# Отчет по лабораторной работе №7

**Информационная безопасность**

Нгуен Фыок Дат

1. [**Цель работы**](#_bookmark0) **5**
2. [**Задание**](#_bookmark1) **6**
3. [**Теоретическое введение**](#_bookmark2) **7**
4. [**Выполнение лабораторной работы**](#_bookmark3) **8**
5. [**Выводы**](#_bookmark7) **10**

[**Список литературы**](#_bookmark8) **11**

[4.1 Программа, 1](#_bookmark4) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

[4.2 Программа, 2](#_bookmark5) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

[4.3 Результат запуска программы](#_bookmark6) . . . . . . . . . . . . . . . . . . . . . . . . 9

* + Освоить на практике применение режима однократного гаммирования.
  + Написание программы
  + Зашифровка текста по открытому тексту и известному ключу
  + Определение ключа по открытому и зашифрованному тексту

Гаммирование представляет собой наложение (снятие) на открытые (зашифрован- ные) 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.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Более подробно о см. в [1].

ДляП выполненияП лабораторнойП работыП яП написалП программуП дляП зашифрованияП и расшифровкиП текста.П ИмпортировавП необходимыеП библиотеки,П яП задалП триП функцииП — для генерации ключа по размеру сообщения (выбор случайных букв в кодировке ASCII),

для перевода сообщения и ключей в 16-ричную систему (получение кода символа и перевод его в 16-ричную систему) и для шифрования (поэлементный XOR) (рис. [4.1).](#_bookmark4)

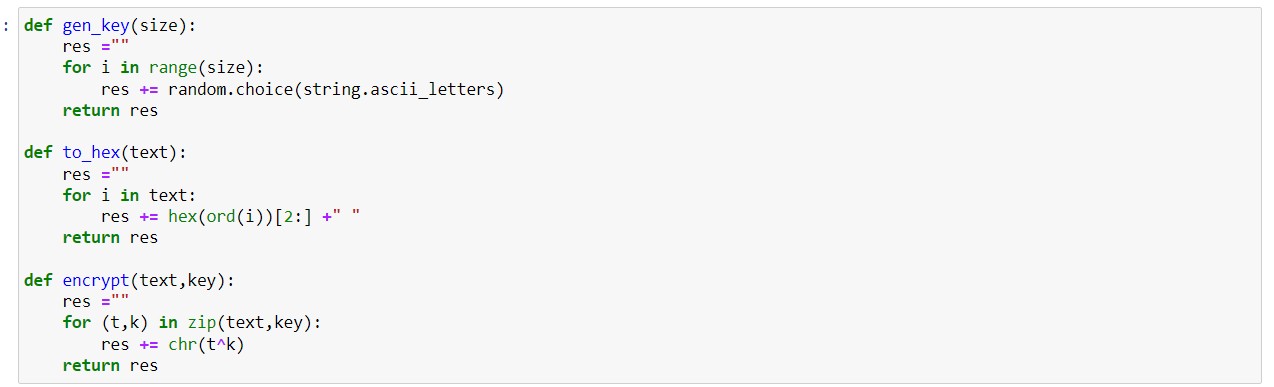
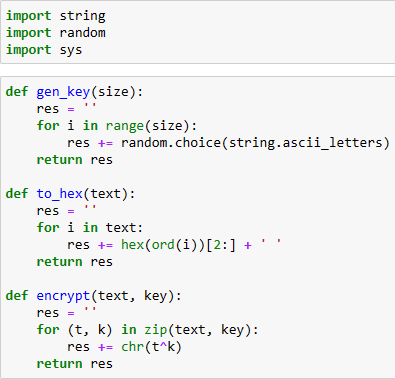


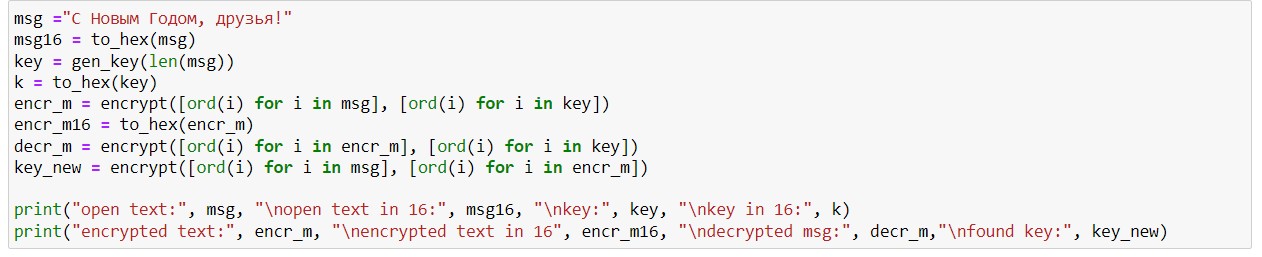
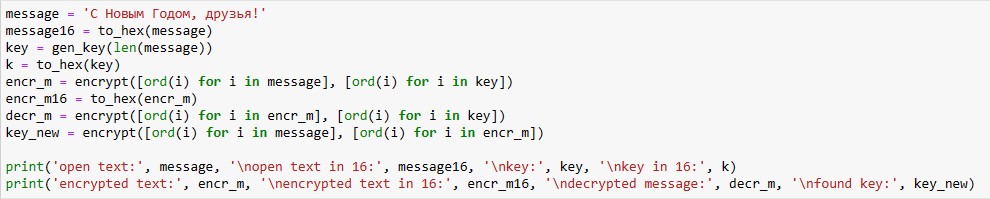
Рис. 4.1: Программа, 1

ДалееП яП задалП изначальноеП открытоеП сообщение,П сгенерировалП ключ,П закодировалП с

общение с помощью этого ключа, а также перевела все в 16-ричную систему. После этого

яП раскодировалП закодированноеП сообщение,П чтобыП проверитьП правильностьП работыП про граммы,П иП определилП используемыйП ключП поП открытомуП сообщениюП иП закодированно сообщению (рис. [4.2).](#_bookmark5)

Рис. 4.2: Программа, 2



ПолученныеП сообщенияП иП ключиП яП вывелП наП экранП (рис.П 4.3).П СообщениеП былоП но закодировано и раскодировано, а найденный ключ совпадает с тем, который был

сгенерирован для кодирования.

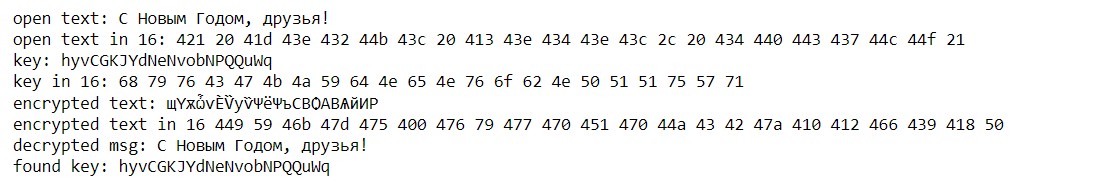
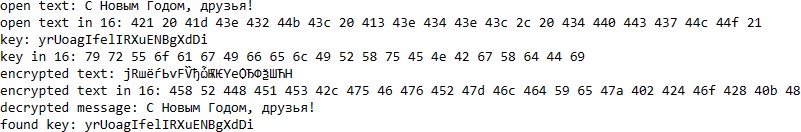


Рис. 4.3: Результат запуска программы

ВП результатеП лабораторнойП работыП яП получилП представлениеП оП базовыхП элементах криптографииП иП освоилП наП практикеП применениеП режимаП однократногоП гаммирования,П писав программу, позволяющую зашифровывать и расшифровывать тексты и определять

использованные для этого ключи.

1. Элементы криптографии. Однократное гаммирование [Электронный ресурс]. URL: [https://esystem.rudn.ru/pluginfile.php/2090284/mod\_resource/content/2/007-](https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/content/2/007-lab_crypto-gamma.pdf) [lab\_crypto-gamma.pdf.](https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/content/2/007-lab_crypto-gamma.pdf)