Отчёт по лабораторной работе № 8

Информационная безопасность

Надиа Эззакат

Содержание

## Цель работы

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

## 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. В данном случае для двух шифротекстов будет две формулы: С1 = 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. Более подробно см. в [1].

## Выполнение лабораторной работы

Код программы

Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом,Часть 1

• In[43]: импорт необходимых библиотек 6 • In[44]: функция, реализующая сложение по модулю два двух строк • In[45]: открытые/исходные тексты (одинаковой длины) • In[46]: создание ключа той же длины, что и открытые тексты • In[47]: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ • In[48]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны шифротексты и ключ

Рис. 8.2: Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 2

• In[53]: сложение по модулю два двух шифротекстов с помощию функции, созданной ранее • In[50]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов • In[51]: получение части первого открытого текста (срез) • In[52]: 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

## 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

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