Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование поточных шифров.**

Студент: Плотников Д.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

# Постановка задачи

В результате выполнения лабораторной работы было нужно изучить и приобрести практические навыки разработки и использования приложений для реализации потоковых шифров.

По поему варианту было нужно разработать две программы шифрования для алгоритмов BBS и RC4. Оба алгоритма являются потоковыми и используют генераторы псевдослучайных чисел, общий принцип шифрования которых показан на рисунке 1.

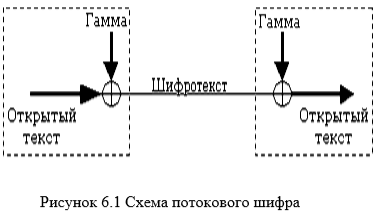


Рисунок 1 – Общий принцип потоковых шифров.

# 2. Описание приложения

Приложение представляет собой две HTML странички, реализующих алгоритмы BBS и RC4. Начать следует с RC4, т.к. он представляет наибольший интерес. Главный вид приложения показан на рисунке 2.

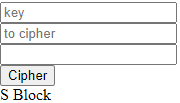


Рисунок 2 – Главный вид приложения

Как можно заметить, оно состоит из трех текстовых полей. Первое предназначено для ввода ключа, на основании которого будет сгенерирован и перемешан S блок. Второе текстовое поле предназначено для ввода сообщения, которое должно быть зашифровано, а соответственно в третьем результат шифрования. По заполнению ключа, после текста «S Block» можно увидеть S блок в перемешанном на основе ключа виде, как это и показано на рисунке 3.

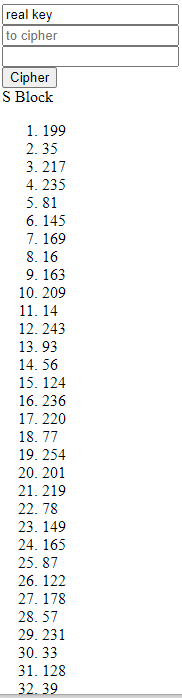


Рисунок 3 – Результат перемешивания блока на основе ключа.

По окончанию можно ввести во второе желанный для шифрования текст и получить в зашифрованном виде уже в последнем текстовом поле, как показано на рисунке 4.

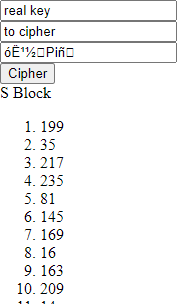


Рисунок 4 – Пример шифрования текста алгоритмом RC4.

Таким образом выполняется шифрование в разработанной программе.

# Вывод

В результате лабораторной работы было разработано приложения для выполнения шифрования алгоритмом RC4. Так же в задании было задание связанное с потоковым шифром BBS, но его реализовать было невозможно т.к. число n = 256 данное в варианте, к сожалению не раскладывается на два простых множителя p и q.