

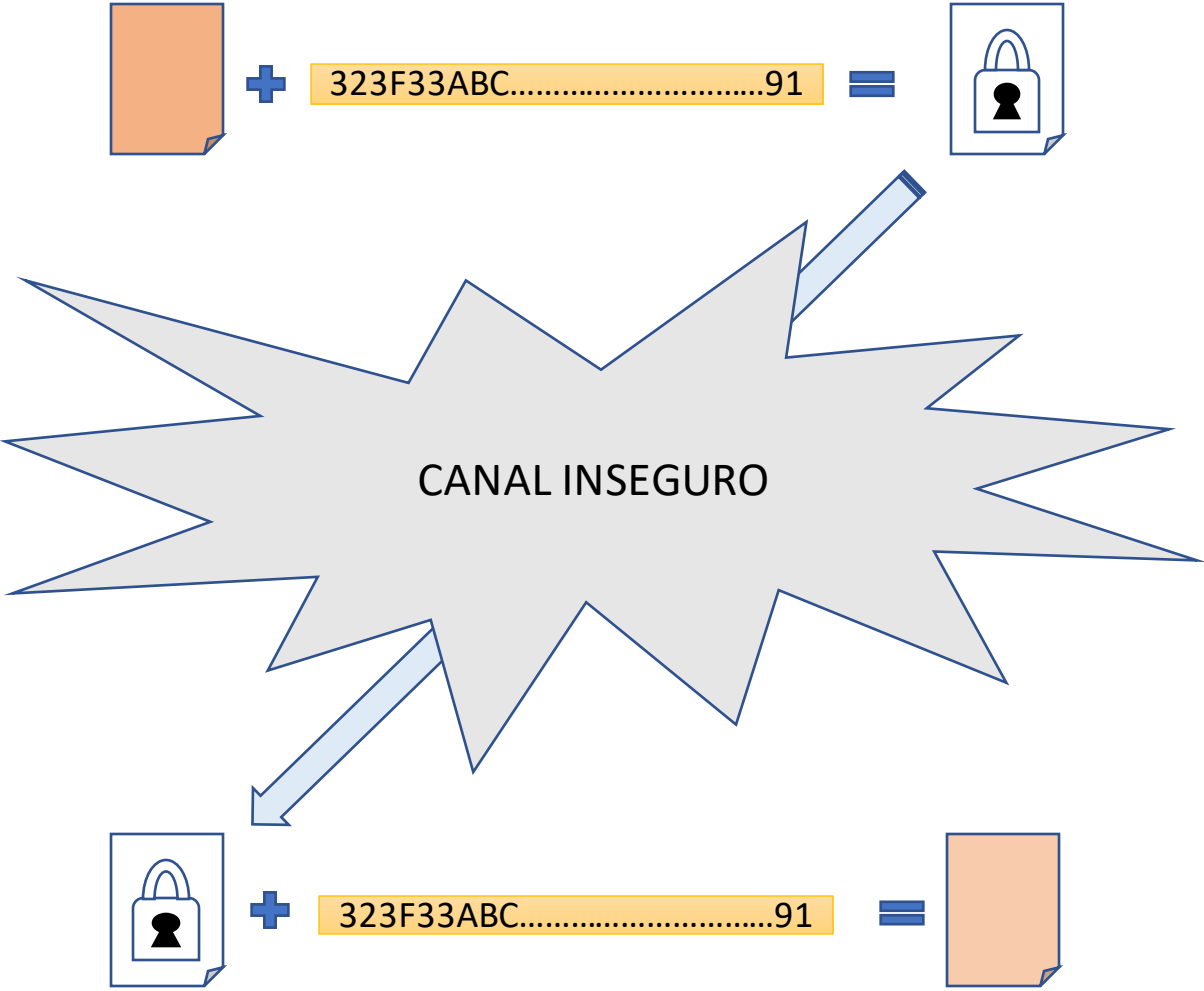
## 2. Securitización de las comunicaciones. Protocolos, Traffic sniffing, Robo de credenciales

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

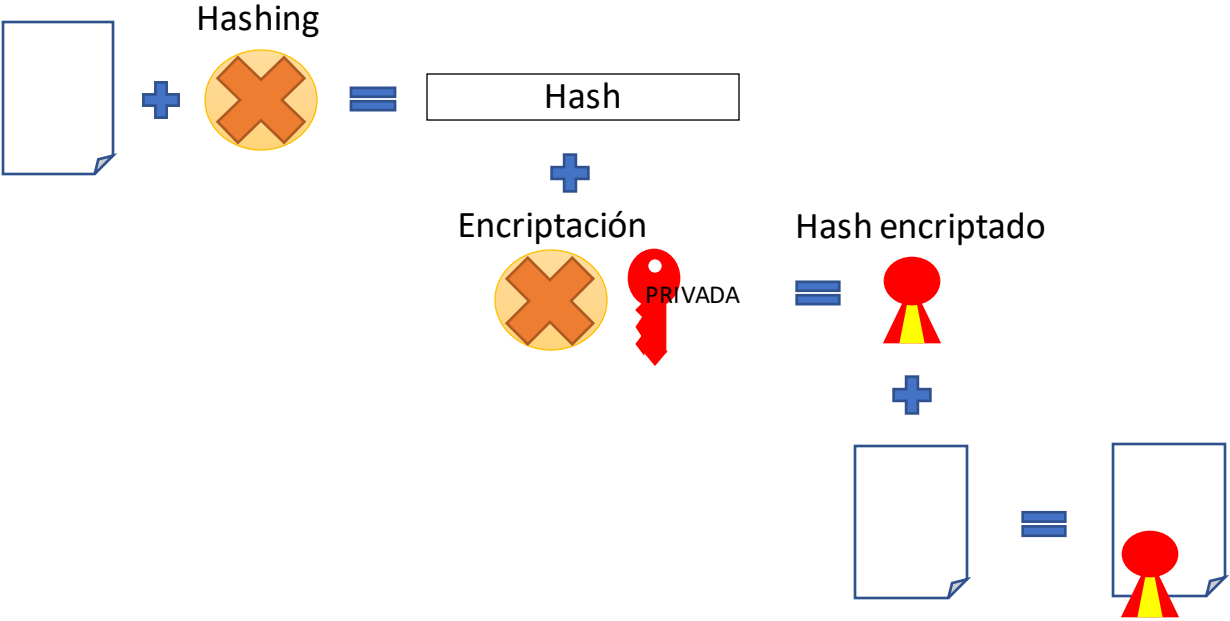
## 4. Firewalls y seguridad de red

# 5. Técnicas de encriptación y hashing

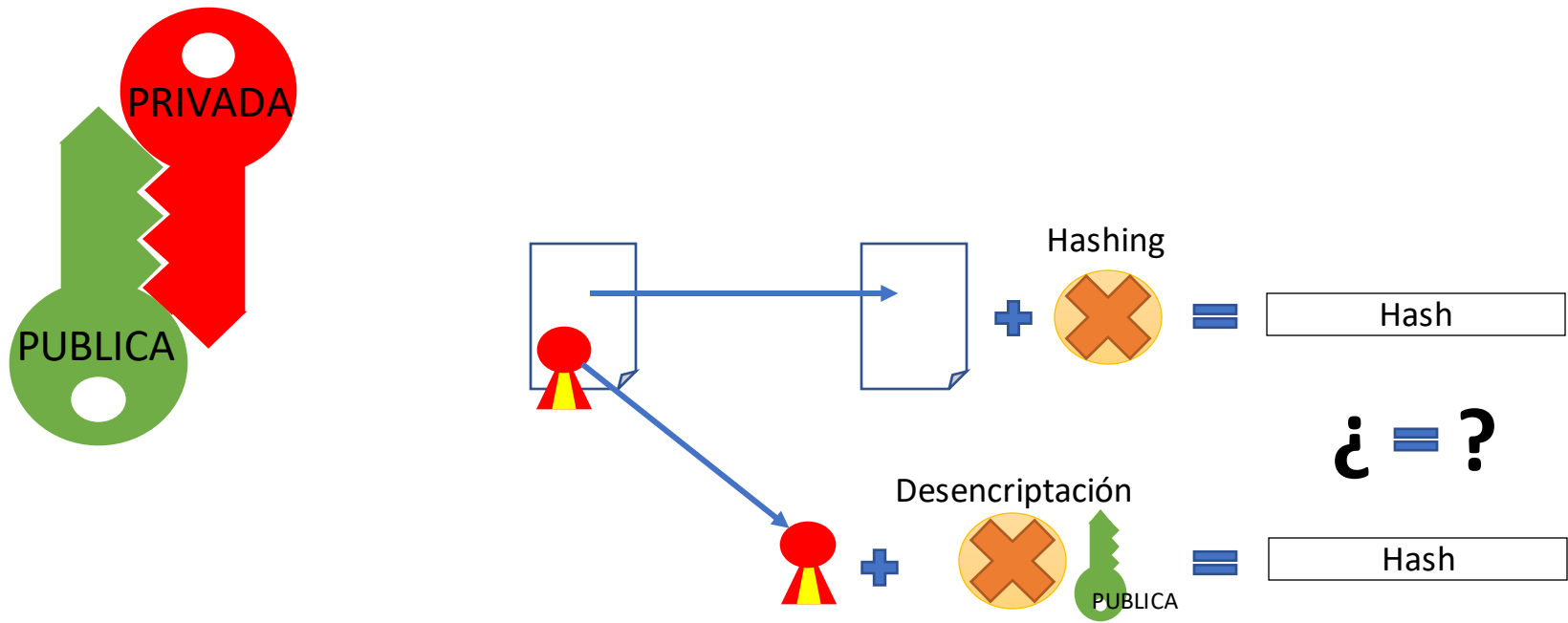
# Clave simétrica



# Clave pública: Firma



# Clave pública: Verificación

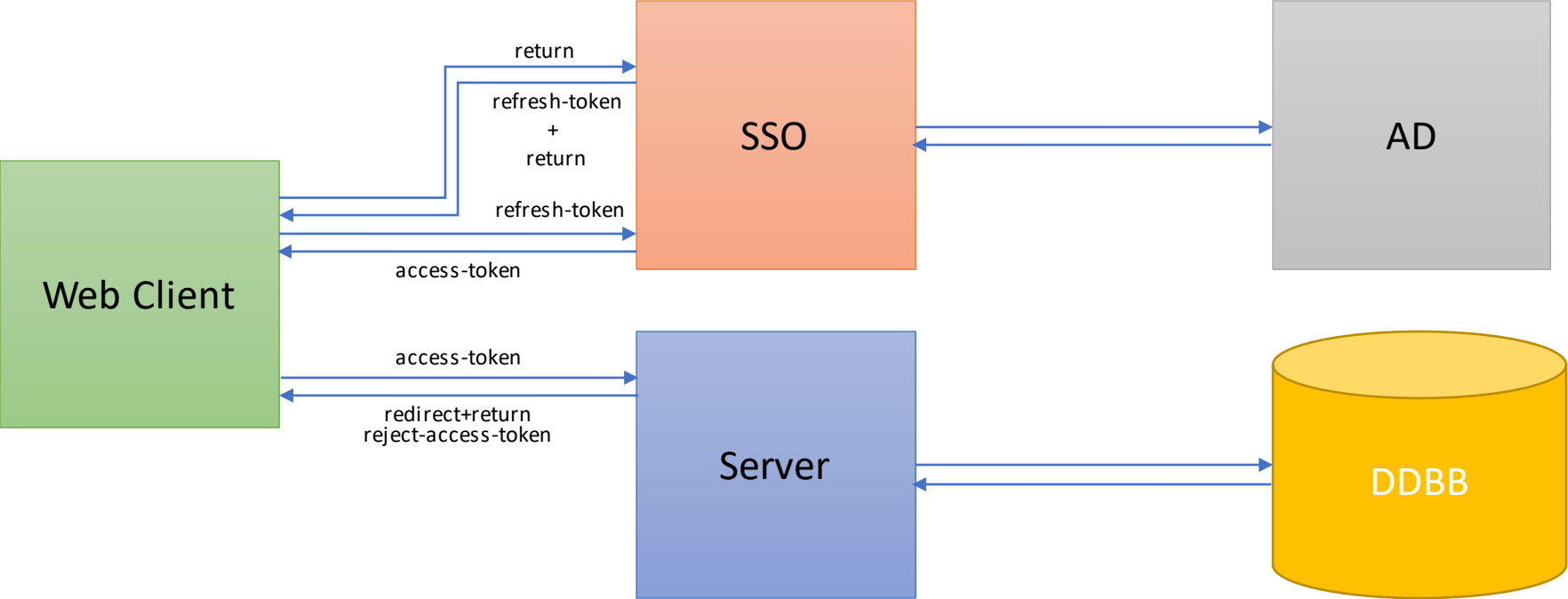


## 6. Securitización de recursos críticos (ficheros de parametrización)



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

# SSO Flow



# 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>

**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>