Uso de la Herramienta GNU Privacy Guard (GPG) para Criptografía, Firmas Digitales y Correo Electrónico Cifrado

Miguel Astor Romero

CICORE - Esc. de Computación - UCV - 22 de julio de 2020

Agenda

Introducción

- La confidencialidad de las comunicaciones es uno de los pilares fundamentales de la Internet actual.
- La criptografía es la forma de garantizar confidencialidad en las comunicaciones.
- Existen varias formas de llevar la criptografía al usuario final:
  - OpenPGP.
  - PKI.
  - S/MIME.

Criptología

- Ciencia que se encarga del estudio y diseño de mecanismos para garantizar la confidencialidad de las comunicaciones
- Se divide en dos disciplinas complementarias:
  - Criptografía.
  - Criptoanálisis.

Criptografía

Definición

Disciplina que se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial. [1]

[1] A. F. Sabater et al., *Técnicas Criptográficas de Protección de Datos*, 2nd ed. Alfaomega Ra-Ma, 2001.

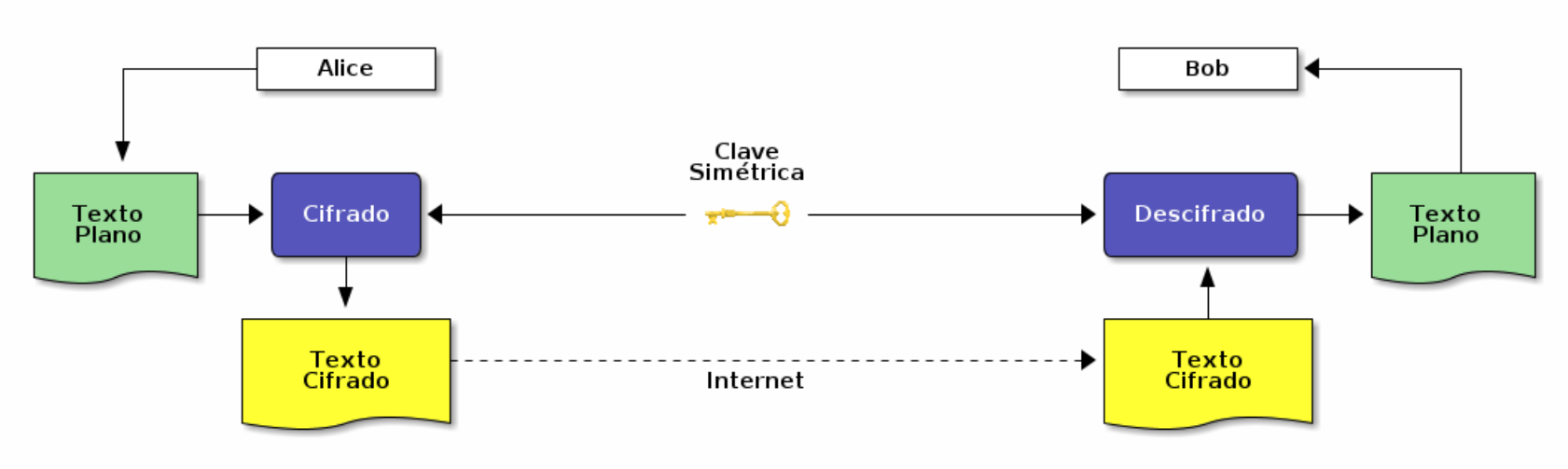
Criptoanálisis

Definición

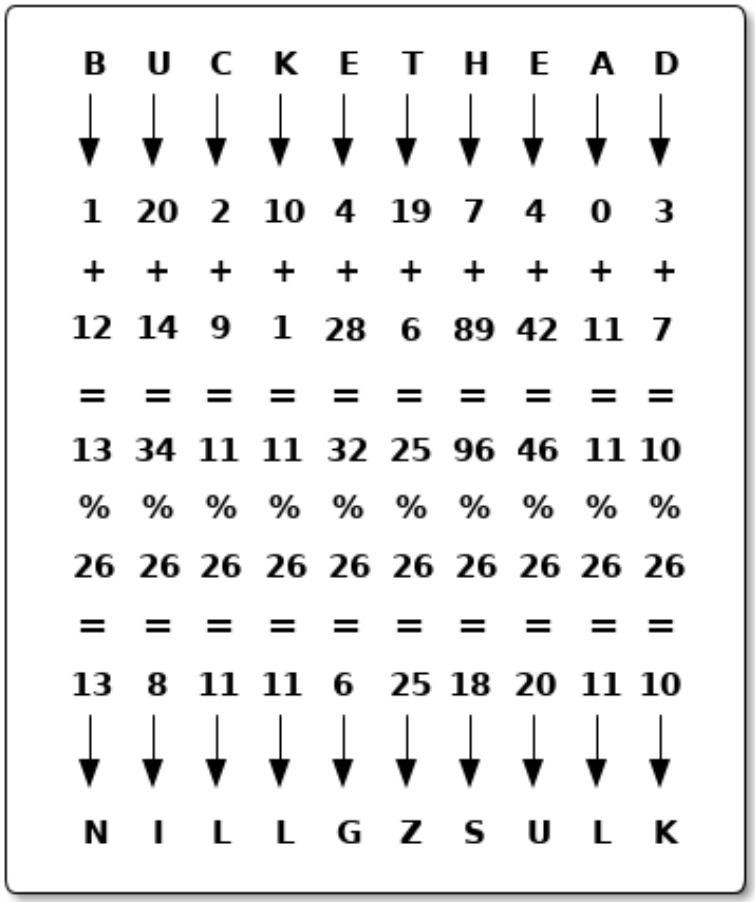
Es la ciencia de recuperar el texto plano de un mensaje sin tener acceso a la clave. [2]

[2] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, John Wiley & Sons, 2015.

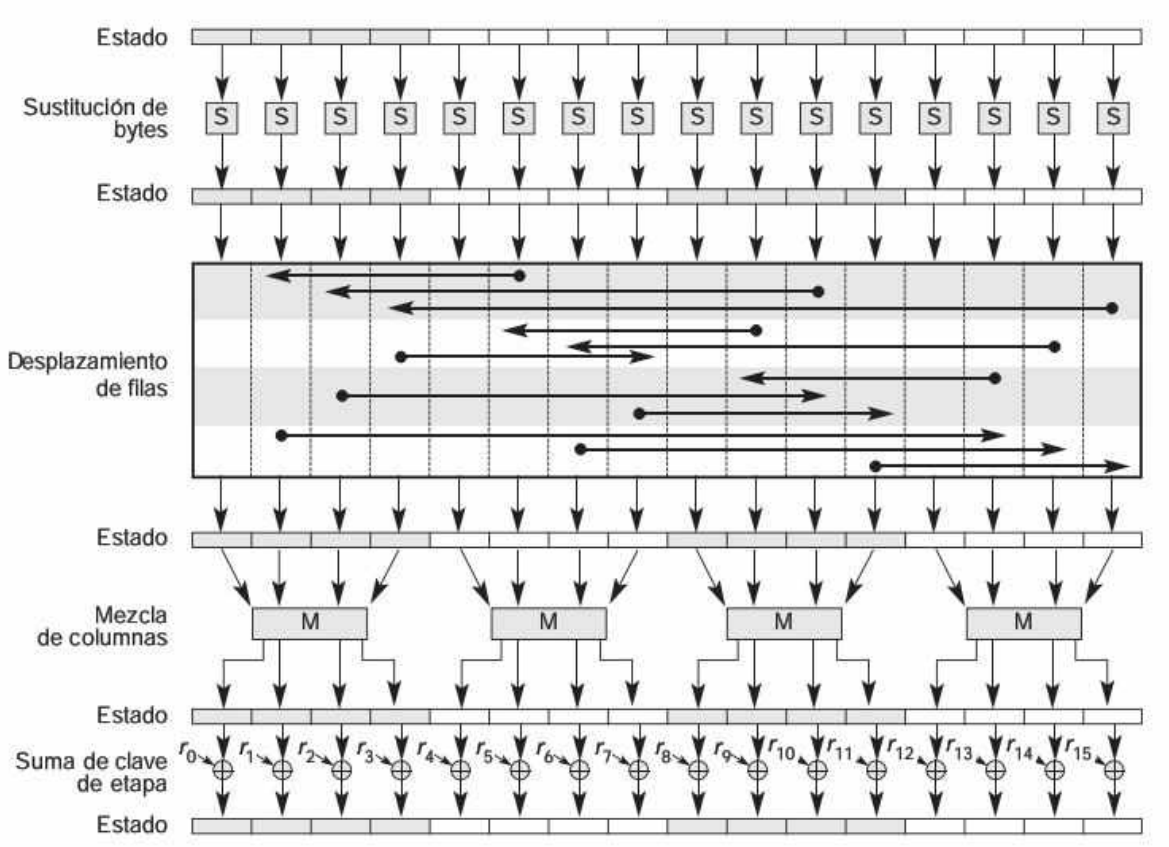
Criptografía Simétrica



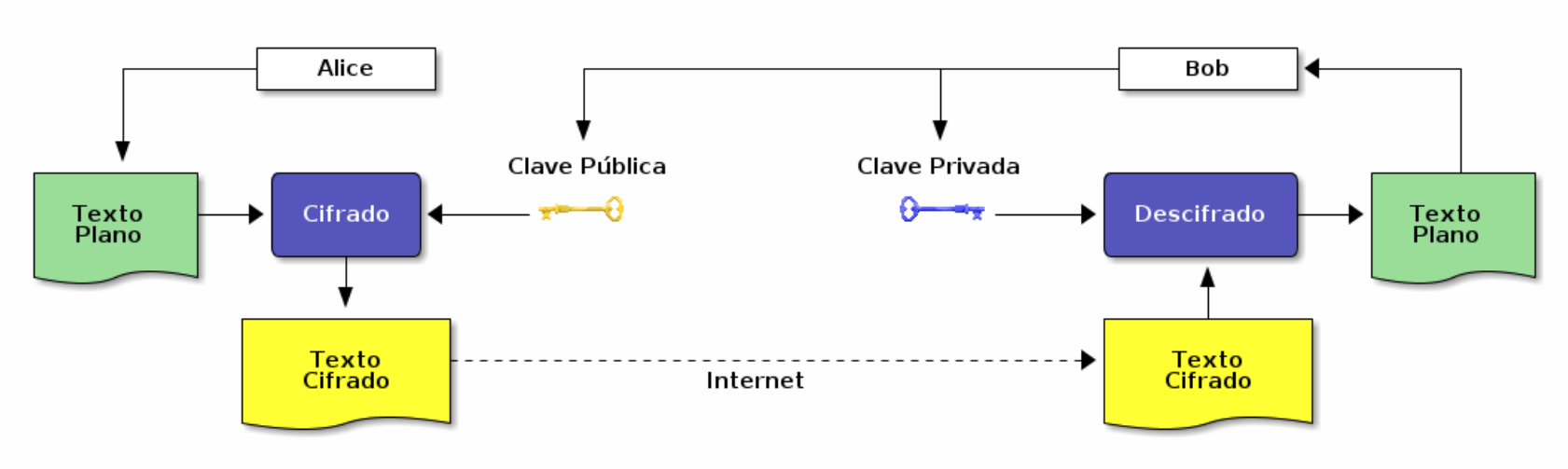
Ejemplo: Cifrado Simétrico Básico



Ejemplo: Cifrado AES



Criptografía Asimétrica



Ejemplo: Cifrado RSA

- Esquema de cifrado de clave pública inventado por Rivest, Shamir y Adleman.
- Basado en la dificultad de factorizar enteros grandes.

Cifrado

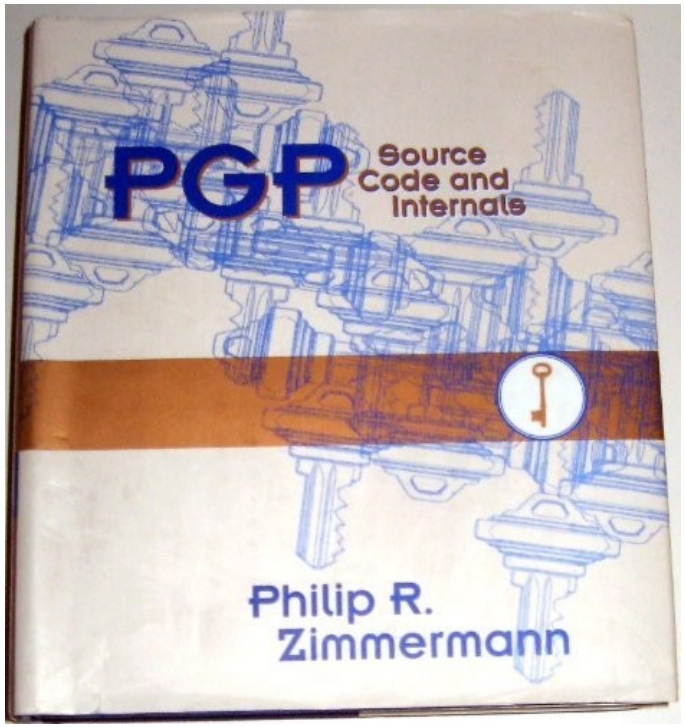
$$c = p^e \text{ mód } n$$

Descifrado

$$p = c^d \text{ mód } n$$

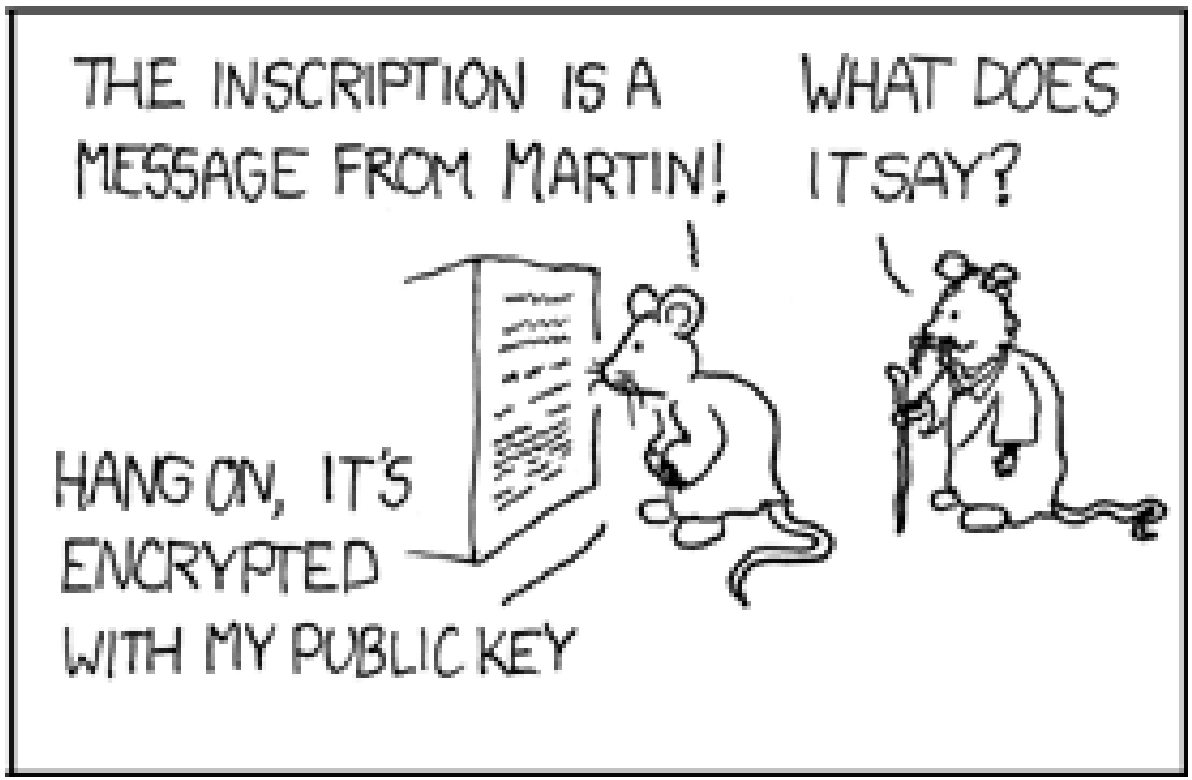
PGP

- Siglas de *Pretty Good Privacy*.
- Programa para cifrado de datos.
- Creado por Phil Zimmerman en 1991.
- Acto de protesta contra la ley del Senado No. 266 de Estados Unidos.
- Base del estándar OpenPGP (RFC 4880).



GPG - GnuPG - GNU Privacy Guard

- Implementación de OpenPGP del proyecto GNU.
- Software libre según licencia GPL versión 3.


THE INSCRIPTION IS A MESSAGE FROM MARTIN!
WHAT DOES IT SAY?
HANG ON, IT'S ENCRYPTED WITH MY PUBLIC KEY

Características de GPG

- Disponible para prácticamente todo sistema operativo.
- Permite:
  - Cifrar y descifrar datos.
  - Crear y verificar firmas digitales.
  - Validar identidad de claves.
- Funciona exclusivamente por linea de comandos.

Opciones de Manipulación de Claves

Comando	Acción
`gpg --list-keys`	Listar todas las claves.
`gpg --full-generate-key`	Crear un nuevo par de claves.
`gpg --export`	Exportar clave pública.
`gpg --export-secret-keys`	Exportar claves privadas.
`gpg --import`	Importar claves.
`gpg --delete-key`	Elimina un par de claves.
`gpg --edit-key`	Editar propiedades de una clave.

Opciones para Cifrado de Datos

Comando	Acción
`gpg -r`	Especificar clave a usar para cifrar.
`gpg -e`	Cifrar datos.
`gpg -d`	Descifrar datos.

Opciones para Verificación de Firmas

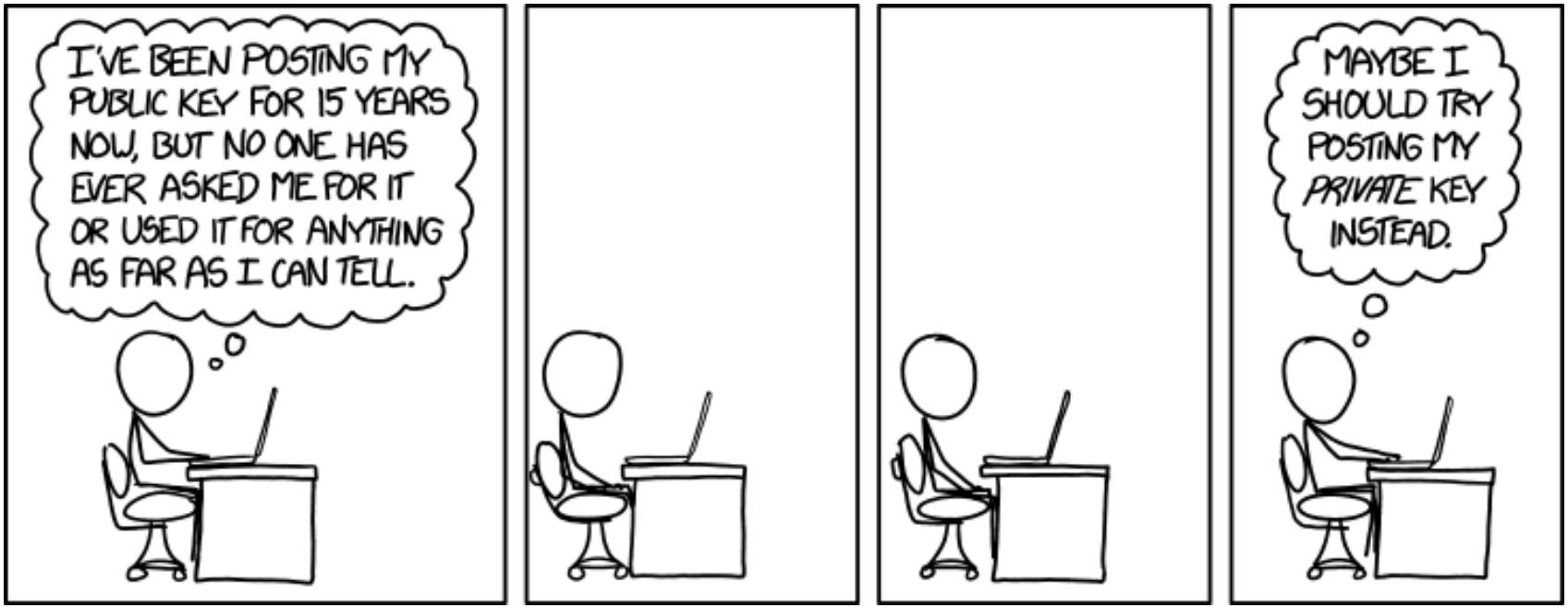
Comando	Acción
`gpg -u`	Especificar clave a usar para firmar.
`gpg --sign`	Generar firma de datos[3].
`gpg --clearsign`	Generar firma de datos[4].
`gpg --detach-sig`	Generar firma separada.
`gpg --verify`	Importar clave pública.

[3] Con compresión.

[4] Sin compresión.

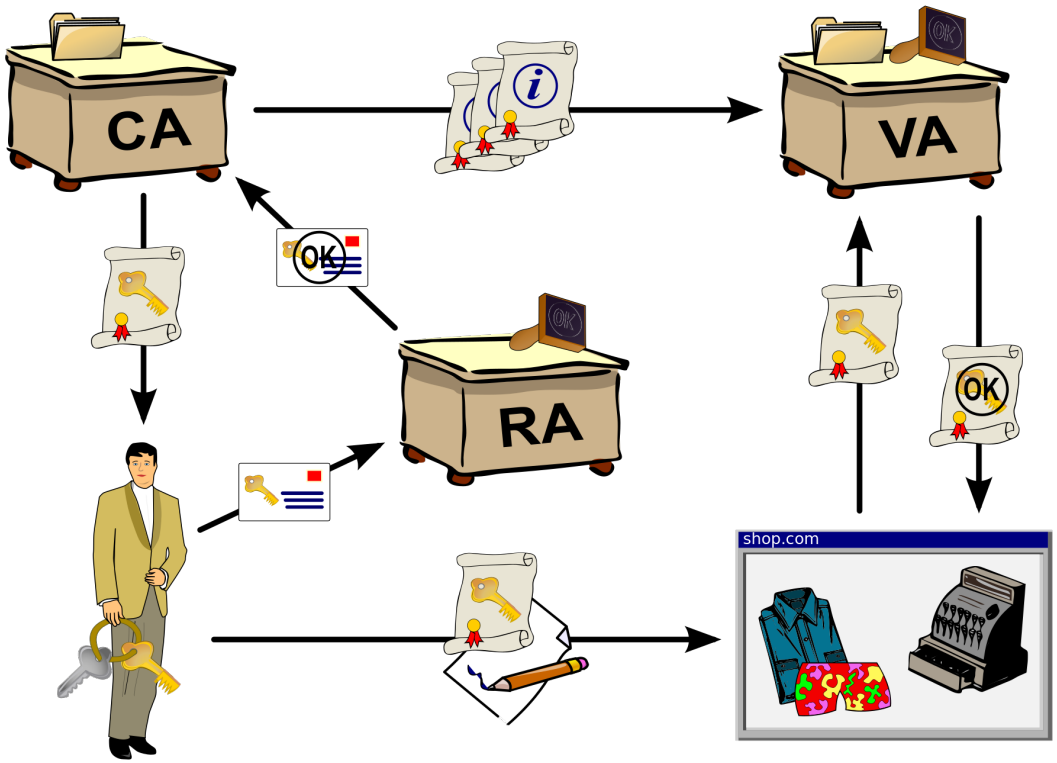
Opciones adicionales

Comando	Acción
`gpg --enarmor`	Conversión de binario a base 64.
`gpg --dearmor`	Conversión de base 64 a binario.

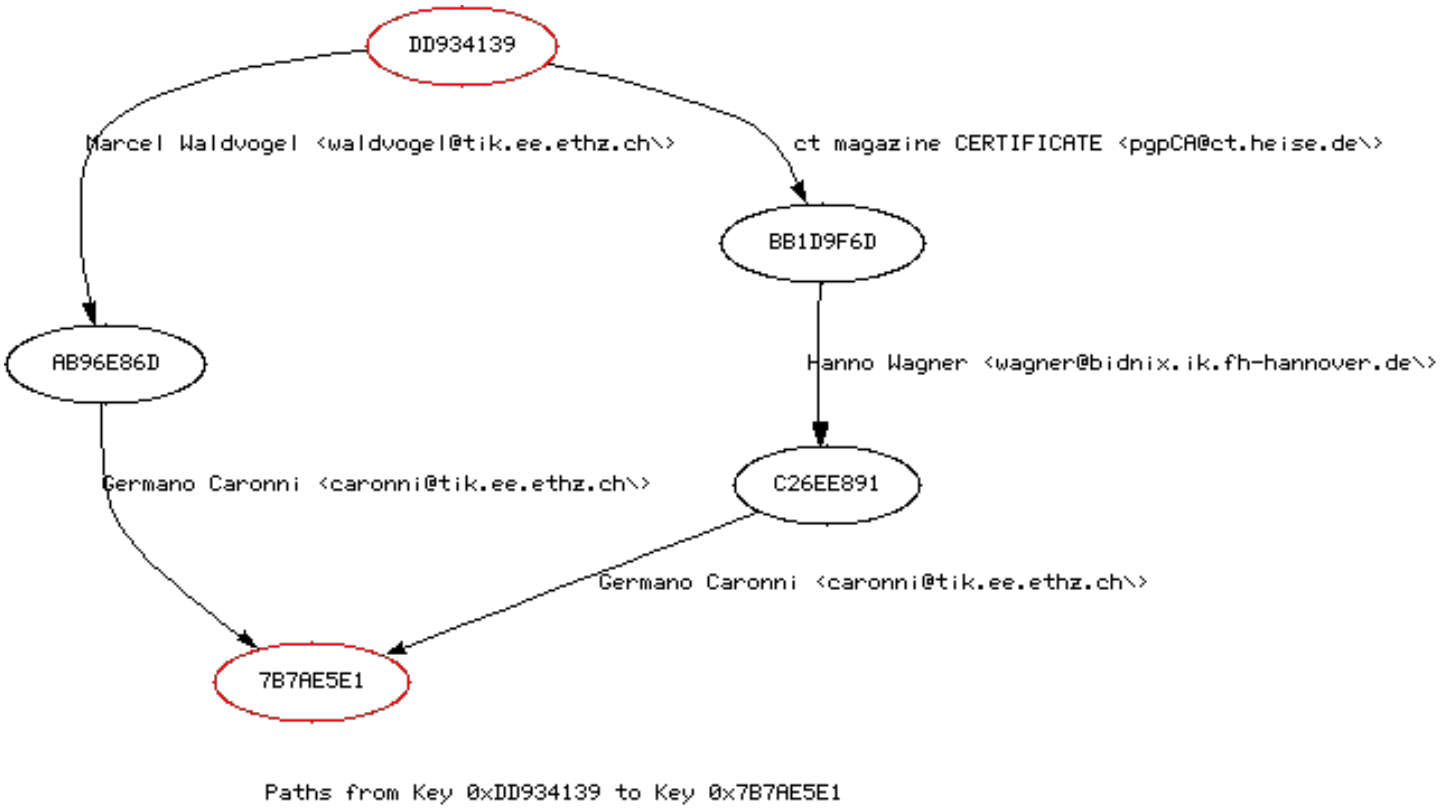

I'VE BEEN POSTING MY PUBLIC KEY FOR 15 YEARS NOW, BUT NO ONE HAS EVER ASKED ME FOR IT OR USED IT FOR ANYTHING AS FAR AS I CAN TELL.
MAYBE I SHOULD TRY POSTING MY PRIVATE KEY INSTEAD.

El Problema de la Verificación de Identidad

Soluciones: Infraestructura de Clave Pública



Soluciones: Red de Confianza



Servidores de Claves

- Son servidores que almacenan y distribuyen claves públicas.
- GPG tiene funcionalidades para cargar y recibir claves de un servidor de claves.
- Base para la implementación de la red de confianza.
- Servidores importantes:
  - `https://pgp.mit.edu/`
  - `https://keyring.debian.org/`

Comandos de Edición

Comando	Acción
`check`	Revisar las firmas de la clave.
`fpr`	Ver la huella dactilar de la clave.
`sign`	Firmar la clave.
`trust`	Cambiar el nivel de confianza de la clave.
`revkey`	Revocar clave.

La Red de Confianza es Delicada


HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP:
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

Cliente de Correo Thunderbird

- Cliente de correo software libre.
- Desarrollado por la Fundación Mozilla.
- Soporte de OpenPGP:
  - Nativo (versión >= 78).
  - Extensión (versión <= 68).

Enigmail

- Extensión que conecta a Thunderbird con GnuPG.
- Obsoleta desde Thunderbird 78.

Conclusiones

- OpenPGP es un estándar que define una suite de herramientas criptográficas descentralizadas.
- GnuPG es la implementación libre del estándar OpenPGP del proyecto GNU.
- GnuPG se caracteriza por ser fácil de usar.
- OpenPGP es una pieza muy importante de la infraestructura de los sistemas tipo Unix.
- De cara al usuario final, OpenPGP ha sido desplazado completamente por la PKI.

Contactos

Prof. Miguel Astor

- miguel.astor@ciens.ucv.ve
- miguel.a.astor@ucv.ve

Gracias por su atención