

Criptografía con GnuPG



Federico Ponce de León

fefu@fefu.eu

<http://fefu.eu>

Agenda

- ¿Qué es la criptografía?
- En correo electrónico
- GnuPG - Manos a la obra
- Conclusiones




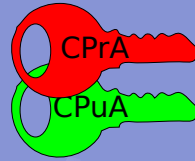
¿Qué es la criptografía?


- Etimología
- Algoritmos
- Aplicaciones



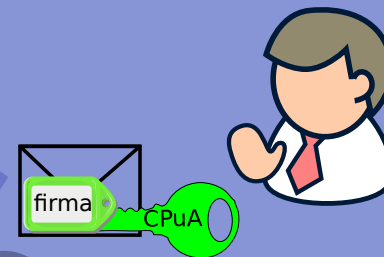
Correo electrónico - Firma

1
 Ariadna crea su par de claves (pública y privada) y envía sólo su CPu a Baco

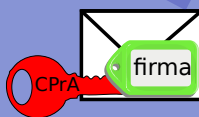


4
 Baco asocia el mensaje a la identidad de Ariadna

2
Luego escribe un mail y lo firma con su clave privada



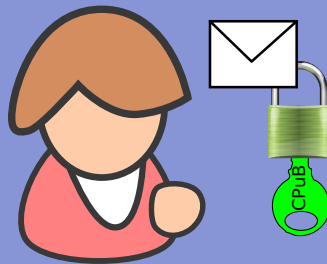
3
Baco certifica el mensaje usando la clave pública de Ariadna



El mensaje firmado viaja por un medio inseguro



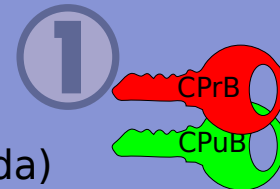
En correo electrónico - Cifrado



Ariadna escribe un mail y lo cifra **2** con la clave pública de Baco



Baco crea su par de claves (pública y privada) y envía **sólo** su CPu a Ariadna



4

Baco lee el mensaje

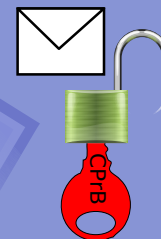


3

Baco descifra el mensaje usando su clave privada.



El mensaje cifrado viaja por un medio inseguro



GnuPG - Manos a la obra

```
# sudo apt install gnupg2 # Instala GnuPG
# mkdir -p ~/.gnupg/
# cat >> ~/.gnupg/gpg.conf <<EOF
cert-digest-algo SHA256
default-preference-list SHA512 SHA384 SHA256
SHA224 AES256 AES192 AES CAST5 ZLIB BZIP2
ZIP Uncompressed
EOF
gpg --gen-key
```



Revisión de conceptos

Criptografía = comunicaciones
confidenciales sin intermediarios

Algoritmo de clave asimétrica con llave
pública y llave privada

Firmado y cifrado de información



Conclusión

La comunicación es una necesidad y un derecho. La privacidad también. Los canales de comunicación seguros...



nos hacen **libres** !!



Agradecimientos

Diabolo

HacKan

Jon Hall

Beatriz Busaniche

A ustedes

Muchas Gracias



Bibliografía recomendada

- El escarabajo de oro (cuento de Edgar Allan Poe)
- Monopolios artificiales sobre bienes intangibles
- Un mundo patentado? La privatización de la vida y el conocimiento
- Prohibido pensar, propiedad privada
- Producing oss (K. Fogel)
- Guía práctica sobre Software Libre. Su selección y aplicación local en América Latina
- La ética del hacker - Pekka Himanen
- The Art of Unix Programming. Eric Steven Raymond
- Software libre para una sociedad libre. Richard M. Stallman



Filmografía recomendada

- The Corporation
- Revolution OS
- Freedom Downtime
- 1984 de George Orwell
- Ed Snowden addresses question from Philip Zimmermann,
10NOV2016



Licencia

- Esta presentación (C) Copyright 2008 Federico Ponce de León. Puedes distribuirla sin modificación o con modificaciones como copias derivadas usando:
 - Creative Commons Attribution-ShareAlike License version 2.5 or greater
 - GNU GPL version 2 or greater
 - GNU Free Documentation License (GFDL) version 1.2 or greater
- Por favor, incluir una referencia a:
<http://fefu.eu> / <http://www.fefu.eu>

