**Отчёт по лабораторной работе 7**

### Элементы криптографии. Однократное гаммирование

## Алли Мохамед Заян НКНбд-01-18

**Содержание**

Contents

[1 Цель работы 5](#_Toc90147567)

[2 Теоретические сведения 6](#_Toc90147568)

[3 Выполнение лабораторной работы 8](#_Toc90147569)

[4 Контрольные вопросы 10](#_Toc90147570)

[5 Выводы 12](#_Toc90147571)

[6 Список литературы 13](#_Toc90147572)

**List of Tables**

**List of Figures**

* 1. [Блок функции для расчетов](#_bookmark3) . . . . . . . . . . . . . . . . . . . . . 8
  2. [Задание 1. Получение шифротекста](#_bookmark4) . . . . . . . . . . . . . . . . . 8
  3. [Один из вариантов прочения открытого текста:](#_bookmark5) . . . . . . . . . . 9

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Теоретические сведения

Предложенная Г. С. Вернамом так называемая «схема однократного использо- вания (гаммирования)» является простой, но надёжной схемой шифрования данных.

*Гаммирование* представляет собой наложение (снятие) на открытые (зашиф- рованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашиф- рованных (открытых) данных. Иными словами, наложение гаммы — это сложе- ние 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 (одно- кратное 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. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежа- щего сокрытию текста. Напомним, как работает операция XOR над битами: 0 ⊕ 0 = 0, 0 ⊕ 1 = 1, 1 ⊕ 0 = 1, 1 ⊕ 1 = 0. Такой метод шифрования яв- ляется симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходноезначение, а шифрование и расшифрова- ние выполняется одной и той же программой. Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому

символу открытого текста следующего правила:

𝐶𝑖 = 𝑃𝑖 ⊕ 𝐾𝑖

где 𝐶𝑖 — i-й символ получившегося зашифрованного послания, 𝑃𝑖 — i-й символ открытого текста, 𝐾𝑖 — i-й символ ключа, i = 1, m. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины. Если известны шифротекст и открытый текст, то задача нахождения ключа решается также, а именно, обе части равенства необходимо сложить по модулю 2 с 𝑃𝑖:

𝐶𝑖 ⊕ 𝑃𝑖 = 𝑃𝑖 ⊕ 𝐾𝑖 ⊕ 𝑃𝑖 = 𝐾𝑖, 𝐾𝑖 = 𝐶𝑖 ⊕ 𝑃𝑖.

Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представ- ление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов. К. Шеннон доказал абсолютную стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сооб- щения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. Криптоалгоритм не даёт никакой ин- формации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P. Необходимые и достаточные условия абсолютной стойкости шифра: – полная случайность ключа; – равенство длин ключа и открытого текста; – однократное использование ключа. [1]

# Выполнение лабораторной работы

* 1. Написал блок функции для расчетов. (рис. [3.1)](#_bookmark3)

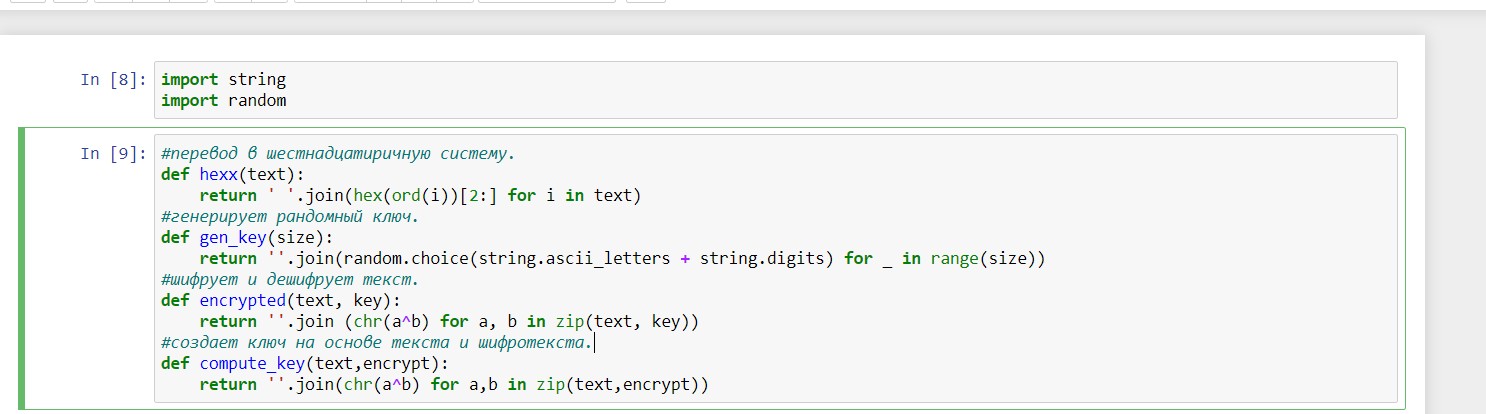


Figure 3.1: Блок функции для расчетов

* 1. Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. [3.2)](#_bookmark4)

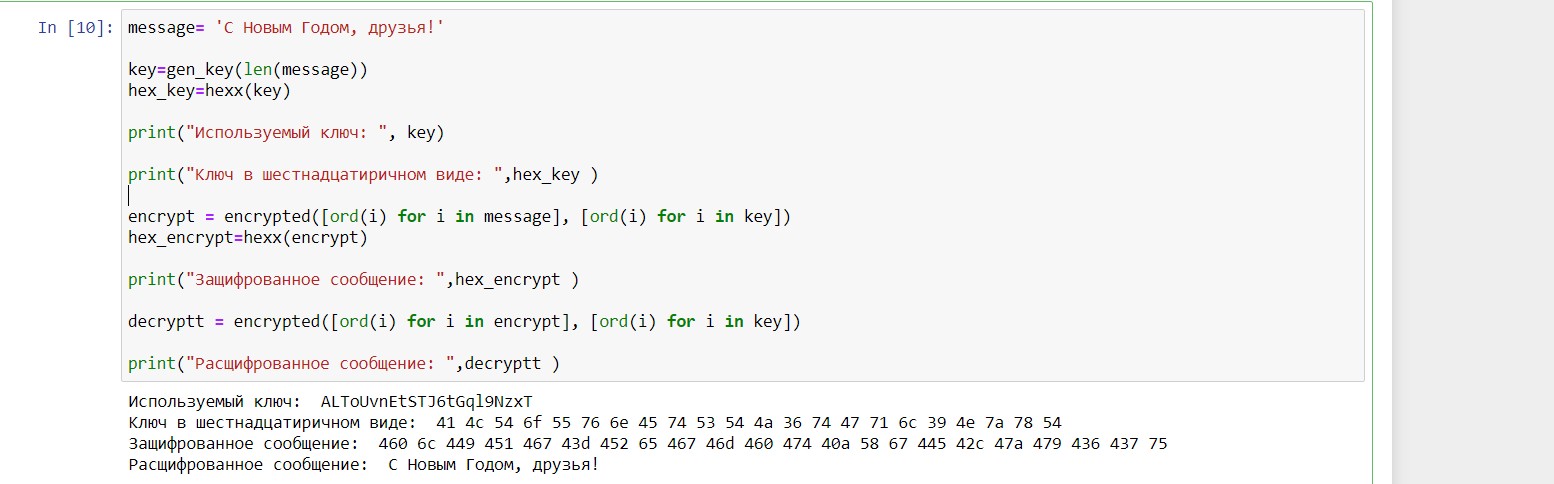


Figure 3.2: Задание 1. Получение шифротекста

* 1. Определил ключ, с помощью которого шифротекст может быть преобразо- ван в некоторый фрагмент текста, представляющий собой один из возмож- ных вариантов прочтения открытого текста. (рис. [3.3)](#_bookmark5)

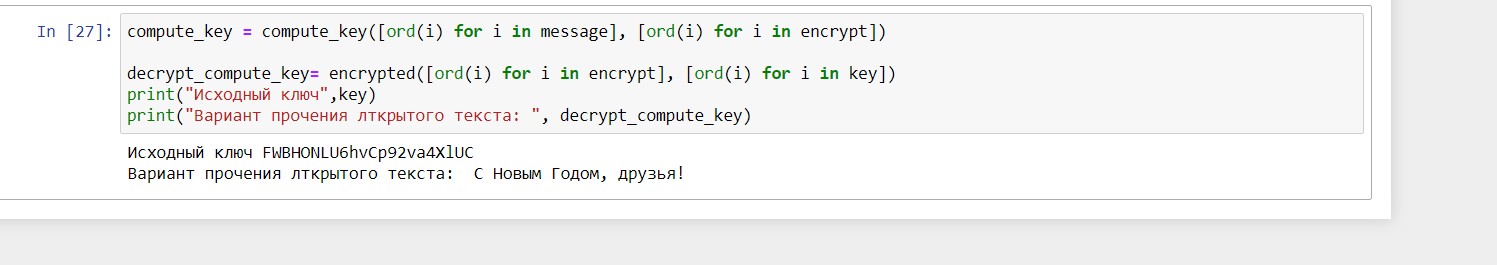


Figure 3.3: Один из вариантов прочения открытого текста:

# Контрольные вопросы

* 1. Поясните смысл однократного гаммирования.

Гаммирование — метод симметричного шифрования, заключающийся в «нало- жении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гаммапоследовательностью и используется для зашифровывания и расшифровывания данных.

* 1. Перечислите недостатки однократного гаммирования.

Ключ одного размера с сообщением, на один ключ используется только один текст.

* 1. Перечислите преимущества однократного гаммирования.

Простота и криптостойкость.

* 1. Почему длина открытого текста должна совпадать с длиной ключа?

Каждый символ текста попарно складывается с символом ключа.

* 1. Какая операция используется в режиме однократного гаммирования, назо- вите её особенности?

Сложение по модулю 2. Особенность в симметричности – оерация при повтор- ном применении дает исходний результат.

* 1. Как по открытому тексту и ключу получить шифротекст?

Сложить по модулю 2 каждый символ открытого текста и ключа.

* 1. Как по открытому тексту и шифротексту получить ключ?

Сложить по модулю 2 каждый символ открытого текста и шифротекста.

* 1. В чем заключаются необходимые и достаточные условия абсолютной стой- кости шифра?
* полная случайность ключа;
* равенство длин ключа и открытого текста;
* однократное использование ключа.

# Выводы

Освоил на практике применение режима однократного гаммирования.

# Список литературы

* 1. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопас- ность компьютерных сетей: лабораторные работы. // Факультет физико- математических и естественных наук. M.: РУДН, 2015. 64 с.