Отчёт по лабораторной работе №8

Попов Олег Павлович

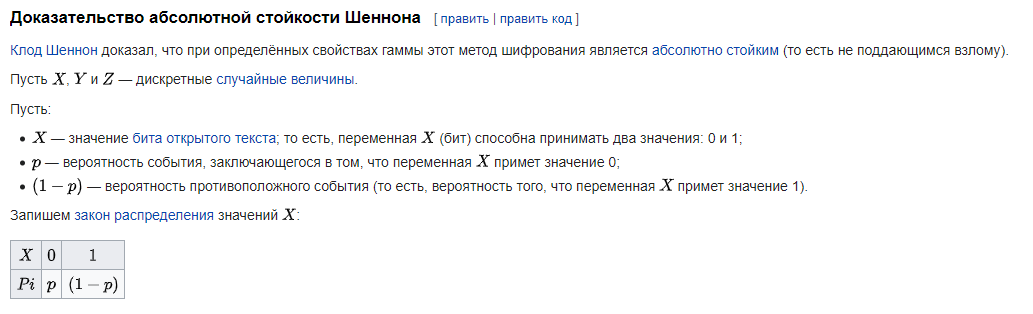
Содержание

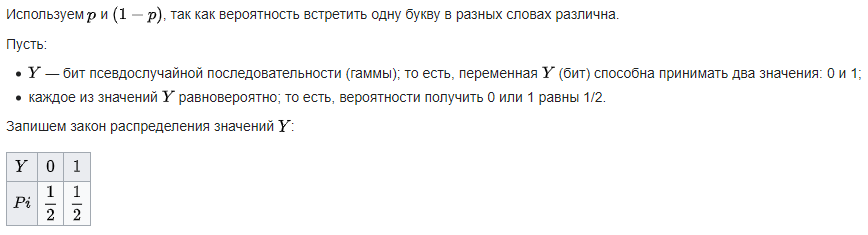
# Цель работы

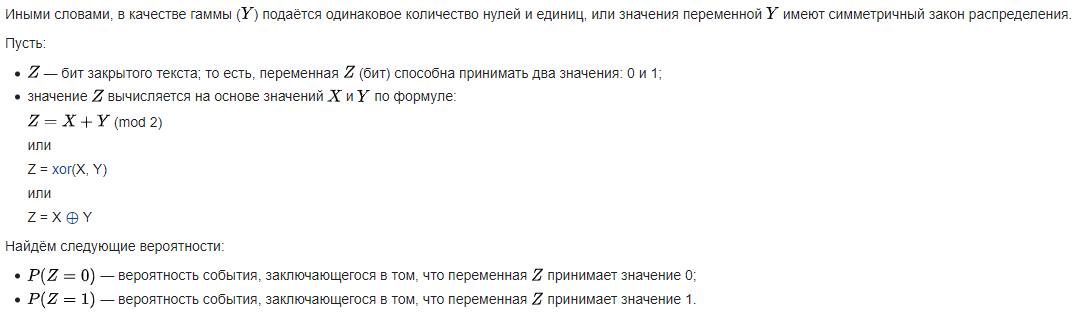
Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

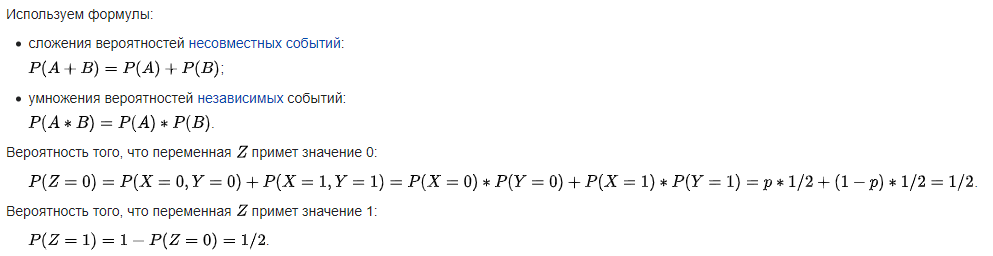
# Выполнение лабораторной работы

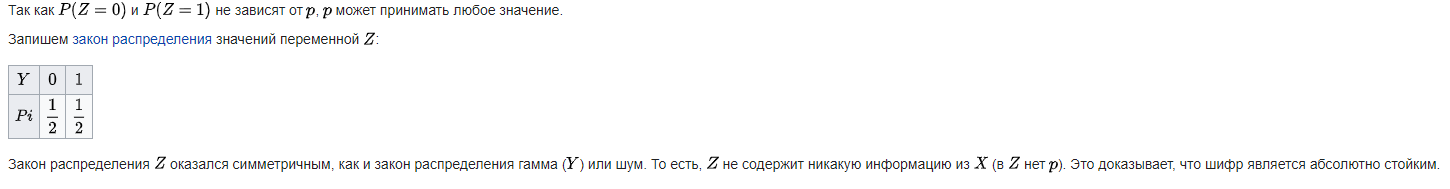
Перед реализацией новой функции в приложении нужно изучить теорию:





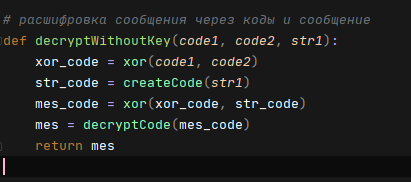






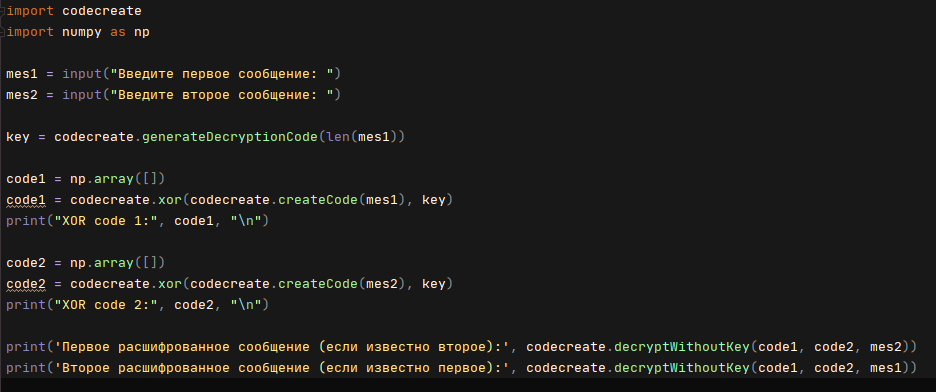
В итоге можно сделать вывод, что расшифровать код невозможно без ключа или одного из исходных текстов сообщений. Значит, можно реализовать функцию, которая будет расшифровывать сообщение с помощью кодов всех сообщений и текста одного из сообщений.

Функция:



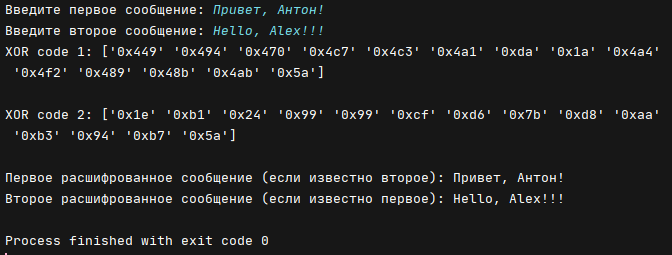
Эта функция основана на функциях, написанных в седьмой лабораторной: сначала через xor получаем код, потом переводим сообщение в его исходный код, снова перемножаем коды через xor и дешфруем полученный в итоге код.

Код main:



Сначала на вход подаются две строки, генерируется ключ, строки шифруются через ключ и в конце через написанную функцию переводим строки из шифрованных кодов.

Вывод:



Как мы видим, из зашифрованных кодов и известного сообщения можно найти второе сообщение.

# Выводы

В ходе данной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.