Applied Cryptography

Lectures and Exam information

Luca Campa - Arnab Roy

Department of Computer Science
Universität Innsbruck

06 March, 2025

Overview

1. Lectures
2. Evaluation
3. Announcements
4. Materials

Topics

- Block cipher and encryption modes; Introduction to TLS; Message authentication and encryption in TLS; Encryption (mode) of Telegram; Cryptanalytic attacks on (selected) encryption modes and their real-world effect
- Hash functions and applications; Time memory tradeoff attacks; Cryptanalytic attacks on MD4/5
- Public key cryptography: RSA, Diffie-Hellman, Digital Signature; PKI and CA authority; Forging certificates
- PRNG, PRNG with crypto libraries; PRNG in linux systems; Breaking PRNGs
- SSL library for cryptographic functions;
- Key-derivation function (KDF); HKDF and application in Signal protocol

Scheduling

- 8:45 - 11:45
- Most of the times divided into:
  - Lecture
  - Lab session (hands-on code)

Evaluation

- 3 projects, 60% (each project counts as 20%)
- 2 Quizzes, 40% (each quiz counts as 20%)

Grading rules (https://informationsecurity.uibk.ac.at/teaching/):

- 1: $> 87\%$
- 2: $> 75\%$
- 3: $> 62\%$
- 4: $> 50\%$
- 5: otherwise

Projects

Projects will be composed by:

- 10% Implementation:
  - 2% if the code is running
  - 8% if the code returns correct results on all the test inputs (we will provide you with some of them, but not all)
- 10% Oral presentation

It is not mandatory, you can do the project in groups of **maximum 2** students.
Project presentations:

- 03 April 2025
- 15 May 2025
- 12 June 2025

The project's submission deadline will be 1 week before the presentation.
Note: you will not be allowed to present if you do not submit your project on time.

Quizzes

Quizzes are in writing mode. The types of questions can be:

- Short answers
- Code analysis
- Small script implementation
- Multiple choice
- ...

- Quiz 1: 10 April 2025
- Quiz 2: 26 June 2025

Course Administration

Important Announcements will be made in the **FORUM** on OLAT.
If you have quick questions **you can ask on the course's Matrix chat**.

Please check them regularly!

Necessary material

VM:

- Install VirtualBox on you machine or use of the machines in the IT room. Those computers should already have VirtualBox or VMWare installed.
- Download the course VM from `https://fileshare.uibk.ac.at/f/8578f4b610df4797a76a/`

The VM provides all the basic tools we will need for the course. If we will use additional Python packages we'll install it on the fly.

Additional (optional) material

Books:

- Understanding Cryptography

Training CTF Platform:

- `http://ifi-ctf.uibk.ac.at/`
- Use the university VPN: `https://www.uibk.ac.at/zid/anleitungen/vpn/vpn.html.de` and `https://vpntoken.uibk.ac.at/vpntoken/`

A note on the CTF platform

- It is a game
- You are not obliged to use it
- It is for training purposes
- **If you want to use it**, put a tick on the paper next to your name.

Enjoy and play!