CAA 24-25

Exercise Sheet on Symmetric Crypto 1

1 Modes of Operation

For ECB, CBC, CFB, OFB, and CTR, study the following points

- Does the mode of operation transforms the block cipher into a stream cipher?
- Is the encryption or the decryption parallelizable
- Is it possibility to do partial decryption and/or partial reencryption?
- What are the consequences if we reuse an IV?
- What are the implications on the plaintext of a 1 bit change in the ciphertext?
- Is padding required?
- When implementing it, do you need both encryption and decryption or only one of them?
- Is there an attack if the IV is predictable (e.g. an incremented counter)? For this, consider an attacker that can do chosen-plaintext attacks and the goal of which is to verify a guess on a plaintext.
- Do you find other security issues in this mode of operation? (e.g. birthday attack)

2 Forensics on SHA-3

You infiltrated the building of a criminal group which is known to use a very complex 70 characters password internally. You also know that they are paranoids and that they use SHA-3 to hash their password.

During your infiltration, you managed to copy the RAM of a machine that was computing the SHA-3 of the complex password. In the RAM, you managed to recover the **full** state final state (1600 bits), i.e., the final inner and outer state of the sponge construction. Explain how to recover the secret password.

Bonus: Do the SHA-3 challenge on `https://root-me.org`.