

PUBLIC KEY CRYPTOGRAPHY - Mathematics

Project 1 (Weeks 1-2)

Topics: complexity, greatest common divisor.

- You will prepare and explain a written homework on one of the following questions, which will be assigned to you during the seminars:
 1. Explain what is the vertex cover problem. Give some examples that illustrate why the problem is NP-complete.
 2. Explain what is the chromatic number problem. Give some examples that illustrate why the problem is NP-complete.
 3. Explain what is the exact cover problem. Give some examples that illustrate why the problem is NP-complete.
 4. Explain what is the partition problem. Give some examples that illustrate why the problem is NP-complete.
 5. Prove that the complexity of computing the greatest common divisor of two natural numbers $a, b \leq n$ by the Euclidean Algorithm is at most $O(\log^3 n)$.
 6. Explain Stein's Algorithm for computing the greatest common divisor of two natural numbers, and apply it in an example.
 7. Explain Dijkstra's Algorithm for computing the greatest common divisor of two natural numbers, and apply it in an example.
 8. Explain Lehmer's algorithm for computing the greatest common divisor of two natural numbers, and apply it in an example.
 9. Explain Bishop's algorithm for computing the greatest common divisor of two natural numbers, and apply it in an example.
 10. The greatest common divisor of two Fibonacci numbers may be computed as follows. Let $m, n \in \mathbb{N}$ and let F_n be the n -th Fibonacci number. Show that $\gcd(F_m, F_n) = F_{\gcd(m, n)}$, and apply it in an example.

Points

- **1 point** if handed in by Week 3 or Week 4.
- **0.5 points** if handed in by Week 5 or Week 6.