Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Форис Анастасия Дмитриевна

Содержание

## 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

## 2 Выполнение лабораторной работы

Код программы (рис.7).

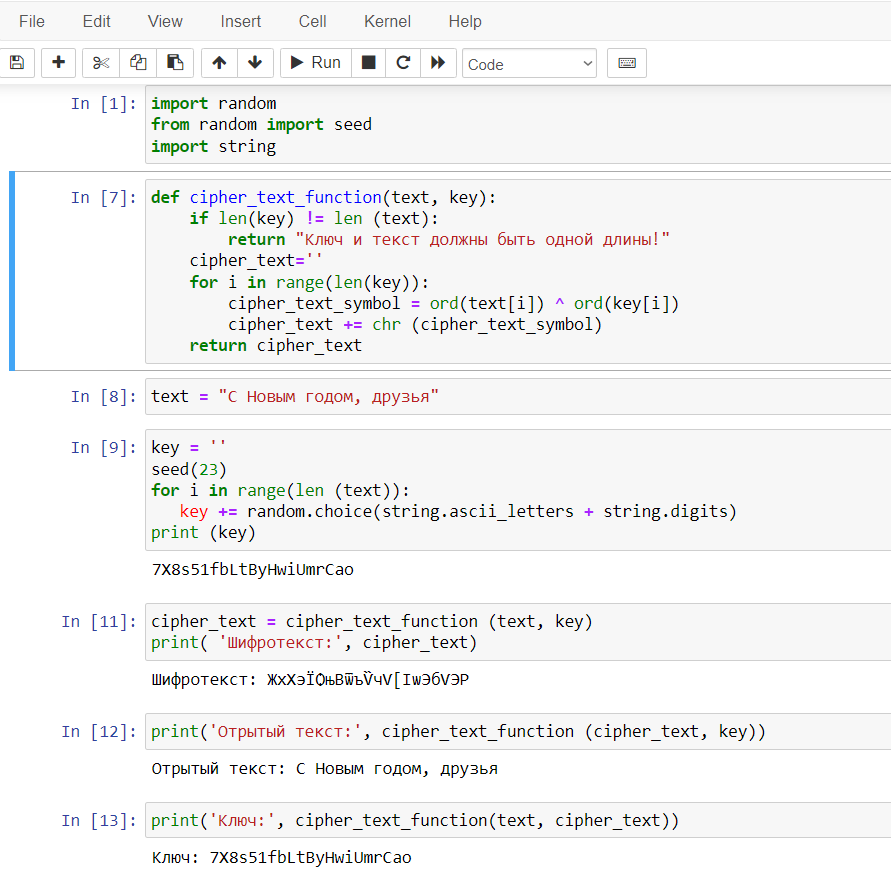


Рис. 7:Приложение, реализующее режим однократного гаммирования

• In[21]: импорт необходимых библиотек

• In[22]: функция, реализующая сложение по модулю два двух строк

• In[23]: открытый/исходный текст

• In[24]: создание ключа той же длины, что и открытый текст

• In[25]: получение шифротекста с помощию функции, созданной ранее, при условии, что известны открытый текст и ключ •

In[26]: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ

• In[27]: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

## 3 Выводы

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