Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование потоковых шифров**

Выполнил:

Студент 3 курса 5 группы

Специальности ПОИТ

Сивак М.Н.

Минск 2020

**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.

**Вариант 12**

**Основное** **задание**.

1. Разработать авторские многооконные приложения в соответствии с целью лабораторной работы. При этом можно воспользоваться готовыми библиотеками либо программными кодами, реализующими заданные алгоритмы.

*Приложение 1* должно реализовывать генерацию ПСП в соответствии с вариантом из табл.

|  |  |  |
| --- | --- | --- |
| 5 | Линейный конгруэнтный генератор | а = 421, с = 1663, n = 7875 |

*Приложение 2* должно реализовывать алгоритм RC4 в соответствии с вариантом из табл.

|  |  |  |
| --- | --- | --- |
| 12 | 8 | 122, 125, 48, 84, 201 |

В качестве шифруемого сообщения может быть выбран произвольный текст

2. 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 текстов на основе алгоритма шифрования RC4. Приложение написано с использованием сторонней библиотеки для node.js – crypto, которая упрощает работу и сокращает время и объём написанного кода. В приложении также есть генератор псевдослучайных чисел, которые используются в потоковых шифров, каким RC4 и является.

1. **Методика выполнения поставленных задач**

Методы шифрования и дешифрования вынесены в отдельный модуль программы, чтобы сделать работу более удобной для написания, а также сделать код более читабельным и понятным. Эти методы принимают на вход исходный и зашифрованный текст соответственно, а также ключи для шифрования. В основном модуле программы происходит инициализация ключа, как можно увидеть на рисунке 2.1.



Рисунок 2.1 – Инициализация ключа

На рисунке 2.2 можно увидеть код, где вызываются методы шифрования и дешифрования с передачей параметров из главного файла приложения.

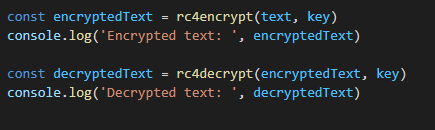


Рисунок 2.2 – Вызов методов шифрования и дешифрования

Далее после вызова методов и передачи параметров происходит шифрование входного текста и вывод результата на консоль, после чего происходит дешифрование и вывод его также в консоль, как видно на рисунке 2.3.

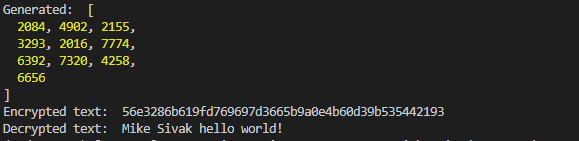
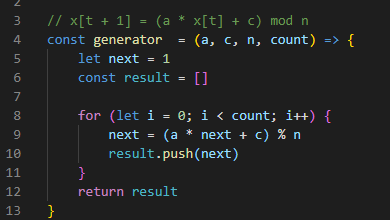


Рисунок 2.3 – Результат выполнения программы

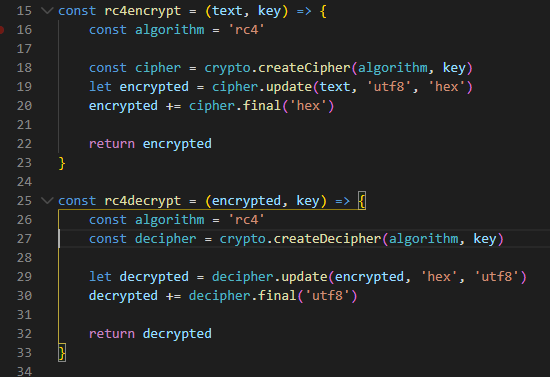
Также ниже можно приведены несколько листингов с исходным кодом генератора чисел, а также методов шифрования и дешифрования.

**Листинги:**

Функция генерации псевдослучайных чисел:



Функциии RC4:



**Вывод**

В ходе выполнения лабораторной работы я получил опыт в создании программы для шифрования и дешифрования текстов на основе поточного шифра RC4. Так же я узнал много нового и полезного в теоретической части в целом. Я ознакомился с поточными шифрами и узнал о алгоритме их работы, что может быть довольно полезным при решении задач на безопасность передаваемых данных.