Отчёт по лабораторной работе 8

Элементы криптографии. Шифрование (кодирование)различных исходных текстов одним ключом

Максимова Ксения НБИбд-02-18

Содержание

List of Figures

1 Цель работы

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

2 Задание

Разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе.

3 Теоретическое введение

Смысл однократного гаммирования заключается в наложении (снятии) на открытые (зашифрованные) данные последовательности элементов других данных,полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования [1].

Преимущества однократного гаммирования[1]: 1. Абсолютная стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. 2. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении все различные ключевые последовательности возможны и равновероятны

При всех очевидных приемуществах, есть один весомый недостаток, который сразу бросается в глаза, - это необходимость иметь огромные объемы данных, которые можно было бы использовать в качестве гаммы. Для этих целей обычно пользуются датчиками настоящих случайных чисел[2].

Необходимые и достаточные условия абсолютной стойкости шифра[1]: - полная случайность ключа; - равенство длин ключа и открытого текста; - однократное использование ключа

4 Выполнение лабораторной работы

Программа, позволяющая шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования с использованием одного ключа.

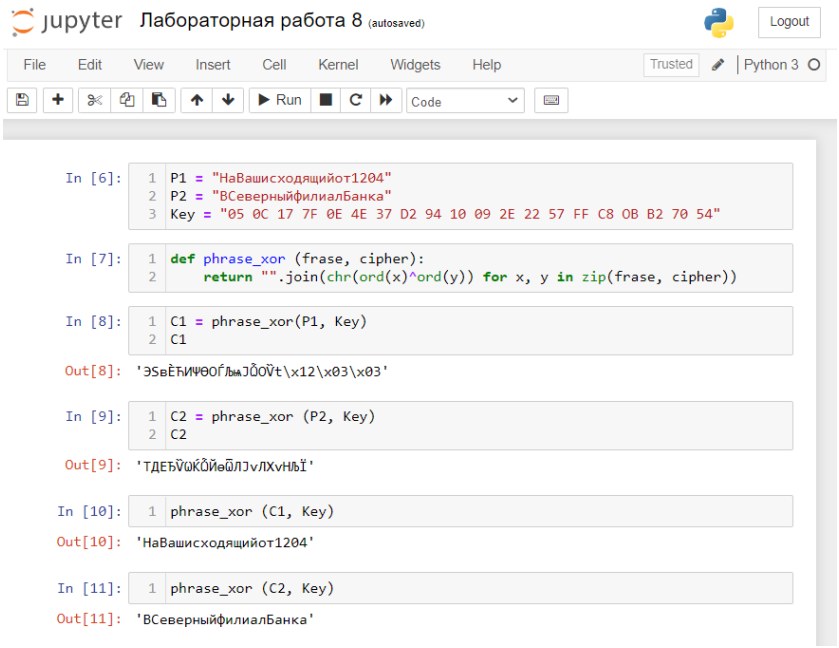

Figure 4.1: Рис 1.Код программы

Рисунок 1

5 Выводы

Разработано приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования с использованием одного ключа.

Список литературы

1. Элементы криптографии. Однократное гаммирование
2. Прикладные задачи шифрования