Project Description

Substitutions (S-box) play very important role in ensuring high-level security for modern ciphers. They are used in symmetric cryptography for providing confusion. Up to date an important question of generation of substitutions with optimal characteristics to prevent all known types of attacks remains open. However, very often, inverse problem occurs: it is necessary to check which level of security provides a substitution. Unfortunately there is still no universal tool for solving this problem.

After completing the project, the issue will be fully or partially solved. Mostly students will have own programming part and special tasks. Nevertheless it will be also a few theoretical seminars.

Prerequisites

Main: work in Linux/BSD-based OS, experience in one of the programming languages (python, C or java) and basic knowledge of linear algebra.

Additional requirements (not obligatory): knowledge of any version control system (subversion, git or mercurial). INF234 and INF240 would be an advantage.

Working Language

English

Course Completion

After completing the course, students should be able to

1. explain cryptographic characteristics of substitutions;
2. write code in python/sage;
3. work with git and/or mercurial;
4. work as a team.