Лабораторная работа №3

Дисциплина: Математические основы защиты информации и информационной безопасности

Аветисян Давид Артурович

Содержание

# 1 Цель работы

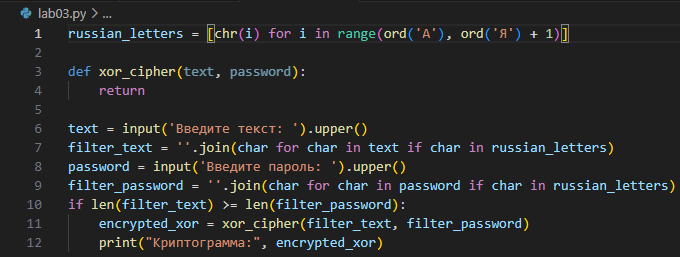
Познакомиться с шифрованием гаммированием.

# 2 Задание

1. Реализовать шифрование гаммированием.

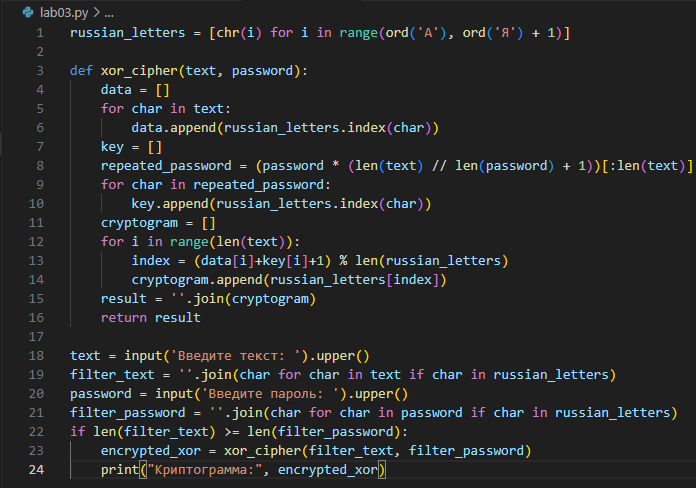
# 3 Выполнение лабораторной работы

1. Я решил реализовать шифрование гаммированием на языке Python. Сначала я задал матрицу с русскими буквами, а также реализовал запрос текста и пароля у пользователя. Все буквы в тексте и пароля я сделал заглавными, а затем я отфильтровал текст и пароль, оставив в нём только русские буквы.



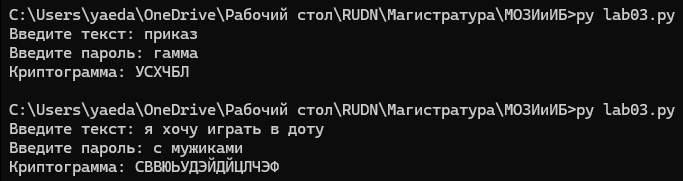
Запрос текста и пароля у пользователя

1. Далее я реализовал само шифрование гаммированием. Я задал три матрицы: для текста, для гаммы и для результата. Пароль я увеличил повторением до длины текста, как указано в теории к лабораторной работе №3. Далее я, опираясь на матрицу с русскими буквами, заполнил первые две матрицы значениями, на которых стоят буквы из текста и пароля соответственно. А уже затем я заполнял третью матрицу складывая значения из первой и второй матрицы и находя остаток от деления. После чего я преобразовал каждое значение из третьей матрицы в букву, исходя из матрицы с русскими буквами, и вывел пользователю.



Шифрование гаммированием на языке Python

1. Далее я запустил два теста через командную строку. Один тест как в теории к лабораторной работе №3. Второй тест для дополнительной проверки. Шифрование совпало с тестом в лабораторной работе №3, и реализовано верно.



Проверка метода шифрования гаммированием

# 4 Выводы

Я реализовал шифрование гаммированием.