**A-6** Consider the zero-knowledge proof in Figure 1 of the lecture notes. Show the special soundness property, i.e., given two transcripts of the protocol (a', b' , c, r) and (a', b', c' , r' ), show that it is possible to recover s.

**Grading:** 1.0
**Motivation:**
Correct answer. Goes well with the lecture slides as well as these lecture notes:
https://www.cs.jhu.edu/~susan/600.641/scribes/lecture10.pdf

**A-7** Give two isomorphic graphs of at least ten nodes each. (Do not just tweak the example from the slides; construct the example from scratch.) Give the isomorphism. Explain how these graphs (or at least larger graphs) can be used in a zero-knowledge proof. You do not have do give an explicit example of the zero-knowledge proof.

**Grading:** 1.0
**Motivation:**
Correct graphs and a good explanation. Similar information is provided on page 11-15 in the lecture slides.

**A-8** Briefly explain the properties Completeness, Soundness and Zero-Knowledge regarding zero-knowledge proofs.

**Grading:** 1.0
**Motivation:**
Chapter 3.3 gives the same explanation. Correct answer once again.

**A-9** Explain how the zero-knowledge property of a zero-knowledge proof is related to a simulator.

**Grading:** 1.0
**Motivation:**
Good answer. Agrees with information on page 6 in the lecture notes about electronic voting.

**A-10** In the lecture notes, it is remarked that an interactive zero-knowledge proof can be made noninteractive through a trick, by letting "the challenge provided by Victor be a function of some predetermined parameter". What cryptographic building block would be suitable as such a function?

**Grading:** 1.0
**Motivation:**
Well-put answer. Agrees with the information on the lecture notes about anonymity.

**A-11** Consider the zero-knowledge proof based on graphs. The probability that Peggy can fool Victor in one execution is 2^-1 , so the proof is executed k > 1 times so that the overall probability is 2^–k . In the zero-knowledge proof relating to (h, u) = (g^s , a^s ), explain how k should be chosen.

**Grading:** 1.0
**Motivation:**
Nice answer. It's good with a numeric example, as well as pointing out pros and cons with choosing a big *k* value.

**A-22** In the slides, two main strategies for making an electronic voting scheme are presented. One is that "the vote is posted on the bulletin board in encrypted form, and the person (casting the vote) is not anonymous". Describe a scheme like this, and in particular explain how the vote can be counted without sacrificing privacy/anonymity.

**Grading:** 1.0
**Motivation:**
A very thorough and detailed answer. One of the equations is wrong. However, this doesn't affect the overall answer (it's probably just a typo). Goes well with chapter 4.3.2 in the lecture notes.

**A-24** In the slides regarding homomorphic encryption based voting, it is stated that if the sum of mi is moderate, we can compute the discrete log. Why does the sum need to be moderate?

**Grading:** 1.0
**Motivation:**
It is indeed difficult to calculate the discrete logarithm for a large number *m*. The answer agrees with for example the part about ElGamal encryption in the lecture notes. Information about discrete logarithms can be read here: https://en.wikipedia.org/wiki/Discrete_logarithm

## **Total score:** 8.0