Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование блочных шифров**

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Мазенков И.В.

Препадаватель:

Сазонова Дарья Владимировна

Минск 2023

1. Разработать авторское приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться готовыми библиотеками либо программными кодами, реализующими некоторые блочные алгоритмы, из приложения в [4].

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

По желанию студент может разработать приложение и выполнить связанные исследования для любого другого блочного алгоритма, не указанного в табл. 5.5.

2. Проанализировать влияние слабых ключей (табл. 5.3) и полуслабых ключей (табл. 5.4) на конечный результат зашифрования и на лавинный эффект.

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

4. Результаты оформить в виде отчета по установленным правилам

1. **Описание приложения**

Приложение написано на языке программирования javascript на платформе node.js и предназначено для шифрования и дешифрования текстовых файлов на основе алгоритма шифрования des.

Приложение написано с использованием сторонней библиотеки для node.js – crypto, которая упрощает работу и сокращает время и объём написанного кода.

Для шифрования и дешифрования использовался обновлённая версия алгоритма des – aes.

1. **Методика выполнения поставленных задач**

Методы шифрования и дешифрования вынесены в отдельный модуль программы, чтобы сделать работу более удобной. Эти методы принимают на вход исходный и зашифрованный текст соответственно, а также версию алгоритма шифрования, ключ и вектор и возвращают зашифрованный и дешифрованный текст соответственно. В основном модуле программы происходит инициализация ключа и вектора, как можно увидеть на рисунке 2.1.

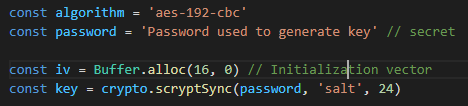


Рисунок 2.1 – Инициализация ключа и вектора

Также использовался встроенный модуль node.js – fs, который предназначен для работы с файловой системой. Он был использован для чтения и записи зашифрованного и расшифрованного текстов из файла и в файл соответственно. На рисунке 2.2 можно увидеть код, где вызываются методы шифрования и дешифрования с передачей параметров из главного файла приложения.

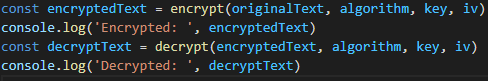
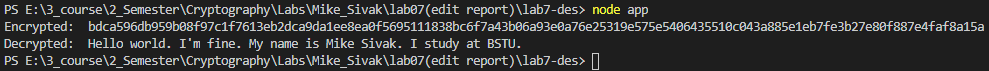


Рисунок 2.2 – Вызов методов шифрования и дешифрования

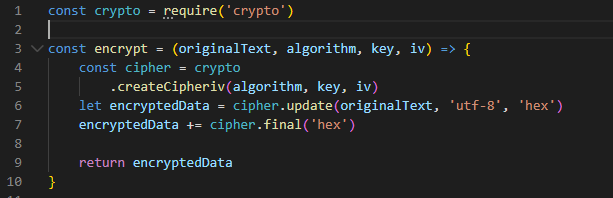
Далее представлены некоторые листинги программы, а также результаты её работы.

**Результаты работы программы:**

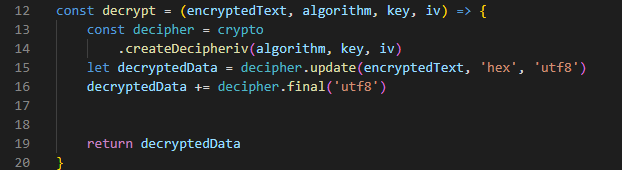


**Листинги программы**:

Функция шифрования



Функция расшифрования



**Вывод**

В ходе выполнения данной лабораторной работы я получил хороший и полезный опыт в разработке программного обеспечения, позволяющего проводить шифрование и дешифрование текстовых файлов на основе современной модификации алгоритма des – aes, который был выпущен в 2001 году.