Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе №3

Шифрование гаммированием

Терентьев Егор Дмитриевич 1132236902

Содержание

# 1 Цель работы

Освоить на практике шифрование гаммированием.

# 2 Выполнение лабораторной работы

Требуется реализовать:

1. Шифрование гаммированием

## 2.1 Шифрование гаммированием

Шифрование гаммированием - это метод симметричного шифрования, при котором каждый символ или байт исходного сообщения комбинируется с соответствующим символом или байтом ключа (гаммы) с помощью определенной операции, чаще всего XOR.

Основные шаги:

1. Выбор гаммы (ключа): Гамма — это последовательность, которая комбинируется с исходным сообщением. Гамма может быть случайной или генерироваться на основе ключа.
2. Применение гаммы к сообщению: Гамма “наложится” на исходное сообщение. Если гамма короче сообщения, она циклически повторяется.
3. Комбинирование гаммы и сообщения: Наиболее популярная операция для этого — XOR. Если мы говорим о символьном шифровании, то комбинирование может включать в себя сложение (или вычитание для дешифрования) позиций символов в алфавите.
4. Дешифрование: Чтобы дешифровать сообщение, мы применяем ту же операцию комбинирования к зашифрованному сообщению и той же гамме. Если использовалась операция XOR, то повторное применение XOR с той же гаммой вернёт исходное сообщение.

Чтобы реализовать программу был написал след. код на python:

1. Функции получения пар значений ключа и сообщения
2. Функция шифрования, которая берет пары значений и складывает их место в алфавите получая нужную букву шифрования fig. 1.

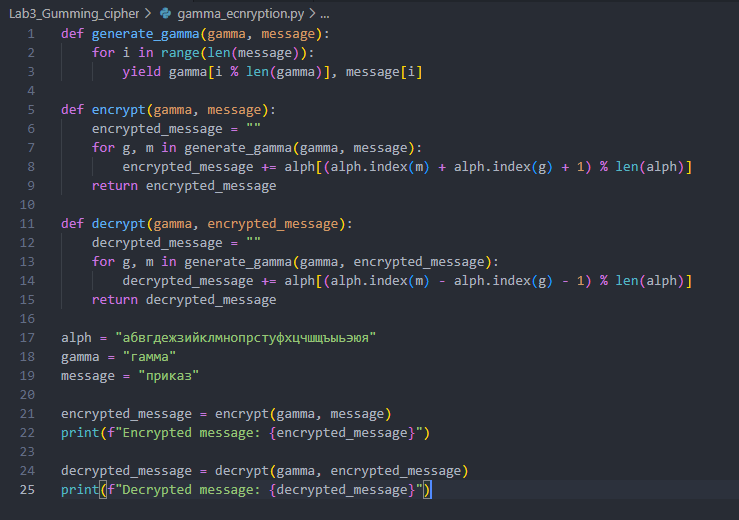


Figure 1: main\_func

Выходные значения программы (пример из методички) fig. 2.

output

Figure 2: output

# 3 Выводы

В результате выполнения работы я освоил на практике применение шифрование гаммированием.

# 4 Список литературы

1. Методические материалы курса