Project 4 (Weeks 9-12)

Topic: public key cryptography.

- Each team of two students will prepare and explain a written homework on one of the following questions, which will be assigned to you during the seminars:

  1. Describe the Knapsack cryptosystem, and apply it in an example.
  2. Describe the Paillier cryptosystem, and apply it in an example.
  3. Describe the Cramer–Shoup cryptosystem, and apply it in an example.
  4. Describe the McEliece cryptosystem, and apply it in an example.
  5. Describe the Goldwasser–Micali cryptosystem, and apply it in an example.

Points

- **1.5 points** for each member of the team if handed in by Week 13 or Week 14.