Pen-Testing

1. Planificación y reconocimiento
2. Escaneo
3. Obteniendo acceso
4. Mantener el acceso
5. Análisis y contramedidas
6. … vuelta al 1

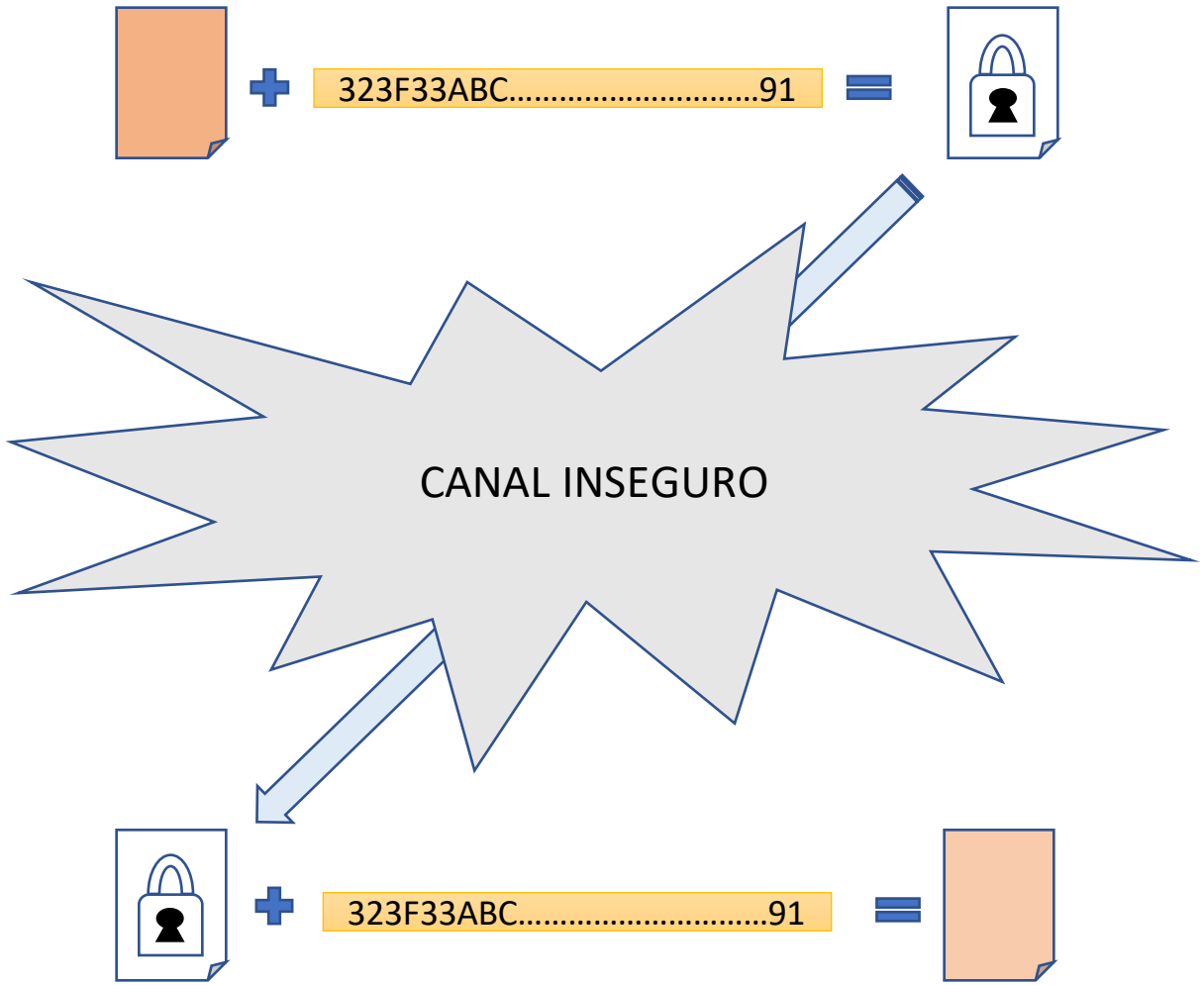
2. Securización de las comunicaciones. Protocolos, Traffic sniffing, Robo de credenciales

3. Securización de Bases de Datos: Ataques de inyección SQL

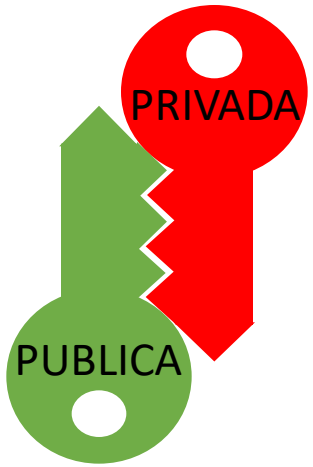
4. Firewalls y seguridad de red

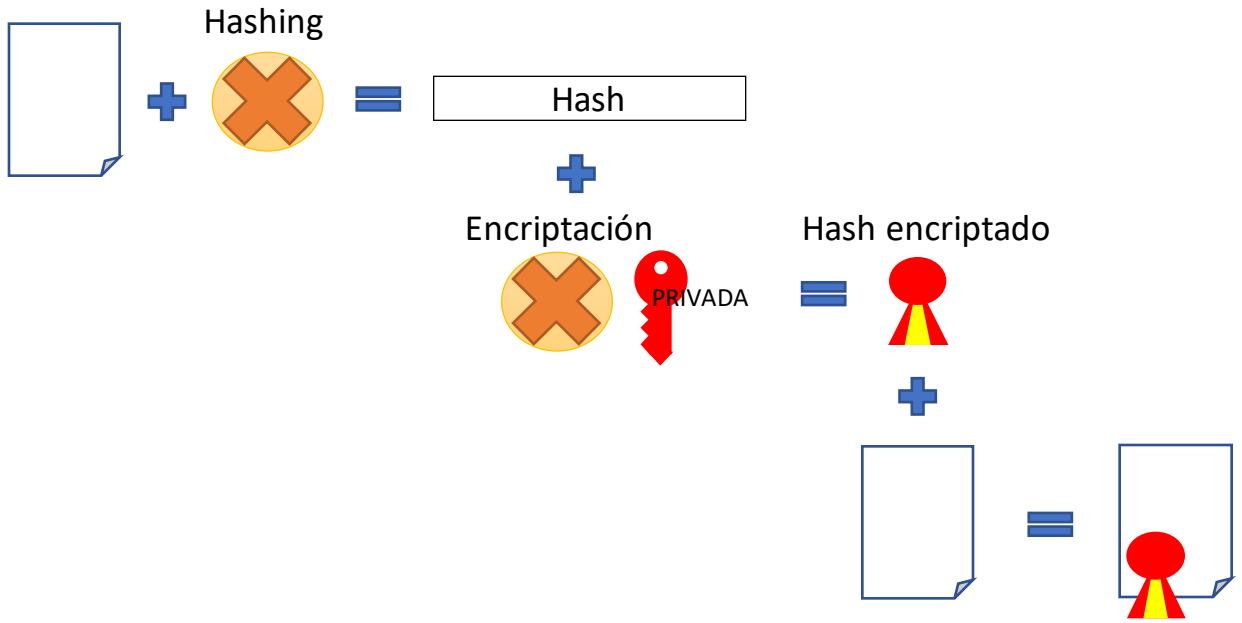
5. Técnicas de encriptación y hashing

Clave simétrica

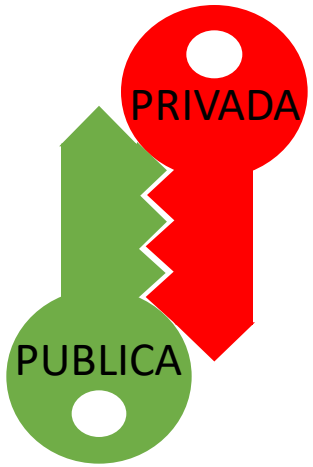


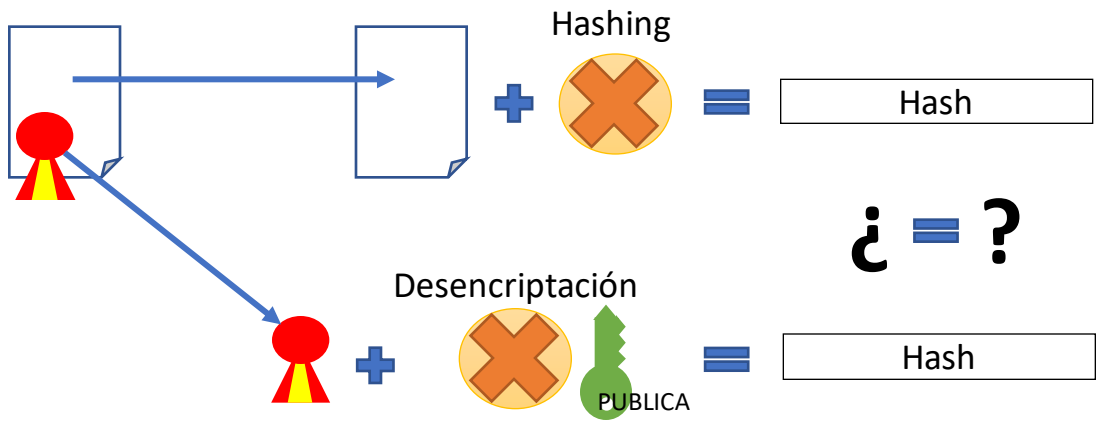
Clave pública: Firma





Clave pública: Verificación





6. Securización de recursos críticos (ficheros de parametrización)

7. Sistemas externos de autenticación, control de acceso y monitorización

Recursos del segundo día

Wireshark: inspección de tráfico

Snoopwpf: similar a Spy++ para wpf, permite no sólo la inspección sino también alteración de la estructura

- https://github.com/snoopwpf/snoopwpf/releases

Nmap: Permite realizar operaciones de scaneo de redes y puertos

- https://nmap.org/

Echo mirage: Interceptación y tampering de las comunicaciones de una aplicación

- https://sourceforge.net/projects/echomirage.oldbutgold.p

ILSpy: Descompilador de .Net disponible desde VSCode

Process Monitor: Inspección de procesos, recursos, acceso a ficheros, registros, red…

- https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

WinAppDriver: Controlador tipo Webdriver para poder gestionar desde Test las aplicaciones (Appium Desktop)

- https://github.com/Microsoft/WinAppDriver

Dentro de su repositorio prestamos atención al proyecto de test de la calculadora de Windows

- https://github.com/Microsoft/WinAppDriver/tree/master/Samples/C%23/CalculatorTest