
Front matter

title: "Отчёт по лабораторной работе № 7" subtitle: "Информационная безопасность" author: "Надия Эззакат"

Generic options

lang: ru-RU toc-title: "Содержание"

Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt
linestretch: 1.5 papersize: a4 documentclass: scrreprt

l18n polyglossia

polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true polyglossia-otherlangs:
name: english

l18n babel

babel-lang: russian babel-otherlangs: english

Fonts

mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions:
Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase
monofontoptions: Scale=MatchLowercase,Scale=0.9

Biblatex

biblatex: true biblio-style: "gost-numeric" biblatexoptions:

- parenttracker=true
- backend=biber
- hyperref=auto
- language=auto
- autolang=other*
- citestyle=gost-numeric

Pandoc-crossref LaTeX customization

figureTitle: "Рис." tableTitle: "Таблица" listingTitle: "Листинг" lofTitle: "Список иллюстраций" lotTitle:
"Список таблиц" lolTitle: "Листинги"

Misc options

indent: true header-includes:

- `\usepackage{indentfirst}`
 - `\usepackage{float} # keep figures where there are in the text`
 - `\floatplacement{figure}{H} # keep figures where there are in the text`
-

Цель работы

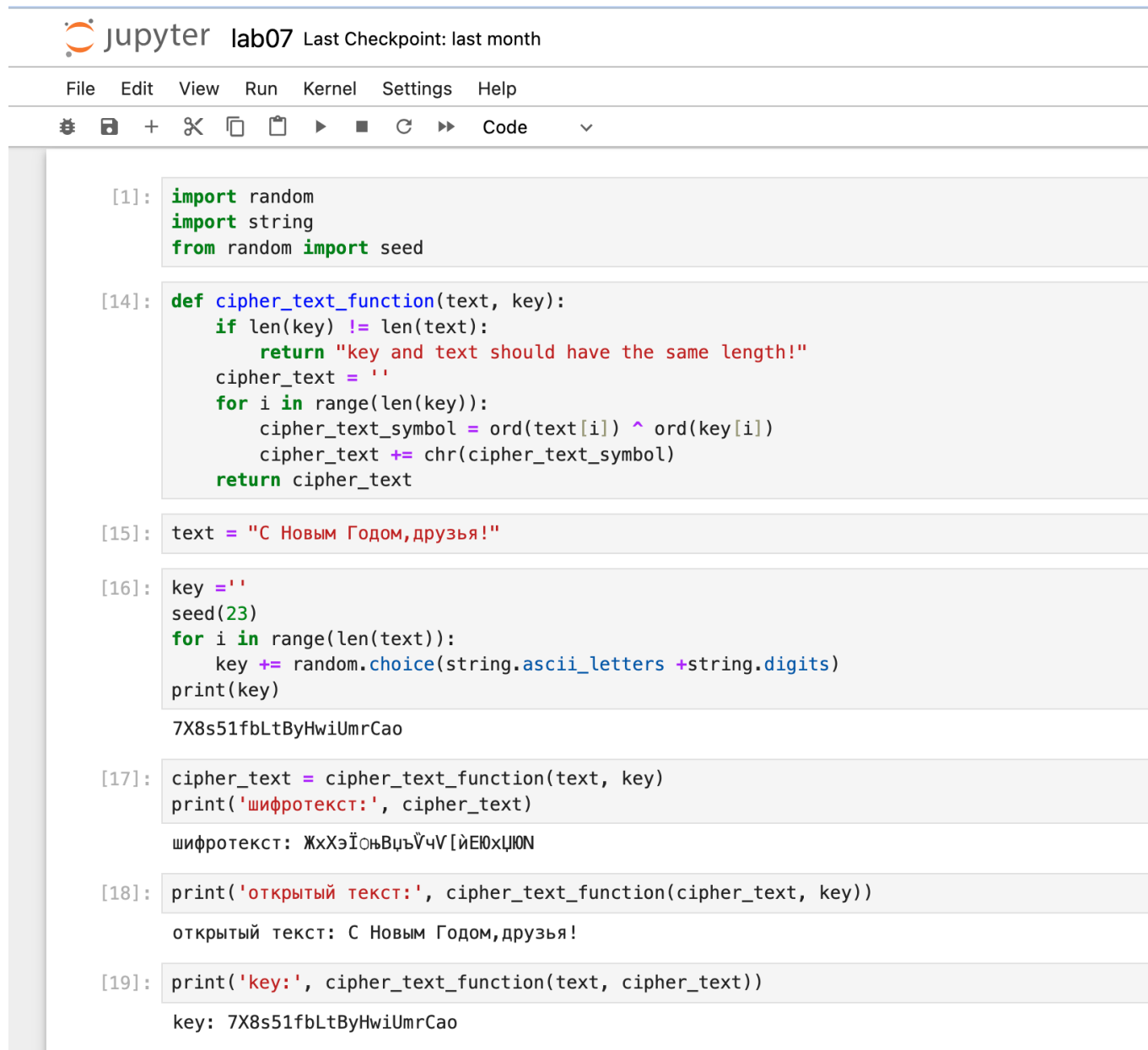
Освоить на практике применение режима однократного гаммирования.

Теоретическое введение

Гаммирование - наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Основная формула, необходимая для реализации однократного гаммирования: $C_i = P_i \text{ XOR } K_i$, где C_i - i -й символ зашифрованного текста, P_i - i -й символ открытого текста, K_i - i -й символ ключа. Аналогичным образом можно найти ключ: $K_i = C_i \text{ XOR } P_i$. Необходимые и достаточные условия абсолютной стойкости шифра: • длина открытого текста равна длине ключа • ключ должен использоваться однократно • ключ должен быть полностью случаен

Выполнение лабораторной работы

Код программы(рис. 7.1).



```
[1]: import random
import string
from random import seed

[14]: def cipher_text_function(text, key):
    if len(key) != len(text):
        return "key and text should have the same length!"
    cipher_text = ''
    for i in range(len(key)):
        cipher_text_symbol = ord(text[i]) ^ ord(key[i])
        cipher_text += chr(cipher_text_symbol)
    return cipher_text

[15]: text = "С Новым Годом, друзья!"

[16]: key = ''
seed(23)
for i in range(len(text)):
    key += random.choice(string.ascii_letters + string.digits)
print(key)

7X8s51fbLtByHwiUmrCao

[17]: cipher_text = cipher_text_function(text, key)
print('шифротекст:', cipher_text)

шифротекст: ЖхХЭЇонѢцъŸчѴ[йЕЮхЦЮN

[18]: print('открытый текст:', cipher_text_function(cipher_text, key))

открытый текст: С Новым Годом, друзья!

[19]: print('key:', cipher_text_function(text, cipher_text))

key: 7X8s51fbLtByHwiUmrCao
```

- In[1]: импорт необходимых библиотек
- In[14]: функция, реализующая сложение по модулю два двух строк
- In[15]: открытый/исходный текст
- In[16]: создание ключа той же длины, что и открытый текст
- In[17]: получение шифротекста с помощью функции, созданной ранее, при условии, что известны открытый текст и ключ
- In[18]: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ
- In[19]: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

Выводы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

Список литературы

Однократное гаммирование [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/1651639/mod_resource/content/2/007-lab_cryptogamma.pdf.