Selected topics in Cryptography

HOMEWORK #3.

Deadline: December 17, 2023, midnight

Basic rules for submitting your homework:

- the file has to be named: "firstname-lastname-HW3.pdf"
- clearly mark which problem is being solved and list the solutions in the order of the problems from the assignment
- write the solutions carefully providing sufficient details; when in doubt, write more
- HW is to be turned in via *moodle* in the *pdf* format
- late homeworks only accepted in justified situations

1. (15 pts) Devise a secret sharing scheme for five people in which one specific person, Alice, can calculate the secret with any three of the other four people, but no group not containing Alice can calculate the secret.
2. (15 pts)
   a) Show that each point on an elliptic curve has an additive inverse.
   b) Consider Example 7.9 on page 282 in Stinson's textbook where E is a cyclic group of order 13. Then consider Theorem 7.1 on page 285 in this textbook. What are the numbers n_1 and n_2 for the group E from Example 7.9?
   c) Find two non-isomorphic elliptic curves over $\mathbb{Z}_{11}$. Is there an elliptic curve over $\mathbb{Z}_{11}$ that is not cyclic?
3. (15pts) A yes/no knapsack problem is a problem where, given a set of weights, one answers the question whether there exists a solution to the problem for these given weights. A certificate is a solution vector for the problem.
   a) Devise a zero-knowledge proof protocol based on the yes/no knapsack problem.
   b) How would you get a large number of random knapsack problems for which the answer is yes?
   c) How would you get a large number of random knapsack problems for which the answer is yes and there is exactly one solution?
4. (5 pts) Solve Exercise 14.4.3 from the 'other' textbook, Chapter 14.