Název práce: Použití ACO algoritmu na řešení jednoduché substituční šifry
Autor: Luboš Turek
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: doc. RNDr. Jiří Tůma, DrSc.
e-mail vedoucího: jiri.tuma@mff.cuni.cz

Abstrakt: V předložené práci studujeme kombinatorickou metaheuristiku Ant Colony Optimization a zkoumáme možné způsoby jejího použití k prolomení jednoduché substituční šifry. Součástí práce je návrh a implementace programu. Tento program je srovnán s genetickým algoritmem.

Klíčová slova: jednoduchá substituční šifra, ant colony optimization, ACO, kryptologie, kryptografie

Title: Application of ACO to simple subsitution ciphers
Author: Luboš Turek
Department: Department of Algebra
Supervisor: doc. RNDr. Jiří Tůma, DrSc.
Supervisor's e-mail address: jiri.tuma@mff.cuni.cz

Abstract: In the present work we study combinatorial metaheuristic Ant Colony Optimization and we search for its application to the problem of cracking simple subtitution cipher. Functional implementation is a part of the thesis. The program is compared to genetic algorithm.
Keywords: simple substitution cipher, ant colony optimization, ACO, cryptology, cryptography