Лабораторная работа №8

Информационная безопасность

Маметкадыров Ынтымак | НПМбд-02-20

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 [@Gamma:bash].

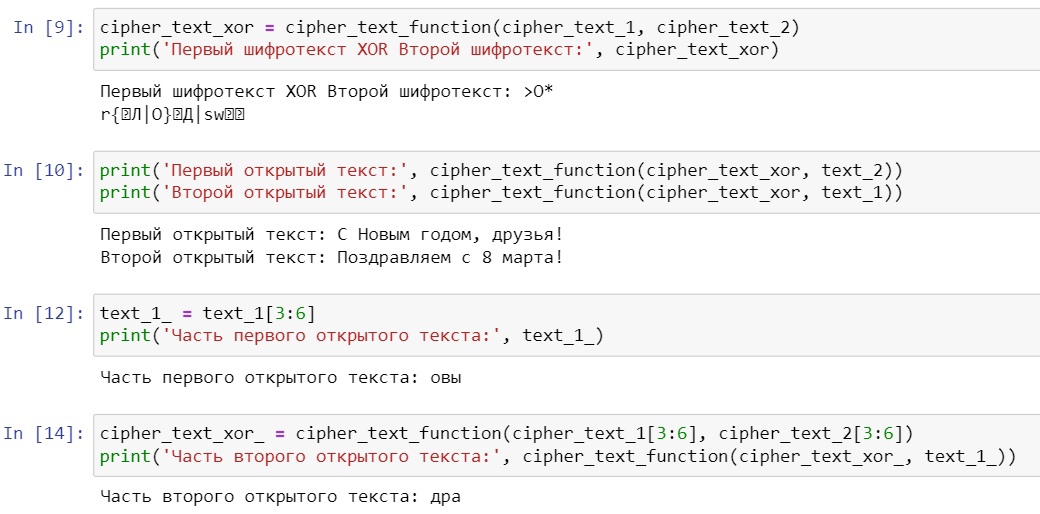
# Выполнение лабораторной работы

Код программы (рис. [-@fig:001]).



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

* In[1]: импорт необходимых библиотек
* In[2]: функция, реализующая сложение по модулю два двух строк
* In[15]: открытые/исходные тексты (одинаковой длины)
* In[6]: создание ключа той же длины, что и открытые тексты
* In[8]: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ
* In[9]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны шифротексты и ключ



Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 2

* In[11]: сложение по модулю два двух шифротекстов с помощию функции, созданной ранее
* In[12]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов
* In[16]: получение части первого открытого текста (срез)
* In[17]: 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 мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы