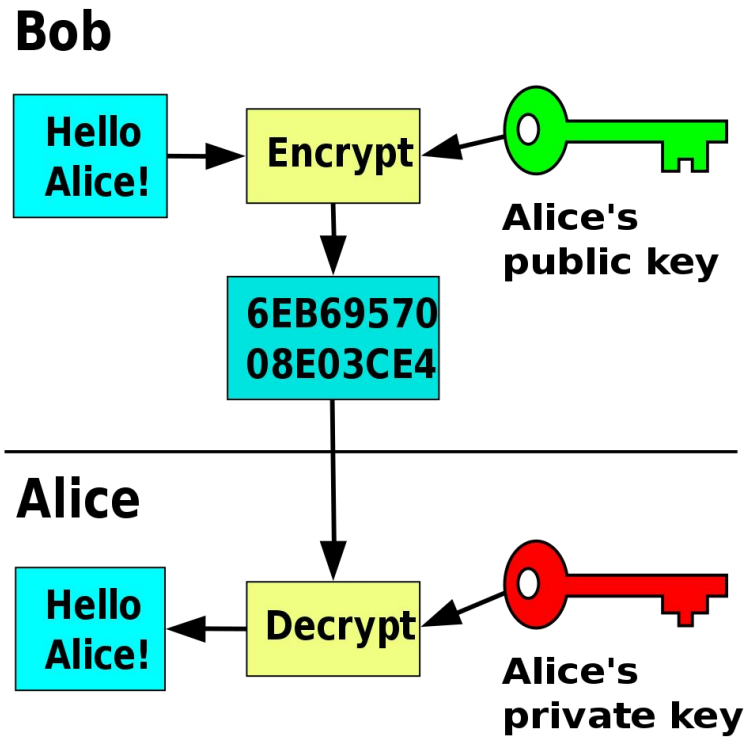
-----END PGP PUBLIC KEY BLOCK-----

Importar chaves públicas de outros

gpg --import D76ABDEC.asc

gpg **--list-keys**

Encriptar unha mensaxe para outro



1. Obter a súa chave pública
2. Compoñer a mensaxe
3. Cifrar a mensaxe
4. Enviar a mensaxe

Cifrar unha mensaxe para outros

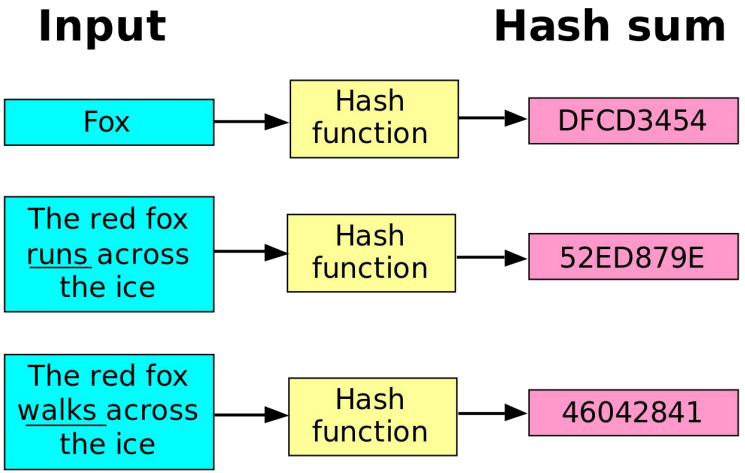
gpg **--encrypt** mensaxe.txt

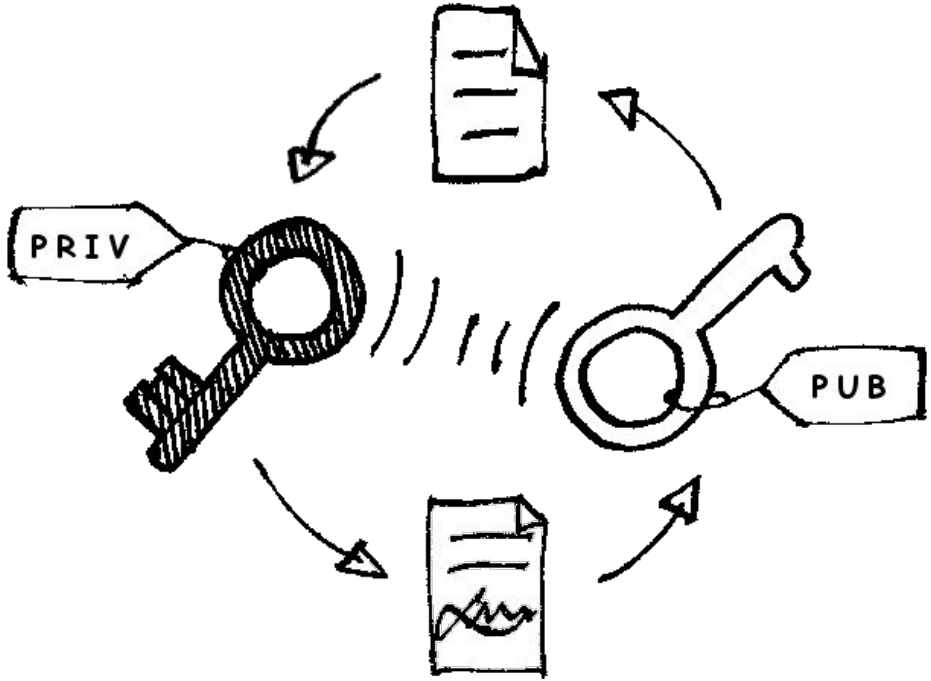
Nota: é interesante **engadir o noso identificador** para que tamén o poidamos descifrar un mesmo.

Descifrar unha mensaxe

gpg **--decrypt** mensaxe.txt.gpg

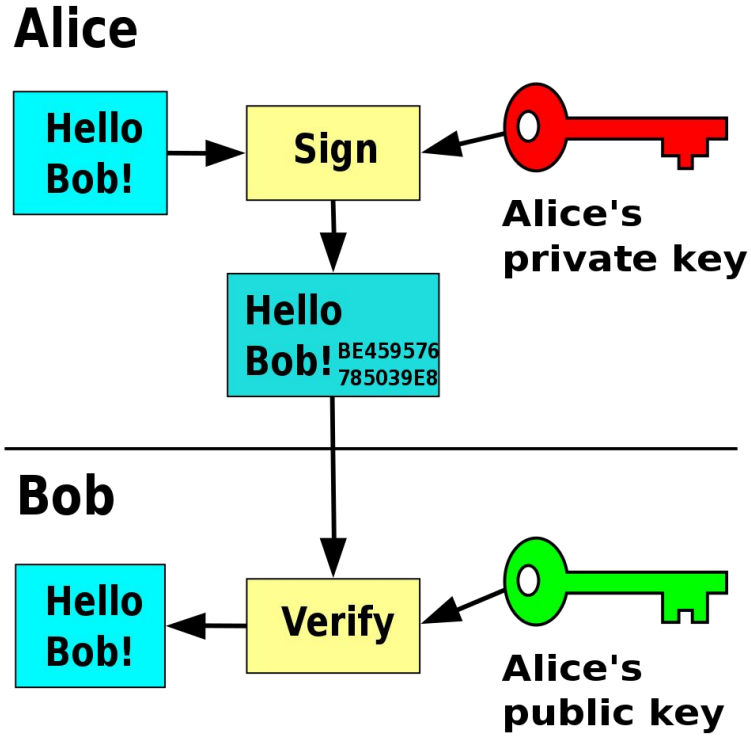
Sinaturas dixitais





- **Integridade** (o contido non se alterou)
- **Autenticación** (é quen di ser)

Asinar unha mensaxe (son quen digo ser)



1. Compoñer a mensaxe
2. Asinar a mensaxe
3. Enviar a mensaxe asinada

1. Recibir a mensaxe asinada
2. Obter a chave pública
3. Verificar sinatura

Asinar unha mensaxe con GnuPG

gpg --armor **--clearsign** mensaxe.txt

gpg --armor **--detach-sign** mensaxe.txt

Nota: usa **--output** para escoller o nome do ficheiro producido

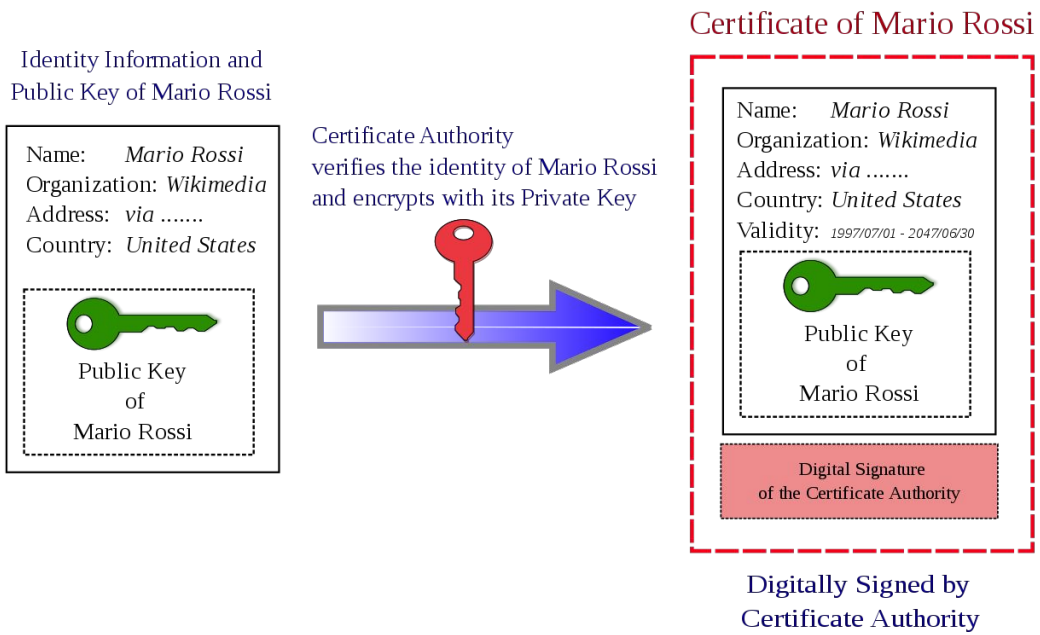
Verificar unha mensaxe con GnuPG

gpg **--verify** mensaxe.txt.asc

gpg **--verify** mensaxe.txt.asc mensaxe.txt

Intercambio de chaves públicas

Public Key Infrastructure (PKI)



Confianza distribuida!

- Intercambio persoal
- Key signing parties
- PGP key servers

Intercambio de chaves públicas FOSDEM 2008

Establecer o grao de confiabilidade da chave

gpg **--edit-key** D76ABDEC

gpg> help

gpg> **uid**

gpg> **tsign**

Exportar a túa chave nun formato distribuíble

gpg **--output** D76ABDEC.key **--armor --export** D76ABDEC

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

mI0EXSiCagEEAONaj8boV+jvAfCyU59SoZggmiLdpSvUWaGAKyreirAdGvj+Nze8
SPTKSF0rVmbFu2K5bWqERrxTxhJTQrQWglwrZJAOG/IKae6jbpt/t5oN91J4I+JY
4pQBzGCciYFNC9RJyfoZAXOqq/NjuVXsummRN2pXlqG9cJCFpyrOlQ3bABEBAAG0
IlJhZmEgQ291dG8gPGNhbGlnYXJpQHRyZWJvYWRhLm5ldD6IzgQTAQgAOBYhBPOZ
7ckaaSvFgtjIz50PIqYzg+kJBQJdKIJqAhsDBQsJCAcCBhUICQoLAgQWAgMBAh4B
AheAAAoJEJ0PIqYzg+kJbsED/2475QTLNEBAv1cAN/SJ+MNUMtCxJuIi8sKPEnLK
Dm6b436YGVqtrOtquB3gU3SN5VSEfTZjGwnwEjycZGLQ4Z/Ys/Q7ZBRnkc/EwFC8
WMV5C59OD/g0tUNVN78yw7MgK5rxEWjrrZedOdzY2YiYTAxRbdUIlcp1z/aqx9gc
4StmuI0EXSiCagEEAMmU1TF47be/eGi3zu1LqQMOc/Udswlcpvcf5g63GNBTW2bo
6xUo1GfKcf0Dd2JmPCzmZxA7JilmlDXmveexN2QCuvgQ+Uk+4FsMFwnpUk+S2iXt
gpjybWTn/rQYProCLb5gnc6bGBB545LIMoPrWJVuhBlVgA+0kMXcaRRz9naNABEB
AAGItgQYAQgAIBYhBPOZ7ckaaSvFgtjIz50PIqYzg+kJBQJdKIJqAhsMAAoJEJ0P
IqYzg+kJlQMEAJbU3BxOC0scFiZEPR5ILS65iKIjPycH++At0I4n//TrLp2cOlKL
zw8xbzlBfSqHzpAM64PtVkxbxj0WCtX+RMOOVMDotOSY6HgMnFbMj/i5vX344Cej
EYv4On5f1s8YHRJpUOMloKmWC43PorCShPbPDmZyFeiplwVGhrA3F7t5
=QPah
-----END PGP PUBLIC KEY BLOCK-----
```

Servidores de chaves

gpg **--send-keys** D76ABDEC

gpg **--keyserver** pgp.mit.edu --send-keys D76ABDEC

gpg --keyserver pgp.mit.edu **--recv-keys** D76ABDEC

~/.gnupg/gpg.conf: **keyserver** pgp.mit.edu

gpg **--refresh-keys**

https://www.rediris.es/keyserver (+email)

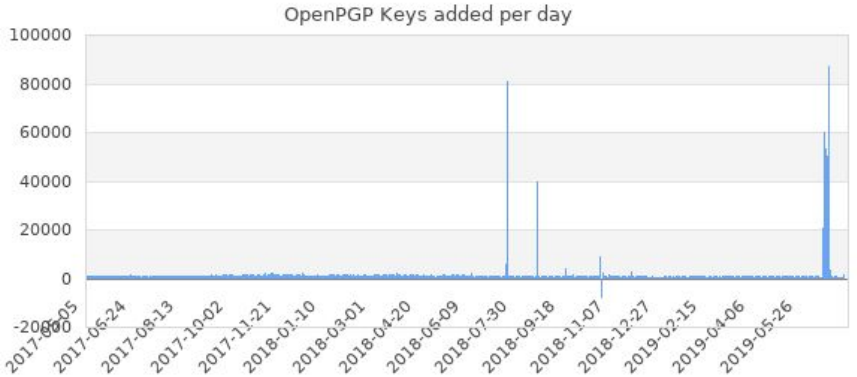
Ataque aos servidores de claves

https://**sks-keyservers.net**/status/

Servers in the pool

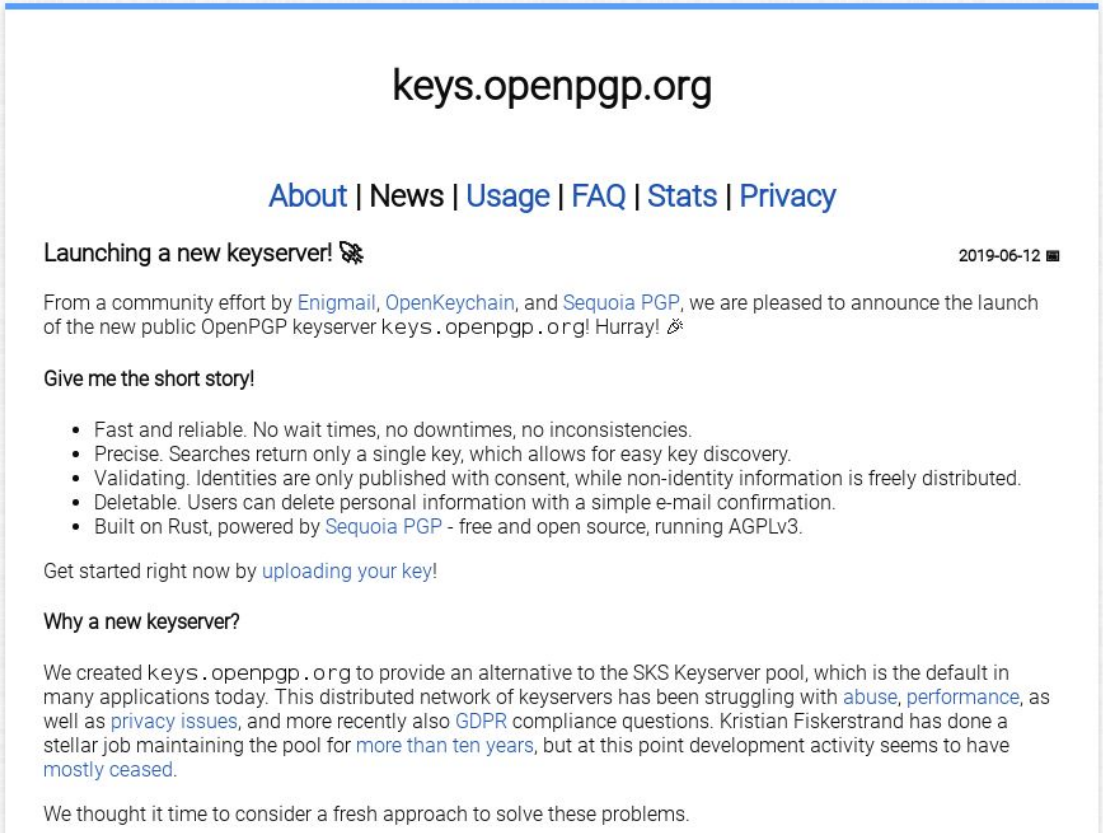
Information about the various pools is found here

	Hostname	IPv6	RProx	Port 80	hkps	Tor	Software	ΔKeys	SRV (EU)	SRV (NA)	SRV (OC)	Stats	Meta
1	agora.cenditel.gob.ve[@]						1.1.6	2,986	265	271	266	Stats	Meta
2	cheipublice.ro[@]						1.1.6	3,863	329	336	352	Stats	Meta
3	gozer.rediris.es						1.1.6	3,834	353	387	354	Stats	Meta
4	key.adeti.org[@]						1.1.6	2,934	454	414	415	Stats	Meta
5	keys.andreas-puls.de[@]						1.1.6	3,946	424	407	419	Stats	Meta
6	keys.communityrack.org[@]						1.1.6	3,843	367	386	332	Stats	Meta
7	keys.fedoraproject.org[@]						1.1.6	3,853	306	588	297	Stats	Meta
8	keys.void.gr[@]						1.1.6	-2,803	341	337	315	Stats	Meta
9	keys2.kfwebs.net[@]						1.1.6	4,272	629	603	600	Stats	Meta
10	keyserver-01.2ndquadrant.com[@]						1.1.6	4,538	472	361	0	Stats	Meta
11	keyserver-02.2ndquadrant.com[@]						1.1.6	4,305	530	361	0	Stats	Meta
12	keyserver-03.2ndquadrant.com[@]						1.1.6	4,305	544	364	0	Stats	Meta
13	keyserver.escomposlinux.org[@]						1.1.6	3,404	529	382	379	Stats	Meta
14	keyserver.insect.com[@]						1.1.6	4,038	358	483	0	Stats	Meta
15	keyserver.mattrude.com[@]						1.1.6+	4,019	420	0	509	Stats	Meta
16	keyserver.zap.org.au[@]						1.1.6	4,060	320	430	612	Stats	Meta
17	pgp.circl.lu[@]						1.1.6+	4,109	360	388	0	Stats	Meta
18	pgp.gwolf.org[@]						1.1.6	-4,172	347	534	444	Stats	Meta



keyserver hkps://keys.openpgp.org

Long live the OpenPGP! (and GnuPG)



keys.openpgp.org

About | News | Usage | FAQ | Stats | Privacy

Launching a new keyserver! 2019-06-12

From a community effort by Enigmail, OpenKeychain, and Sequoia PGP, we are pleased to announce the launch of the new public OpenPGP keyserver `keys.openpgp.org`! Hurray!

Give me the short story!

- Fast and reliable. No wait times, no downtimes, no inconsistencies.
- Precise. Searches return only a single key, which allows for easy key discovery.
- Validating. Identities are only published with consent, while non-identity information is freely distributed.
- Deletable. Users can delete personal information with a simple e-mail confirmation.
- Built on Rust, powered by Sequoia PGP - free and open source, running AGPLv3.

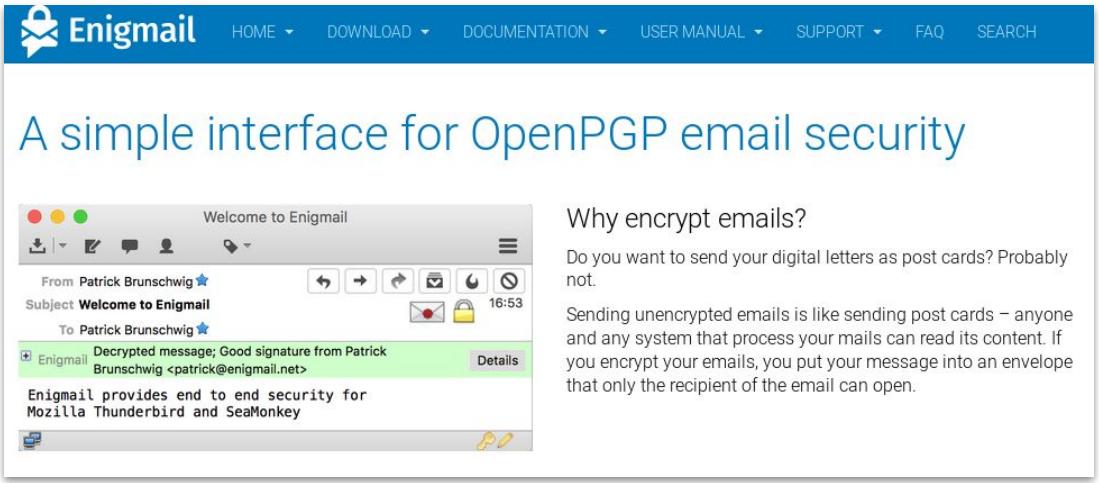
Get started right now by uploading your key!

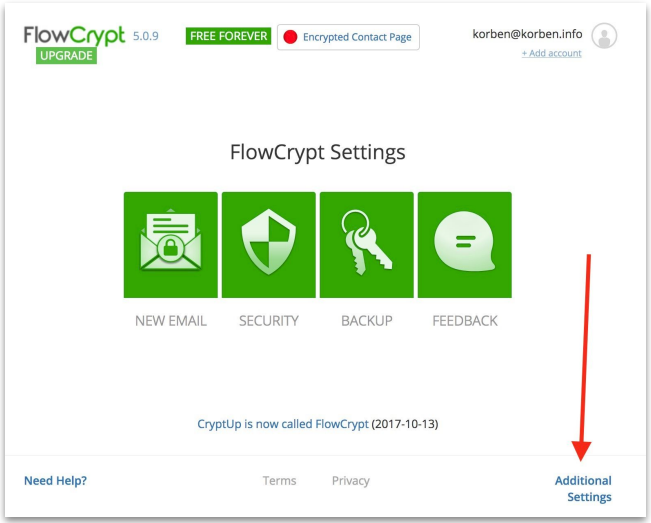
Why a new keyserver?

We created `keys.openpgp.org` to provide an alternative to the SKS Keyserver pool, which is the default in many applications today. This distributed network of keyservers has been struggling with abuse, performance, as well as privacy issues, and more recently also GDPR compliance questions. Kristian Fiskerstrand has done a stellar job maintaining the pool for more than ten years, but at this point development activity seems to have mostly ceased.

We thought it time to consider a fresh approach to solve these problems.

Integración en aplicacións





En definitiva

GnuPG para todos!

Cuestións?

email: **caligari@treboada.net**

twitter: **@caligari_pub**

gpg-id: **D76ABDEC**