Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056.53

БОЛТАК
Светлана Владимировна

# АНАЛИЗ И РАЗРАБОТКА ПОТОКОВОГО МЕТОДА ШИФРОВАНИЯ НА БАЗЕ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

**АВТОРЕФЕРАТ**
диссертации на соискание степени магистра

по специальности 1-40 80 04 – Информатика и технологии программирования

Минск 2024

Работа выполнена на кафедре информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **ЯРМОЛИК Вячеслав Николаевич,**
доктор технических наук, профессор кафедры программного обеспечения информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ШЕШОЛКО Владимир Константинович,**
кандидат физико-математических наук, доцент кафедры управления информационными ресурсами Академии управления при Президенте РБ

Защита диссертации состоится «28» июня 2024 г. года в $9^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. Гикало, 9, корп. 4, ауд. 111, тел. 293-85-91, e-mail: inform@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

# ВВЕДЕНИЕ

С развитием цифровых технологий и интернета, количество информации, передаваемой и хранимой онлайн, значительно увеличилось. Это делает приватность данных более уязвимой и подверженной риску нарушения. Шифрование помогает защитить приватность пользователей от массового слежения и сбора данных со стороны правительственных агентств, компаний и киберпреступников.

На сегодняшний день существует множество методов шифрования, каждый из которых имеет свои характеристики. Потоковые шифры остаются одними из наиболее востребованных по следующим причинам: высокая скорость шифрования и дешифрования данных, низкие требования к ресурсам (процессорному времени и памяти), простота реализации, поддержка потоковых данных (хорошо подходят для защиты потоковых данных, таких как потоковое видео и аудио), устойчивость к атакам (хорошо разработанные потоковые шифры могут обеспечить высокий уровень безопасности и устойчивость к различным типам криптографических атак).

Области применения потоковых шифров:

1 Защищенная передача данных в сети Интернет и сетях мобильной связи.

2 Использование в беспроводных коммуникациях, таких как Wi-Fi, Bluetooth и NFC для защиты передачи данных между устройствами.

3 Защита IoT (Интернет вещей).

4 Использование в различных криптографических протоколах и алгоритмах для обеспечения безопасности данных, таких как SSL/TLS для защищенной передачи данных в Интернете и WPA/WPA2 для защиты Wi-Fi сетей.

Характерной особенностью потоковых криптосистем является использование криптографического ключа большой длины, равного длине шифруемого сообщения, для чего применяются генераторы М-последовательностей (псевдослучайных последовательностей).

М-последовательность – псевдослучайная двоичная последовательность, которая имеет максимальную длину, и сгенерирована регистром сдвига с линейной обратной связью (Linear Feedback Shift Register – LFSR). Статистические свойства М-последовательностей, которые практически не отличаются от свойств идеальных случайных последовательностей, делают эти генераторы наиболее часто используемыми, несмотря на развитие нейросетей и появление новых генераторов псевдослучайных чисел. Генераторы на базе М-последовательностей выигрывают за счет простоты реализации.

С развитием цифровых технологий и увеличением вычислительных мощностей появляются новые возможности для злоумышленников в области взлома информации, поэтому криптостойкость существующих систем шифрования становится все более важной задачей для обеспечения безопасности данных. Необходимо постоянно совершенствовать их и увеличивать уровень защиты.

Все вышеизложенное, а также популярность и востребованность потоковых шифров на базе М-последовательностей доказывает актуальность данного исследования.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования**

Современные потоковые шифры, как и любые другие криптоиситемы, обладают определенными уязвимостями, обусловленными их строением. Анализ и улучшение потоковых шифров на базе М-последовательностей является важным шагом для обеспечения надежной защиты информации и противодействия потенциальным угрозам безопасности.

Развитие нейросетей, рост вычислительных мощностей, развитие технологий Big Data и другие современные тенденции в области цифровых технологий требуют увеличения стойкости шифров к взлому, а также новых методов шифрования.

Простота, надежность и востребованность потоковых шифров на базе М-последовательностей делает актуальным анализ таких систем и разработку улучшений для увеличения характеристик надежности.

**Степень разработанности проблемы**

Исследование уязвимостей алгоритма A5/1 проводилось с использованием работ таких специалистов в области криптографии как R. Anderson, E. Biham, J. Golic, J. Keller, Е. Максимов, Т. Порнин, А. Бирюков, A. Shamir, D. Wagner и др.

Применение частотного анализа для взлома потоковых шифров, а также модификация процесса инициализации A5/1 в этих работах не рассматривались.

**Цель и задачи исследования**

*Целью* диссертационной работы является криптоанализ потокового алгоритма шифрования на базе М-последовательностей, а также разработка улучшений для алгоритма A5/1.

Для достижения поставленной цели необходимо решить следующие задачи:

1 Провести обзор существующих криптосистем на базе М-последовательностей.

2 Провести сравнительный анализ существующих методов и алгоритмов криптоанализа потоковых шифров.

3 На основе сравнительного анализа предложить собственный алгоритм взлома потоковых криптосистем.

4 Ознакомиться с документацией алгоритма A5/1 и предложить обоснованные улучшения.

5 Реализовать предложенные алгоритмы и провести экспериментальные исследования.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность использования частичного частотного анализа для взлома потоковых шифров, а также возможность улучшения A5/1 на этапе инициализации регистров.

**Область исследования**

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-40 80 04 «Информатика и технологии программирования».

**Теоретическая и методологическая основа исследования**

В основу диссертации легли работы российских и зарубежных ученых в области криптоанализа потоковых шифров, а также анализ технической документации по рассматриваемой тематике.

*Информационная база* исследования сформирована на основе литературы, открытой информации, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

**Научная новизна**

*Научно-теоретическая* и *практическая* значимость исследования определяется описанием нового подхода к анализу уязвимостей потоковых шифров на базе М-последовательностей и новому способу инициализации регистров алгоритма A5/1.

**Основные положения, выносимые на защиту**

1 Алгоритм взлома потоковых шифров на базе М-последовательностей, позволяющий найти порождающий полином для регистра сдвига с линейной обратной связью.

2 Метод инициализации генератора A5/1, позволяющий улучшить криптостойкость шифра, а также статистические свойства генерируемой М-последовательности.

**Апробация диссертации и информация об использовании ее результатов**

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на Международной научной конференции «Информационные технологии и системы» (г. Минск, Беларусь, 2023), 59-ой научной конференции аспирантов, магистрантов и студентов БГУИР (г. Минск, Беларусь, 2023), LXXXIV международной научно-практической конференции «Технические науки: проблемы и решения» (г. Москва, Россия, 2024).

Отдельные положения диссертации могут быть использованы при преподавании дисциплины «Теория информации».

**Публикации**

По теме диссертации опубликовано 4 печатных работы в сборниках материалов международных научных конференций. Из них 1 работа в сборнике трудов и материалов международной конференции ИТС-2023 БГУИР, 1 работа в сборнике материалов Международной научно-практической конференции «Технические науки: проблемы и решения» и 2 работы в сборниках трудов и материалов научных конференций БГУИР.

Общий объем публикаций по теме диссертации составляет 9 страниц.

**Структура и объем работы**

Диссертация состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

**В первой главе** приведен обзор существующих потоковых криптосистем на базе М-последовательностей, выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения.

**Во второй главе** представлен разработанный алгоритм поиска порождающего полинома.

**В третьей главе** предложена разработка потокового метода шифрования на базе алгоритма А5/1.

**В четвертой главе** представлены экспериментальные исследования. В ней приведены результаты тестирования алгоритма поиска порождающего полинома, а также результаты тестирования разработанного потокового метода шифрования.

**В приложении** представлены публикации автора.

Общий объем работы составляет 82 страницах, из которых основного текста – 59 страниц, 17 рисунков, 12 таблиц, список использованных источников из 30 наименований на 2 страницах и 2 приложений на 21 странице.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** показана важность шифрования в современном обществе, а также популярность потоковых систем шифрования на базе М-последовательностей. Описано обоснование актуальности темы исследова- ния.

В **общей характеристике работы** показана актуальность исследования, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

**В первой главе** приведен пример простейшего LFSR и описаны свойства М-последовательностей, а также сделан обзор и анализ существующих потоковых криптосистем на базе М-последовательностей.

Исследование свойств М-последовательностей показало, что такие последовательности являются полезными для шифрования, генерации ключей и других криптографических задач. Они формируются с помощью сдвиговых регистров, а также схем суммирования по модулю два. М-последовательности служат основой для формирования других ПСП. Например, последовательности Голда формируются путем сложения по модулю 2 двух М-последовательностей одинаковой длины.

Из анализа существующих криптосистем на базе М-последовательностей следует, что вне зависимости от порождающего полинома LFSR остается линейным устройством, поэтому на практике используются комбинированные ге-

нераторы ключевой последовательности на его основе. Использование комбинированных генераторов позволяет увеличить период и избавиться от свойства линейности.

Свойства М-последовательностей, а также простая аппаратная реализация LFSR, позволяют генераторам ПСП на их основе оставаться одними из наиболее востребованных.

**Во второй главе** представлен разработанный алгоритм поиска порождающего полинома, а также описаны возможные атаки на потоковые системы.

Суть предложенного алгоритма – использование такого свойства М-последовательности, как периодичность. Предлагается применение частичного частотного анализа с использованием улучшенного метода Касиски.

*Предлагаемые улучшения*

Для более точного нахождения длины ключа необходимо исключить те расстояния между повторяющимися *l*-граммами, которые могут привести к неверному результату, так как если хотя бы одно из расстояний случайно, оно изменит результат вычисления длины ключа для всех остальных расстояний.

Шаги алгоритма анализа расстояний для нахождения длины ключевой последовательности (М-последовательности) с внесенными ограничениями:

1 Взять первое расстояние.

2 Взять следующее расстояние.

3 Найти НОД двух расстояний.

4 Если НОД равен 1, записать в результирующий массив -1.

5 Если НОД не равен 1 перейти к шагу 6.

6 Если полученное значение не является простым числом, а также не равно ни одному из чисел, участвующих в вычислении НОД – текущему расстоянию присвоить найденный НОД.

7 Повторять шаги 2-6 пока в массиве расстояний не останется одно число.

Описанный выше алгоритм применяется для всех найденных ранее *l*-грамм. В результате каждому массиву расстояний будет поставлено в соответствие одно число. Далее из массива удаляются все -1 и находится НОД оставшихся чисел. Это число и будет являться длиной искомого ключа.

Найденный в результате анализа период М-последовательности можно использовать для поиска порождающего полинома, выразив длину регистра из формулы периода через логарифм.

Алгоритм анализа изображен на рисунке 1.

На схеме используются следующие обозначения:

– *N* хранит текущее расстояние для анализа;

– *vector*[]– вектор расстояний;

– *Nod* хранит наибольший общий делитель двух расстояний;

– *gcd*() функция поиска НОД двух расстояний по алгоритму Евклида;

– *Primery*() функция проверки числа на простоту.

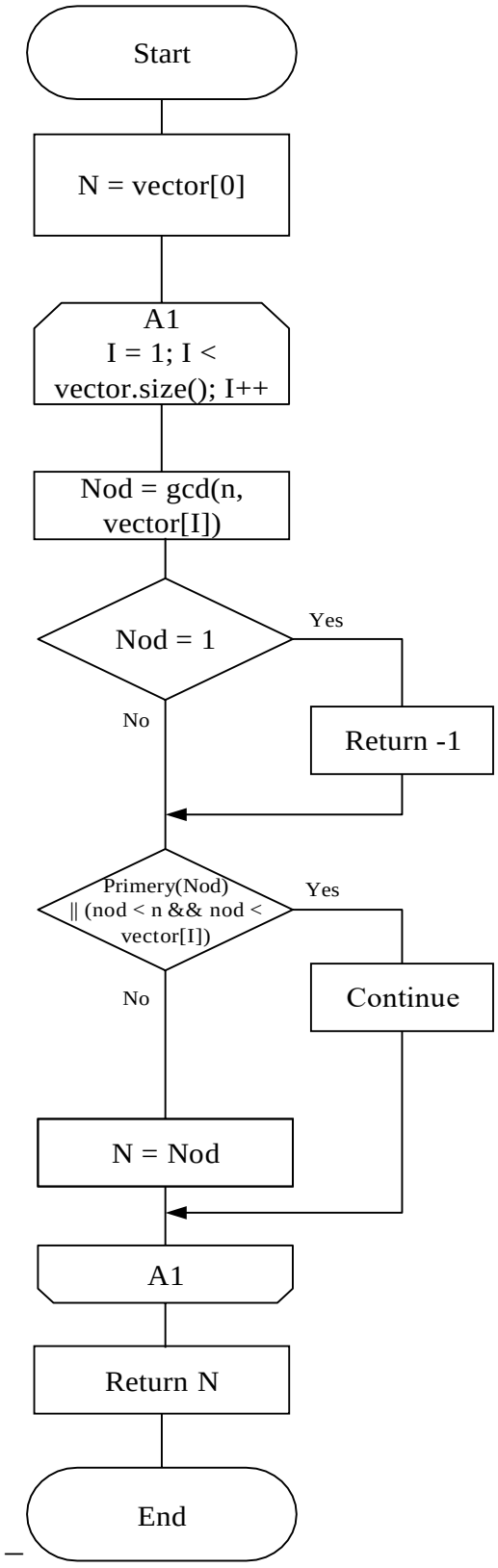



**Рисунок 1 – Алгоритм анализа расстояний для одной *l*-граммы**

В результате работы алгоритма будет найдена длина М-последовательности, по которой вычисляется степень искомого полинома.

**В третьей главе** представлена модификация потокового шифра A5/1. Предлагается внести изменения в алгоритм на этапе инициализации.

Для повышения устойчивости A5/1 к корреляционным атакам и улучшения статистических свойств генерируемой М-последовательности, предлагается увеличить сложность линейной зависимости при загрузке битов ключа и фрейма, а также увеличить количество холостых ходов.

*Шаги при инициализации регистров в алгоритме A5/1:*

1 Все регистры сбрасываются в ноль. Алгоритм переходит в состояние $S^0$.

2 Каждый регистр выполняет 64 такта, при которых на каждом шаге выполняется операция сложения по модулю 2 над очередным битом сеансового ключа $K_c$ и младшим битом каждого регистра, а результат операции записывается в самый младший бит каждого регистра. Регистры при этом сдвигаются на каждом шаге (без учета режима управления сдвигами). После выполнения данного шага ячейки всех регистров заполнены начальными значениями. Алгоритм переходит в состояние $S^{64}$.

3 Все регистры тактируются 22 раза. На каждом шаге выполняется операция сложения по модулю 2 над очередным битом номера кадра (фрейма) и младшим битом каждого регистра, а результат операции записывается в самый младший бит каждого регистра. Регистры при этом сдвигаются на каждом шаге (без учета режима управления сдвигами). Алгоритм переходит в состояние $S^{86}$.

4 Каждый регистр выполняет 100 тактов с управлением сдвигами регистров, но без генерации последовательности, что обеспечивает перемешивание ключевой битовой последовательности. Алгоритм переходит в состояние $S^{186}$.

Выдвигаемая гипотеза:

– увеличение количества холостых тактов перед генерацией М-последовательности, а также количества линейных операций, над которыми производится операция XOR (шаги 2 и 3), должно увеличить криптостойкость алгоритма, а также привести к генерации более непредсказуемой битовой последовательности.

Согласно выдвинутой гипотезе, этап инициализации алгоритма A5/1 примет следующий вид:

1 Все регистры сбрасываются в ноль. Алгоритм переходит в состояние $S^0$.

2 Каждый регистр выполняет 64 такта, при которых на каждом шаге выполняется операция сложения по модулю 2 над очередным битом сеансового ключа $K_c$ и тремя младшими битами каждого регистра, а результат операции записывается в самый младший бит каждого регистра. Регистры при этом сдвигаются на каждом шаге (без учета режима управления сдвигами). Алгоритм переходит в состояние $S^{64}$.

3 Все регистры тактируются 22 раза. На каждом шаге выполняется операция сложения по модулю 2 над очередным битом номера кадра (фрейма) $F_n$ и тремя младшими битами каждого регистра, а результат операции записывается в самый младший бит каждого регистра. Регистры при этом сдвигаются на каждом шаге (без учета режима управления сдвигами). Алгоритм переходит в состояние $S^{86}$.

4 Каждый регистр выполняет 223 такта с управлением сдвигами регистров, но без генерации последовательности. Количество холостых ходов увеличено вдвое, число является простым. Алгоритм переходит в состояние $S^{309}$.

**В четвертой главе** представлены экспериментальные исследования по подтверждению эффективности разработанного алгоритма поиска полинома, а также потокового метода шифрования.

Чтобы протестировать работу алгоритма, был реализован регистр сдвига с линейной обратной связью для любого примитивного полинома, а также сам алгоритм.

Тестирование проводилось с текстовыми, аудио и видео файлами.

Процент успешного поиска полинома для файлов разных типов показан в таблице 1.

Таблица 1 – Процент верной работы алгоритма по типам файлов

| Тип файла | Процент верной работы, % |
|---|---|
| текстовый | 92 |
| графический | 90,5 |
| аудио | 96 |

По результатам тестирования можно сделать следующие выводы:

1 Разработанный алгоритм демонстрирует высокий уровень успешности работы, превышающий 90%. Это означает, что в большинстве случаев алгоритм успешно справляется с поиском полинома.

2 На время, необходимое для взлома, содержимое файла влияет незначительно.

3 Время взлома зависит от степени искомого полинома.

4 Процент сбоя алгоритма составил от 4 до 9,5 %.

Исследования показали, что алгоритм демонстрирует стабильную работу и ограничен лишь возможностями вычислительных ресурсов.

*Тестирование качества М-последовательностей модифицированного А5/1*

Для проверки выдвинутой гипотезы была смоделирована работа А5/1 и его модификации. Моделирование работы исследуемых алгоритмов проводилось с помощью программы, разработанной на языке программирования C#.

Для более глубокого исследования влияния внесенных изменений на качество генерируемых М-последовательностей, модифицированный А5/1 прошел два этапа тестирования:

1 С использованием реализованных тестов NIST (ручное тестирование).

2 С использованием готовой библиотеки NIST SP 800-22 (автоматическое тестирование).

Оба этапа тестирования были необходимы для полной и всесторонней оценки генерируемых М-последовательностей.

*Ручное тестирование.*

Для самостоятельной реализации были выбраны наиболее популярные 8 тестов:

1 Частотный побитовый тест.

2 Частотный блочный тест.
3 Тест на последовательность одинаковых битов.
4 Тест на самую длинную последовательность единиц в блоке.
5 Тест рангов бинарных матриц.
6 Спектральный тест.
7 Универсальный статистический тест Маурера.
8 Тест на линейную сложность.

Для оценки влияния внесенных изменений в алгоритм инициализации, сгенерированные обоими алгоритмами М-последовательности проверялись тестами на статистические свойства.

Длина М-последовательности, а также размеры блоков для анализа задавались согласно рекомендациям документации NIST.

Результаты тестирования представлены на рисунках 2 – 4.


**Рисунок 2 – Результат выполнения теста №1**


**Рисунок 3 – Результат выполнения теста №2**

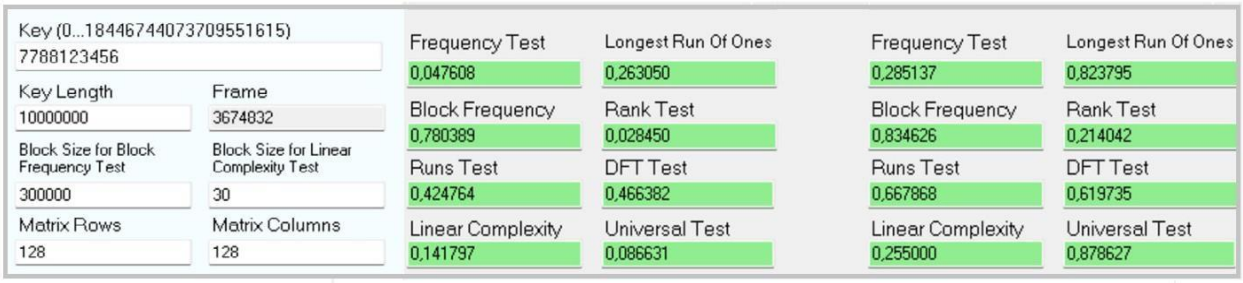



**Рисунок 4 – Результат выполнения теста №3**

Из проведенных тестов видно, что внесенные изменения в алгоритм приводят к улучшению его работы. В частности, наблюдается более равномерное распределение значений, что говорит о более эффективной работе алгоритма. Также отмечается снижение автокорреляции, что является важным показателем

для генераторов, построенных на базе LFSR. Улучшение других ключевых статистических характеристик также говорит о том, что внесенные модификации действительно повышают эффективность работы алгоритма.

*Тестирование с помощью пакета NIST SP 800-22.*

Для тестирования был установлен компилятор gcc и утилита make, которые позволили скомпилировать и запустить программу для обработки битовых последовательностей. В ходе тестирования были использованы битовые последовательности различной длины – от 1 миллиона до 10 миллионов бит. Каждая последовательность была разбита на 100 потоков для параллельной обработки.

Окно запуска тестов NIST изображено на рисунке 5.

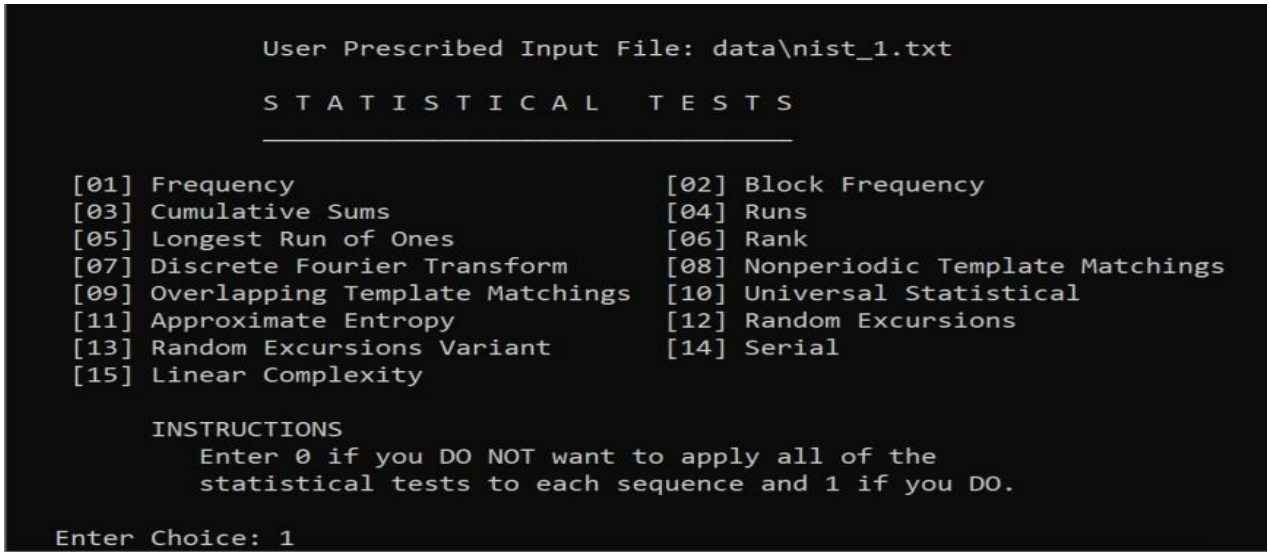
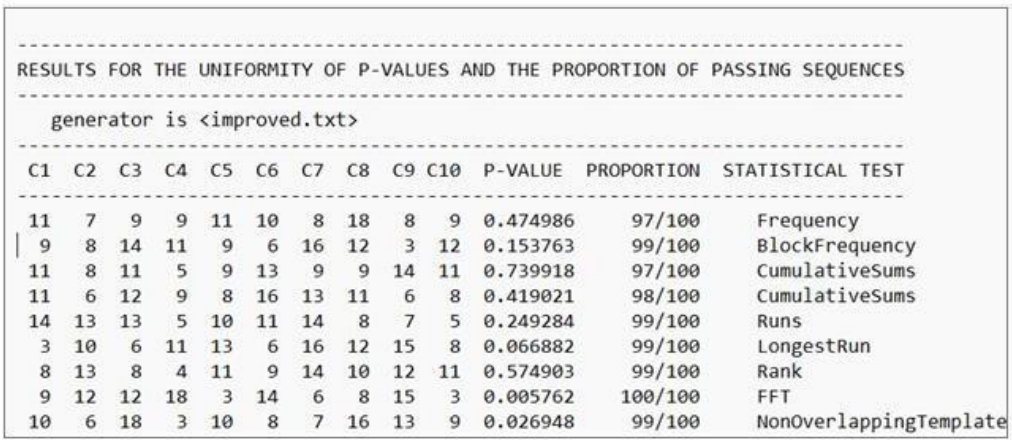



**Рисунок 5 – Окно запуска пакета тестов NIST**

Результаты анализа записываются в файл для дальнейшего удобного доступа и анализа. В файле отображается статистика по всем 15 тестам, включая рассчитанное значение *P-value* и количество пройденных тестов из общего числа возможных (100). Пример содержимого файла с результатами анализа приведен на рисунке 6



RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <improved.txt>

| C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | P-VALUE | PROPORTION | STATISTICAL TEST |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 7 | 9 | 9 | 11 | 10 | 8 | 18 | 8 | 9 | 0.474986 | 97/100 | Frequency |
| 9 | 8 | 14 | 11 | 9 | 6 | 16 | 12 | 3 | 12 | 0.153763 | 99/100 | BlockFrequency |
| 11 | 8 | 11 | 5 | 9 | 13 | 9 | 9 | 14 | 11 | 0.739918 | 97/100 | CumulativeSums |
| 11 | 6 | 12 | 9 | 8 | 16 | 13 | 11 | 6 | 8 | 0.419021 | 98/100 | CumulativeSums |
| 14 | 13 | 13 | 5 | 10 | 11 | 14 | 8 | 7 | 5 | 0.249284 | 99/100 | Runs |
| 3 | 10 | 6 | 11 | 13 | 6 | 16 | 12 | 15 | 8 | 0.066882 | 99/100 | LongestRun |
| 8 | 13 | 8 | 4 | 11 | 9 | 14 | 10 | 12 | 11 | 0.574903 | 99/100 | Rank |
| 9 | 12 | 12 | 18 | 3 | 14 | 6 | 8 | 15 | 3 | 0.005762 | 100/100 | FFT |
| 10 | 6 | 18 | 3 | 10 | 8 | 7 | 16 | 13 | 9 | 0.026948 | 99/100 | NonOverlappingTemplate |

**Рисунок 6 – Содержимое файла с результатами анализа**

Сравнительная таблица значений приведена в таблице 2.

Таблица 2 – Результаты тестирования A5/1 и его модифицированной версии

| Название теста | A5/1 | | Модифицированный A5/1 | |
|---|---|---|---|---|
| | *P-value* | К-во пройденных тестов | *P-value* | К-во пройденных тестов |
| Frequency | 0.366916 | 98/100 | 0.935716 | 98/100 |
| BlockFrequency | 0.637119 | 99/100 | 0.798139 | 100/100 |
| CumulativeSums | 0.319084 | 98/100 | 0.759756 | 99/100 |
| Runs | 0.455937 | 98/100 | 0.102526 | 100/100 |
| LongestRun | 0.554420 | 99/100 | 0.437274 | 97/100 |
| Rank | 0.108791 | 100/100 | 0.616305 | 100/100 |
| FFT | 0.191687 | 96/100 | 0.437274 | 100/100 |
| NonOverlappingTemplate | 0.554420 | 100/100 | 0.419021 | 100/100 |
| OverlappingTemplate | 0.334538 | 98/100 | 0.978072 | 99/100 |
| Universal | 0 | 0/100 | 0 | 0/100 |
| ApproximateEntropy | 0.153763 | 96/100 | 0.171876 | 98/100 |
| RandomExcursions | 0.534116 | 10/10 | 0.171876 | 7/7 |
| RandomExcursionsVariant | 0.238309 | 14/14 | 0.171876 | 7/7 |
| Serial | 0.554420 | 99/100 | 0.759756 | 99/100 |
| LinearComplexity | 0.275709 | 98/100 | 0.983453 | 99/100 |

Анализируя результаты автоматического тестирования по сводной таблице 2, можно видеть, что количество пройденных тестов для модифицированного A5/1 возросло. Также видно, что при равном количестве пройденных тестов значение *P-value* для модифицированного A5/1 ближе к единице, а, значит, M-последовательности, сгенерированные таким образом ближе к идеальной случайной последовательности.

## ЗАКЛЮЧЕНИЕ

### Основные научные результаты диссертации

1 Основываясь на известных уязвимостях потоковых криптосистем, был предложен, реализован и протестирован алгоритм нахождения порождающего полинома. Этот алгоритм основан на методе Касиски, который позволяет находить длину М-последовательности, используемой для генерации ключевого потока. Затем на основе этой длины вычисляется степень порождающего полинома LFSR, а, следовательно, и сам полином. Тестирование алгоритма показало его устойчивую работу при условии, что длина файла достаточна для проведения анализа.

2 Исследование недостатков алгоритма A5/1 привело к выявлению уязвимостей данного генератора. Для улучшения криптостойкости были предложены изменения, которые позволили повысить устойчивость к различным видам атак, включая корреляционную атаку, предложенную Эдхалем. После внесения изменений было проведено моделирование работы обоих алгоритмов и проведено исследование статистических свойств М-последовательностей, генерируемых таким образом. Используя пакет тестов NIST, было показано, что шифрогаммы, полученные с использованием улучшенного алгоритма, улучшили свои статистические свойства по ряду тестов. Это означает, что шифр стал более надежным и устойчивым к взлому.

### Рекомендации по практическому использованию результатов

Полученные результаты могут быть использованы в обучающих целях на практических занятиях по таким предметам как «Теория информации», «Защита информации» и других предметах, связанных с криптологией и криптографией.

## СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

*Тезисы конференций*

1. Болтак, С.В. Применение теста Касиски при потоковом шифровании / С.В. Болтак, П.А. Шлык // Компьютерные системы и сети: сборник статей 59-й научной конференции аспирантов, магистрантов и студентов, Минск, 17–21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – с. 210 – 211.

2. Boltak, S. V. The use of neural networks in pseudo-random number generators development // Актуальные вопросы экономики и информационных технологий : сборник тезисов и статей докладов 59-ой научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17–21 апреля 2023 г. /

Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – с. 360–361.

3. Болтак, С.В. Анализ уязвимостей потоковых криптосистем на базе М-последовательностей / С.В. Болтак, Е. С. Русакович // Информационные технологии и системы 2023 (ИТС 2023) = Information Technologies and Systems 2023 (ITS 2023): материалы Международной научной конференции, Минск, 22 ноября 2023 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2023. – с. 177–178.

4. Болтак, С.В. Исследование статистических свойств псевдослу-чайных последовательностей, сгенерированных модифицированным алгоритмом А5/1 / С. В. Болтак, Б. О. Гридюшко, Е. С. Панкратьев // Технические науки: проблемы и решения: сб. ст. по материалам LXXXIV Международной научно-практической конференции «Технические науки: проблемы и решения». – № 5(78). – М., Изд. «Интернаука», 2024. – с. 73 – 77.