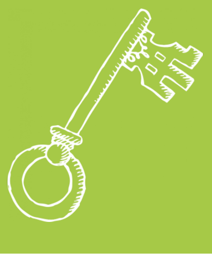
IAIK | Institute of Applied Information Processing and Communications



Easy Crypto Homework Framework 2

Advisor: **Maria Eichlseder**

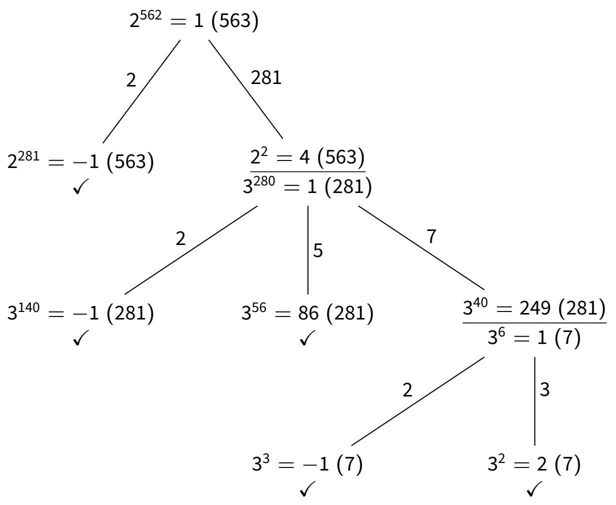
Motivation

To understand a new algorithm or method, such as a cryptanalytic attack or mathematical algorithm, it is useful to first apply it to some simple examples by hand. Such examples are useful for practicing, but also for personalized tasks and exams. However, inventing many new **“simple” examples (with few computation steps, “nice” numbers, etc.)** takes time for the teacher.

The goal of this thesis is to extend an existing **framework to generate, solve, and print** “simple” examples for a variety of cryptographic algorithms covered in the “Cryptography” course, such as differential attacks. This framework was developed during a previous bachelor’s thesis and should be extended with new task types and for new applications (e.g., individual exam tasks).

Goals and Tasks

- Understand selected tasks and algorithms (e.g., elliptic curves, differential cryptanalysis)
- Identify which properties make these tasks solvable
- Implement solution and print solution steps
- Extend existing framework with new examples



Literature

- Lecture “Cryptography”
  Homework Exercises
  https://www.iaik.tugraz.at/cryptography 2020
- R. Gruber
  Cryptography Task Generator
  Bachelor’s Thesis 2020

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor’s Thesis**
Project code
Thesis
Final presentation

Recommended if you’re studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in cryptography and mathematical basics
- Python programming

Advisor / Contact

maria.eichlseder@iaik.tugraz.at