Отчет по лабораторной работе №3

Дисциплина: Математические основы защиты информации и информационной безопасности

Живцова Анна

Содержание

Список иллюстраций

Список таблиц

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 y_i, которому соответствует символ гаммы g_i, получается зашифрованный символ $c_i = (y_i + g_i) \mathrm{mod} x$.

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
```

Тут *al* – это алфавит, *mod* – это основание для сложения по модулю, *text* – это исходный текст, а *gamma* – это строка гаммы (ключ).

Функциональность данной функции была протестирована в среде jupyter notebook (см. рис. 4.1).

```
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))])
```

```
alphabet = 'а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я'.split(' ')
alphabet_lat = 'a b c d e f g h i j k l m n o p q r s t u v w x y z'.split(' ')
gamma('приказ', 'гамма', 33, alphabet)
```

```
'трхчак'
```

Рис. 4.1: 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.