Отчёта по лабораторной работе № 8

Информационная безопасность

Адоле Фейт Эне

Содержание

Список иллюстраций

Список таблиц

0.1 Цель работы

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

0.2 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. В данном случае для двух шифротекстов будет две формулы: C1 = P1 xor K и C2 = 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].

0.3 Выполнение лабораторной работы

Код программы (рис. 8.1).

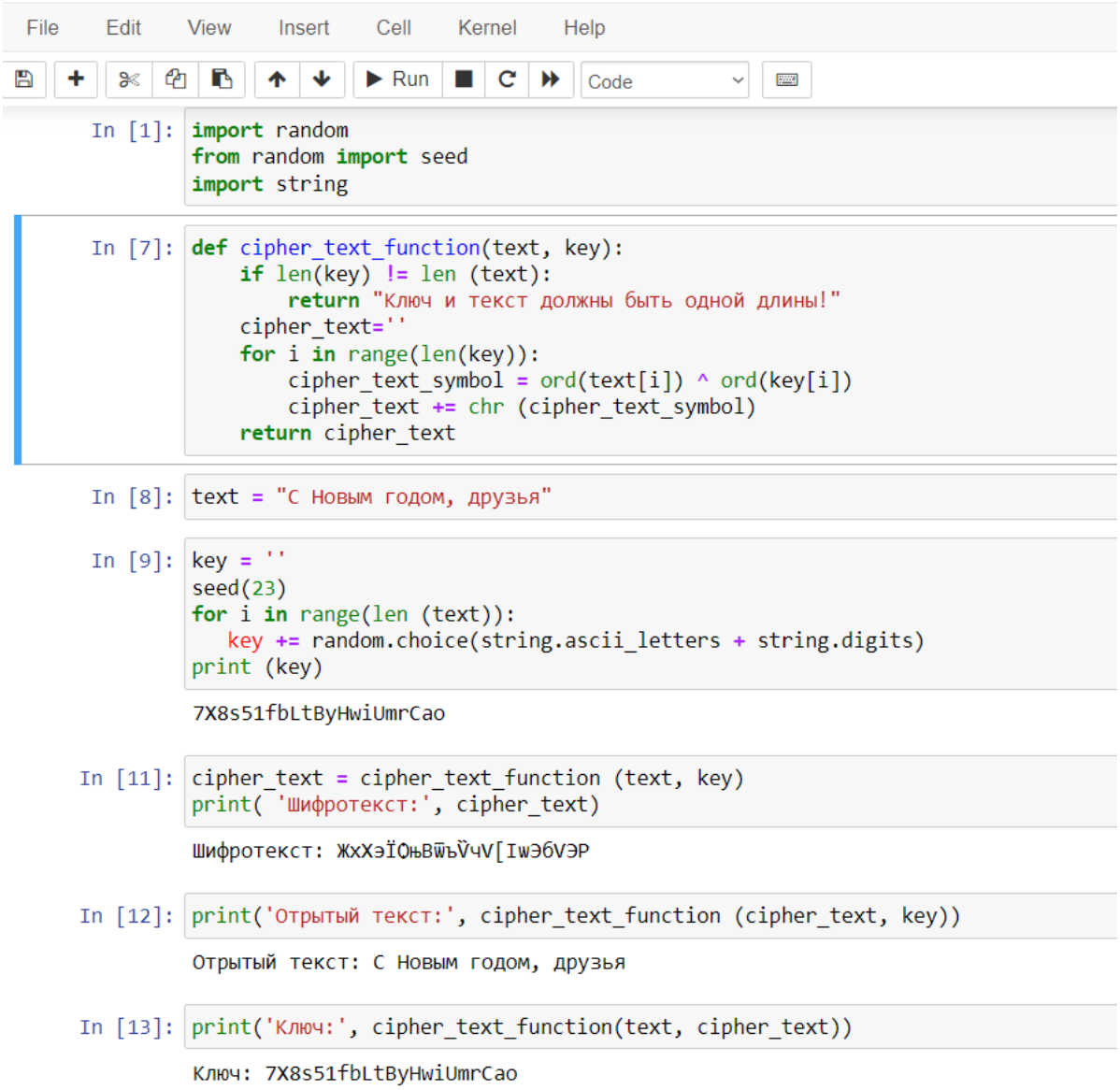

Рис. 1: Рис. 8.1: Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 1

• In[1]: импорт необходимых библиотек In[2]: функция, реализующая сложение по модулю два двух строк • In[3]: открытые/исходные тексты (одинаковой длины) • In[5]: создание ключа той же длины, что и открытые тексты • In[7]: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ • In[8]: 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

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

In[9]: сложение по модулю два двух шифротекстов с помощию функции, созданной ранее • In[10]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов • In[12]: получение части первого открытого текста (срез) • In[14]: 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

0.4 Выводы

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