МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6 НА ТЕМУ:

Исследование потоковых шифров

Выполнила:

Студентка 3 курса 1 группы ФИТ

Шимчёнок Елизавета Константиновна

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации потоковых шифров.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости потоковых шифров.
2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования.
3. Выполнить анализ криптостойкости потоковых шифров.
4. Оценить скорость зашифрования/расшифрования реализованных шифров.
5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теоретические сведения**

Потоковый шифр (иногда говорят «поточный») – симметричный шифр, преобразующий каждый символ *mi* открытого текста в символ шифрованного *ci*, зависящий от ключа и расположения символа в тексте.

Термин «потоковый шифр» обычно используется в том случае, когда шифруемые символы открытого текста представляются одной буквой, битом или реже – байтом. Все потоковые шифры делятся на синхронные и асинхронные.

Основной задачей потоковых шифров является выработка некоторой последовательности (гаммы) для зашифрования, т. е. выходная гамма является ключевым потоком (ключом) для сообщения.

Синхронные потоковые шифры (СПШ) характеризуются тем, что поток ключей генерируется независимо от открытого текста и шифртекста. Главное свойство СПШ – нераспространение ошибок. Ошибки отсутствуют, пока работают синхронно шифровальное и дешифровальное устройства отправителя и получателя информации. Один из методов борьбы с рассинхронизацией – разбить отрытый текст на отрезки, начало и конец которых выделить вставкой контрольных меток.

СПШ уязвимы к атакам на основе изменения отдельных битов шифртекста.

В самосинхронизирующихся потоковых шифрах символы ключевой гаммы зависят от исходного секретного ключа шифра и от конечного числа последних знаков зашифрованного текста. Основная идея заключается в том, что внутреннее состояние генератора потока ключей является функцией фиксированного числа предыдущих битов шифртекста. Поэтому генератор потока ключей на приемной стороне, приняв фиксированное число битов, автоматически синхронизируется с генератором гаммы.

Недостаток этих потоковых шифров – распространение ошибок, так как искажение одного бита в процессе передачи шифротекста приведет к искажению нескольких битов гаммы и, соответственно, расшифрованного сообщения.

Для генерации ПСП часто используется линейный конгруэнтный генератор (ЛКГ). Его достоинствами считается простота и высокая скорость получения псевдослучайных значений. ЛКГ находят применение при решении задач моделирования и математической статистики, однако в криптографических целях их нельзя рекомендовать к использованию, так как специалисты по криптоанализу научились восстанавливать всю последовательность ПСП по нескольким ее значениям.

Генератор практически не используется в криптографии в силу низкой криптостойкости. Тем не менее он полезен для решения задач моделирования.

*RC*4 – это потоковый шифр, который использует генератор псевдослучайных битов для создания зашифрованных сообщений. Для генерации псевдослучайных битов на вход генератора подается ключ переменной длины, а на выходе получаются псевдослучайные биты. Длина ключа может быть от 40 до 2048 битов.

Алгоритм *RC*4 определяется параметром *n* - размером блока или слова. Внутреннее состояние шифра определяется массивом слов (*S*-блоком) размером 2*n*. Когда *n* = 8, элементы блока представляют собой перестановку чисел от 0 до 255, а сама перестановка зависит от ключа переменной длины. Другими элементами внутреннего состояния являются 2 счетчика (каждый размером в одно слово; обозначаются *i* и *j*) с начальными значениями, равными нулю. Вычисления в алгоритме *RC*4 выполняются по модулю 2*n*.

Генератор ключевого потока *RC*4 переставляет значения, хранящиеся в *S*, и каждый раз выбирает различное значение из *S* в качестве результата. В одном цикле алгоритма *RC*4 определяется одно *n*-битное слово *K* из ключевого потока, которое в последующем суммируется с исходным текстом для получения зашифрованного текста.

**Ход работы**

В ходе лабораторной работы было реализовано приложение, решающее несколько задач:

- генерация ПСП (алгоритм генерации – линейный конгруэнтный генератор; параметры: *а* = 430, *с* = 2531, *n* = 11 979);

- реализация *RC*4 (*n* = 8; ключ: 122 125 48 84 201);

- оценка скорости выполнения операций генерации ПСП.

Линейный конгруэнтный генератор описывается следующим рекуррентным соотношением:

*,*

где *xt* – предыдущий элемент, а *xt*+1 – текущий член числовой последовательности. А остальные члены уравнения – константы со значениями, приведенными в описании заданий к работе.

Линейный конгруэнтный генератор – это простой метод генерации псевдослучайных чисел, который может быть полезен для многих приложений. Однако его периодичность может быть достаточно низкой, особенно при выборе неправильных параметров. В данном случае выбранные параметры могут гарантировать периодичность не более 11979.

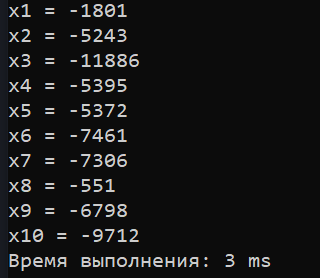


Рис 1 – Сгенерированная последовательность чисел

Также требовалось проанализировать время выполнения расчета членов последовательности, и результат можно увидеть на рисунке 1 – программа сгенерировала ПСП из 10 чисел за 3 миллисекунды. Это достаточно быстро, но существуют и более эффективные методы генерации псевдослучайных чисел.

Далее было необходимо реализовать зашифрование и расшифрование потоковым шифром под названием *RC*4, описание которого было приведено в теоретической части.

Результат операций шифрования и дешифрования приведена на рисунке 2.

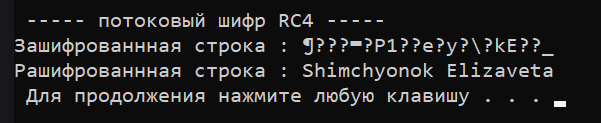


Рис 2 – Шифртекст и расшифрованный текст с использованием RC4

**Ответы на вопросы**

1. В чем состоит особенность потоковых шифров?

Каждый символ сообщения заменяется на шифросимвол, который зависит от ключа и положения исходного символа в тексте сообщения.

2. В чем состоят преимущества и недостатки синхронных и асинхронных потоковых шифров?

Преимущества синхронных потоковых шифров состоят в высокой скорости шифрования и расшифрования данных, низкой задержке при передаче данных и простоте реализации.

Недостатки синхронных потоковых шифров – это отсутствие механизма обнаружения ошибок, уязвимость к атакам на основе известного шифротекста и выбранного шифротекста.

Преимущества асинхронных потоковых шифров:

- высокий уровень защиты данных благодаря использованию открытого и закрытого ключей;

- механизм обнаружения ошибок в данных благодаря использованию контрольной суммы;

- уязвимость к атакам с целью подмены открытых ключей.

Недостатки асинхронных потоковых шифров:

- низкая производительность;

- сложность ключевого управления и вычисления;

- уязвимость к атакам по времени.

3. Какими свойствами должен обладать генератор псевдослучайных чисел для использования криптографических целях?

Необходимо, чтобы генератор был **криптографически стойким**. Это означает, что выходные данные должны быть статистически непредсказуемыми и не должны содержать никакой информации о входных данных. Генератор должен иметь **высокую скорость генерации**, чтобы обеспечить высокую производительность в криптографических приложениях. Он должен быть **определенного размера**, чтобы обеспечить устойчивость к атакам. Генератор должен **иметь достаточную длину периода**, чтобы обеспечить достаточный уровень стойкости. Он должен быть **нечувствительным к исходным данным**, чтобы предотвратить утечку информации о ключе. Генератор должен быть **детерминированным**, то есть при одинаковых входных данных должен выдавать одинаковый выход.

4. Дать характеристику линейным конгруэнтным генераторам. Области их применения.

Линейные конгруэнтные генераторы основаны на рекуррентной формуле, которая генерирует последовательность чисел, используя предыдущие числа, начальное значение и два параметра: множитель и приращение. Они просты в реализации и как правило используются там, где необходима высокая производительность (высокая скорость генерации множества чисел).

6. Представить общую структурную схему генератора ПСП на основе регистров сдвига с линейной обратной связью. Пояснить особенности его функционирования.

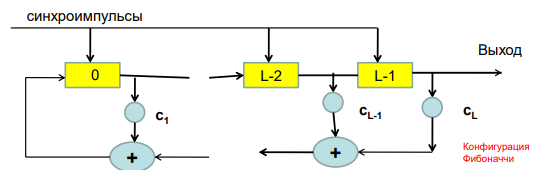
****

Рис 3 – Общая схема ПСП на основе регистра сдвига

7. Синтезировать структурную схему генератора ПСП на основе регистров сдвига с линейной обратной связью, формально обозначаемого следующим образом: б) 520.

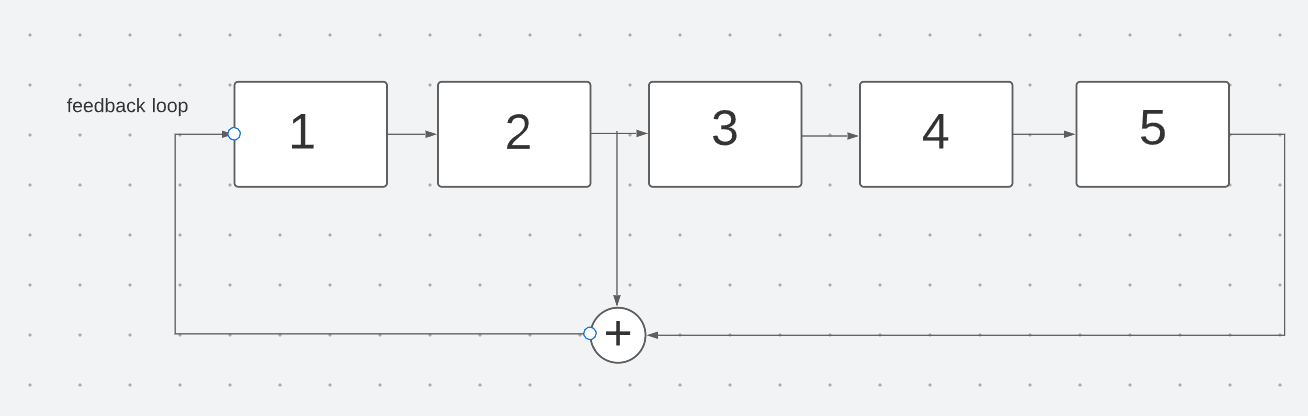
****

Рисунок 4 – Структурная схема генератора 520

8. Определить первые 12 бит ПСП, задаваемого формально в виде чисел 5410, если начальные состояния ячеек (слева направо) соответствуют последовательности 10101.

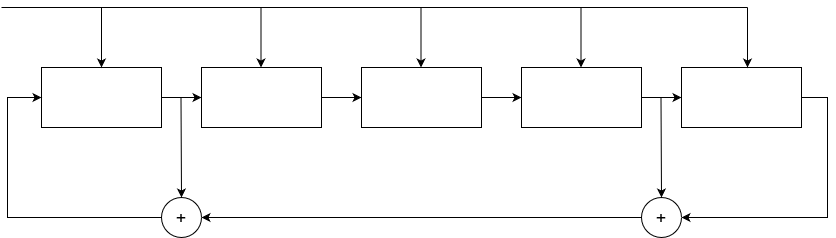
****

Рисунок 1.4 – Структурная схема генератора 5410

Первые 12 бит выходной последовательности: 1010101010101010.

9. Как устроен генератор ПСП на основе RSA? На чем основана криптостойкость реализуемого алгоритма?

Генератор псевдослучайных чисел (ПСП) на основе RSA на вычислительной сложности факторизации больших простых чисел.

Криптостойкость этого генератора основана на сложности факторизации больших простых чисел.

10. Вычислить *х*1, *х*5, *х*9, *х*11 по методу генерации псевдослучайных чисел *BBS*, если *p* = 11, *q* = 19, *х* = 3.

*х*1 = 1; *x*5 = 0, *x*9 = 1; *x*11 = 0.

**Вывод:** в ходе лабораторной работы были приобретены практические навыки разработки и использования приложений для реализации потоковых шифров на примере *RC*4. Также были исследованы способы генерации псевдослучайных чисел и проанализирована производительность вычислений.