**Лабораторная работа N° 7**

Информационная безопасность

Леон Фернандо Хосе Фернандо | НПМбд02-20

Оглавление

[**1 Цель работы** 2](#_Toc148661049)

[**2 Теоретическое введение** 2](#_Toc148661050)

[**3** **Выполнение лабораторной работы** 2](#_Toc148661051)

[**4 Выводы** 3](#_Toc148661052)

[**5 Список Литературы** 3](#_Toc148661053)

# **1 Цель работы**

Освоить на практике применение режима однократного гаммирования

# **2 Теоретическое введение**

Гаммирование - наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Основная формула, необходимая для реализации однократного гаммирования:

Ci = Pi XOR Ki, где Ci - i-й символ зашифрованного текста, Pi - i-й символ открытого текста, Ki - i-й символ ключа.

Аналогичным образом можно найти ключ: Ki = Ci XOR Pi.

Необходимые и достаточные условия абсолютной стойкости шифра:

* длина открытого текста равна длине ключа
* ключ должен использоваться однократно
* ключ должен быть полностью случаен

# **Выполнение лабораторной работы**

Код программы

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, линия, белый

Автоматически созданное описание

* In[1]: импорт необходимых библиотек
* In[3]: функция, реализующая сложение по модулю два двух строк
* In[4]: открытый/исходный текст
* In[5]: создание ключа той же длины, что и открытый текст
* In[6]: получение шифротекста с помощью функции, созданной ранее, при

условии, что известны открытый текст и ключ

* In[7]: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ
* In[8]: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

# **4 Выводы**

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

# **5 Список Литературы**

1. Однократное гаммирование [Электронный ресурс]. URL: https://esystem. rudn.ru/pluginfile.php/1651639/mod\_resource/content/2/007-lab\_cryptogamma.pdf.