

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

- 1 Introducción
- 2 Fundamentos
- 3 Uso Básico de GPG
- 4 Red de Confianza
- 5 Correo Electrónico Cifrado
- 6 Conclusiones

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

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

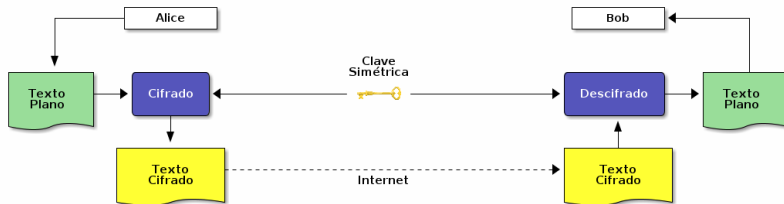
Criptografía

Definición

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

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

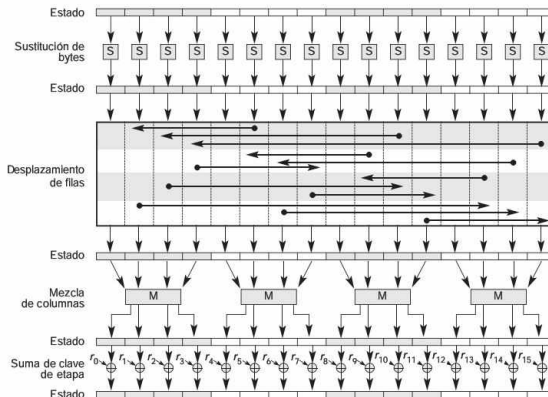
Criptografía Simétrica



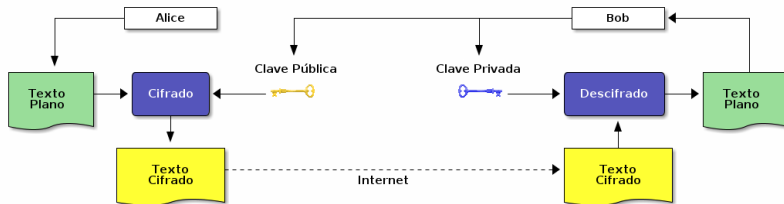
Ejemplo: Cifrado Simétrico Básico

B	U	C	K	E	T	H	E	A	D
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	20	2	10	4	19	7	4	0	3
+	+	+	+	+	+	+	+	+	+
12	14	9	1	28	6	89	42	11	7
=	=	=	=	=	=	=	=	=	=
13	34	11	11	32	25	96	46	11	10
%	%	%	%	%	%	%	%	%	%
26	26	26	26	26	26	26	26	26	26
=	=	=	=	=	=	=	=	=	=
13	8	11	11	6	25	18	20	11	10
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
N	I	L	L	G	Z	S	U	L	K

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

$$c = p^e \text{ mód } n$$

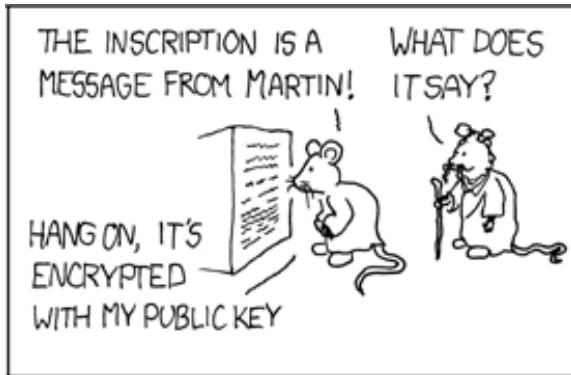
Descifrado

$$p = c^d \text{ mód } n$$

GPG - GnuPG - GNU Privacy Guard



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



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 línea de comandos.

Opciones de Manipulación de Claves

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

Opciones para Cifrado de Datos

Comando	Acción
gpg -u	Especificar clave a usar.
gpg -e	Cifrar datos.
gpg -d	Descifrar datos.

Opciones para Verificación de Firmas

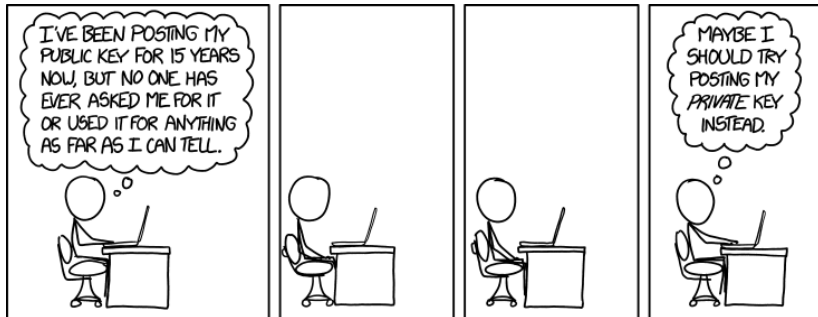
Comando	Acción
<code>gpg --sign</code>	Generar firma de datos ³ .
<code>gpg --clearsign</code>	Generar firma de datos ⁴ .
<code>gpg --detach-sig</code>	Generar firma separada.
<code>gpg --verify</code>	Importar clave pública.

³Con compresión.

⁴Sin compresión.

Opciones adicionales

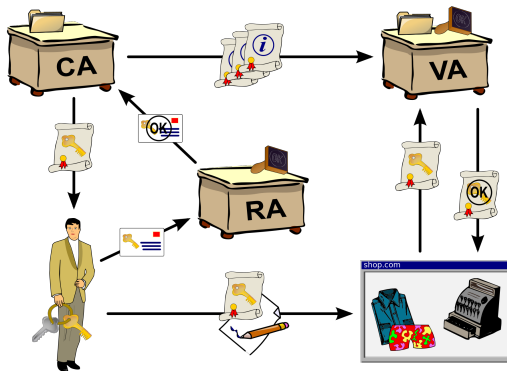
Comando	Acción
gpg --enarmor	Conversión de binario a base 64.
gpg --dearmor	Conversión de base 64 a binario.



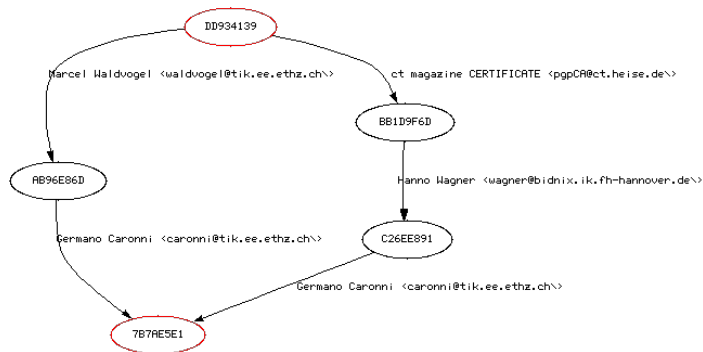
El Problema de la Verificación de Identidad



Soluciones: Infraestructura de Clave Pública



Soluciones: Red de Confianza



Paths from Key 0xDD934139 to Key 0x7B7AE5E1

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.

HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:

LOOK FOR THIS
TEXT AT THE TOP:



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

