Rozprawa doktorska mgr. Kamila Dworaka pt. „*Algorytmy memetyczne w kryptoanalizie różnicowej symetrycznych szyfrów blokowych*", napisana pod opieką prof. dr hab. Urszuli Boryczki, zawiera opracowanie autorskiego algorytmu memetycznego usprawniającego proces kryptoanalizy różnicowej. Zadaniem zaproponowanego ataku jest odgadnięcie klucza deszyfrującego, niezbędnego do odszyfrowania kryptogramu wygenerowanego za pomocą wybranego symetrycznego szyfru blokowego, w czasie znacznie krótszym, niż robi to obecnie metoda kryptoanlizy różnicowej. Kolejnymi etapami realizacji celu nadrzędnego są:

- Przedstawienie stanu wiedzy dotyczącej aktualnie istniejących metod kryptoanalizy na przykładzie szyfrów: *FEAL* oraz *DES*,
- Przekształcenie zagadnień związanych z kryptoanalizą symetrycznych szyfrów blokowych w klasyczny problem optymalizacji funkcji, ze szczególnym uwzględnieniem opracowania funkcji przystosowania osobnika.
- Przygotowanie podstawowej wersji algorytmu memetycznego, na przykładzie szyfrów: *FEAL* oraz *DES* wraz z opracowaniem modyfikacji algorytmu memetycznego związanych głównie z usprawnieniem procesu przeszukiwania lokalnego,
- Zaprojektowanie i zaimplementowanie oprogramowania pozwalającego na automatyczną ewolucyjną kryptoanalizę różnicową,
- Przebadanie zaproponowanego algorytmu pod kątem wartości parametrów, wyboru najkorzystniejszej modyfikacji oraz określenie ich wpływu na wyniki uzyskane przez algorytm.

W pracy postawiono następującą tezę:

Zastosowanie algorytmów memetycznych, w procesach kryptoanalizy różnicowej, dla wybranych symetrycznych szyfrów blokowych, poprawia efektywność samego ataku, a tym samym jego skuteczność.

Teza została potwierdzona badaniami przedstawionymi w poszczególnych rozdziałach rozprawy. Rozprawa składa się z 8 rozdziałów oraz dwóch dodatków. Po przedstawieniu tematyki oraz postawieniu celów rozprawy, w rozdziale 2, opisano najważniejsze aspekty teoretyczne, takie jak podstawowe zagadnienia związane z tematem kryptografii oraz kryptoanalizy. Przedstawiono również główne zasady projektowania symetrycznych szyfrów blokowych oraz uogólniony podział algorytmów szyfrujących wraz z szczegółowym opisem szyfrów *FEAL* oraz *DES*. Na samym końcu rozdziału „pochylono" się nad tematem dwóch najczęściej wykorzystywanych ataków w tego typu algorytmach szyfrujących, mianowicie nad kryptoanalizą różnicową i liniową.

Rozdział 3 zawiera opis podstawowego algorytmu ewolucyjnego oraz innych technik ewolucyjnych. W rozdziale przestawiono ideę samego algorytmu, a także jego po szczególne mechanizmy. W szczególności skupiono się na podstawowych operatorach genetycznych, takich jak krzyżowanie czy mutacja, z uwzględnieniem najczęściej wykorzystywanych wariantów owych operatorów. Zawarto również szczegółowy opis najpopularniejszych technik selekcji.

W rozdziale 4 skupiono się na idei algorytmów memetycznych. Ta część zawiera dokładny opis podstawowego algorytmu memetycznego oraz charakterystykę najczęściej wykorzystywanych algorytmów przeszukiwania lokalnego. Wśród nich znaleźć można opis algorytmu wspinaczki, symulowanego wyżarzania oraz przeszukiwania z listą Tabu.

Rozdział 5 to szczegółowy opis dwóch oddzielnych wariantów autorskiego ataku memetycznego, dedykowanego każdemu z rozpatrywanych algorytmów szyfrujących. Zagadnienia poruszane w tej

części rozprawy dotyczyć będą ewolucyjnej kryptoanalizy różnicowej. W rozdziale opisane zostaną również dwa dodatkowe ataki ewolucyjne.

Rozdział 6 został poświęcony opisowi przygotowanych wcześniej zbiorów testowych dla każdego z ataków przedstawionych w rozdziale piątym. Następnie skupiono się na szczegółowym opisaniu środowiska uruchomieniowego dla wszystkich przetestowanych algorytmów oraz przedstawieniu wszystkich dobranych parametrów dla każdego z przebadanych ataków.

Rozdział 7 zawiera dokładną analizę skuteczności opracowanych ataków, zarówno pod kątem liczby sprawdzonych podkluczy, jak i pod kątem czasu odszyfrowania kryptogramu. Na zakończenie przedstawione zostały wnioski, wynikające z przeprowadzonych eksperymentów.

Rozprawa zakończona jest krótkim podsumowaniem dotyczącym poszczególnych etapów badań oraz przedstawionych we wstępie zrealizowanych celach pracy. W ramach tego rozdziału zaproponowano również dalsze kierunki rozwoju badań.

Do pracy dołączono dodatek A, opisujący szczegółowe wyniki dla charakterystyk Ω szyfru *DES* oraz pozostałe wartości funkcji przystosowania, nie zamieszczone w pracy, dla algorytmu *DPSO* i szyfru *DES*.

Ponadto do rozprawy dołączono również dodatek B, zawierający spis wszystkich wykorzystanych w procesie kryptoanalizy różnicowej par tekstów jawnych oraz odpowiadających nim szyfrogramów dla charakterystyki Ω_1, pozwalających na zreprodukowanie zaproponowanych ataków.

Na samym końcu rozprawy znajduje się dodatkowo spis symboli i skrótów oraz słownik pojęć.