Отчет по лабораторной работе №3

Дисциплина: Математические основы защиты информации и информационной безопасности

Живцова Анна

Содержание

# 1 Цель работы

Изучить алгоритм шифрования гаммированием. Реализовать шифрование с помощью конечной гаммы.

# 2 Задание

Реализовать шифрование с помощью конечной гаммы.

# 3 Теоретическое введение

Известно, что простейшей и наиболее надежной хемой шифрования является схема однократного использования. Однако в данной схеме длина ключа совпадает с длиной передаваемых данных, что затруднительно. Отсюда вытекает идея гаммирования

Гаммирование — это метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Подробнее в источниках [1,2].

В данной работе будем использовать конечную гамму, в которой ключ формируется повторением заданного конечного слова. В таком шифровании из символа исходного текста , которому соответствует символ гаммы , получается зашифрованный символ mod.

# 4 Выполнение лабораторной работы

Для реализации шифрования с помощью гаммирования на языке Python была написанна следующая функция.

def gamma(text, gamma, mod, al):   
 return ''.join([al[(al.index(text[i]) + al.index(gamma[i%len(gamma)]))%mod] for i in range(len(text))])

Тут – это алфавит, – это основание для сложения по модулю, – это исходный текст, а – это строка гаммы (ключ).

Функциональность данной функции была протестирована в среде jupyter notebook (см. рис. 1).



Рис. 1: Тестирование шифрования с помощью гаммирования

# 5 Выводы

В данной работе я изучила алгоритм шифрования гаммированием и реализовала шифрование с помощью конечной гаммы.

# Список литературы

1. Kulyabov D., Korolkova A., Gevorkyan M. Информационная безопасность компьютерных сетей: лабораторные работы. 2015.

2. Самуйлов К.Е. и др. Сети и телекоммуникации : Учебник и практикум. Издательство Юрайт, 2019. С. 1–363.