*Mateusz Buczek*
*Wojskowa Akademia Techniczna*
*Instytut Matematyki i Kryptologii*

# Analiza bezpieczeństwa szyfrów w oparciu o twierdzenia Luby–Rackoffa

Celem referatu jest zaprezentowanie wyników uzyskanych w pracy magisterskiej *Analiza bezpieczeństwa szyfrów w oparciu o twierdzenie Luby–Rackoffa*.

W pracy został zaproponowany pakiet testów umożliwiający określenie przydatności pseudolosowego generatora funkcji do zastosowania w strukturze Feistela o ograniczonej ilości rund. Przebadane zostały najbardziej znane algorytmy oparte o tę strukturę od standardu DES po kandydata na AES — szyfr Deal.

Praca jako pierwsza wykazuje empirycznie poprawność twierdzenia, a zaproponowany pakiet stanowi ciekawe narzędzie pracy zarówno dla kryptoanalityka, umożliwiając znajdowanie słabych punktów algorytmów, jak i dla tworzącego szyfry. Pozwala on bowiem, na mocy twierdzenia, na budowanie szyfrów o dowolnie długim bloku danych szyfrowanych w jednym przebiegu, których bezpieczeństwo łatwo jest dowieść. Opiera się ono bowiem na bezpieczeństwie tylko małego ich fragmentu oraz zachowaniu odpowiedniej struktury.

Szyfry takie mogą następnie zostać użyte w szeregu zastosowań od prostego szyfrowania po tworzenie skrótów w strukturze Daviesa–Meyera.