

IN3210/4210 2020 Exercise 2 - Symmetric encryption

Note: You may for instance use `xxd` for displaying hex, and `ghex` or `blex` for hex-editing.

You are to perform the following tasks from the SEED Secret-Key Encryption Lab:

- 2.2 Task 2: Encryption using Different Ciphers and Modes
- 2.3 Task 3: Encryption Mode – ECB vs. CBC
- 2.6 Task 6: Initial Vector (IV)
 - Skip the question about Cipher Feedback Mode (CFB).
 - Note: You may use `xxd -p filename` to output the contents of a file in hex. `xxd -r -p filename` performs the reverse operation. `echo -n "string" > filename` may be used to save a string to file without adding a newline. XOR may be calculated using for instance an online XOR calculator.

The SEED Secret-Key Encryption Lab is found at:

https://seedsecuritylabs.org/Labs_16.04/PDF/Crypto_Encryption.pdf

The exercise is not to be submitted.