Лабораторная работа 3

Попов Дмитрий Павлович, НФИмд-01-23

Содержание

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

дисциплина: Математические основы защиты информации и информационной безопасности

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИмд-01-23

МОСКВА

2023 г.

# 1 Цель работы

Целью данной работы является приобретение практических навыков в шифровании гаммированием.[1]

# 2 Выполнение лабораторной работы

Требуется реализовать:

1. Шифрование гаммированием конечной гаммой

## 2.1 Шифрование гаммированием конечной гаммой

Гаммирование — процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, т.е. псевдослучайной последовательности (ПСП) с выходов генератора G. Псевдослучайная последовательность по своим статистическим свойствам неотличима от случайной последовательности, но является детерминированной, т.е. известен алгоритм ее формирования.

Входной текст преобразовывается в номера букв из алфавита, соответствующим буквам фразы, затем так же преобразовывается гамма. Далее используется операция побитового сложения по модулю, равному длине алфавита. Получаем итоговую последовательность чисел, которая переводится в буквы в соответствии с алфавитом и получаем конечную криптограмму.

Чтобы реализовать программу был написал код на Python(fig. 1)(fig. 2):

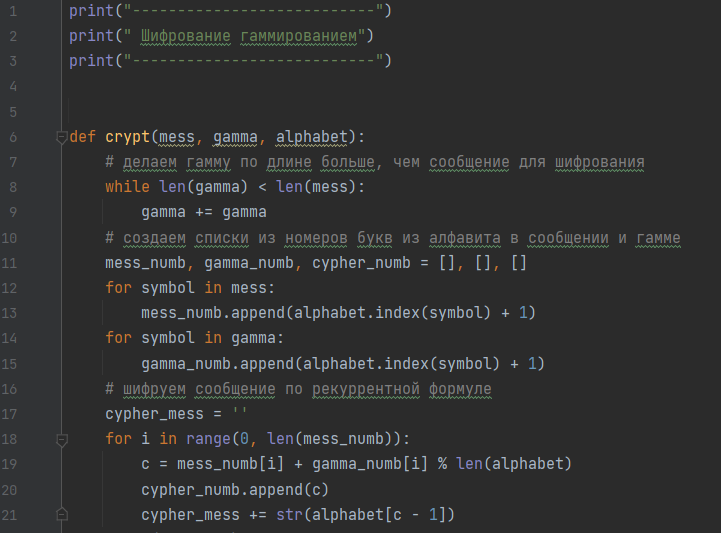


Figure 1: gamma1

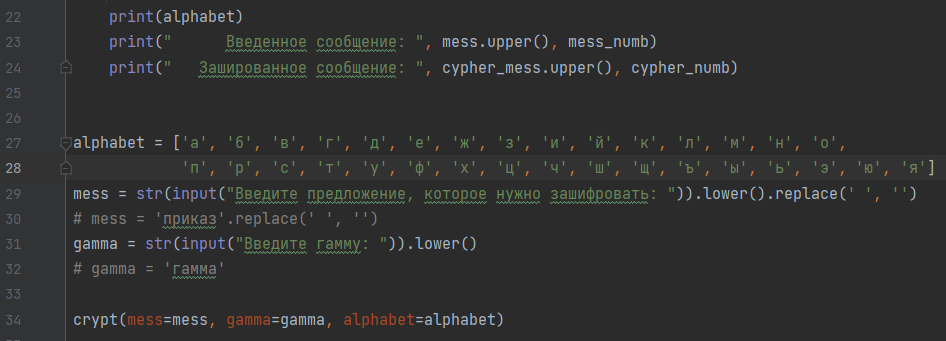


Figure 2: gamma2

Затем я запустил программу, ввел гамму и исходное сообщение. Получил зашифрованное сообщение. Вывод работы программы (fig. 3)

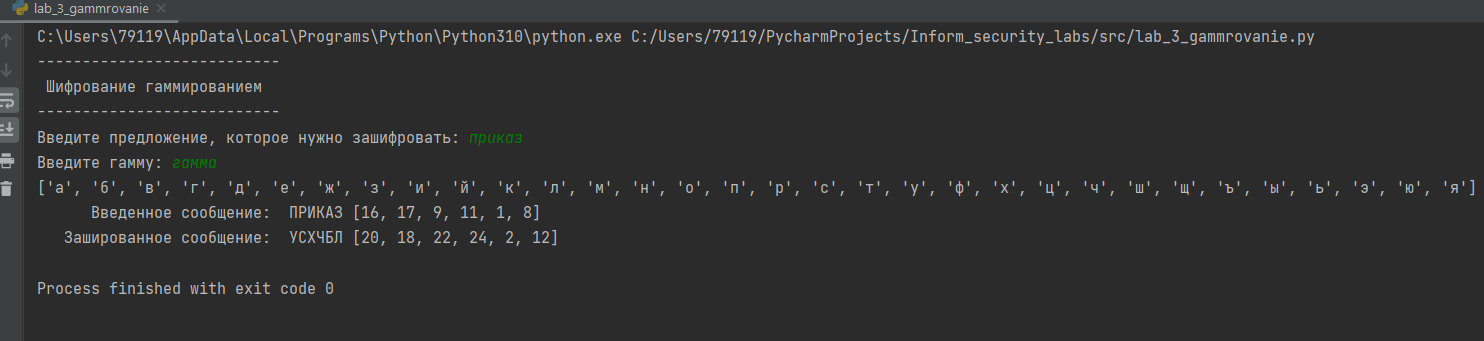


Figure 3: gamma\_out

# 3 Выводы

В результате выполнения работы я освоил на практике применение шифрования с гаммированием конечной гаммой.

# 4 Список литературы

1. Методические материалы курса