МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №7**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ БЛОЧНЫХ ШИФРОВ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

**Содержание**

[Практические задания 4](#_Toc136173733)

[Задание 1 4](#_Toc136173741)

[Задание 2 4](#_Toc136173742)

[Задание 3 7](#_Toc136173743)

[Выводы 8](#_Toc136173744)

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации блочных шифров (рассчитана на 4 часа аудиторных занятий).

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости блочных шифров.
* Разработать приложение для реализации указанных преподавателем методов блочного зашифрования/расшифрования.
* Выполнить анализ криптостойкости блочных шифров.
* Оценить скорость зашифрования/расшифрования реализованных шифров.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **Практические задания**

Разработать авторское приложение в соответствии с целью лабораторной работы.

Приложение должно реализовывать следующие операции:

* разделение входного потока данных на блоки требуемой длины с необходимым дополнением последнего блока;
* выполнение требуемых преобразований ключевой информации;
* выполнение операций зашифрования/расшифрования;
* оценка скорости выполнения операций зашифрования/расшифрования;
* пошаговый анализ лавинного эффекта с подсчетом количества изменяющихся символов по отношению к исходному слову.

Задание 1:

С помощью разработанного приложения зашифровать сообщение «бота №5», используя ключи «Информац», «зопаснос», «лаборато». Алгоритм – DES-EEE3 (шифруется 3 раза с 3 разными ключами (операции шифрование-шифрование-шифрование).

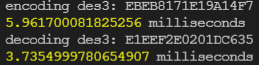


Рисунок 1 — Зашифрование/расшифрование сообщения при помощи алгоритма DES-EEE3

Задание 2:

Проанализировать влияние слабых ключей и полуслабых ключей на конечный результат зашифрования и на лавинный эффект.

Для этого возьмем слабый ключ и с помощью него зашифруем 2 сообщения.

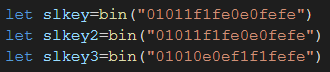


Рисунок 2 — Слабые ключи, взятые для шифрования и расшифрования сообщения

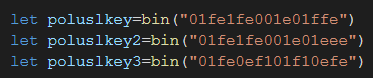


Рисунок 3 — Полулабые ключи, взятые для шифрования и расшифрования сообщения

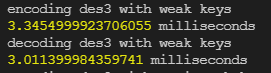


Рисунок 4 — Время выполнения операций зашифрования/расшифрования сообщения «бота №5» при помощи слабых ключей

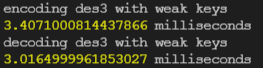


Рисунок 5 — Время выполнения операций зашифрования/расшифрования сообщения «бота №6» при помощи слабых ключей

Можно заметить, что при использовании слабого ключа лавинный эффект очень незначительный.

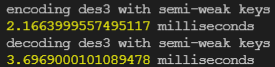


Рисунок 6 — Время выполнения операций зашифрования/расшифрования сообщения «бота №5» при помощи полуслабых ключей

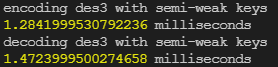


Рисунок 7 — Время выполнения операций зашифрования/расшифрования сообщения «бота №6» при помощи полуслабых ключей

В данном случае можно заметить, что уже больше символов изменяется при изменении одного символа.



Рисунок 8 — Зашифрование сообщения «бота №5»



Рисунок 9 — Зашифрование сообщения «бота №6»

Можно заметить, что все символы изменились, это говорит о высоком лавинном эффекте данного алгоритма.

При использовании слабого и полу слабого ключа можно заметить, как уменьшился лавинный эффект, то есть изменение одного бита в исходном сообщении может не привести к изменению битов в зашифрованном сообщении в той же мере, как при использовании сильного ключа. Это может сделать криптоанализ более простым, так как злоумышленник может использовать данную информацию для раскрытия ключа или зашифрованного сообщения. Поэтому, при использовании криптографических алгоритмов, необходимо использовать сильные ключи, чтобы обеспечить надежную защиту данных.

Для оценки скорости работы алгоритмы построим график зависимости скорости работы от кол-ва символов в сообщении.

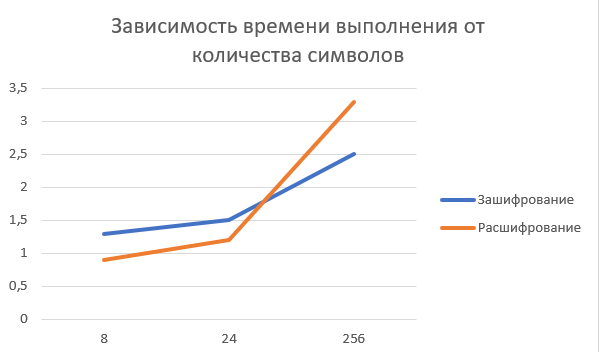


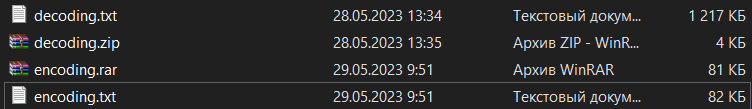
Рисунок 10 — График зависимости времени выполнения от количества символов в сообщении

На данных диаграммах можно заметить, что при увеличении длинны сообщений, увеличивается время, затраченное на шифрование, расшифрование текста.

Задание 3:

Оценить степень сжатия (используя любой доступный архиватор) открытого текста и соответствующего зашифрованного текста. Дать пояснения к полученному результату.

Для данного задания я создала два текстовых документа, которые потом заархивировала и в итоге данные файлы, имея первоначальный размер в 82 кб и 1217 кб, стали весить 81 кб и 4 кб соответственно.

Рисунок 11 – пример сжатия двух файлов

# **Выводы**

В ходе выполнения лабораторной работы было разработано приложение, позволяющие шифровать и расшифровывать сообщение при помощи алгоритма DES-EEE3. Так же были построены графики зависимости времени выполнения от количества символов в сообщении.

На примере степени сжатия можно сказать, что после обработки алгоритмом, файл сжимается намного хуже, чем необработанный текст.