Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование ассиметричных шифров**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

Изучение и приобретение практических навыков разработки и использования приложений для реализации блочных шифров.

1. **Задание**

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. 6.6.

Приложение 2 должно реализовывать алгоритм RC4 в соответствии с вариантом из табл. 6.7, а также дополнительно выполнять оценку скорости выполнения операций генерации ПСП.

1. **Ход работы**

В соответствии с заданиями, необходимо было реализовать генерацию сверхвозрастающей последовательности (в простейшем случае принимается z = 6 (для кодировки Base64) и z = 8 (для кодировки ASCII)), вычисление нормальной последовательности (открытого ключа), зашифрование сообщения, состоящего из собственных фамилии, имени и отчества, расшифрование сообщения, оценку времени выполнения операций зашифрования и расшифрования. Для реализации всех этих функций был разработан класс RanceCipher, представленный на рисунке 3.1.

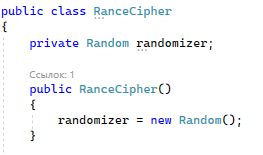


Рисунок 3.1 – Класс RanceCipher

В этом классе были реализованы функции для генерации сверхвозрастающей последовательности (закрытого ключа) и для генерации нормальной последовательности (открытого ключа). Эти функции представлены на рисунках 3.2 – 3.3.

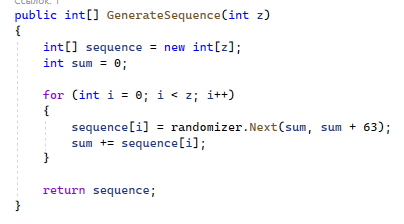


Рисунок 3.2 – Функция GenerateSuperincreasingSequence

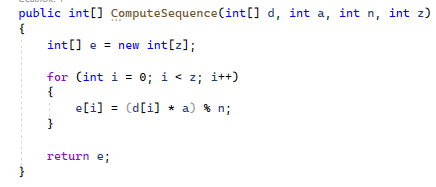


Рисунок 3.3 – Функция ComputeNormalSequence

А для шифрования и расшифрования сообщения были разработаны функции Encrypt() и Decrypt(), представленные на рисунках 3.4 – 3.5.

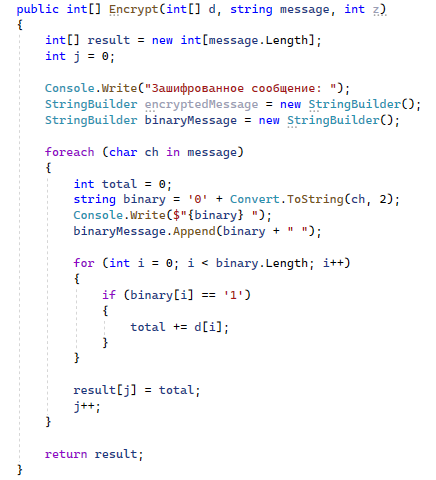


Рисунок 3.4 – Функция Encrypt

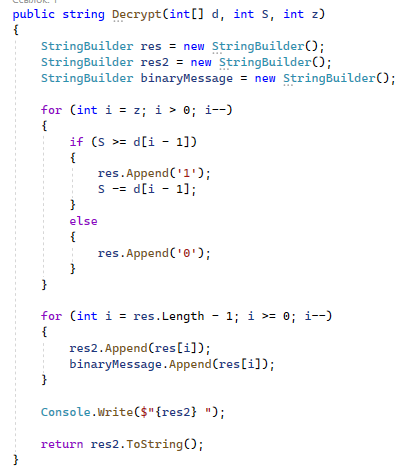


Рисунок 3.5 – Функция Decrypt

В результате, при сгенерированных *d* и *e* с помощью разработанных выше функций, *M* = «Budanowa Ksenya Andreevna», *n* = 8, *a* = 31, получим следующий вывод, представленный на рисунке 3.6.

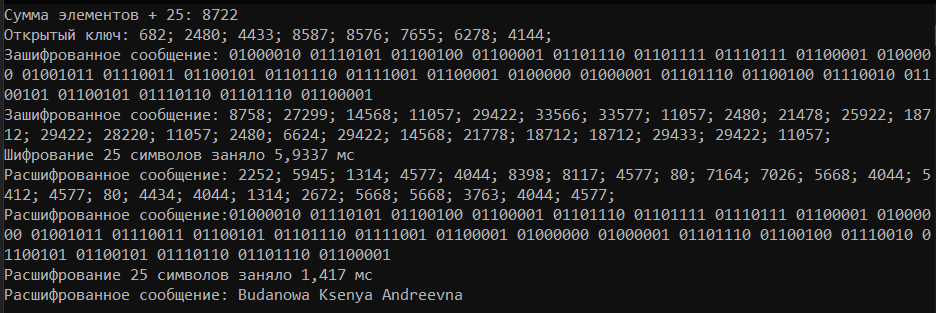


Рисунок 3.6 – Результат работы класса RanceCipher

Также, надо было оценить скорость выполнения операций шифрования и дешифрования. Результаты мы можем увидеть на рисунках 3.7 – 3.8.

Рисунок 3.7 – Оценка скорости шифрования

Рисунок 3.8 – Оценка скорости расшифрования

**Вывод**

В ходе лабораторной работы были изучены и приобретены практические навыки разработки и использования приложений для реализации ассиметричных шифров.

Также было разработано авторское приложение в соответствии с целью лабораторной работы.