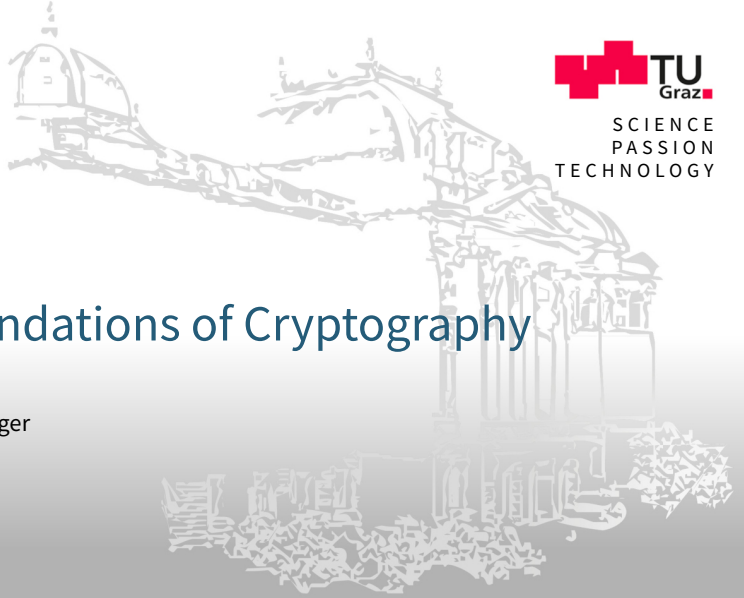
TU Graz

SCIENCE
PASSION
TECHNOLOGY



Mathematical Foundations of Cryptography

Lukas Helminger & Reinhard Lüftenegger

Introduction – WT 2020/21

Why this seminar?

Mathematics is the Language of the Universe.

Therefore, we want to understand the mathematics behind cryptographic primitives to

- design them,
- analyse them, and
- implement them.

Why are you here?

1. You had already crypto courses and want to understand them in more depth.
2. You are planning to attend crypto courses and want to be prepared?
3. Different motivation.

Course Organisation

- The weekly seminar unit takes place every **Thursday** and starts at **10:15h**.
- On 10 out of overall 15 seminar dates we **lecture** about **selected aspects of mathematics** in cryptography. Each lecture lasts 2 academic hours (which is 1.5 real-time hours).
- During the remaining part of the seminar you **give a talk and present exercises** on specified topics (details follow below).
- The seminar is a **continuous assessment course** (“prüfungsimmanent”).

Content

- L1 – Groups
- L2 – Rings
- L3 – Fields and Finite Fields
- L4 – Elliptic Curves
- L5 – Discrete Logarithm
- L6 & L7 – Gröbner Bases
- L8 & 9 – Lattices
- L10 – Boolean Functions

Goals

At the end of this course you know how to ...

- ... **describe** the most important **algebraic structures** used in cryptography.
- ... **represent** (certain) **cryptographic primitives** as polynomials and **conduct algebraic cryptanalysis** with this representation.
- ... **analyse** the **hardness of the discrete logarithm problem** in different groups and the implications for security parameters.
- **have** the necessary **foundations** for new cryptography (homomorphic encryption, post-quantum encryption).
- ... **assess boolean functions** and identify their applications in codes and lattices.

How to Get Your Grade

Exercises (Prerequest)

You do **paper and pen exercises (two sessions)**. To get a positive grade in this seminar you have to solve at least 60% of the exercises. If you solve more than 85% your grade will improve by one.

Seminar paper (50%)

You write **a paper** about predefined topics. The topics will be announced at mid January. Submission deadline is **February 5th**.

Seminar presentation (50%)

You work on a topic of your own choosing (related to the seminar).You will then present your results in form of a **seminar talk**. Your talk lasts approximately **20 minutes**. The dates for presentations are **November 12th**, and **January 7th**.

Further Information

- Course website

  https://www.iaik.tugraz.at/course/seminar-cryptology-and-privacy-mathematical-foundations-of-cryptography

- Seminar papers

  Send us your seminar papers in PDF via Email to {christian.rechberger, reinhard.lueftenegger, lukas.helminger}@iaik.tugraz.at.

- Seminar talk
  - Coordinate your topic and the intended content with us **before you start**.
  - Make an appointment and meet us **1 week before your talk** in one of our offices IF01{112, 010} to inform us about your presentation slides.
  - Send us your presentation slides in PDF **one day before your talk** via Email.

Questions?