МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Исследование ассиметричных шифров»**

Студент:

Храмых Владислав Олегович

Преподаватель:

Блинова Евгения Александровна

Минск 2020

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке крипто-стойкости асимметричных шифров.

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.

3. Выполнить анализ криптостойкости асимметричных 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.

**Ход работы**

В данной лабораторной работе мы работали с шифром на основе укладки рюкзака. Это асимметричный шифр. В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования (открытый или публичный ключ), другой – для расшифрования (тайный ключ). Отметим, что указанная пара ключей принадлежит получателю зашифрованного сообщения.

Меркль и Хеллман предложили использовать задачу об укладке ранца (рюкзака) для асимметричного шифрования. Она относится к классу NP-полных задач и формулируется следующим образом. Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению? Более формально задача формулируется так: дан набор значений M1, M2, ..., Мn и суммарное значение S; требуется вычислить значения bi такие что:

**S = b1М1 + b2М2 + ... + bnМn,**

где **n** - количество предметов;

**bi** - бинарный множитель. Значение bi = 1 означает, что предмет i кладут в рюкзак, bi = 0 - не кладут.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки ранца. Предметы из кучи выбираются с помощью блока открытого текста, длина которого (в битах) равна количеству предметов в куче. При этом биты открытого текста соответствуют значениям b, a текст является полученным суммарным весом. Пример шифрограммы, полученной с помощью задачи об укладке ранца, показан в следующей таблице.

Суть использования данного подхода для шифрования состоит в том, что на самом деле существуют две различные задачи укладки ранца - одна из них решается легко и характеризуется линейным ростом трудоемкости, а другая, как принято считать, нет. Легкий для укладки ранец можно превратить в трудный. Раз так, то можно применить в качестве открытого ключа трудный для укладки ранец, который легко использовать для шифрования, но невозможно - для дешифрования. А в качестве закрытого ключа применить легкий для укладки ранец, который предоставляет простой способ дешифрования сообщения.

В качестве закрытого ключа (легкого для укладки ранца) используется сверхвозрастающая последовательность. **Сверхвозрастающей** называется последовательность, в которой каждый последующий член больше суммы всех предыдущих.

В данной лабораторной работе необходимо было разработать приложение, которое реализует алгоритм генерации шифрования на основе укладки ранца. Основная реализация шифрования представлена на рисунке 1 (рис.1):

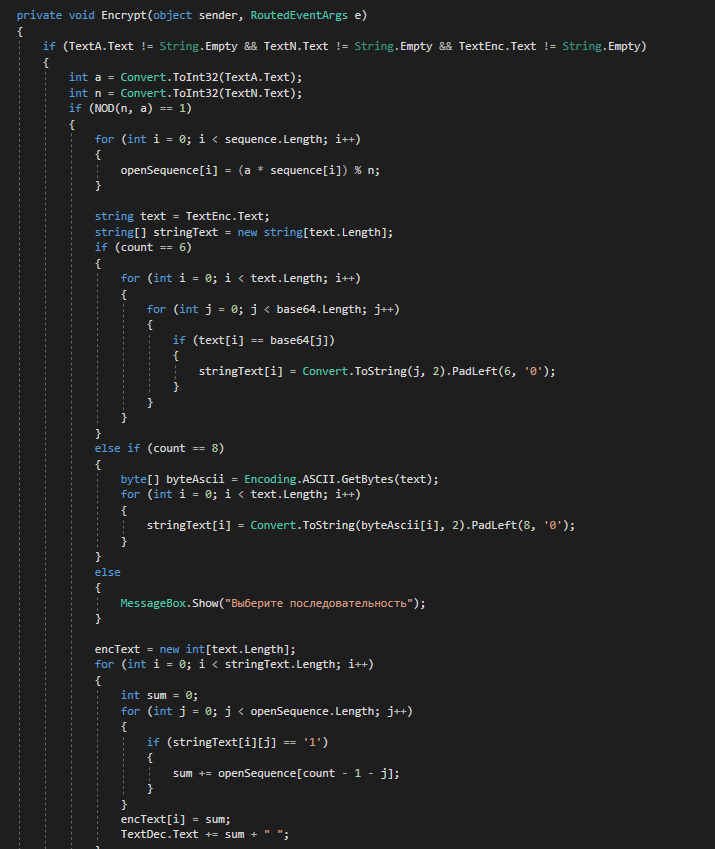
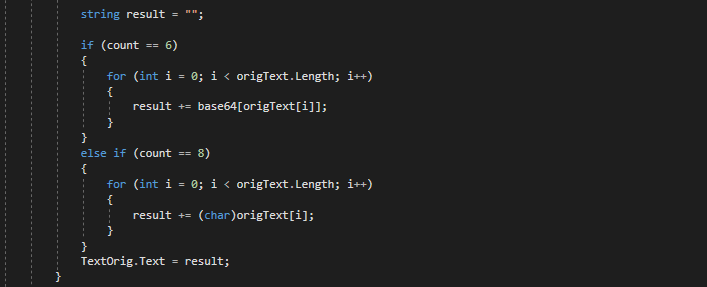
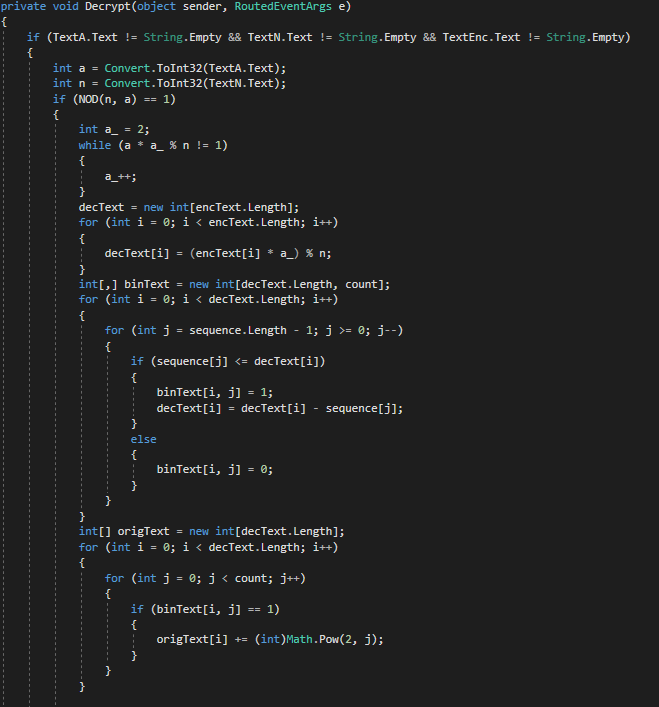


Рисунок 1 – Шифрование на основе укладки ранца

Функция расшифрования показана ниже на рисунке 2:



Результат выполнения этого алгоритма представлен ниже (рис. 3):

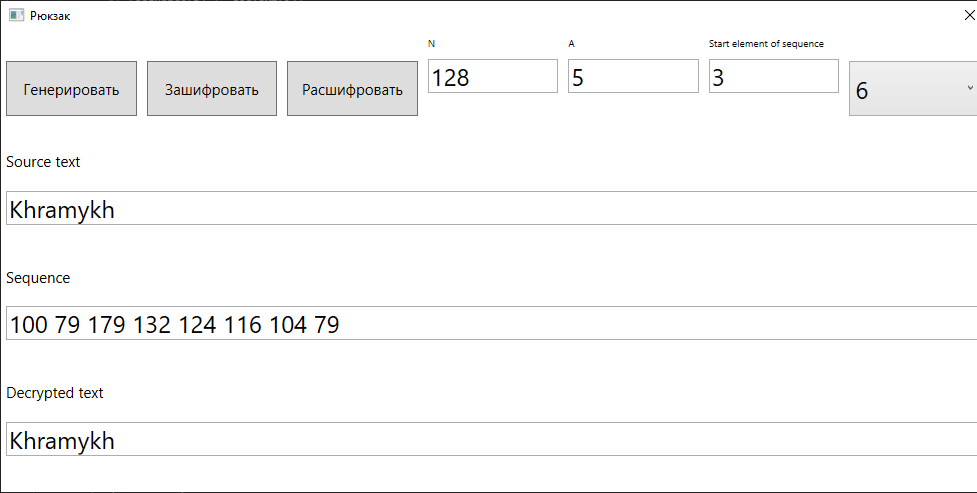


Рисунок 3 – Результат

**Вывод**

Таким образом, в ходе лабораторной работы были программно реализованы шифрование на основе укладки ранца.