Comenius University in Bratislava
Faculty of Mathematics, Physics and Informatics

THESIS ASSIGNMENT

Name and Surname: Bc. Ladislav Pápay
Study programme: Computer Science (Single degree study, master II. deg., full time form)
Field of Study: Computer Science, Informatics
Type of Thesis: Diploma Thesis
Language of Thesis: English
Secondary language: Slovak

Title: Use of SAT Solvers in Cryptanalysis

Aim: Automatic translation of cryptographic constructions and problems into a format suitable for solving by SAT solvers. Implementation of a tool for automatic translation, and optimization of generated formulas.

Supervisor: doc. RNDr. Martin Stanek, PhD.
Department: FMFI.KI - Department of Computer Science
Head of department: doc. RNDr. Daniel Olejár, PhD.

Assigned: 04.12.2014

Approved: 12.12.2014   prof. RNDr. Branislav Rovan, PhD.
                                                           Guarantor of Study Programme

....
               Student   Supervisor