Лабораторная работа № 3

Шифрование гаммированием

Пак Мария НФИмд-02-22"

Содержание

# Лабораторная работа №3 [Цель работы](#цель-работы) [Задание](#задание) [Теоретическое введение](#теоретическое-введение) [Оборудование](#оборудование) [Выполнение лабораторной работы](#выполнение-лабораторной-работы) [Выводы](#выводы) [Список литературы](#список-литературы)

## Цель работы

Освоить на практике применение режима однократного гаммирования.

## Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
   1. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

## Теоретическое введение

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» является простой, но надёжной схемой шифрования данных. Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. [[1]](#X9a11f83b1ef3906df5df95cff9123f28b5a945b).

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. В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.[[2]](#X9a11f83b1ef3906df5df95cff9123f28b5a945b)

Гаммирование является симметричным алгоритмом. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и дешифрование выполняется одной и той же программой [[3]](#X9a11f83b1ef3906df5df95cff9123f28b5a945b).

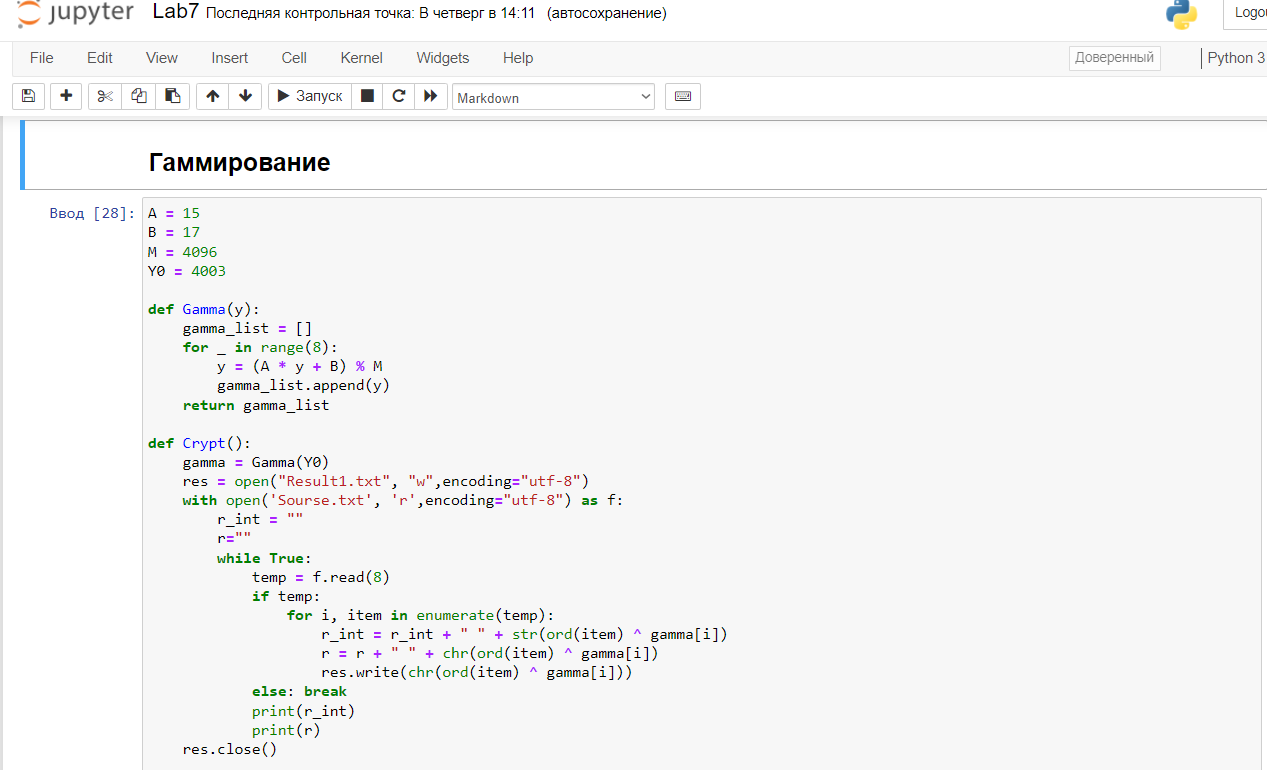
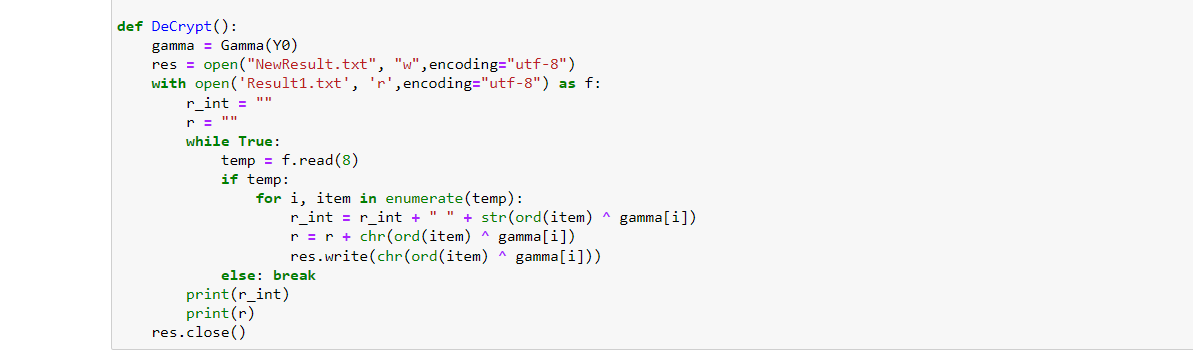
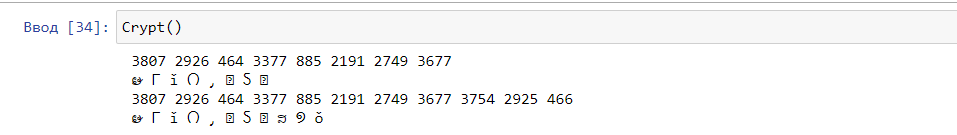
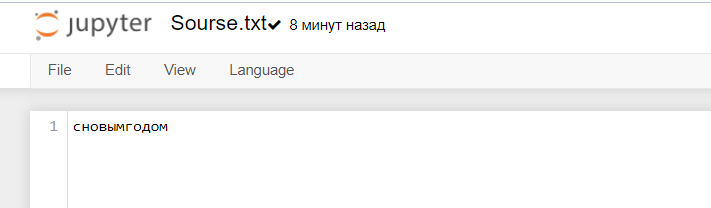
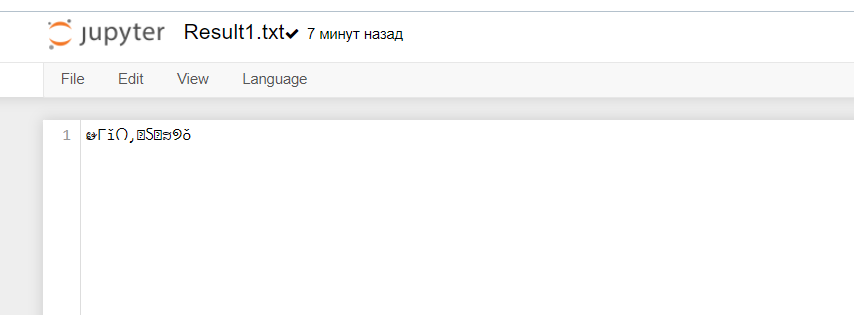
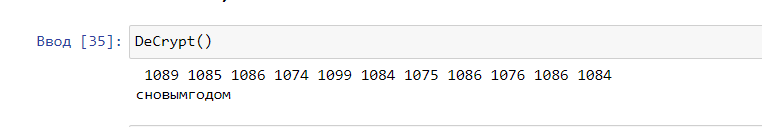
## Оборудование

Лабораторная работа выполнялась дома со следующими характеристиками техники:

– Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz 2.81GHz  
– ОС Майкрософт Windows 10  
– VirtualBox верс. 6.1.26

# Выполнение лабораторной работы

1. Разработала программу, позволяющею шифровать и дешифровать данные в режиме однократного гаммирования. Программа имеет следующий вид.

* (рис. -@fig:001)  
  
* (рис. -@fig:002)  
  
* Приложение написано на python 3. Я запускала его через jupiter Notebook. В данном коде имеется 3 основные функции. 1 - создает гамму, 2 - шифрует текст, 3 - расшифровывает шифротекст.
  1. Программа работает по следующему алгоритму. Сначала пользователь вводит свой текст, который хочет зашифровать в файл source.txt. Далее пользователь заходит в ноутбук, запускает функцию шифрование. Зашифрованный текст и гамма появляются в файле result.txt.
  + (рис. -@fig:003)  
    
  + (рис. -@fig:006)  
    
  1. Для расшифровки текста, пользователь запускает функцию расшифровки в ноутбуке. Функция на основе нашего шифротекста использует гамму и мы получаем исходный текст.
  + (рис. -@fig:005)  
    
  + (рис. -@fig:004)  
    

## Выводы

Освоен на практике применение режима однократного гаммирования. Написана программа по шифровке и дешифровке.

## Список литературы

1. Шифры замены и табличного гаммирования // Хабр URL: <https://habr.com/ru/post/583616/> (дата обращения: 10.12.2021).
2. Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование // Туис URL: <https://esystem.rudn.ru/pluginfile.php/1198312/mod_resource/content/2/007-lab_crypto-gamma.pdf> (дата обращения: 9.12.2021).
3. Простейшие методы шифрования с закрытым ключом // НОУ ИНТУТ URL: <https://intuit.ru/studies/courses/691/547/lecture/12373?page=4> (дата обращения: 9.12.2021).