**Лабораторная работа N° 8**

Информационная безопасность

Леон Фернандо Хосе Фернандо | НПМбд02-20

Оглавление

[**1 Цель работы** 2](#_Toc148662459)

[**2 Теоретическое введение** 2](#_Toc148662460)

[**3 Выполнение лабораторной работы** 2](#_Toc148662461)

[**4 Выводы** 3](#_Toc148662462)

[**5** **Список Литературы** 3](#_Toc148662463)

# **1 Цель работы**

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# **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, t Ci - i-й символ зашифрованного текста, Pi - i-й символ открытого текста, Ki - i-й символ ключа. В данном случае для двух шифротекстов будет две формулы: С 1 = P1 xor K и С2 = P2 xor K, где индексы обозначают первый и второй шифротексты соответственно.

Если нам известны оба шифротекста и один открытый текст, то мы можем найти другой открытый текст, это следует из следующих формул: C1 xor C2 = P1 xor K xor P2 xor K = P1 xor P2, C1 xor C2 xor P1 = P1 xor P2 xor P1 = P2.

# **3 Выполнение лабораторной работы**

Код программы

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, линия, снимок экрана

Автоматически созданное описание

* In[1]: импорт необходимых библиотек
* In[2]: функция, реализующая сложение по модулю два двух строк
* In[11]: открытые/исходные тексты (одинаковой длины)
* In[12]: создание ключа той же длины, что и открытые тексты
* In[13]: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ
* In[14]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны шифротексты и ключ

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

* In[15]: сложение по модулю два двух шифротекстов с помощью функции, созданной ранее
* In[16]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов
* In[17]: получение части первого открытого текста (срез)
* In[18]: получение части второго текста (на тех позициях, на которых расположены символы части первого открытого текста) с помощью функции, созданной ранее, при условии, что известны оба шифротекста и часть первого открытого текста

# **4 Выводы**

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

# **Список Литературы**

1. Однократное гаммирование [Электронный ресурс]. URL: https://esystem. rudn.ru/pluginfile.php/1651641/mod\_resource/content/2/008-lab\_cryptokey.pdf.