Criptografía y Seguridad *(72.44)*

TRABAJO PRÁCTICO 1: CIFRADO POR BLOQUES

Algunas aclaraciones.

Ante las preguntas de algunos grupos, van las siguientes aclaraciones.

- se tiene que usar la librería de openssl.
- los archivos que se les enviaron fueron probados en pampero.
- Para cifrado con feedback tienen dos opciones:
    - Asumir un número de bits de feedback por default (por ej. 8 bits)
    - Pedir que el usuario ingrese el valor por linea de comandos.

  En cualquier caso, ***documentar cómo se considerará***
- Para cifrado con password en modo que no sea ECB, como no hay una función en openssl que derive el password en Key distinto de IV, tienen dos opciones:
    - Derivar en Key = IV
    - Diseñar una función que derive el password en Key distinto de IV

  En cualquier caso, ***documentar cómo se considerará***
- Mucho cuidado con el Key e IV de AES. Si no se escribe de **exactamente 16 bytes**, se los completa con basura, con lo cual no podran encriptar / desencriptar correctamente. Tenerlo en cuenta al derivar una password en Key / IV.