Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №8**

**Тема «****Исследование потоковых шифров»**

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.

**Потоковый шифр**

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.

**Генератор ПСП на основе алгоритма BBS**

Начальное значение x0 генератора вычисляется на основе соотношения.

*x*0 ≡ *x*2 mod *n*

*p*, *q* – простые числа. *p* mod 4=3, *p* mod 4=3, НОД(*x*, *n*)=1, *n*=*pq*, *n* так же называют числом Блюма.

Выходом генератора на *t*-м шаге является младший бит числа *xt*:

*xt* ≡ (*xt* – 1)2 mod *n*

Пример кода и его результат работы предоставлен на рисунках 1.1 и 1.2 соответственно.

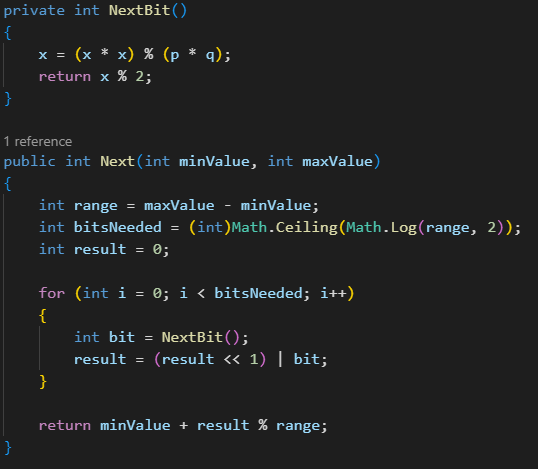


Рисунок 1.1 – Пример кода генератора ПСП на основе алгоритма BBS

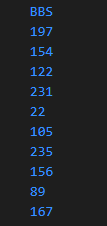
****

Рисунок 1.2 – Результат работы генератора ПСП на основе алгоритма BBS

Время генерации псевдослучайных чисел предоставлена на рисунке 1.3

Рисунок 1.3 – Время генерации псевдослучайных чисел

**Потоковый шифр RC4**

Алгоритм *RC*4, как и любой потоковый шифр, строится на основе генератора псевдослучайных битов (генератора ПСП). На вход генератора записывается ключ, а на выходе читаются псевдослучайные биты.

Ядро алгоритма состоит из функции генерации ключевого потока. Другая часть алгоритма – функция инициализации, которая использует ключ переменной длины *Ki* для создания начального состояния генератора ключевого потока.

В основе алгоритма – размер блока или слова, определяемый параметром n. Обычно *n* = 8, но можно использовать и другие значения. Внутренне состояние шифра определяется массивом слов (S-блоком) размером 2*n*.

Шифрование и дешифрование происходит по одному и тому же алгоритму.

Пример кода реализации алгоритма *RC*4 и его результат предоставлен на рисунках 1.4 и 1.5 соответственно.

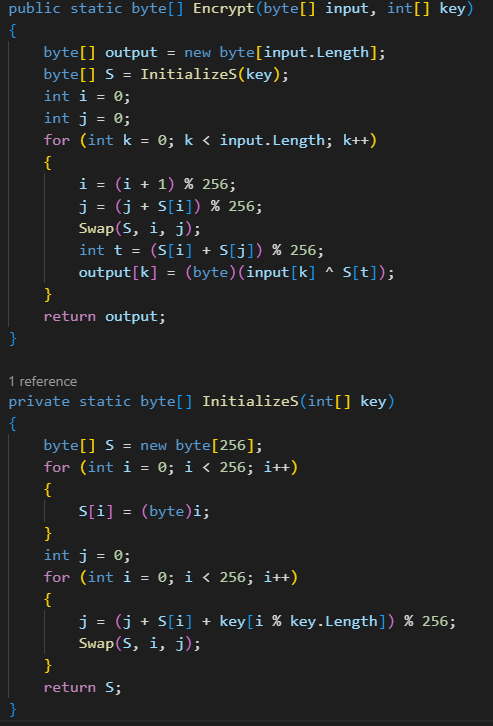


Рисунок 1.4 – Код реализации алгоритма *RC*4

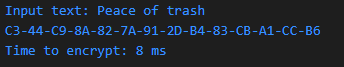


Рисунок 1.5 – Результат работы алгоритма *RC*4

Время, затраченное на выполнение программы предоставлено на рисунке 1.6

**Вывод**

В ходе выполнения лабораторной работы я приобрёл и закрепил навыки практические навыки разработки приложения для реализации потоковых шифров.