## Project Description

There are many symmetric cryptoalgorithms nowadays. The best of them are defined in standards such as FIPS 197, ISO/IEC18033-3, GOST 28147, KS X 1213, etc. The most famous of them is Advanced Encryption Standard (AES), which is used in many cryptosystems. The block and key length were chosen in a way to satisfy modern conditions and do not allow to use computers to analyze the full version of the cipher.

One of the ways to involve available resources is scaling ciphers to manageable sizes (e.g. 16 or 32 bits). This method opens several directions for research, which are proposed to students in the project. These include

- creation of scale-down models of existing block and stream ciphers;
- creation universal cryptographic transformation for scale models;
- cryptanalysis of scale cryptoprimitives.

## Prerequisites

Programming, compile and run code in Linux/BSD-based operation systems and experience in C/C++. Passed INF240 and INF243 will be an advantage.

## Working Language

English

## Course Completion

After completing the project students will be able to explain the main principles lying in modern symmetric ciphers, work with existing open source libraries, write programs oriented on high performance, write scientific reports.