Отчёт по лабораторной работе 8

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

Максимова Ксения НБИбд-02-18

Содержание

[Цель работы 1](#_Toc90738341)

[Задание 1](#_Toc90738342)

[Теоретическое введение 1](#_Toc90738343)

[Выполнение лабораторной работы 2](#_Toc90738344)

[Выводы 3](#_Toc90738345)

[Список литературы 3](#_Toc90738346)

# Цель работы

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

# 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.

# 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]](https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf).

Преимущества однократного гаммирования[[1]](https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf): 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]](https://bugtraq.ru/library/books/crypto/chapter7/).

Необходимые и достаточные условия абсолютной стойкости шифра[[1]](https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf): - полная случайность ключа; - равенство длин ключа и открытого текста; - однократное использование ключа

# Выполнение лабораторной работы

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

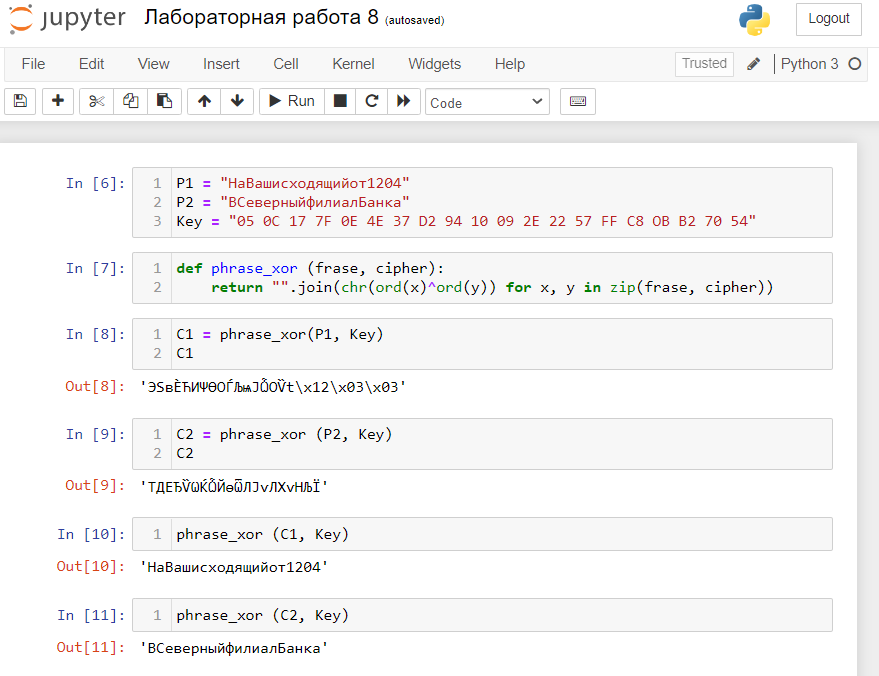


Рис 1.Код программы

[Рисунок 1](image/1.png)

# 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](https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf)

[2. Прикладные задачи шифрования](https://bugtraq.ru/library/books/crypto/chapter7/)