АННОТАЦИЯ

диссертационной работы Алғазы Күнболат Тілеуханұлы на тему «Разработка и исследование алгоритмов шифрования на базе различных подходов», представленной на соискание степени доктора философии (PhD) по специальности «6D100200 - Системы информационной безопасности»

Актуальность темы исследования обусловлена современным развитием информационно-коммуникационных технологий и необходимостью совершенствования моделей защиты электронной информации в целях обеспечения информационной безопасности. Процессы обработки, хранения, передачи и использования информации стали приоритетными в современном обществе и во многом зависят от уровня развития и использования средств связи и способов передачи информации. При нынешней ситуации необходимость защиты информации нужна не только государственному сектору, но и простому пользователю и негосударственным организациям. Одним из актуальных вопросов обеспечения безопасности информации является обеспечение необходимого уровня ее защиты путем создания современных средств защиты информации.

Информационные и коммуникационные технологии играют важную роль для суверенного государства. В Казахстане в 2017 году была принята Концепция кибербезопасности («Киберщит Казахстана»). Целью концепции является достижение и поддержание уровня защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз для обеспечения устойчивого развития Республики Казахстан в условиях глобальной конкуренции. В связи с этим создание отечественных систем защиты информации, отвечающих современным требованиям информационной безопасности является актуальным.

В Лаборатории информационной безопасности Института информационных и вычислительных технологий КН МОН РК проводятся научно-исследовательские работы по созданию отечественных средств криптографической защиты информации, а именно по разработке симметричных блочных систем шифрования электронных данных, в том числе и на базе непозиционных полиномиальных систем счисления.

В настоящие время алгоритмы блочного шифрования являются основным средством криптографической защиты информации, хранящейся в компьютерах или передаваемой через общедоступные инфокоммуникационные сети. Востребованность в алгоритмах шифрования этого типа обусловлена преимуществами его практического применения. Благодаря эффективной реализации на основе современных аппаратных и программных устройств гарантируются высокая скорость шифрования и высокий уровень стойкости. Симметричные блочные шифры используются не только как отдельные криптографические алгоритмы, но и как важные

криптографические механизмы, которые являются частью других криптографических алгоритмов и протоколов. Они часто используются на практике в качестве ключевого компонента генераторов псевдослучайных последовательностей и алгоритмов криптографического хеширования.

Еще одно преимущество блочных шифров – это использование коротких ключей. Можно зашифровать несколько больших файлов или других данных одним коротким ключом, длина которого, в основном, находится в пределах от 128 до 256 бит. Это главное преимущество перед поточными шифрами, для которых не рекомендуется использовать ключ более одного раза. Хранение длинных ключей и обмен ими между пользователями требует дополнительной защиты. Учитывая вышеизложенное, наиболее эффективными и подходящими для использования шифрами являются блочные шифры. Поэтому алгоритмы симметричного блочного шифрования в настоящее время являются основным криптографическим средством для обеспечения конфиденциальности информации.

Вместе с развитием криптографии эволюционировали криптографические атаки и методы криптоанализа. Понятия криптографии и криптоанализа стали неразрывно связаны друг с другом: это две составные части криптологии. Для того, чтобы создать систему, устойчивую ко взлому, необходимо учесть все возможные способы атак на неё. Значение криптографии и криптоанализа будет только возрастать, поэтому разработка криптографических алгоритмов является **актуальной** как в научных исследованиях, так и в практических приложениях.

В Казахстане в основном используют зарубежные криптографические средства и программное обеспечение для защиты информации, поэтому разработка казахстанских отечественных средств криптографической защиты определенно актуальна и необходима.

Цель диссертационный работы. Разработка итеративного блочного шифра и функции генерации раундовых ключей шифрования с использованием возможностей непозиционных полиномиальных систем счисления (НПСС). Исследование криптостойкости разработанных алгоритмов.

Задачи исследования:

- анализ существующих симметричных блочных алгоритмов криптографической защиты информации;
- обзор и анализ известных методик криптоанализа и криптографических атак;
- разработка алгоритмов симметричного блочного шифрования на основе подстановочно-перестановочной сети и функции разворачивание раундовых ключей шифрования с применением непозиционных полиномиальных систем счисления (НПСС);
- исследование методами криптоанализа стойкости разработанных алгоритмов шифрования;
- программная реализация разработанных итеративных блочных алгоритмов шифрования.

Объект исследования. Системы шифрования, непозиционные полиномиальные систем счисления, криптографические атаки, методы криптоанализа.

Предмет исследования. Симметричные блочные криптографические алгоритмы шифрования, в том числе на базе НПСС.

Методы исследования. В работе использованы методы теории булевых функций, линейной алгебры и теории вероятности, а также различные криптографические методы и алгоритмы, и методы криптоанализа.

Научная новизна исследования:

- построен новый симметричный алгоритм блочного шифрования с архитектурой подстановочно-перестановочной сети, отвечающий общим требованиям алгоритмов шифрования;
- построен симметричный блочный алгоритм шифрования на основе нетрадиционного метода (НПСС), использование которого позволяет повысить криптостойкость алгоритма;
- построены узлы нелинейной (S-блок) замены, которые имеют повышенные показатели стойкости к дифференциальному и линейному криптоанализу.

Теоретическая и практическая значимость работы. Проведенные научные исследования и полученные результаты имеют высокую практическую значимость и могут быть использованы для защиты конфиденциальной информации при её хранении и передаче в инфокоммуникационных системах и сетях. Кроме того, эти результаты по созданию и развитию отечественных средств защиты информации расширяют теорию создания эффективных алгоритмов шифрования информации. Разработанный итеративный блочный алгоритм шифрования программно реализованиа и получена авторское свидетельство на «Qamal v 1.0.1», № 5200 от 6 сентября 2019 года, выданное Национальным институтом интеллектуальной собственности МЮ РК.

Главный вывод защиты. Построен новый симметричный алгоритм блочного шифрования, соответсвующий общим требованиям предъявляемый к алгоритмам шифрования. Предложена также вторая версия алгоритма шифрования с применением непозиционных полиномиальных систем счисления. Проведено исследование криптографической стойкости разработанных алгоритмов шифрования методами линейного, дифференциального и алгебраического криптоанализа.

Уровень достоверности и результаты апробации. Достоверность проведенных исследований и полученных результатов диссертации показана в третьем разделе.

Результаты диссертации были доложены и обсуждены на следующих научно-практических конференциях:

1) III Международная научно-практическая конференция «Информатика и прикладная математика» (Алматы, 26-29 сентябрь 2018).
2) International Conference on Wireless Communication, Network and Multimedia Engineering, WCNME-2019 (Гуйлинь, Китай, 2019).

3) IV Международная научно-практическая конференция «Информатика и прикладная математика» (Алматы, 25-29 сентябрь 2019).

4) International Conference on Security of Information and Networks (Sochi, Russia, September, 2019).

5) Международная научно-практическая конференция «Актуальные проблемы информационной безопасности в Казахстане АПИБК-2020» (Алматы, 15 январь 2020).

6) V Международная научно-практическая конференция «Информатика и прикладная математика» (Алматы, 29 сентябрь – 1 октябрь 2020).

Связь темы диссертации с планами научно-исследовательских работ. Диссертационная работа выполнена в соответсвии с планом докторской диссертации PhD, утвержденном Институтом информационных и вычислительных технологий КН МОН РК и с планом научно-исследовательских работ проекта программно-целевого финансирования «Разработка программных и програмно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» (2018-2020, государственный регистрационный номер: BR05236757). Полученные результаты проведенных исследований по данной диссертационной работе включены в отчеты этого проекта ПЦФ за 2018-2020 годы.

Объем и структура работы. Диссертация состоит из введения, четырех разделов, заключения и списка литературы. Общий объем диссертации: 118 страниц письменного текста, в том числе 23 рисунка, 42 таблицы, список литературы из 94 источников, 4 приложения.

Публикация результатов. Количество опубликованых научных статей при проведении научно-исследовательских работ - 21. В том числе 3 статьи в журналах индексируемые в базах Scopus и Thomson Reuters («Cogent Engineering» и «International Journal of Electronics and Telecommunications»), 8 статей в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МОН РК, 10 статей опубликованы в сборниках международных научных конференций.

Во введении обосновывается актуальность диссертационной работы. Сформулированы цель работы, объект и предмет научно-исследовательской работы. Определены научная новизна и практическая значимость. Описаны результаты проведенных исследований. Приведена информация об апробации результатов исследования и публикации.

В первом разделе описана классификация и основные направления исследований в алгоритмах защиты информации. Приведены термины, используемые в криптографии и диссертационной работе. Описываются криптоалгоритмы, разделенные по степени безопасности, требования к симметричным блочным шифрам и режимы шифрования, используемые при шифровании. Рассматриваются основные виды криптоанализа, применяющиеся к современным алгоритмам шифрования.

Во втором разделе описаны новый алгоритм симметричного блочного шифрования «Qamal», разработанный на основе SP-сети и предложенная

вторая версия этого алгоритма «Qamal NPNS» из-за особенностей использования ключа. Подробно описываются все используемые преобразования в этих алгоритмах. Длина блока шифрования и ключа алгоритма может принимать три разных значения в соответствии с различными уровнями безопасности. Приведена структура созданного S-блока для разработанного алгоритма шифрования. Поскольку «Qamal NPNS» является алгоритмом, разработанным на основе НПСС, приводится информация о построении непозиционных полиномиальных систем счислении и их использование при шифровании и расшифровании. Приведен пример шифрования данных по разработанному алгоритму.

В третьем разделе представлены результаты, полученные при исследовании надежности разработанного алгоритма шифрования. Анализ начинается с проверки статистической безопасности зашифрованного текста, полученного с помощью алгоритма шифрования. Затем, проверяются свойства лавинного эффекта шифра, что является одним из необходимых условий в криптографии. Криптостойкость алгоритма проверена алгебраическими, дифференциальными, линейными и другими методами криптоанализа. Приведены проверенные на конкретных примерах теоретические криптоатак. Также исследовано и установлено влияние алгоритма шифрования с использованием НПСС на криптостойкость.

В четвертом разделе приведено описание созданного программного обеспечения, реализующего разработанный симметричный блочный алгоритм шифрования, а также язык программирования, системные требования, описание работы прогаммного обеспечения и т. д. Для оценки вычислительной скорости программы рассматривается три различных способа реализации преобразования Mixer2, используемого в разработанном алгоритме шифрования. Проведено сравнение полученных результатов.

В заключении сформулированы основные полученные результаты в диссертации.