

Всероссийская молодежная
научная конференция
студентов, аспирантов и
молодых ученых
«Все грани математики и
механики»

(23–27 апреля 2019 г.)

Сборник тезисов докладов

(Тезисы представлены в авторской редакции)

Применение нейронных сетей для криптоанализа шифра Плейфера

Куттубек кызы Г. Старченко А. В.

Томский государственный университет, Томск

e-mail: wendiya97@gmail.com

Нейронные сети являются математической моделью способной имитировать процесс работы головного мозга, а их обучение — это многопараметрическая задача нелинейной оптимизации. Симбиоз криптографии и машинного обучения создает множество интересных задач одной из которых является оценка коэффициента пригодности текста. Нейронные сети не подходят для задачи подбора ключей при дешифровании текста, но вполне способны решить проблему с оценкой пригодности дешифрованного текста [1].

В данной работе описан принцип работы многослойного персептрона [2] для оценки пригодности варианта дешифрованного текста. Процесс обучения нейронной сети будет основываться на методе градиентного спуска. Процесс выбора наилучшей оценки пригодности дешифрованного текста производится с помощью алгоритма «имитации отжига», который представляет собой общий метод решения задачи глобальной оптимизации. Алгоритм основывается на имитации физического процесса, который происходит при кристаллизации вещества, в том числе при отжиге металлов. В качестве примера был проведен криптоанализ Шифра Плейфера с помощью разработанной компьютерной реализации программы дешифрования на языке программирования PascalABC.

Список литературы

- [1]. Neural Cryptanalysis of Classical Ciphers[Электронные ресурсы]:Proceedings of the 19th Italian Conference on Theoretical Computer Science/Urbino –Электрон.журн.–2018.–URL:<http://ceur-ws.org/Vol-2243/paper10.pdf>
- [2]. Применение искусственных нейронных сетей и системы остаточных классов в криптографии [Электронный ресурс] // Физматлит: [библиогр. указ.] / сост.:Червяков Н.И., Галушкин А.И., Евдокимов А.А., Лавриненко И.Н., Москва, [: 2012–]. URL: https://www.rfbr.ru/rffi/ru/books/o_1782393#1(дата обращения: 22.03.2019).