Tym Butler
Department of Computer Science
Hood College
Frederick, MD 21701-8575

Advisors: Salem, A., Dimitoglou, G.

Prepared Information for the Conference Poster

Statement of Topic: Approximating a One-Time Pad Using a Genetic Algorithm

Significance and Relevance of the Topic: Security is of great concern in modern times and message cryptography is a large part of security. One-time pads are proven mathematically unbreakable, but some approximation algorithms may be able lower the solution set to be able to approximate solutions. The proposed approach uses a genetic algorithm to approximate simple one-time pads.

Abstract: The one-time pad is a method of cryptography that is unbreakable at short cipher-text lengths. Most current models use statistical and complex methods to approximate solutions to one-time pads. Using a genetic algorithm as a non-deterministic model, it is possible to generate a set of keys to best fit a segment of the encrypted text. In this study, a genetic algorithm is used to generate a set of possible solutions attempting to decrypt a word encrypted with a one-time padalgorithm. Based on program outputs and tests, genetic algorithm processing and a dictionary for feedback, a word encrypted with a one-time pad can be decrypted correctly at least some of the time.