

# LAB



# FreeBSD Security Advisory

- Read FreeBSD-SA-13:11.sendfile
  - File 'FreeBSD-SA-13\_11\_sendfile\_asc.txt' in IS

# AES CBC

- Download AES.zip from IS
- The source code contains the AES in ECB mode
- Implement AES in CBC mode
  - Complete the function:
    - `aes_encrypt_cbc`
  - The source code contains a test of your implementation