Abstrakt

The aim of the thesis was to investigate the usage of PSO algorithm in the area of cryptanalysis. We applied PSO to the problem of simple substitution and to DES attack. By a modified version of PSO algorithm we achieved better or comparable results as by the usage of other biologically motivated algorithms. We suggested a method how to use PSO to attack DES and we were able to break it with the knowledge of only 20 plain texts and corresponding cipher texts. We have analyzed the reasons of failure to break more than a 4 rounds of DES and provided explanation for it. At the end we described the basic principles of differential cryptanalysis for DES and presented a specific modification of PSO for searching optimal differential characteristics for DES. For simple ciphers, PSO is working efficiently but for sophisticated ciphers like DES, without incorporating deep internal knowledge about the process into the algorithm, we could not expect significant outcomes.