БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

ОТЧЕТ ПО КРИПТОГРАФИЧЕСКИМ МЕТОДАМ

студента 2 курса 13 группы

Лабораторная работа №2

Вариант 11

Преподаватель

Ярошеня Ю.С.

Минск 2020

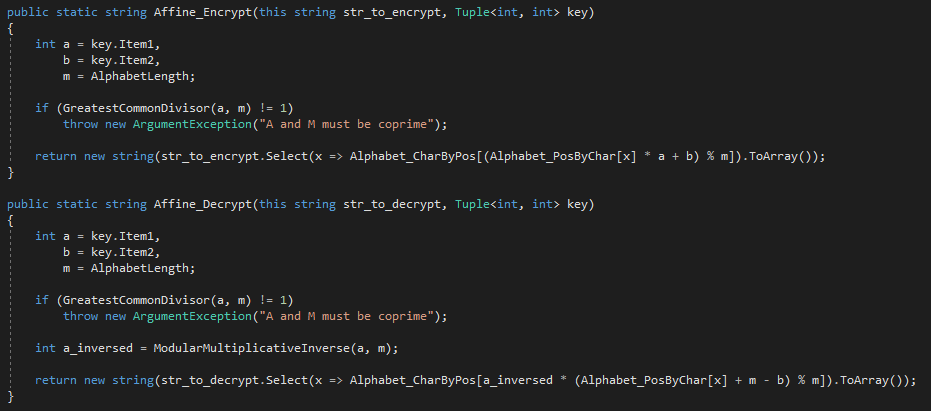
Задание 1

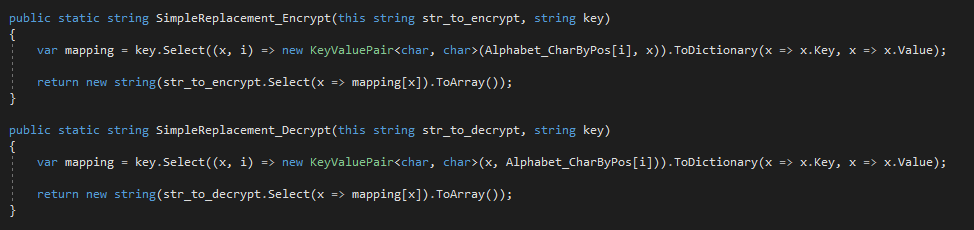
В первом задании нужно было реализовать шифрование/дешифрование с ключами следующих шифров:

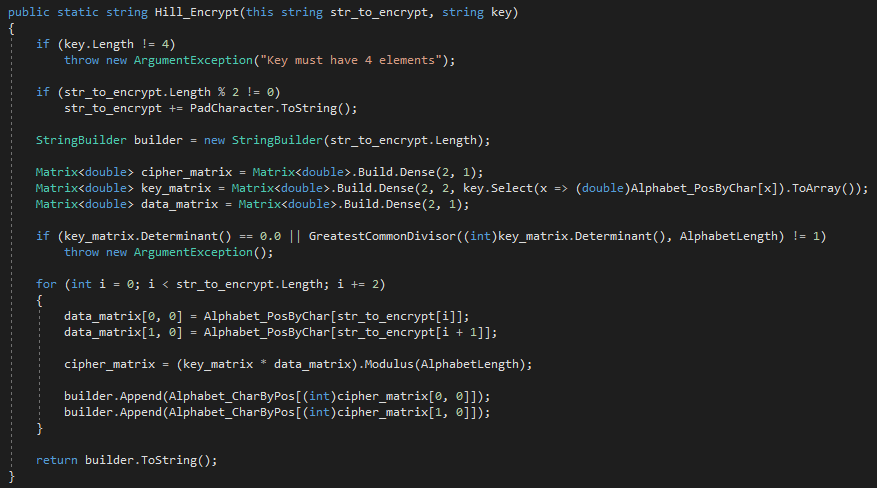
* Аффинный
* Простой замены
* Хилла

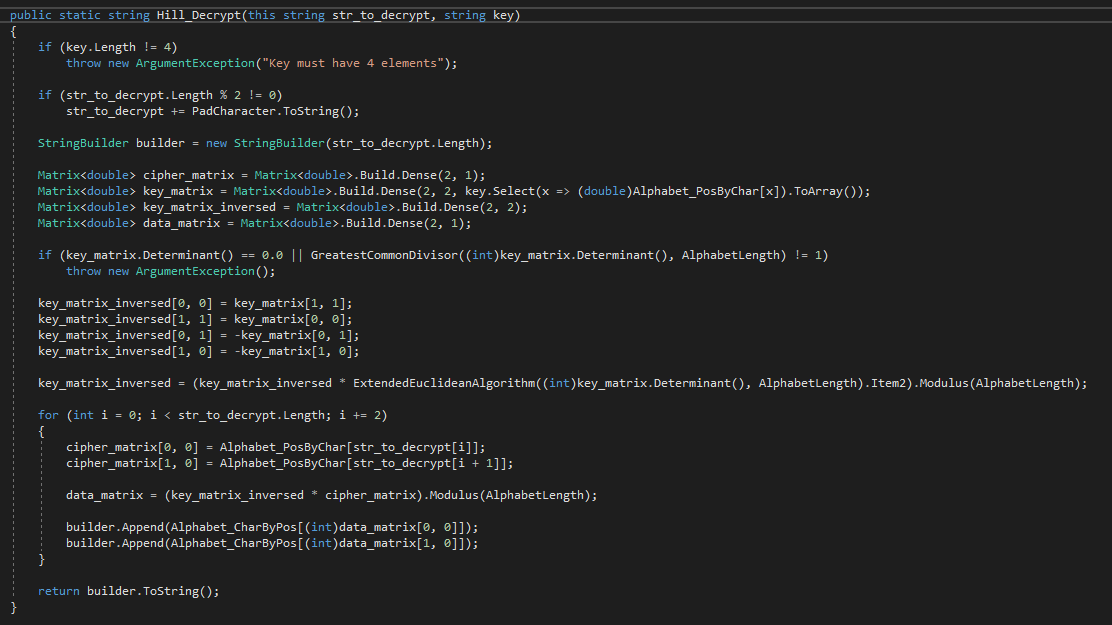
Задание выполнялось на языке C#, использовалась библиотека MathNet.

Реализация:

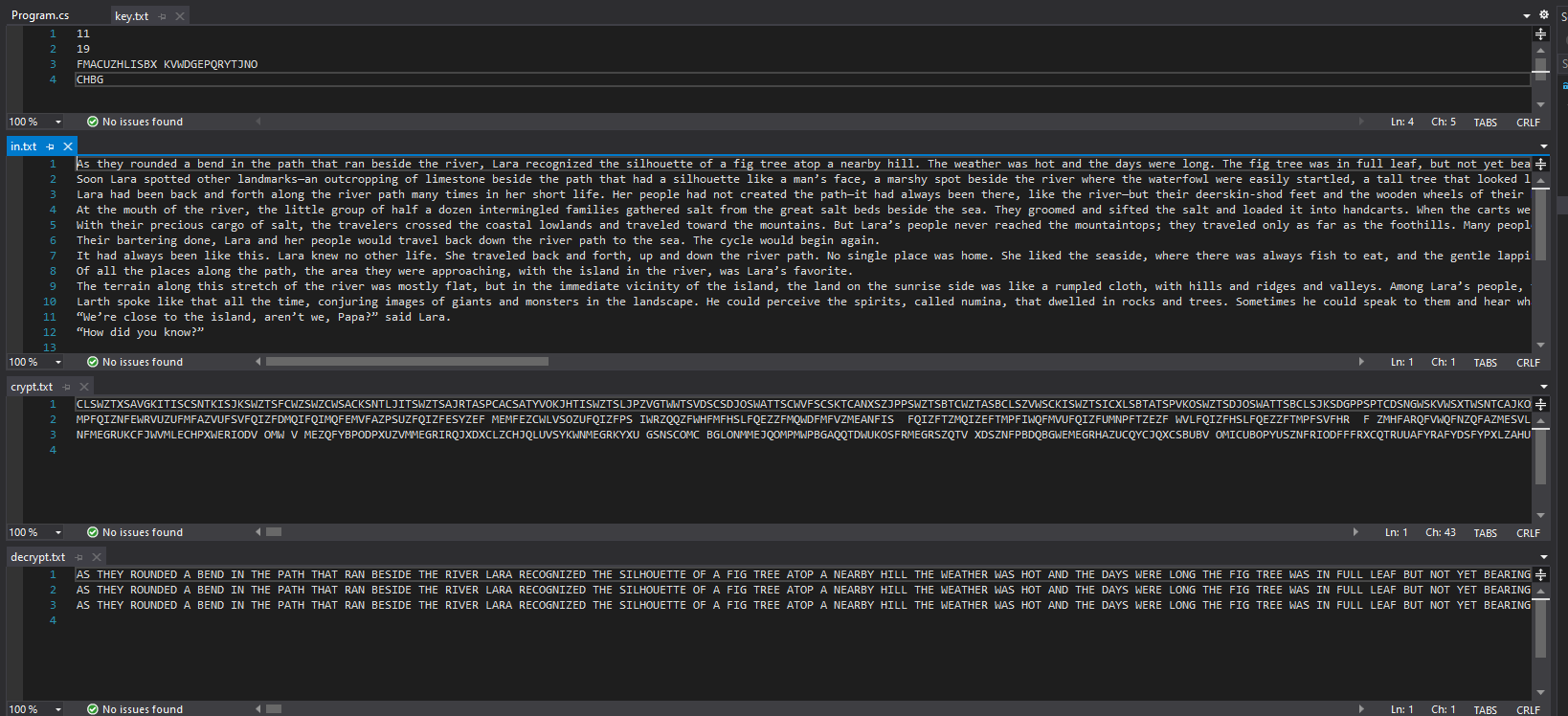








Пример работы:



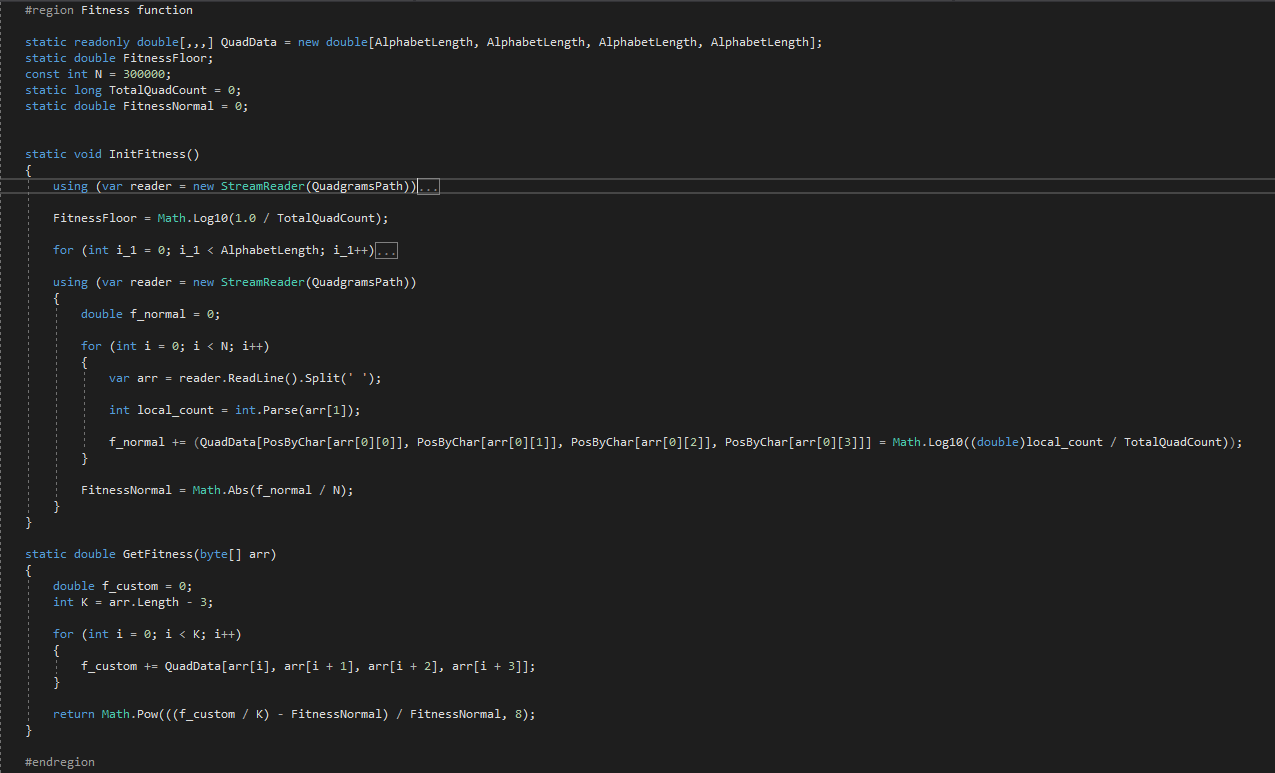
Задание 2

Во втором задании нужно было произвести взлом своих шифров. Аффинный и Хилла я взламывал полным перебором, а для шифра простой замены реализовал генетический алгоритм. Фитнесс функцию из генетического алгоритма позже успешно использовал в переборах Аффинного/Хилла.

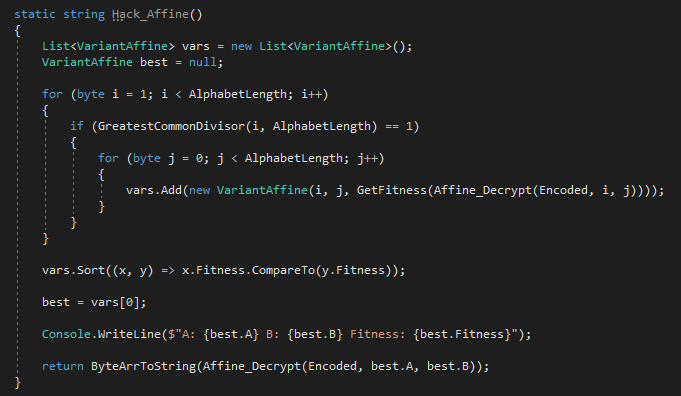
Идею о генетическом алгоритме брал отсюда: <https://planetcalc.com/8047/>. Фитнесс-функция основывается на частотном анализе квадграмм: <https://planetcalc.com/8045/>.

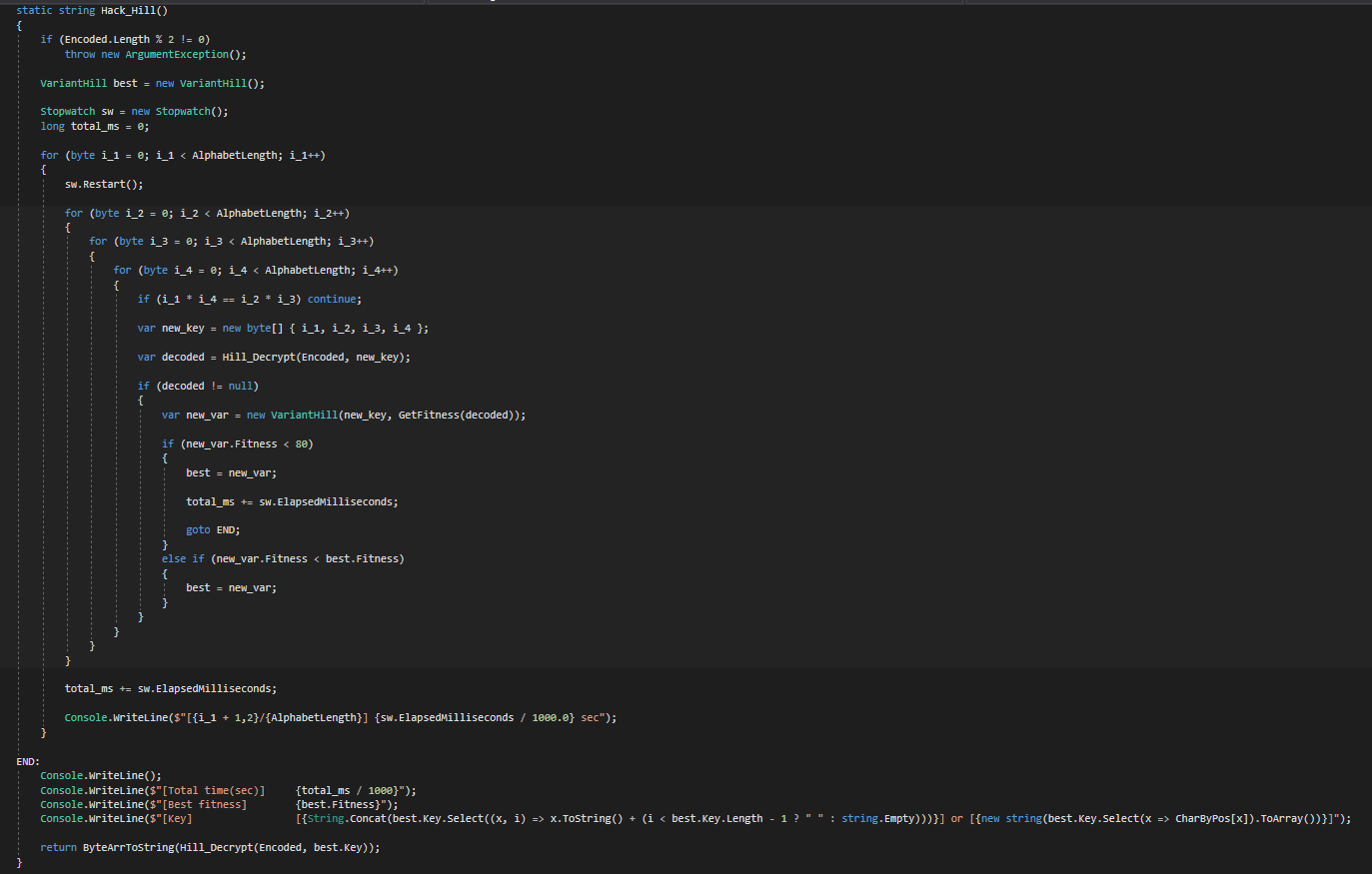
Во многих источниках упоминается что именно она лучше всего подходит для взлома небольших текстов и даже фраз.

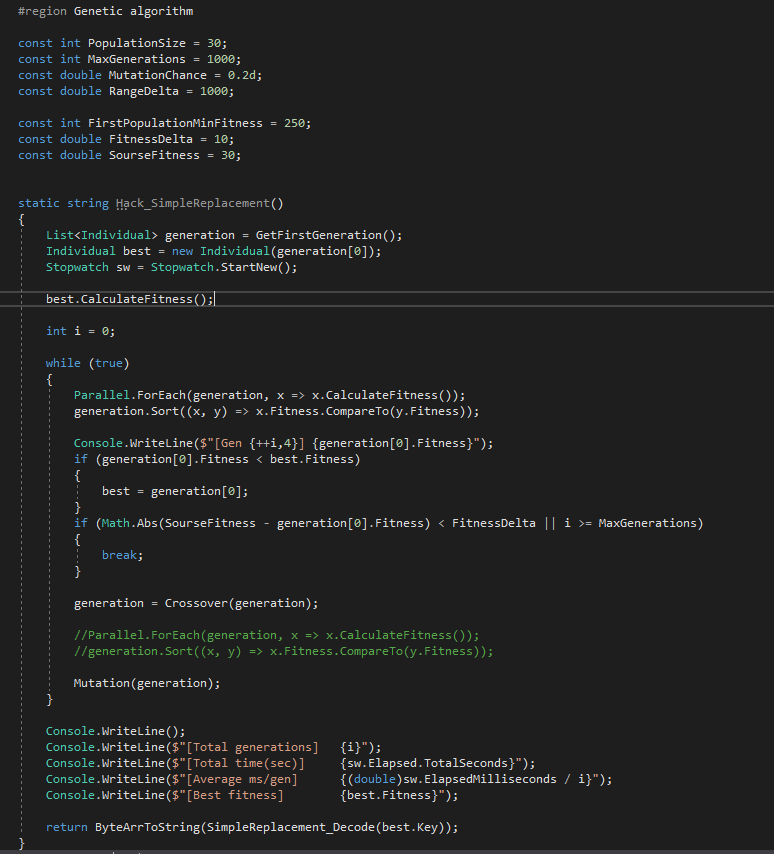
Фитнесс-функция:



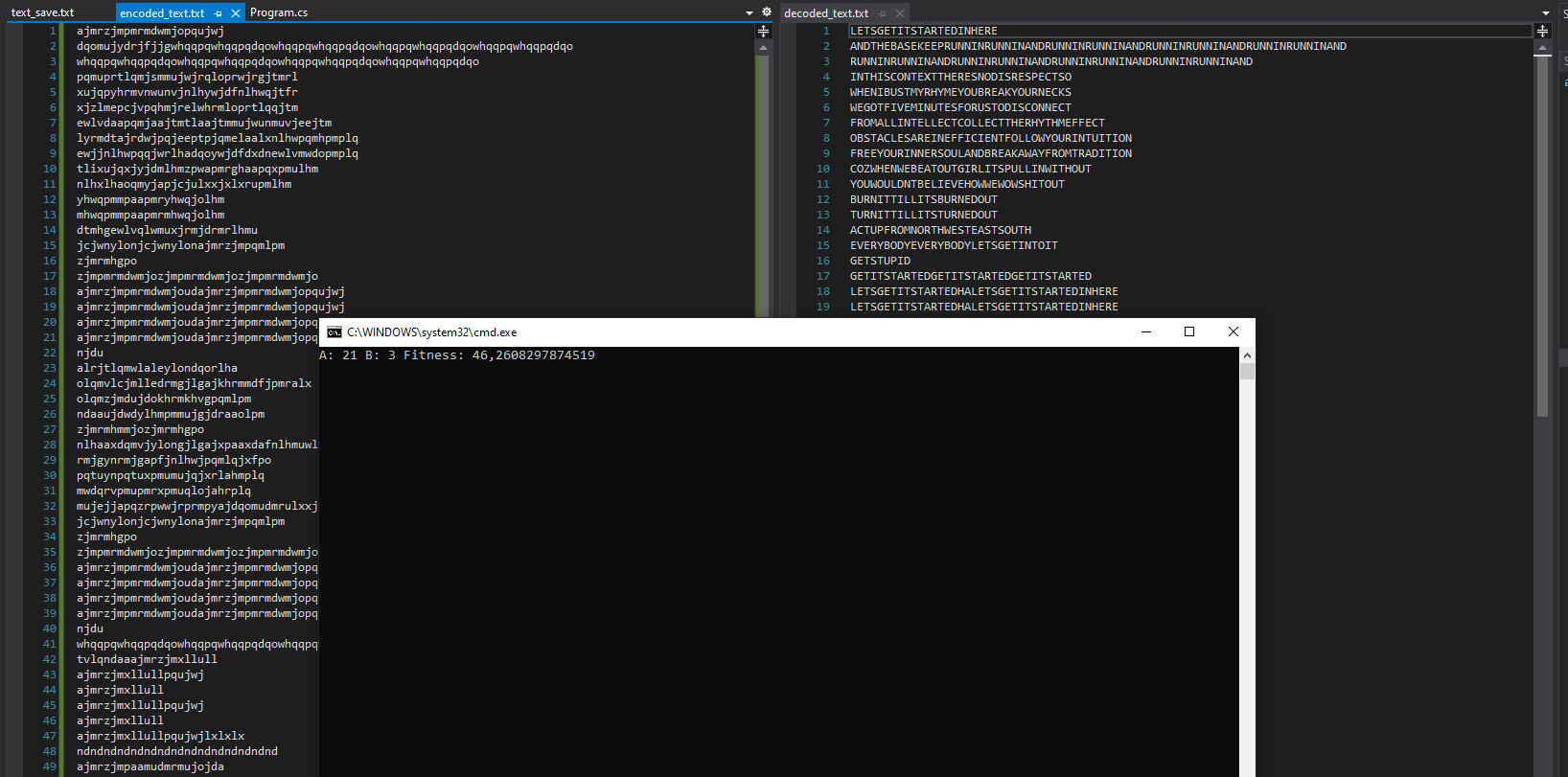
Взломы:

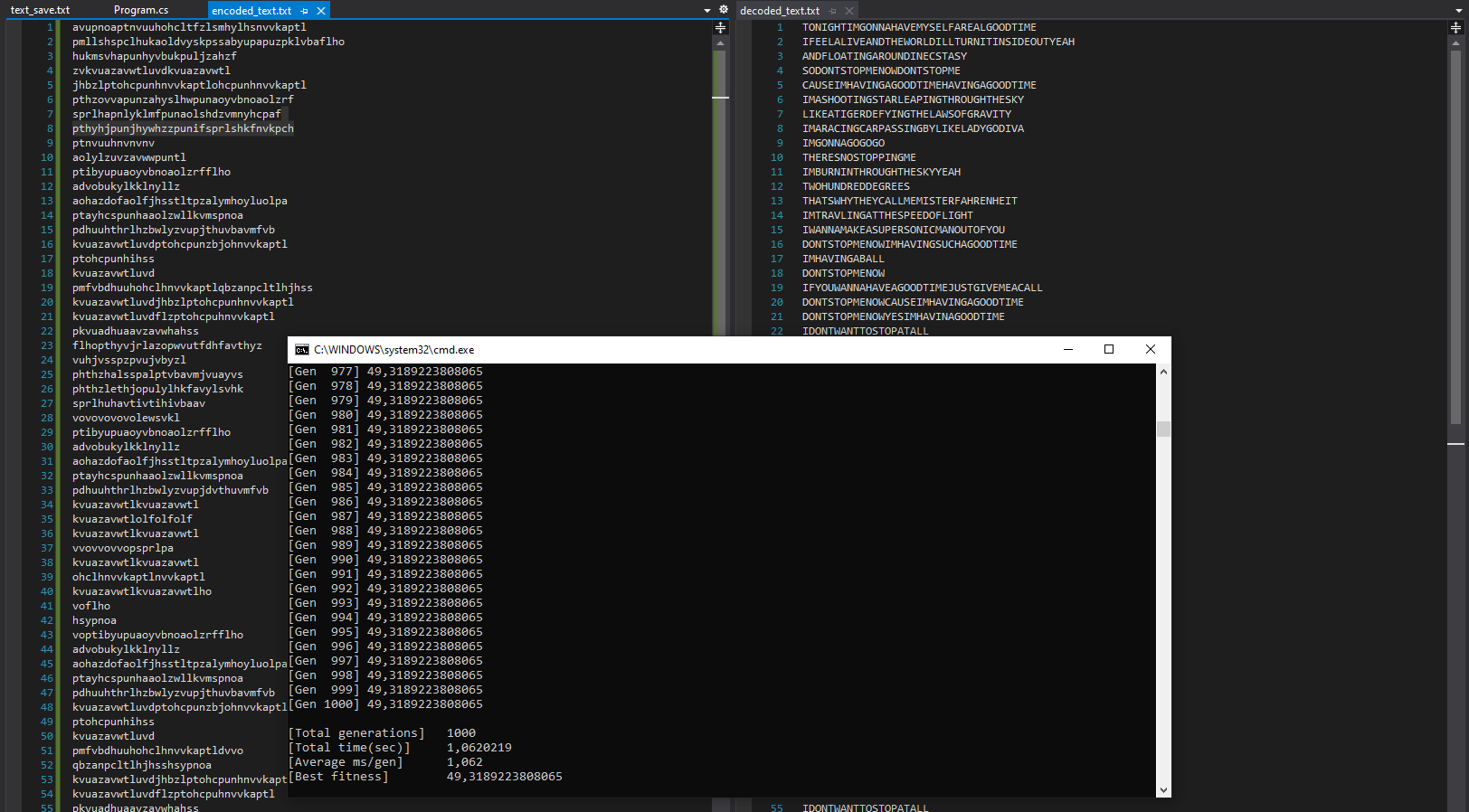


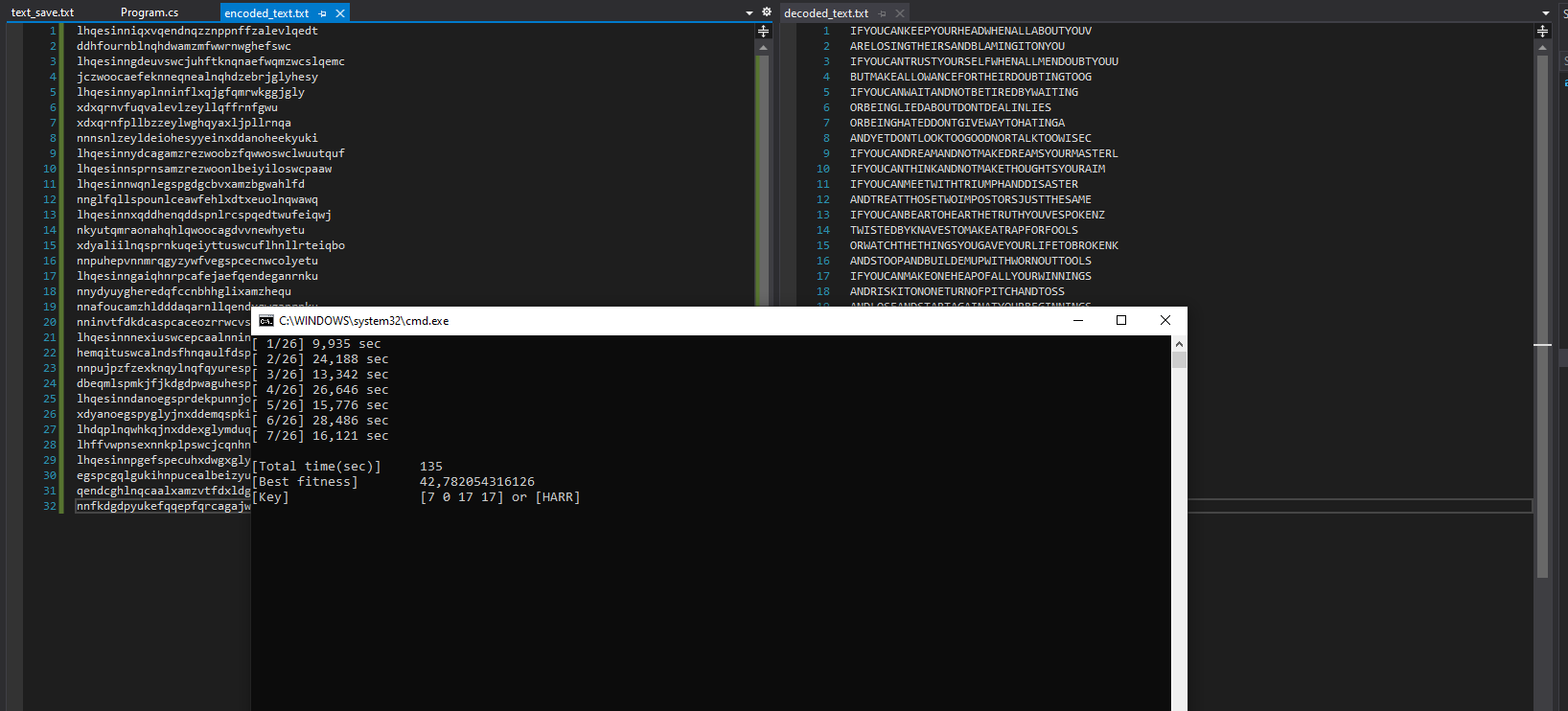




Примеры работы:







Можно видеть, что значения фитнесс-функции у расшифрованных текстов < 50, что в моей реализации означает нормальный английский текст. При значениях > 70 текст сложно читается, но допустим для ручной расшифровки, а значения >90 говорят что скорее всего это не английский текст. Для генетического алгоритма может потребоваться многократный перезапуск, т.к. первое поколение генерируется по большей части случайно и может не дать “хороших” результатов