ПЕРЕДАЧА И ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 004.056.55

АЛГОРИТМ ШИФРОВАНИЯ ДАННЫХ НА ОСНОВЕ ТЕОРИИ ГРАФОВ

Ф.А. Дмитриев, К.Ф. Родичев
«Самарский национальный исследовательский университет имени академика С.П. Королева», г. Самара

Ключевые слова: шифрование, теория графов, алгоритм шифрования на графах, шифрование данных.

В современном мире, с ростом вычислительных мощностей, теория графов получила очень широкое распространение и в большинстве случаев ее аппарат используется для решения сложных оптимизационных задач. Однако, наряду с областями науки, в которых уже сегодня активно используются элементы теории графов, существуют области - такие как криптография - в которых она еще не нашла широкого применения.

Современные стандарты как блочного, так и поточного шифрования не используют теорию графов. При этом существует ряд работ, посвященных ее применению в криптографии (Wael Etaiwi: “Encryption Algorithm Using Graph Theory”, Yamuna M: “Encryption using graph theory and linear algebra”), однако все они лишь предлагают механизмы без реализации и анализа.

Исходя из этого, можно заключить, что актуальность данного исследования заключается не только в новизне предлагаемого алгоритма, но и в его качественном отличии, выраженном в применении теории графов. Практическая же направленность состоит в реализации разработанного алгоритма и его дальнейшем исследовании и анализе.

Целью работы стала разработка и исследование алгоритма шифрования данных с использованием теории графов.

В качестве базы для алгоритма была взята идея о представлении числа с помощью графа из олимпиадной задачи по шифрованию. Так как в ее основе лежит представление шифруемого натурального числа в виде суммы натуральных слагаемых, можно говорить о достаточно большом «криптографическом потенциале», так как представление числа в виде суммы может быть очень вариативным. Но даже при наличии такого

потенциала, данная идея не отвечает современным требованиям, предъявляемым к шифрам.

За основу алгоритма было взято блочное симметрическое шифрование типа SP-сеть. Размеры ключа и блока шифрования были взяты по аналогии с шифрами, использующимися в качестве стандартов в России, США и Европе (ГОСТ 28147-89, AES, IDEA и т.д.) Отталкиваясь от этих данных, можно разрешить вопросы, возникающие при знакомстве с идеей представления числа в виде графа. Ответы на них даны в работе с учетом соображений о криптостойкости и устойчивости к потерям данных при передаче сообщения.

В результате был разработан новый алгоритм шифрования данных с помощью теории графов. На основании его анализа, можно сделать следующие выводы:

Алгоритм соответствует требованиям наличия лавинного эффекта и нелинейности преобразований, что говорит о его общей надежности.

В алгоритме не соблюдаются такие требования абсолютной устойчивости как уникальность генерируемого ключа, его статистическая надежность, а так же избыточность информации в открытом тексте. При этом, как можно заключить из анализа этих требований, выявленные несоответствия нельзя назвать критическими.

Сложность взлома с помощью прямого перебора с учетом закона Мура и других факторов роста производительности компьютеров оценивается 39 годами.

Из всего вышесказанного можно заключить, что разработанный шифр относится к достаточно стойким системам шифрования. Но таковым он будет до тех пор, пока не будет найдена эффективная с экономической и временной точки зрения атака. Реализация такой атаки может стать следующим шагом в исследовательской работе по этой теме.

Список использованных источников

1.Зыков А.А. Основы теории графов / А.А. Зыков. – М.: Вузовская книга, 2004. – 664 с.

2.Е.В. Гошин Теория информации и кодирования. -Самара: изд-во Самар. ун-та, 2018. – 123 с.

3.Narsingh Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice Hall, 2010.- 496 p.

4.Межрегиональная олимпиада по математике и криптографии. [Электронный ресурс]: Олимпиадная задача 2010/2011.URL:http://v-olymp.ru/cryptolymp/archive_task/469/3463/ (дата обращения: 05.12.2019).

Дмитриев Федор Александрович, студент кафедры геоинформатики и информационной безопасности, E-mail: fedor0299@rambler.ru.

Родичев Кирилл Федорович, студент кафедры геоинформатики и информационной безопасности, E-mail: kirill.rodichev38@gmail.com. Научный руководитель: доцент Н.Л. Додонова.

УДК 004.087.4; 004.67

БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ В ИМПЛАНТИРУЕМЫХ RFID-МЕТКАХ

С.В. Жуков, Т.М. Казанцева
«Самарский национальный исследовательский университет имени академика С.П. Королева», г. Самара

Ключевые слова: имплантируемые RFID-метки, методы шифрования, защита данных, обработка численных данных.

В современном мире с переизбытком информации одной из самых актуальных проблем является безопасность данных и их эффективная защита [1]. Для реализации было предложено использование технологичных, удобных для ношения, биосовместимых имплантируемых RFID-чипов. Однако на данном этапе все еще остается нерешенным вопрос о безопасности данных в таких системах.

На данный момент передача данных в имплантируемых метках происходит по радиочастотному каналу в соответствии с протоколом ISO/IEC 14443 — стандарт, описывающим частотный диапазон, метод модуляции и протокол обмена бесконтактных пассивных карт (RFID) ближнего радиуса действия (до 0.1 м) на магнитосвязанных индуктивностях. По частоте метки обычно разделяются на три категории: LF, HF, UHF. Первая (LF, Low frequency) работает на частоте 100—150 кГц, и наиболее часто используется для подкожных имплантируемых меток. Рабочую частоту обычно выбирают среднюю — 125 кГц или 134 кГц. [2]

Примером такой передачи служит EM410x — это обобщенное название семейства совместимых чипов: EM4100, EM4200, TK4100, EM4102, TK28, КБ5004ХК2. Принцип работы таких меток заключается в следующем: считыватель генерирует переменное магнитное поле частотой 125 кГц, попадая в него, карта получает энергию и начинает циклически модулировать магнитное поле считывателя сигналом. Идентификационный код содержит 64 бита, в том числе 40 бит собственно уникального номера, специальная синхронизирующая последовательность и контрольные биты четности.

Данная проблема может иметь три варианта решения:

1. Использование проверенных стандартных алгоритмов.
2. Модификация известных алгоритмов с целью повышения производительности и снижения логической сложности.