Министерство НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

Национальный исследовательский университет ИТМО

**факультет безопасности информационных технологий**

**Основы стеганографии**

Лабораторная работа №1

«Основы текстовой стеганографии»

Работу выполнил:

Студент группы:N3351   
Фам Х.Х.



Работу проверил:

ассистент ФБИТ,

Давыдов В. В.



Санкт-Петербург, 2020

**Цель работы:**

Целью данной лабораторной работы :

* Применение текстовых стеганографических методов для сокрытия
* Извлечение сообщения из стегоконтейнера
* Анализ исходного текста и стегоконтейнера.

**Теоретическая часть:**

Стеганография -Cпособ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения). Этот термин ввёл в 1499 году аббат бенедиктинского монастыря Св. Мартина в Шпонгейме Иоганн Тритемий в своём трактате «Стеганография», зашифрованном под магическую книгу. В данной лабораторной работе были рассмотрены следующие 3 алгоритма:

1. Метод замены символов (метод знаков одинакового начертания);
2. Метод с использованием пробелов (метод хвостовых пробелов);
3. Метод с добавлением служебных символов.

Метод знаков одинакового начертания предполагает подмену (бит 1) или отказ от такой подмены (бит 0) русского символа латинским того же начертания. Например, латинская “c” на кириллическую “c”. В моем случае была реализована замена букв с и р .

Метод хвостовых пробелов предполагает дописывание в конце каждой строки файла-контейнера одного пробела, в случае кодирования единичного бита стеганосообщения. Если нужно закодировать нулевой бит, пробел в конце строки не дописывается.

Метод с добавление служебных символов предполагает добавление служебных символов или подмену одних служебных символов на другие. Кодирование осуществляется таким же образом, как описано выше.

Для того, чтобы зашифровать исходное сообщение, оно преобразуется в двоичный код. Далее двоичная последовательность записывается одним из указанных выше методом. Извлечение информации происходит следующим образом: исходя из выбранного метода текстовый контейнер считывается и записывает полученную последовательность битов. Далее двоичный код преобразуется в зашифрованное сообщение.

**Практическая часть:**

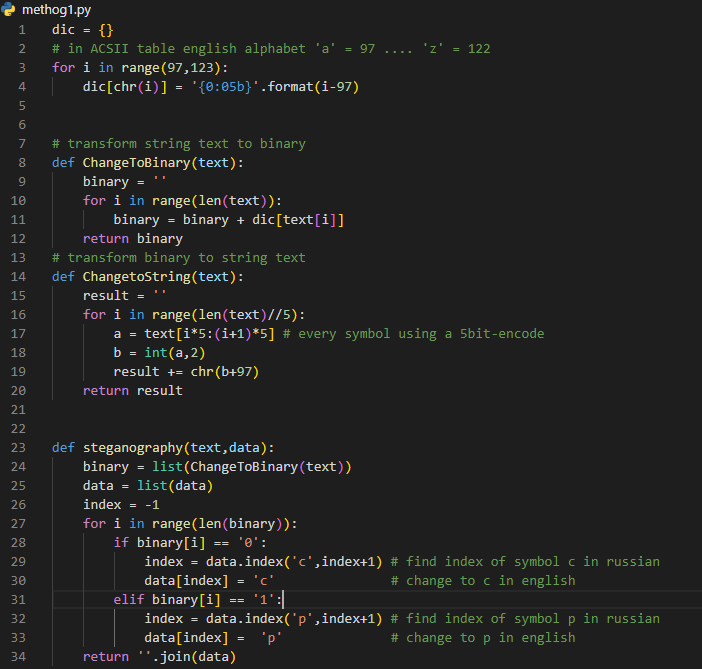
Исходным контейнером в моей работе является рассказ А. П. Чехова «Агафья» состоящий из 19271 символа в кодировке UTF-8.

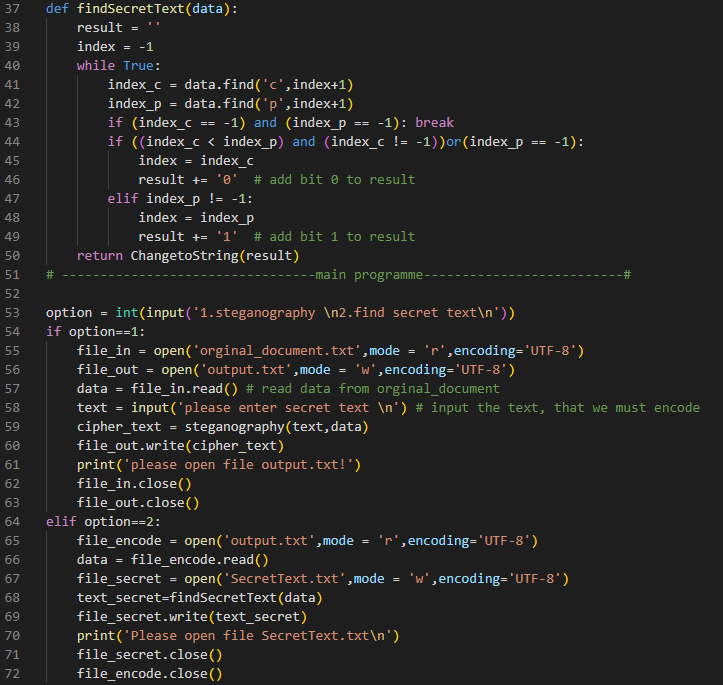
Все алгоритмы были написаны на языке Python. Для каждого метода был написан отдельный файл.

Далее следуют три файла methog1.py, methog2.py и methog3.py, отвечающие за первый, второй и третий методы соответственно. Каждый из скриптов принимает ключи и аргументы. При передаче “1” скрипт будет работать в режиме шифрования. В режиме шифрования нужно один файл становится контейнером(orginal\_document.txt), а во второй происходит запись(output.txt). Ключ “2” нужен для режима дешифрования.

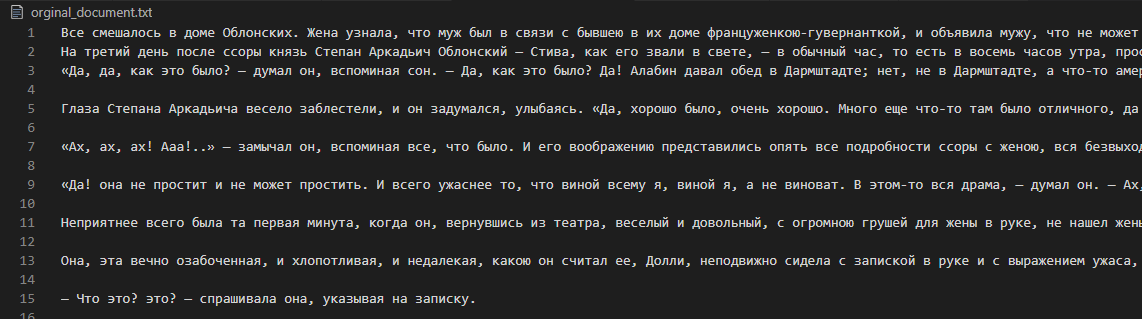
**Метод замены символов (метод знаков одинакового начертания)**

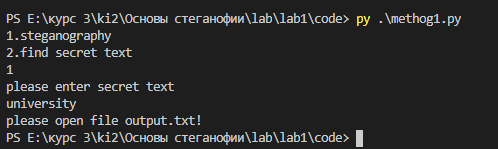
В файле methog1.py происходит посимвольное считывание исходного контейнера и посимвольная запись в файл. Шифрование и извлечение информации происходит описанным выше способом. В моем случае была реализована замена букв с и р .



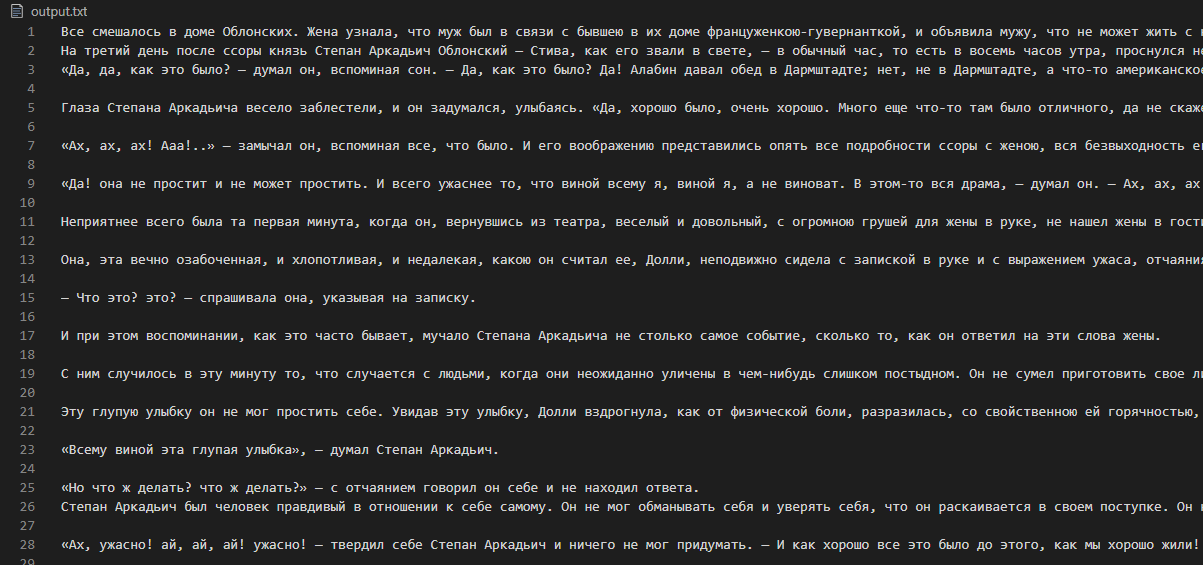


**File orginal\_document.txt(input)**

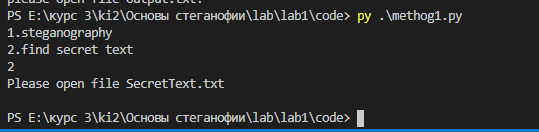


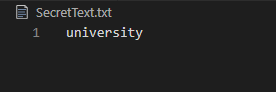


**File output.txt**



**File Secret.txt**

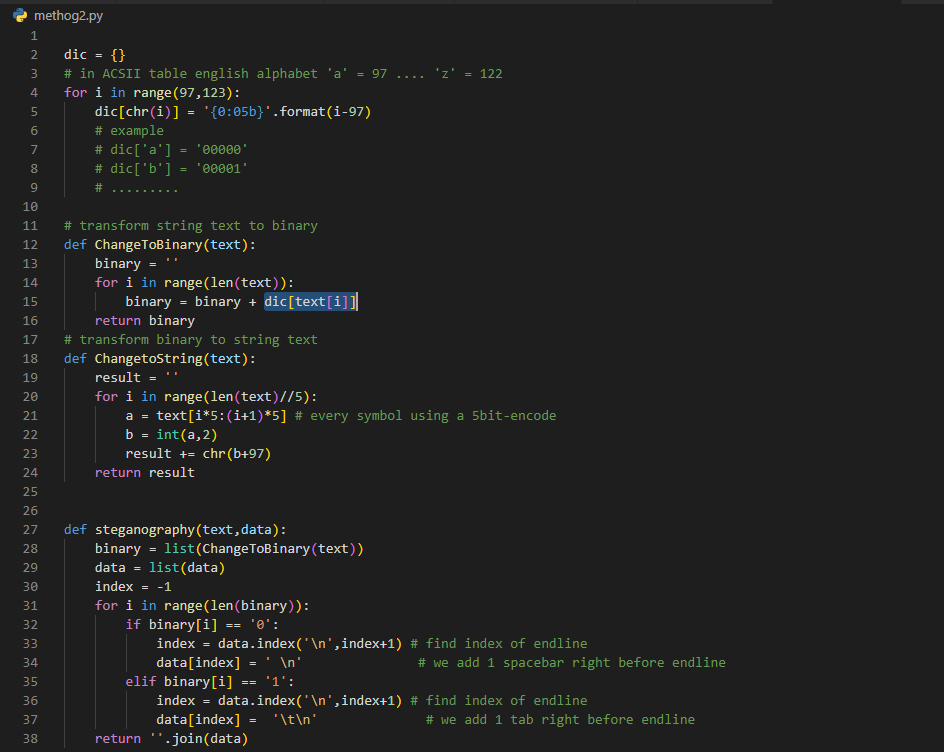


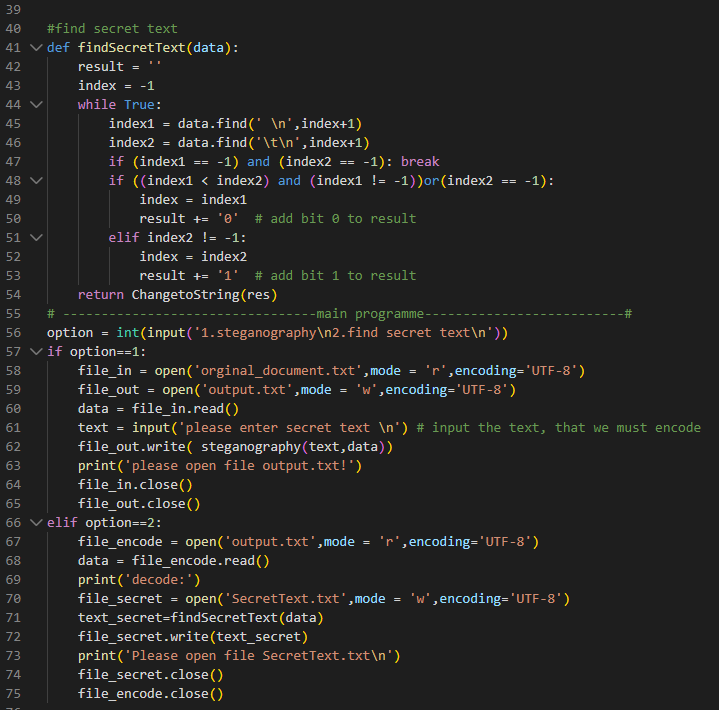


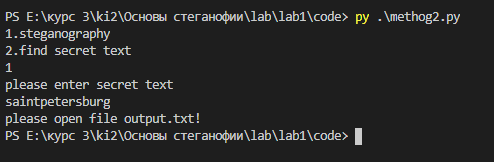
**Метод с использованием пробелов**

В файле methog2.py происходит построковое считывание исходного файла и последующая запись с добавлением или добавлением ”\t” в конце строки.

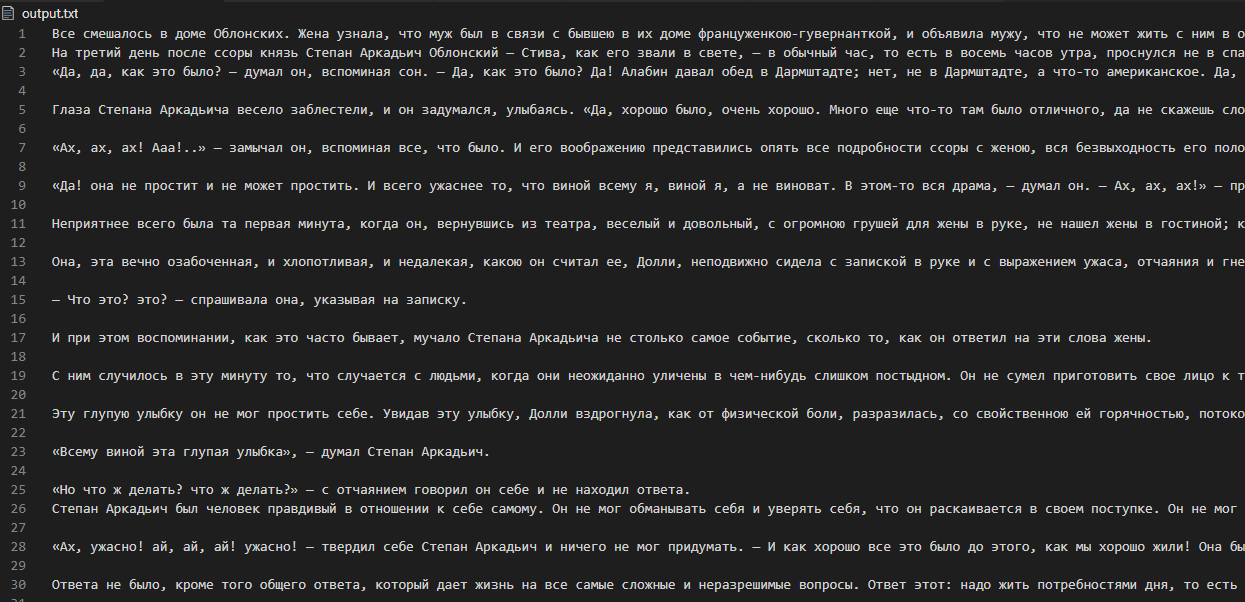
Код:

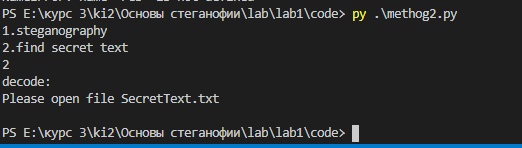




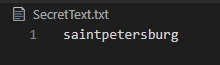


**File output.txt**



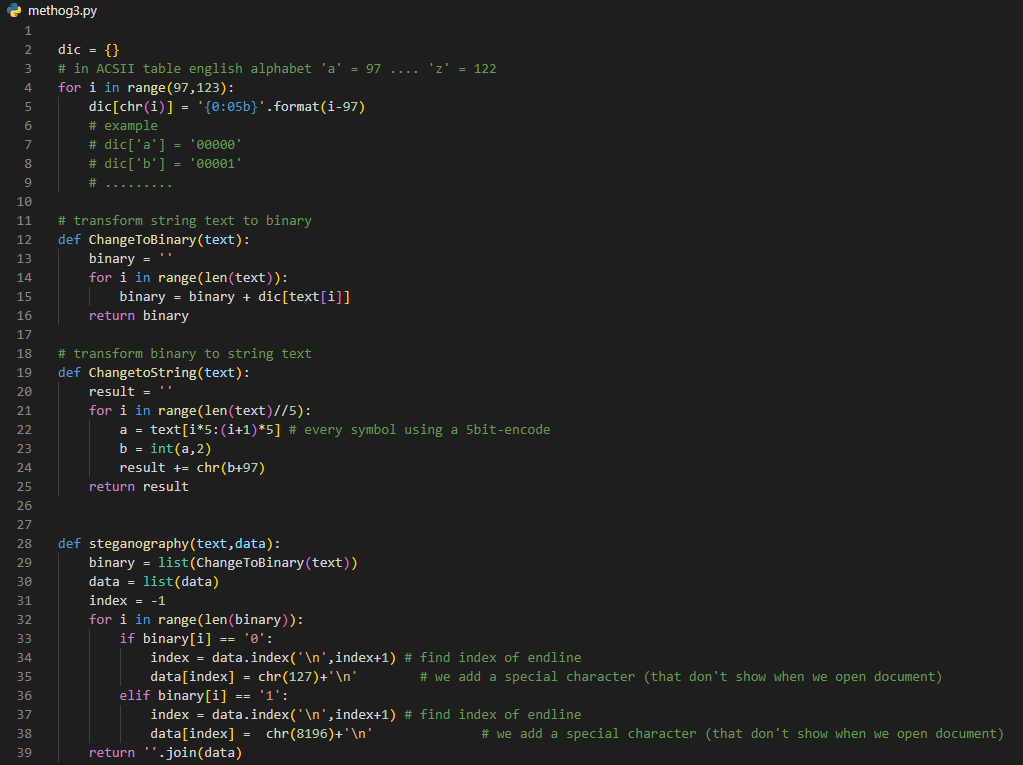


**File SecretText.txt**



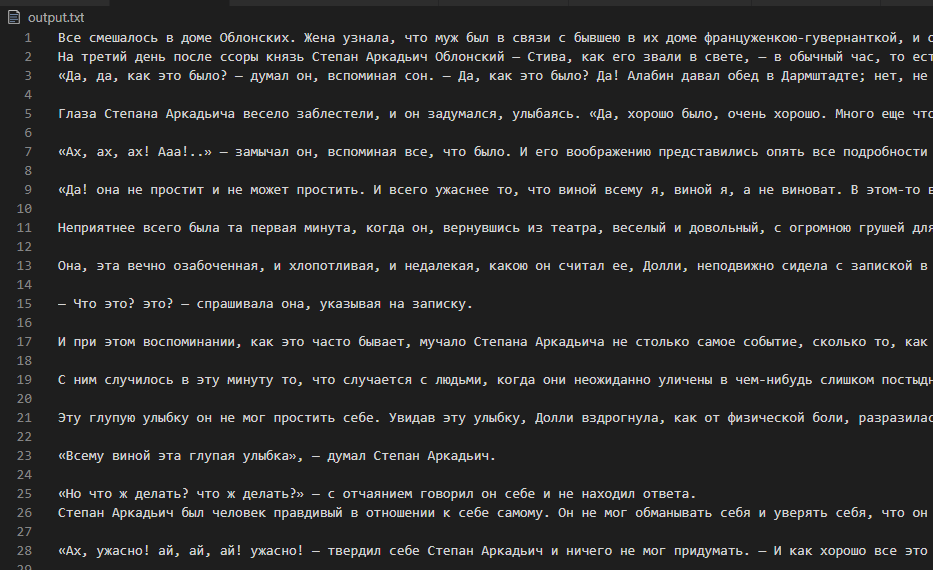
**Метод с добавлением служебных символов**

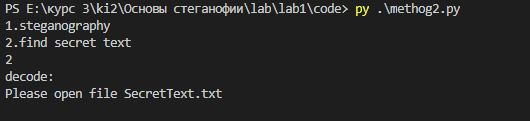
В файле methog3.py также реализовано посимвольное чтение и последующее посимвольная запись с добавление особеных символов



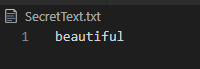


**File output.txt**





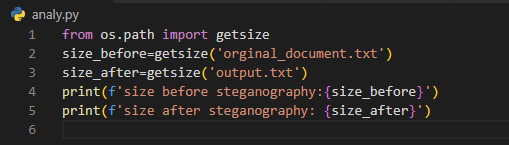
**File SecretText.txt**



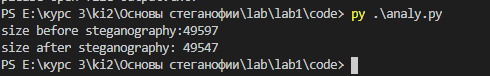
**Проведение экспертной оценки:**

Также мною был написан файл оценщик analy.py. Этот скрипт сравнивает два файла до вставки сообщения и после – выводит размер каждого файла.

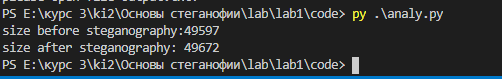
**File analy.py:**



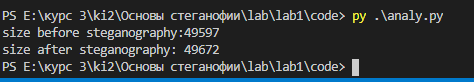
**Метод замены символов**



**Метод с добавлением служебных символов**



**Метод с добавлением служебных символов:**



Можно сделать вывод, что в первых двух случаях встраивание целесообразно, так как текст сам по себе весит внушительное количество байт, из-за чего сообщение скрыто, а вот в третьем случае – нет. Это произошло потому, что изменяются не только необходимые символы, но и все последующие, чтобы обеспечить визуальную незаметность сообщения в стегоконтейнере. К сожалению, размер файла при этом сильно меняется.

Если для просмотра сообщения пользоваться программой, которая не поддерживает отображение всех знаков, то во всех случаях обнаружить сообщение крайне сложно. Если не знать наверняка, что в тексте что-то содержится, то неподготовленный человек ничего не обнаружит. Если же использовать программу, которая позволит отображать все символы, то первый случай сразу же вызовет подозрения, во втором, если приглядываться, тоже можно понять, что что-то не так, а вот в третьем все не так просто. Создается впечатление, что это просто такой стиль письма. Но если иметь исходный текст и стегоконтейнер, полученный с помощью третьего метода, то можно с легкостью сделать вывод, что что-то было встроено, посмотрев на размеры файлов. Этот факт стал для меня решающим при проведении экспертной оценки – данный метод скрытия я не могу назвать успешным.

**Выводы:**

При выполнении данной лабораторной работы мною были изучены основные методы текстовой стеганографии. Я научился применять их и проводить последующую оценку их применению. По результатам работы были сделаны следующие выводы:

Метод замены символов одинакового начертания легко обнаружим при использовании многофункциональных текстовых редакторов, метод хвостовых пробелов трудно заметить даже при использовании таких редакторов, а реализованный мною метод добавления служебных символов вовсе не целесообразен, хоть и обнаружить его при отсутствии исходного текста довольно сложно.

Если я захочу в будущем поместить стего в текст, то, скорее всего, воспользуюсь метод знаков одинакового начертания ,который предполагает замену символа из текста на его аналог из другого языка, которые выглядит точно так же, но имеет другую кодировку

**Список использованной литературы:**

1. <https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%B3%D0%B0%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F>
2. <http://www.nestego.ru/2012/05/blog-post_05.html>
3. http://www.nestego.ru/2012/05/blog-post\_03.html