Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2019 г.

Исследование на криптостойкость систем шифрования с открытым ключом методами машинного обучения

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.03.01.2019.598.ПЗ ВКР

Руководитель проекта,
д.ф.-м.н., профессор
_____ Н.Д. Зюляркина
_____ 2019 г.

Автор проекта,
студент группы КЭ-454
_____ Д.Д. Савин
_____ 2019 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Савин Д.Д. Исследование на криптостойкость систем шифрования с открытым ключом методами машинного обучения – Челябинск: ЮУрГУ, КЭ-454, 50 с., 12 ил., 8 табл., библиогр. список – 45 наим., 2 прил.

Выпускная квалификационная работа выполнена с целью исследования на криптостойкость систем шифрования с открытым ключом методами машинного обучения.

В выпускной квалификационной работе описаны классическая и модифицированная системы Эль-Гамаля, разработаны программа шифрования текста по данным криптосистемам и база данных шифров. Произведено моделирование и обучение искусственной нейронной сети и сделан вывод о влиянии различных модификаций на криптостойкость криптосистем.

Также было разработано методическое пособие, которое может использоваться на практических занятиях по криптографии.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

За последние несколько лет наблюдается повышение интереса к нейронным сетям, которые успешно применяются в самых различных областях – бизнесе, медицине, технике, геологии, физике. Нейронные сети вошли в практику везде, где нужно решать задачи прогнозирования, классификации или управления. Такой впечатляющий успех определяется несколькими причинами:

1). Богатые возможности. Нейронные сети – исключительно мощный метод моделирования, позволяющий воспроизводить чрезвычайно сложные зависимости.

2). Простота в использовании. Нейронные сети обучаются на примерах. Пользователь нейронной сети подбирает представительные данные, а затем запускает алгоритм обучения, который автоматически воспринимает структуру данных. При этом от пользователя, конечно, требуется какой-то набор эвристических знаний о том, как следует отбирать и подготавливать данные, выбирать нужную архитектуру сети и интерпретировать результаты, однако уровень знаний, необходимый для успешного применения нейронных сетей, гораздо скромнее, чем, например, при использовании традиционных методов статистики.

Нейронные сети привлекательны с интуитивной точки зрения, так как они основаны на примитивной биологической модели нервных систем. В будущем развитие таких нейробиологических моделей может привести к созданию действительно «мыслящих» компьютеров.

Области применения нейронных сетей весьма разнообразны – это распознавание текста и речи, семантический поиск, экспертные системы и системы поддержки принятия решений, предсказание курсов акций, системы безопасности, анализ текстов. Также нейросети очень широко применяются в криптографии, есть даже целый раздел, который называется нейрокриптография, изучающий применение стохастических алгоритмов, в частности, нейронных сетей, для шифрования и криптоанализа.

Для современных информационных систем характерны две тенденции. С одной стороны постоянно возрастают объем и ценность информации, с другой- среда для передачи данных становится все более открытой. Это вызывает все больший интерес к разработке новых криптосистем, которые призваны обеспечить большую безопасность. В частности, даже несколько выпускников нашей кафедры посвятили этому свои работы.

При разработке необходимо оценить криптостойкость такой системы, чтобы она была лучше, чем предыдущая. На данный момент для этого можно использовать только теоретические выкладки, моя же задача оценить это на практике с применением нейронных сетей.

Для разработки новых криптосистем используются различные модификации уже известных шифров, в частности для этого очень активно используются группы, например в монографии В.А. Романькова «Алгебраическая криптография» описано применение групп при построении алгебраических систем и протоколов. В своей работе я буду использовать модифицированную с помощью групп схему Эль-Гамаля.