

Лабораторная работа №7

Лабораторная работа №7

Цель работы

Задание

Теоретическое введение

Оборудование

Выполнение лабораторной работы

Выводы

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.
2. 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].

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]

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].

Оборудование

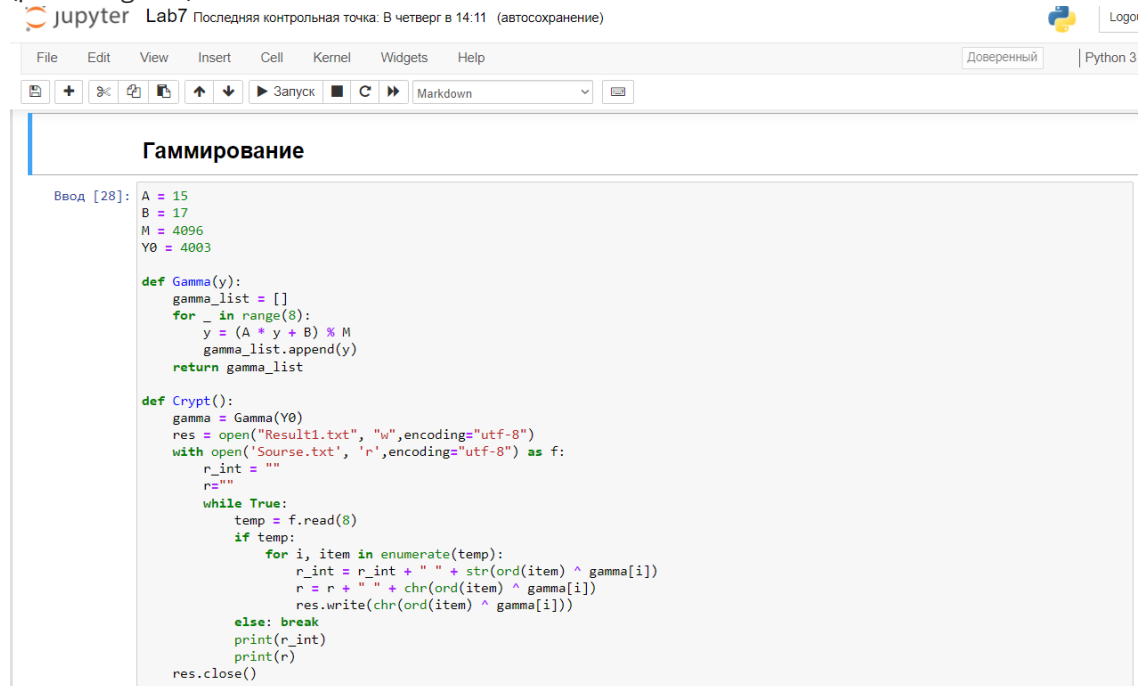
Лабораторная работа выполнялась дома со следующими характеристиками техники:

- 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, позволяющую шифровать и дешифровать данные в режиме однократного гаммирования. Программа имеет следующий вид.

(рис. -@fig:001)



```

Ввод [28]: A = 15
            B = 17
            M = 4096
            Y0 = 4003

def Gamma(y):
    gamma_list = []
    for _ in range(8):
        y = (A * y + B) % M
        gamma_list.append(y)
    return gamma_list

def Crypt():
    gamma = Gamma(Y0)
    res = open("Result1.txt", "w", encoding="utf-8")
    with open('Source.txt', 'r', encoding="utf-8") as f:
        r_int = ""
        r = ""
        while True:
            temp = f.read(8)
            if temp:
                for i, item in enumerate(temp):
                    r_int = r_int + " " + str(ord(item) ^ gamma[i])
                    r = r + " " + chr(ord(item) ^ gamma[i])
                    res.write(chr(ord(item) ^ gamma[i]))
                else: break
            print(r_int)
            print(r)
        res.close()

```

(рис. -@fig:002)

```

def DeCrypt():
    gamma = Gamma(Y0)
    res = open("NewResult.txt", "w", encoding="utf-8")
    with open('Result1.txt', 'r', encoding="utf-8") as f:
        r_int = ""
        r = ""
        while True:
            temp = f.read(8)
            if temp:
                for i, item in enumerate(temp):
                    r_int = r_int + " " + str(ord(item) ^ gamma[i])
                    r = r + chr(ord(item) ^ gamma[i])
                    res.write(chr(ord(item) ^ gamma[i]))
                else: break
            print(r_int)
            print(r)
        res.close()

```

Приложение написано на python 3. Я запускала его через jupyter Notebook. В данном коде имеется 3 основные функции. 1 - создает гамму, 2 - шифрует текст, 3 - расшифровывает шифротекст.

2. 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)

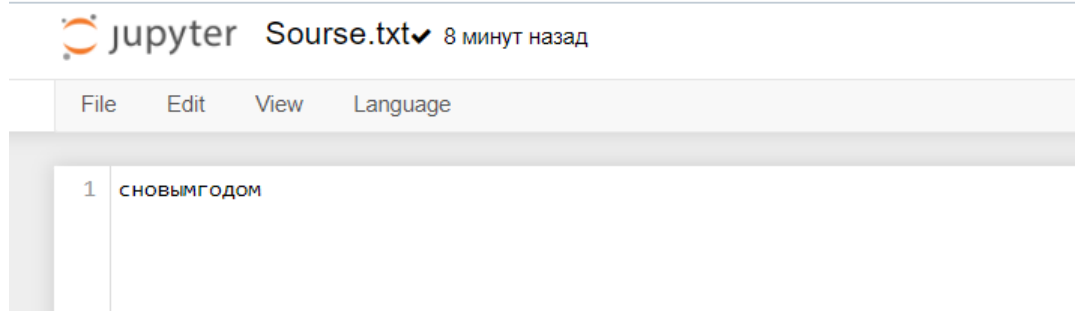
```

Ввод [34]: Crypt()

3807 2926 464 3377 885 2191 2749 3677
❏ Г и О , 5 5
3807 2926 464 3377 885 2191 2749 3677 3754 2925 466
❏ Г и О , 5 5 5 9 6

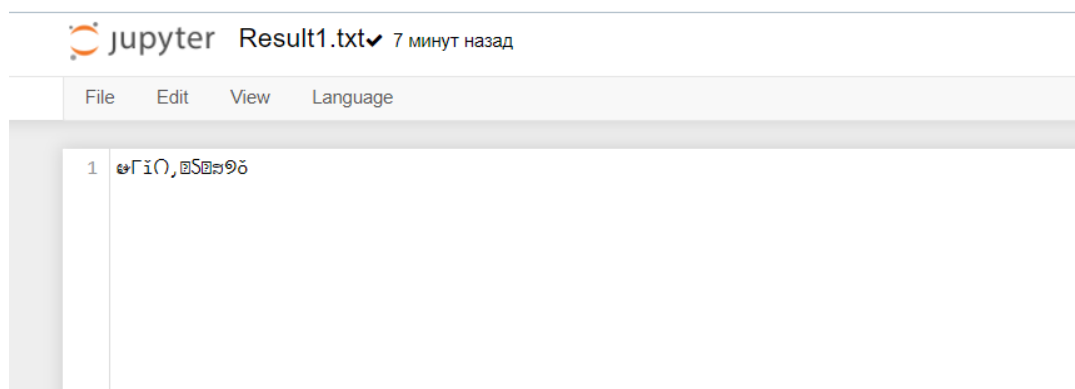
```

(рис. -@fig:006)



3. 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)

Ввод [35]: DeCrypt()
1089 1085 1086 1074 1099 1084 1075 1086 1076 1086 1084
СНОВЫМГОДОМ

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).

