

Ssshhh, it's a secret

Quick introduction to GPG/PGP

Pablo COVES

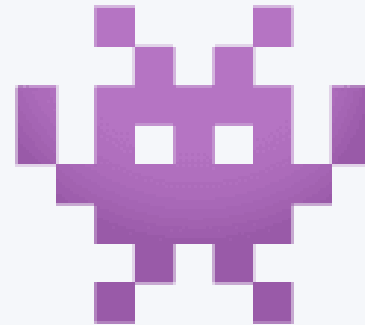
04/11/2025 :: *Human Talks* :: Grenoble

Contents

Once upon a time	1
Lesson learned	4
That's not all	11
Conclusion	16

Once upon a time

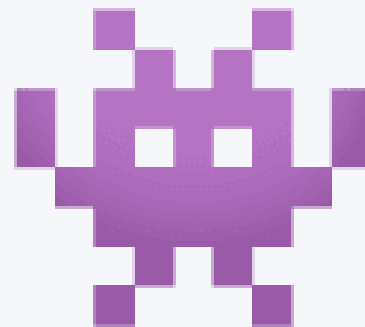
A lovely couple



Up to no good



Hey 🌌!, Wanna
invade 🐵?



But space has ears



Hey 🦿!, Wanna
invade 🐵?

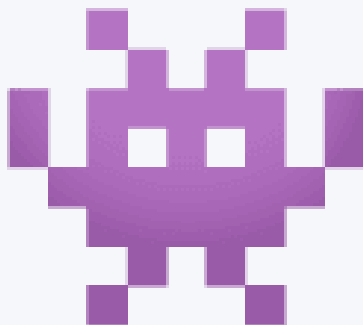


Obviously,

Heroes saved the planet 🦾

Lesson learned

Make a key-pair

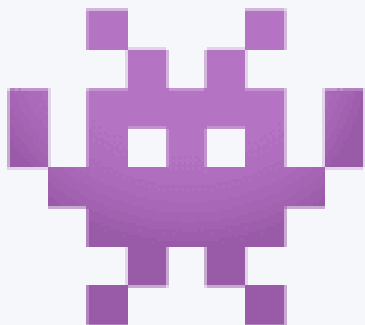


1 > GPG --version

bash

```
1  GPG (GnuPG) 2.4.8
2  libgcrypt 1.11.1
3  Copyright (C) 2025 g10 Code GmbH
4  License GNU GPL-3.0-or-later <https://gnu.org/licenses/gpl.html>
5  This is free software: you are free to change and redistribute it.
6  There is NO WARRANTY, to the extent permitted by law.
7
8  Home: ~/.gnupg
9  Supported algorithms:
10 Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
11 Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
12         CAMELLIA128, CAMELLIA192, CAMELLIA256
13 Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
14 Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

Make a key-pair

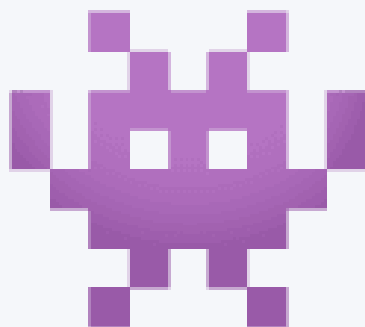


```
1 > GPG --quick-generate-key Monster
```

```
bash
```

```
1 About to create a key for:
2 "Monster"
3 [...]
4 pub  ed25519/0x89C9E1AF73E2085F 2025-09-09 [SC] [expires: 2028-09-08]
5      Key fingerprint = 2E56 1579 A0CA 4000 7136  58C7 89C9 E1AF 73E2 085F
6 uid                                     Monster
7 sub  cv25519/0xFFE520DBBE5E807F 2025-09-09 [E]
```

Make a key-pair

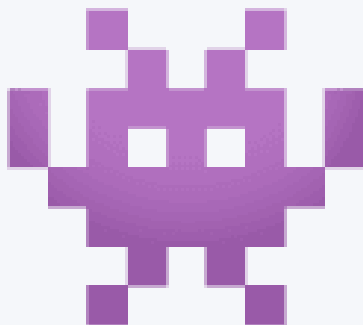


```
1 > GPG --list-secret-keys
```

```
bash
```

```
1 sec  ed25519/0x89C9E1AF73E2085F 2025-09-09 [SC] [expires: 2028-09-08]
2      Key fingerprint = 2E56 1579 A0CA 4000 7136 58C7 89C9 E1AF 73E2 085F
3 uid                               [ultimate] Monster
4 ssb  cv25519/0xFFE520DBBE5E807F 2025-09-09 [E]
```

Export the public key

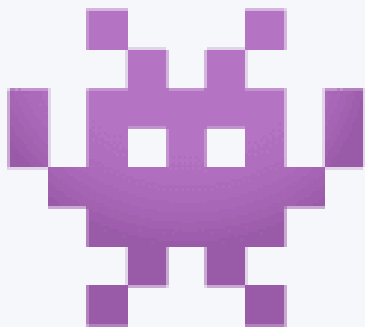


1 > GPG --export --armor Monster

bash

```
1  -----BEGIN PGP PUBLIC KEY BLOCK-----
2
3  mDMEaMCNEBYJKwYBBAHaRw8BAQdAvxJ12U63b3V3g+GqVGcXxY5LFyYR4MuDMZ5v
4  uDeq6Vm0BUFSaWVuiJQEExYKADwWIQQuVhV5oMpAAHE2WMeJyeGvc+IIXwUCaMCN
5  EAIbAwUJBa0agAQLCQgHBBUKCQgFFgIDAQACHgECF4AACgkQicnhr3PiCF821wD/
6  aXM6yPBjv8U3Uc3L/0+PYL69SYXH6I3VDgBLX50sjqoA/jwDf5G/w6UBB/gIo2Y+
7  dD9+9/taYA5tJKM4uP6142cGuDgEaMCNEBIKKwYBBAGXVQEFAQEHEQBAZHfVfAoMH
8  hAf5pBe14TYd7wCV7b95Vu5IQyD9joAPAwEIB4h4BBgWCgAgFiEELLYVeaDKQABx
9  NljHicnhr3PiCF8FamjAjRACGwwACgkQicnhr3PiCF+VmAD+07zTvI+iAYE0SsH+
10 bF1J8KU77ljPyZ6lBixFv/SwXz0BALs78/zMzala6AARJEU703iPQJShqfnIjnXf
11 ccfFPm0H
12 =+5+R
13  -----END PGP PUBLIC KEY BLOCK-----
```

And share



Hey 🛸!, here is
my public key.

— 🌸



Same players play again



```
1 > GPG --import Monster.asc
```

```
bash
```

```
1 GPG: key 0x89C9E1AF73E2085F: public key "Monster" imported
2 GPG: Total number processed: 1
3 GPG:             imported: 1
```

Same players play again



```
1  gpg --encrypt --armor --recipient Monster <<< "🚀🌍💣?"
```

```
bash
```

```
1  -----BEGIN PGP MESSAGE-----
```

```
2
```

```
3  hF4D/+Ug275egH8SAQdAZ983XzASuLqPWGzhjorDfwncDfsr9R7e0kW5VCEHKGww
```

```
4  F2+Vi3vBtwKXDwKQ9aAKL1tY9hEUyV4UyYN0RBPPQf/STnqqwDKj2ALUhk3DIDM
```

```
5  0k4ByjMUeFCfdETtg3Ys5K8zmPsqJutPP+1520MGIGfret7wKsuR5loqP0nnD604
```

```
6  D9UyWC9NNArmrChGr/7FQvtrmUokY/E/I5NJduRMNX0=
```

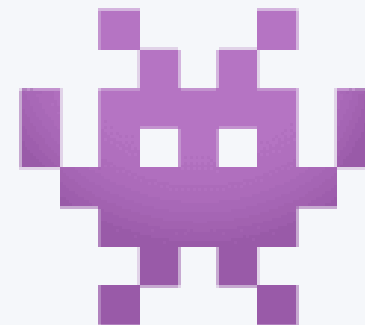
```
7  =iTTh
```

```
8  -----END PGP MESSAGE-----
```

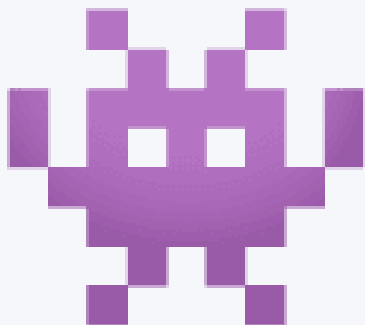
Encrypted this time



A message for
you and you only



For your eyes only



```
1  GPG --decrypt <<< "$MESSAGE"
```

```
bash
```

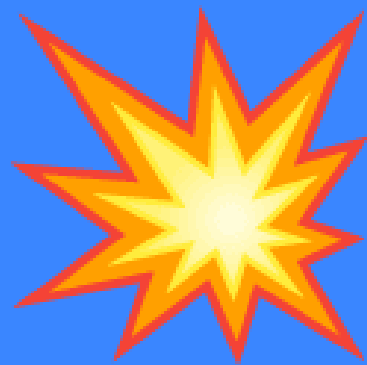
```
1  GPG: encrypted with cv25519 key, ID 0xFFE520DBBE5E807F, created 2025-09-09
```

```
2      "Monster"
```

```
3  🚀🌍💥?
```

Nop, not yours





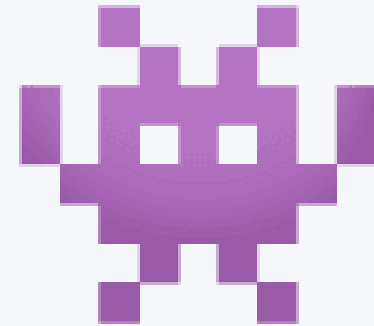
That's not all

`GPG/PGP` is not only about invading earth

Authenticate



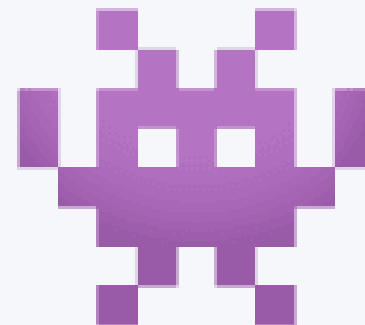
Grant me
privileges



Sign



I'm the author



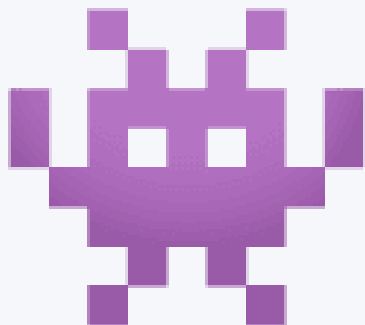
Trust



I trust 🟪 : If you trust me, you can trust them.



Revoke



I lost access to my GPG
keys, stop using them



Tooling



Thunderbird on
Desktop



K9-Mail on
Mobiles



Proton in a
Browser



Password Store
cross-platform

Conclusion

Questions ?

