You have encountered several levels of security:

- Unbreakability,
- Universal Unforgeability,
- Selective Unforgeability,
- Existential Unforgeability;

along with different means for an attacker:

- Key-Only Attack,
- Known Message Attack,
- Single Occurrence Chosen-Message Attack,
- Chosen Message Attack.

Pairing an adversarial goal with an attack model defines a security notion.

**Exercise 11.1.** (4 points) Consider the ElGamal signature scheme. Assume that the DL is hard and decide for each of the 16 security notions whether the scheme is

- secure,
- not secure
- or the answer is unknown.

What can you say, if you assume that DL is easy? Use the connections between the security notions to simplify your argument.
EXERCISE 11.2. (3 points) For a signature scheme, a message is first hashed and then the hash value is signed. Assume that the signature scheme is secure in the EUF-CMA model. Does that imply that the hash function is collision resistant? Prove your answer.