The doctoral dissertation of Kamil Dworak MSc. „*Memetic algorithms in differential cryptanalysis of symmetric block ciphers*", written under the supervisor of prof. dr hab. Urszula Boryczka, discusses the adjustment of a proprietary memetic algorithm to improve the process of differential cryptanalysis. The main goal of the proposed attack is to find a valid decryption key, required to decrypt the ciphertext generated using a chosen symmetric block cipher in a much shorter time than the classic method of differential cryptanlysis. The main goal of the work was broken down into the following goals:

- Presenting the state of knowledge about currently existing methods of cryptanalysis basing on the *DES* and *FEAL* ciphers.
- Transforming the issues related to the cryptanalysis into the classic problem of function optimization, with particular emphasis on the development of the fitness function.
- Preparation of the basic version of the memetic algorithm, basing on the *DES* and *FEAL* ciphers along with the modifications of the algorithm related to the improvement of the local search process.
- Design and implementation of software allowing for automatic evolutionary differential cryptanalysis.
- Examination of the proposed attack in terms of parameter values, selection of the most favorable modification and determination of their impact on the results obtained by the algorithm.

The following thesis of the dissertation was formulated:

The usage of the memetic algorithms in the differential cryptanalysis processes, for selected symmetric block ciphers, improves the efficiency and effectiveness of the attack.

It was confirmed by means of numerous studies presented in the research chapters. The dissertation consists of 8 chapters and two appendices. After presenting the main subject and setting the objectives of the dissertation, the second chapter presents the most important theoretical aspects of cryptography and cryptanalysis. The main principles of designing symmetric block ciphers and a division of encryption algorithms are presented. At the end of the chapter, the author focused on the topic of the two most frequently used attacks: differential and linear cryptanalysis.

The third chapter describes the basic evolutionary algorithm and other metaheuristic techniques. The chapter presents the idea of the algorithm and its specific mechanisms. In particular, the main focus was set to the basic genetic operators such as crossover and mutation. Also, the author included a detailed description of the most popular selection techniques.

The fourth chapter provides a detailed description of the basic memetic algorithm and the characteristics of the most commonly used local search techniques. Among them, you can find a description of the hill climbing, simulated annealing and Tabu search algorithms.

The fifth chapter includes a detailed description of two separate variants of the proprietary memetic attack - dedicated to each of the chosen encryption algorithms. The issues discussed in this part of the dissertation will concern evolutionary differential cryptanalysis. This chapter also describes two additional evolutionary attacks proposed in literature.

In the sixth chapter the author presents a detailed description of the runtime environment for all tested algorithms and the presentation of all selected parameters for each of the tested attacks.

Chapter seventh contains an analysis of the effectiveness of the developed attacks, in terms of the number of checked subkeys and the time of decryption of the ciphertext. At the end, conclusions from the conducted experiments are presented.

The dissertation ends with a short summary of the individual stages of research and the objectives of the work presented in the introduction. This chapter also proposes further directions of research development.

Appendix A was attached to the dissertation. It describes the detailed results for the Ω characteristics of the *DES* cipher and rest fitness function results, not included in the dissertation. In addition, Appendix B was also attached - it contains a list of all pairs of plaintexts and ciphertext used in the differential cryptanalysis for the Ω_1 characteristic.

At the end of the dissertation, there is a list of symbols and a dictionary of terms.