Let’s have a look at some mid- and low-level symmetric primitives. Pick and solve one of the following exercises.

**Exercise 7.1** (GCM: Galois Counter Mode). (10 points)

Find documentation and security proof for GCM.

(i) Describe how the mode works. Which components are used? How are they put together? Argue for correctness.

(ii) For use in which protocols (IPsec, TLS, SSH, GSM/UMTS/LTE, …) is it standardized?

(iii) In which model is it proved secure? Describe which oracles are given to an attacker. How does the model relate to sLHAE?

[I do not need to say that you should do all this in your own words, do I?]

**Exercise 7.2** (BLK-CCM: BLK-CTR & CBC-MAC). (10 points)

Find documentation and security proof for CCM.

(i) Describe how the mode works. Which components are used? How are they put together? Argue for correctness.

(ii) For use in which protocols (IPsec, TLS, SSH, GSM/UMTS/LTE, …) is it standardized?

(iii) In which model is it proved secure? Describe which oracles are given to an attacker. How does the model relate to sLHAE?

[I do not need to say that you should do all this in your own words, do I?]
Exercise 7.3 (SNOW3G). (10 points)

Find the documentation on SNOW3G.

(i) Describe how it works. [A picture is probably helpful.] Argue for correctness.

(ii) For use in which protocols (IPsec, TLS, SSH, GSM/UMTS/LTE, ...) is it standardized?

(iii) What is known about its security? Which attacks are known? Describe one. [It’s ok, if it’s only an attack on a downgraded version. But mention the differences and what it means for the full version.]

[I do not need to say that you should do all this in your own words, do I?]