БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Программный комплекс для распознавания криптографических генераторов на основе сравнения вероятностных распределений»

Закревский Евгений Александрович

Научный руководитель – кандидат физ.-мат. наук, старший преподаватель
В.Ю. Палуха

Минск, 2020

РЕФЕРАТ

Дипломная работа: 42 с., 17 рис., 16 табл., 35 формул, 14 источников, 1 приложение.

Ключевые слова: КРИПТОГРАФИЧЕСКИЙ ГЕНЕРАТОР, ИНФОРМАЦИОННАЯ ЭНТРОПИЯ, АЛГОРИТМ, ФУНКЦИОНАЛ, КЛАСТЕРНЫЙ АНАЛИЗ, C#, PYTHON.

Объект исследования – использующиеся криптографические генераторы случайных и псевдослучайных чисел.

Предмет исследования – вероятностные свойства выходных последовательностей криптографических генераторов различных типов, их уникальные признаки.

Цель работы – реализовать и исследовать алгоритм распознавания криптографических генераторов на основе сравнения вероятностных распределений. Оценить эффективность данного алгоритма.

Задачи:

1. Изучить предложенный алгоритм распознавания с точки зрения теории вероятностей;
2. Реализовать данный алгоритм, по возможности минимизируя время его работы;
3. Разработать графический интерфейс для программы, реализующей исследуемый алгоритм распознавания;
4. Систематизировать и проанализировать результаты, полученные на тестовых данных. Сделать вывод об эффективности алгоритма.

Методы исследования – а) теоретические: изучение научных статей по направлению исследования, обобщение найденной информации б) практические: реализация исследуемого алгоритма и анализ полученных результатов.

Полученные результаты:

1. Изучен предложенный алгоритм распознавания с точки зрения теории вероятностей. Для исследований брались оценки функционалов информационной энтропии трёх видов: Шеннона, Реньи и Тсаллиса;

2. Среди всех возможных способов, был выбран и реализован наиболее эффективный, с точки зрения затрат времени, метод;
3. Для вышеупомянутой программы был разработан графический интерфейс на языке программирования C#;
4. Получены результаты, позволяющие говорить об эффективности исследуемого метода распознавания.

Область применения – организации, занимающиеся сертификацией криптосистем, неотъемлемой частью которых являются генераторы случайных и псевдослучайных последовательностей.

ABSTRACT

Diploma thesis: 42 pages, 17 figures, 16 tables, 35 formulas, 14 sources, 1 attachment.

Keywords: CRYPTOGRAPHIC GENERATOR, INFORMATION ENTROPY, ALGORITHM, FUNCTIONAL, CLUSTER ANALYSIS, C#, PYTHON.

Object of research – cryptographic generators of random and pseudorandom numbers.

Subject of the research – probabilistic properties of output sequences of cryptographic generators of various types, their unique features.

Work purpose – to implement and investigate an algorithm for recognizing cryptographic generators based on comparing probability distributions. Evaluate the effectiveness of this algorithm.

Tasks:

1. Study the proposed recognition algorithm from the point of view of probability theory;
2. Implement this algorithm, minimizing its operation time as much as possible;
3. Develop a graphical interface for the program that implements the recognition algorithm under study;
4. Systematize and analyze obtained results from the test data. Make a conclusion about the effectiveness of the algorithm.

Research methods – a) theoretical: study of scientific articles in the direction of research, generalization of the found information b) practical: implementation of the algorithm under study and analysis of the obtained results.

Results:

1. The proposed recognition algorithm was studied from the point of view of probability theory. The study used estimates of information entropy functionals of three types: Shannon, Renyi and Tsallis;
2. Among all possible methods, the most time-efficient method was selected and implemented;

3. For the above-mentioned program was developed a graphical interface in the programming language C#;
4. The obtained results allow to speak about efficiency of the investigated method of recognition.

Application area – organizations that certify cryptosystems that have a random and pseudorandom sequence generator as an integral part of them.