МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Государственное образовательное учреждение высшего профессионального образования

Кыргызско-Российский Славянский университет

Естественно-Технический факультет

Кафедра Информационно-вычислительных технологий

**Отчет к лабораторной работе**

**По дисциплине «Методы и средства защиты информации»**

**на тему «Реализация алгоритма шифрования с использованием задачи о рюкзаке»**

Выполнил:

Студент 4 курса

Группы ЕПИ-1-20

Астаркулов А.С.

Проверил:

Демиденко А.П.

г. Бишкек 2023 г.

# Условие задачи

Реализация алгоритма шифрования, использующего задачу о рюкзаке. Целью лабораторной работы является реализация алгоритма шифрования. Размерность сверхвозрастающей последовательности должна выбираться и максимальная длина ее=150 элементов. Исходная информация должна вводиться с клавиатуры и из файла.

# Выполненные задачи

1. Реализация алгоритма шифрования c использованием задачи о рюкзаке

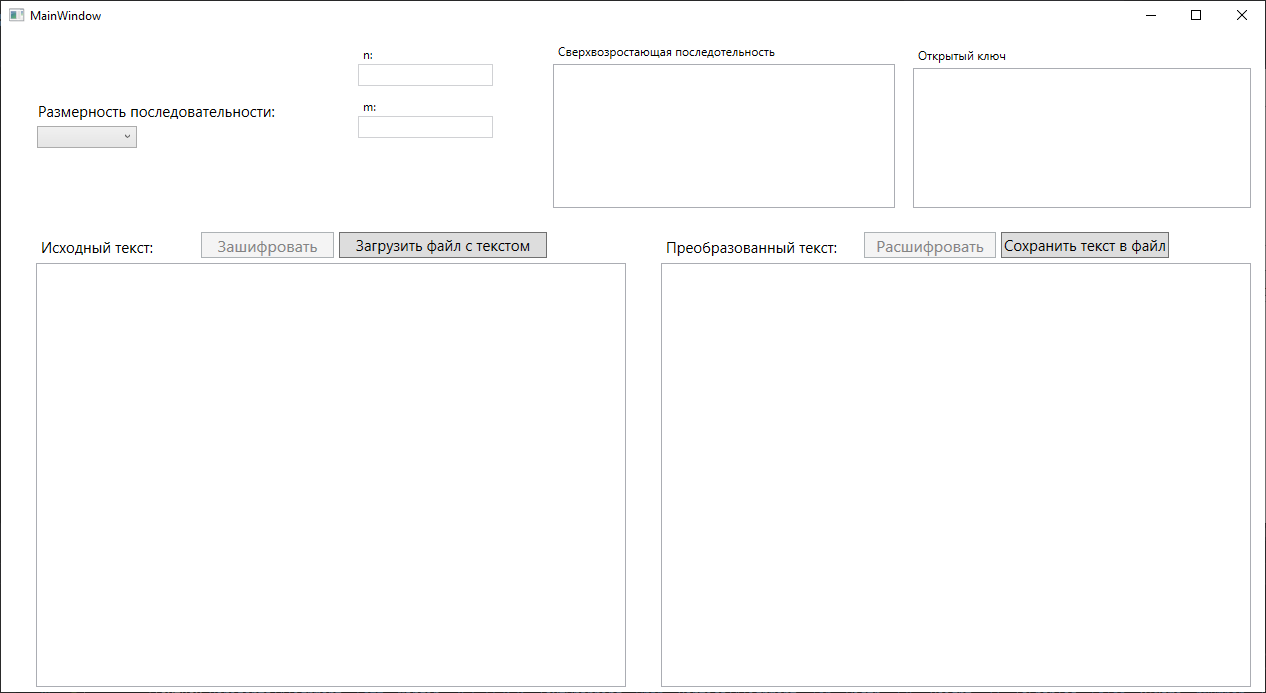


Рисунок 1 Интерфейс программы

Программа была разработана на языке C#, с использованием библиотеки WPF.

В верхней части программы находятся элементы управления: выбор размерности последовательности, ниже находятся поля для ввода текста и поле где будет зашифрованный текст, выше над полями находятся кнопки «Зашифровать», «Загрузить файл с текстом, правее находятся кнопки «Расшифровать», «Сохранить текст в файл»

# Описание выполненных задач

1. Реализация алгоритма шифрования c использованием задачи о рюкзаке

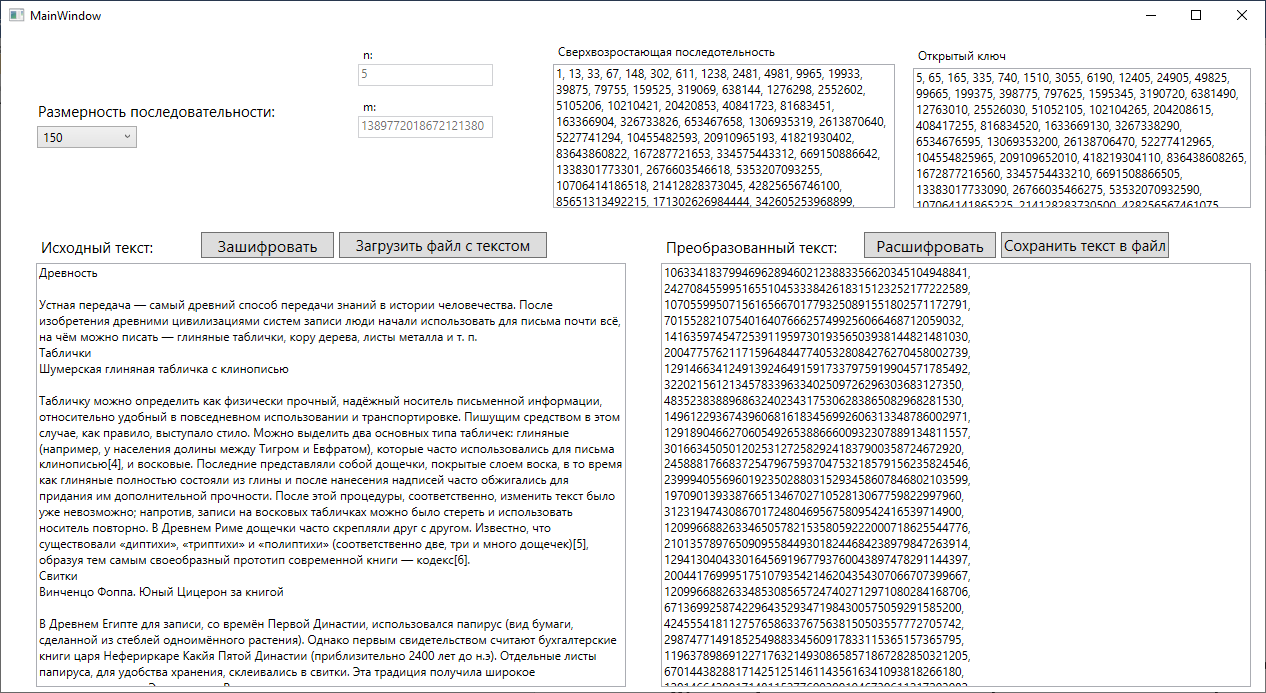


Рисунок 2 Шифровка

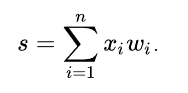
«Задача о рюкзаке» заключается в следующем: зная [подмножество](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D0%BC%D0%BD%D0%BE%D0%B6%D0%B5%D1%81%D1%82%D0%B2%D0%BE) грузов, уложенных в ранец, легко подсчитать суммарный [вес](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D1%81), но, зная вес, непросто определить подмножество грузов. Более подробно, пусть задана последовательность из n положительных [чисел](https://ru.wikipedia.org/wiki/%D0%A7%D0%B8%D1%81%D0%BB%D0%BE) (n — «размер» рюкзака)

*w* = (*w*1, *w*2, …, *wn*) и *s*.

Задача состоит в том, чтобы найти такой бинарный [вектор](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BA%D1%82%D0%BE%D1%80_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0))

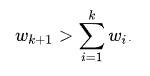
*x* = (*x*1, *x*2, …, *xn*), (*x*i = 0 или 1),

чтобы



Если каждому [двоичному числу](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D0%BE%D0%B8%D1%87%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) *x* поставить в соответствие некоторую букву алфавита, то её можно было бы передавать в зашифрованном виде просто как сумму *s*. Для произвольного набора чисел *w*i задача восстановления *x* по *s* является [NP-трудной](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_NP).

Меркл использовал не произвольную [последовательность](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) *w*i, а супервозрастающую (superincreasing), то есть такую, что



Нетрудно убедиться, что для такого набора чисел решение задачи является тривиальным. Чтобы избавиться от этой тривиальности и понадобилосьввести «секретный ключ», а именно два числа: *q* такое, что

 �>∑�=1���

и *r* такое, что НОД(r, q) =1. И теперь вместо первоначального набора чисел *w*i будем использовать числа *b*i=r*w*i mod *q*. В оригинальных статьях Меркл рекомендовал использовать *n* порядка 100, где n — число элементов супервозрастающей последовательности («размер» рюкзака).

В итоге получаем: открытый ключ — (*b*1, *b*2, …, *bn*), закрытый ключ — (*w*1, *w*2, …, *wn*; *q*, *r*).

**Шифрование**

Сначала исходный текст необходимо представить в [двоичном виде](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D0%BE%D0%B8%D1%87%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) и разбить его на блоки, равные по длине с открытым ключом. Далее из последовательности, образующей открытый ключ, выбираются только те элементы, которые по порядку соответствуют 1 в [двоичной записи](https://ru.wikipedia.org/wiki/%D0%94%D0%B2%D0%BE%D0%B8%D1%87%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F) исходного текста, игнорируя при этом элементы, соответствующие 0 [биту](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82). После этого элементы полученного подмножества складываются. Найденная в результате сумма и есть шифротекст.

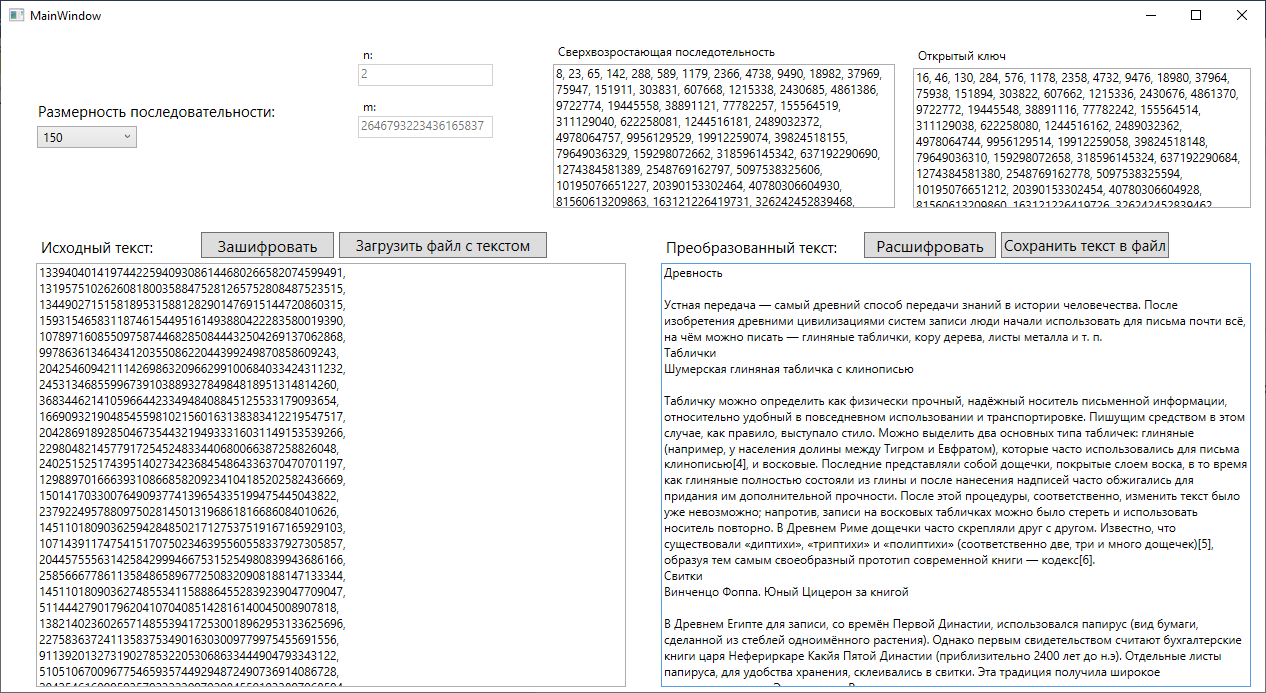


Рисунок 3 Расшифровка

**Дешифрование** является возможным в силу того, что множитель и модуль, используемые для генерации открытого ключа из супервозрастающей последовательности, используются также и для преобразования шифротекста в сумму соответствующих элементов супервозрастающей последовательности. Далее, с помощью простого [жадного алгоритма](https://ru.wikipedia.org/wiki/%D0%96%D0%B0%D0%B4%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC), можно дешифровать сообщение, используя O(n) арифметических операций.

## Генерация ключа

В системе Меркла — Хеллмана ключи состоят из последовательностей. Открытый ключ представляет собой «сложную» последовательность, закрытый ключ состоит из «простой» или супервозрастающей последовательности, а также двух дополнительных чисел — множителя и модуля, которые используются как для преобразования супервозрастающей последовательности в «сложную» (генерация открытого ключа), так и для преобразования суммы подмножества «сложной» последовательности в сумму подмножества «простой» (дешифрование). Последняя задача решается за [полиномиальное время](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_P).

**Выводы**

В ходе выполнения лабораторной работы были изучены и реализованы алгоритм шифрования, использующего задачу о рюкзаке.

В процессе выполнения лабораторной работы были приобретены навыки работы с алгоритмом шифрования с использованием задачи о рюкзаке, что может быть полезно при изучении криптографии и информационной безопасности.