

SSH

Por Hermosilla, Pizzano y Crocco

¿Qué es SSH?

SSH es una forma segura de conectarse de forma a un ordenador o servidor remoto a través de Internet. Para esto se cifran todos los datos que se envían entre los dispositivos, dificultando así que alguien intercepte o robar información sensible



Historia

En los 70 existía **Telnet**, que sirve para conectarse a un servidor remoto pero de forma insegura hasta que **SSH** hace lo mismo de forma segura, se podría decir que es su evolución



Como funciona:

SSH usa conexiones TCP para enviar datos encriptados (incluyendo tamaño y autenticación) entre cliente y servidor. El cliente inicia la conexión, se autentica y abre un canal seguro. La multiplexación permite múltiples conexiones SSH sobre una sola TCP, mejorando velocidad y eficiencia.

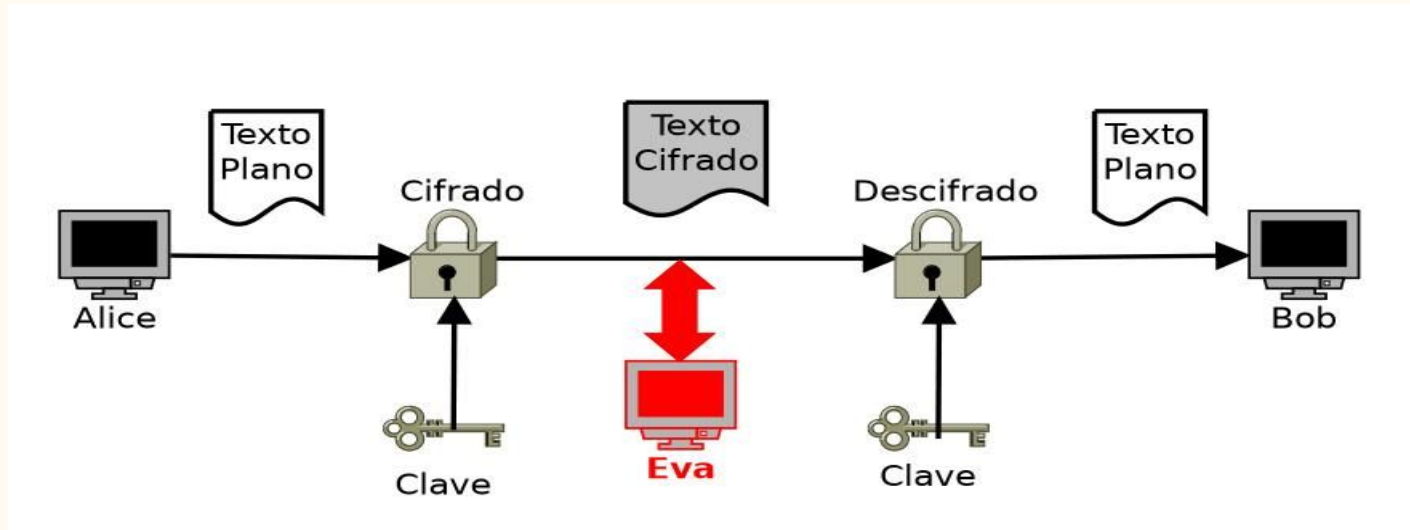
Claves

Hay 3 claves, siendo estas simétrica, asimétrica y hash, ssh utiliza estas 3 técnicas tanto para el cifrar como para descifrar.

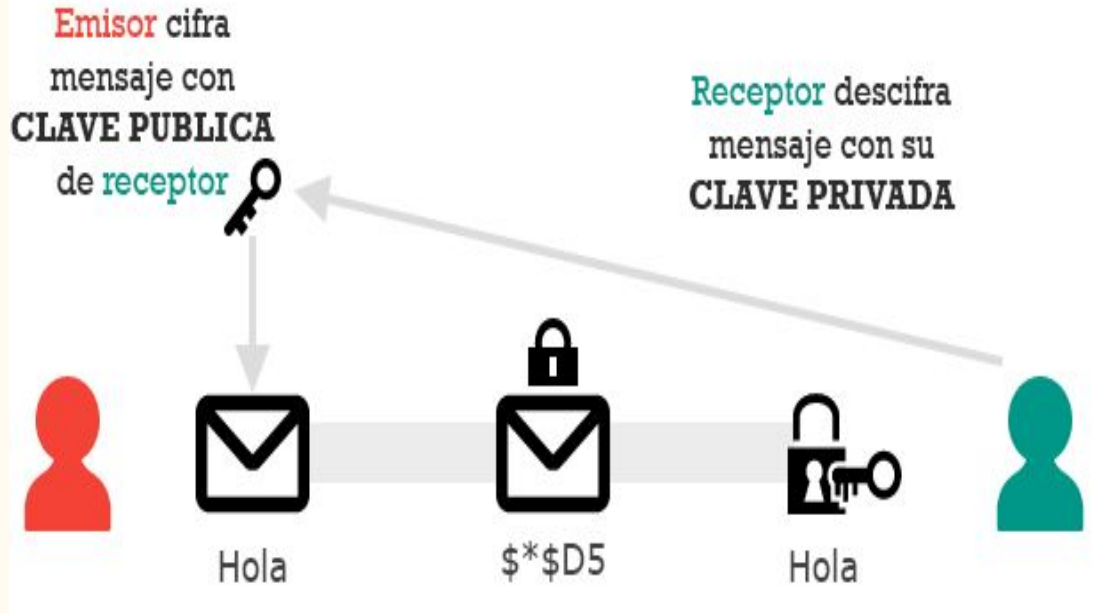


Claves simétricas

- Cifra y descifra
- Cualquiera con acceso a la clave también tiene acceso al mensaje



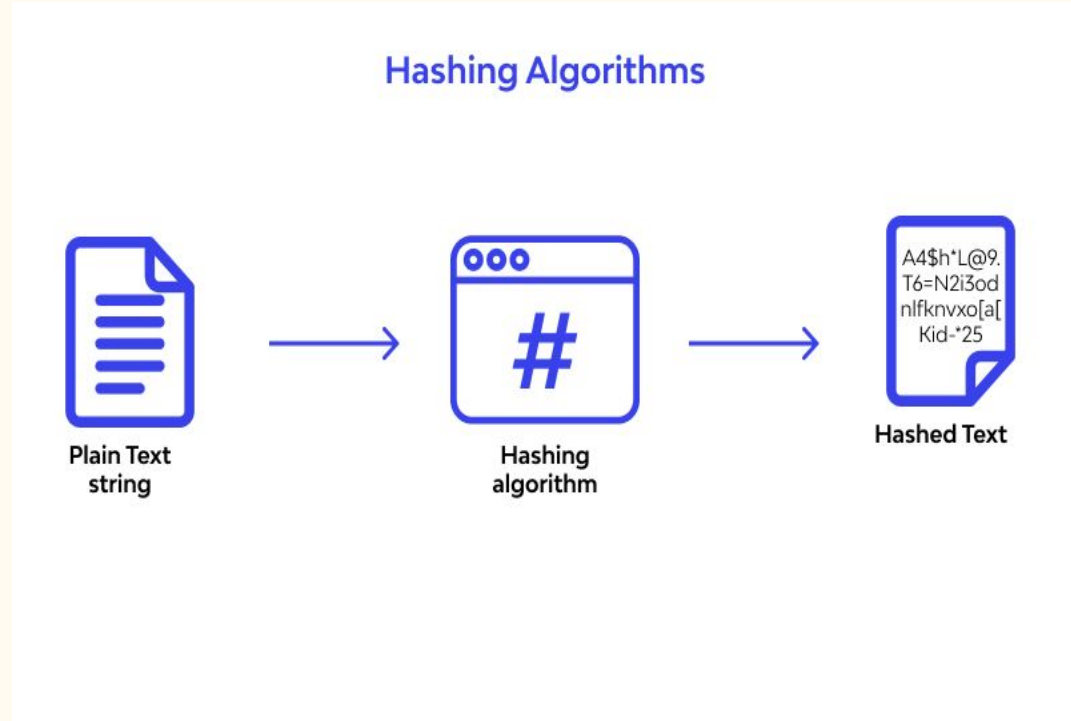
Claves Asimetricas



- Clave pública, la conocen todos y es la que cifra
- Clave privada solo la conoce el receptor, para descifrar

Hash

Funciona como un código de barras de un producto. Cualquier cambio en el archivo cambia su valor hash. Este valor es único y sirve para verificar que un archivo no ha sido modificado.



Usos

- Acceso remoto seguro a servidores Linux, Unix y Windows.
- Transferencia cifrada de archivos con SCP y SFTP.
- Gestión remota de servidores y dispositivos de red.
- Ejecución segura de comandos en sistemas remotos.
- Túneles cifrados para proteger aplicaciones y redes.

Como usarlo

Este es el comando que se usa para conectarse a servers

```
$ssh remote_username@remote_host -p (port)
```

```
Usuario@DESKTOP-VEF431T MINGW64 ~
```

```
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```

1	1	—	—	—	—	—	1	()	1
1	—	\	/	—	1	—	\	/	—
1	()	1	()	1	1	1	()	1	1
1	—	/	\	—	1	1	\	—	1


This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

bandit0@bandit.labs.overthewire.org's password:

Versiones

Primero existio SSH 1, el cual hace uso de muchos algoritmos de cifrado patentados

Luego existio SSH 2, el cual es igual a SSH 1, pero mejor



SSH-1 vs. SSH-2

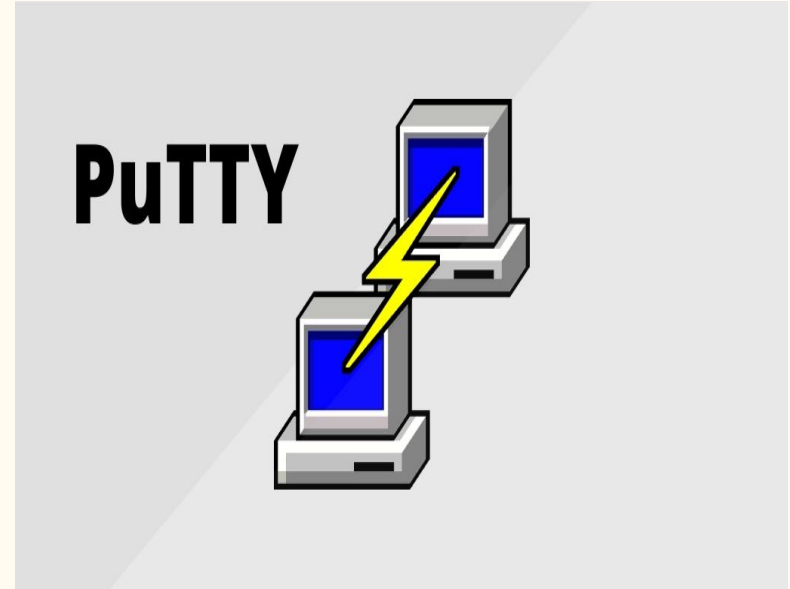
- | | |
|--|---|
| ○ All in one protocol | ○ Separate protocols |
| ○ CRC-32 integrity check | ○ Strong integrity check |
| ○ One session per connection | ○ Multiple sessions per connection |
| ○ No password change | ○ Password change |
| ○ No public-key certificate authentication | ○ provide public-key certificate authentication |

Implementaciones

OpenSSH



PuTTY



OpenSSH

Suite de herramientas open-source para conectarse de forma segura a sistemas remotos mediante el protocolo SSH. Es el estándar en sistemas Unix/Linux y está integrado en macOS y Windows

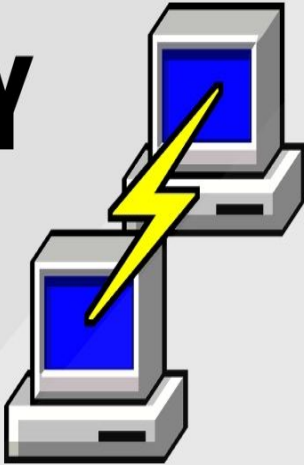
10/11



PuTTY

Cliente SSH gratuito para Windows (sin soporte nativo en Unix). Incluye herramientas como PuTTYgen (generador de claves) y Pageant (gestor de claves)

PuTTY



Ventajas

Open SSH

- Estándar en Unix/Linux: Integrado en sistemas basados en Unix.
- Configuración flexible: Archivos de texto (``config``, ``known_hosts``).
- Mejor para scripting: Comandos como ``scp`` y ``rsync`` sobre SSH.
- Soporte moderno: Algoritmos como ED25519 por defecto.

PuTTY

- Interfaz gráfica (GUI): Ideal para usuarios Windows sin CLI.
- Herramientas adicionales: PuTTYgen, Pageant, Plink.
- Portabilidad: Ejecutable sin instalación (versión portable).
- Soporte legacy: Telnet, Rlogin (útil para dispositivos antiguos)

Desventajas

Open SSH

- Menos intuitivo para usuarios no técnicos.

PuTTY

- - No soporta estándares como `~/.ssh/config` (requiere configuración manual).
- - Formato `.ppk` no compatible con OpenSSH (se requiere conversión).

Comparación

	OpenSSH	PuTTY
Tipo	Suite de herramientas	Cliente SSH/SCP/Telnet
Sistema	Multiplataforma	Windows
Interfaz	Terminal	<u>Grafica</u> + Terminal
Licencia	Open Source	Open Source
Protocolos	SSH, SCP, SFTP	SSH, Telnet, Rlogin, SCP
Almacenamiento	Configuración en archivos de texto	Guarda sesiones en GUI
Uso <u>Tipico</u>	Servidores y sistemas Unix	Clientes Windows

Conclusion

El protocolo SSH (Secure Shell) es una herramienta fundamental en la administración segura de sistemas remotos, porque permite la comunicación cifrada entre dispositivos, protegiendo los datos de hackers