## Front matter

title: "Отчет по лабораторной работе №8" subtitle: "Основы информационной безопасности" author: "Бабенко Константин, НКАбд-01-23"

## Generic otions

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

## I18n polyglossia

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

## I18n 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:

* parentracker=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 на примере кодирования различных исходных текстов одним ключом

# Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты $P\_1$ и $P\_2$ в режиме однократного гаммирования. Приложение должно определить вид шифротекстов $C\_1$ и $C\_2$ обоих текстов $P\_1$ и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

# Теоретическое введение

Исходные данные.

Две телеграммы Центра:

$P\_1$ = НаВашисходящийот1204

$P\_2$ = ВСеверныйфилиалБанка

Ключ Центра длиной 20 байт: K = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$C\_1 = P\_1 ⊕ K$,

$C\_2$ = P\_2 ⊕ K$. (8.1)

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства (8.1) складываются по модулю 2. Тогда с учётом свойства операции XOR

$$1 ⊕ 1 = 0, 1 ⊕ 0 = 1 (8.2)$$

получаем:

$$C\_1 ⊕ C\_2 = P\_1 ⊕ K ⊕ P\_2 ⊕ K = P1 ⊕ P\_2.$$

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C\_1 ⊕ C\_2$ (известен вид обеих шифровок). Тогда зная $P\_1$ и учитывая (8.2), имеем:

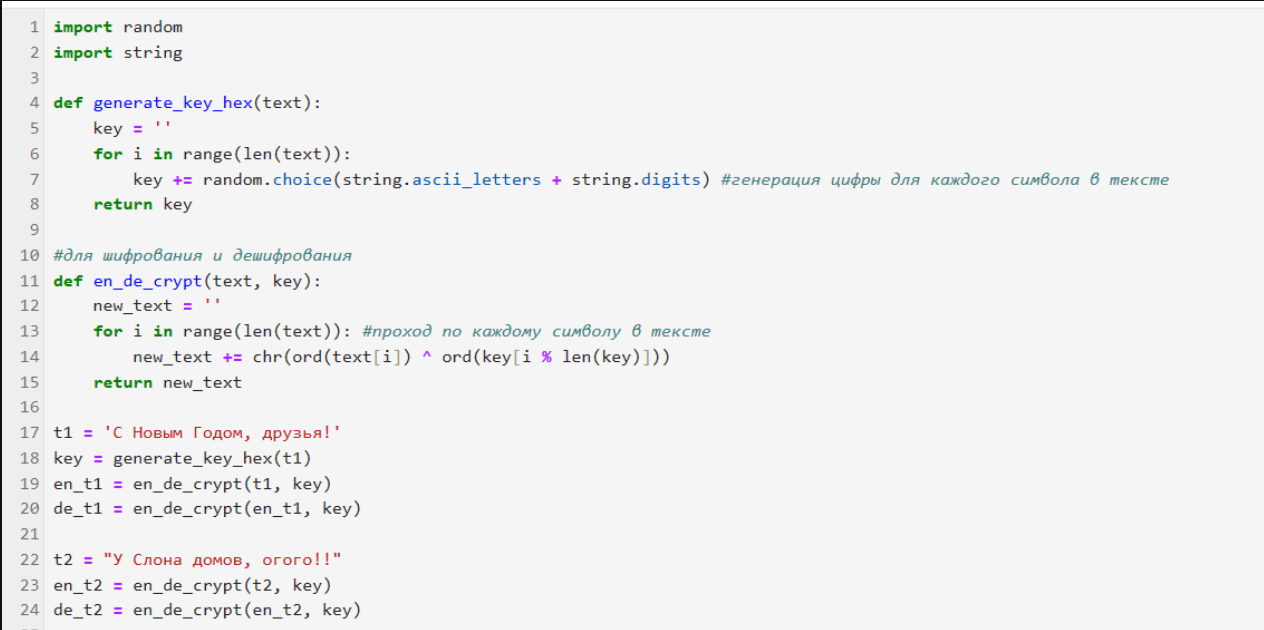
$C\_1 ⊕ C\_2 ⊕ P\_1 = P\_1 ⊕ P\_2 ⊕ P\_1 = P\_2. (8.3)$

Таким образом, злоумышленник получает возможность определить те символы сообщения $P\_2$, которые находятся на позициях известного шаблона сообщения $P\_1$. В соответствии с логикой сообщения $P\_2$, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения $P\_2$. Затем вновь используется (8.3) с подстановкой вместо P1 полученных на предыдущем шаге новых символов сообщения $P\_2$. И так далее. Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска. [@course]

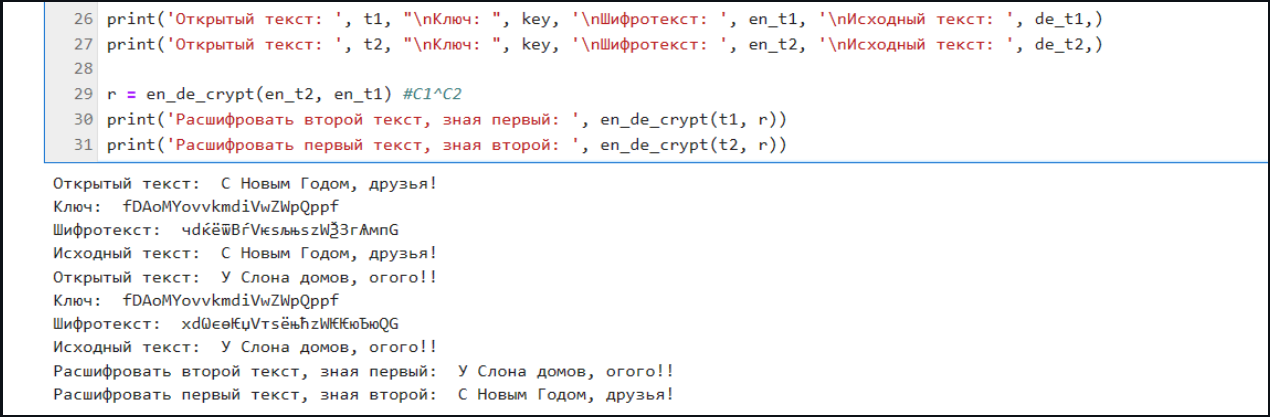
# Выполнение лабораторной работы

Я выполнял лабораторную работу на языке программирования Python, используя функции, реализованные в лабораторной работе №7.

Используя функцию для генерации ключа, генерирую ключ, затем шифрую два разных текста одним и тем же ключом (рис. [-@fig:001]).

{#fig:001 width=70%}

Расшифровываю оба текста сначала с помощью одного ключа, затем предполагаю, что мне неизвестен ключ, но извествен один из текстов и уже расшифровываю второй, зная шифротексты и первый текст (рис. [-@fig:002]).

{#fig:002 width=70%}

Листинг программы 1

import random  
import string  
  
def generate\_key\_hex(text):  
 key = ''  
 for i in range(len(text)):  
 key += random.choice(string.ascii\_letters + string.digits) #генерация цифры для каждого символа в тексте  
 return key  
  
#для шифрования и дешифрования  
def en\_de\_crypt(text, key):  
 new\_text = ''  
 for i in range(len(text)): #проход по каждому символу в тексте  
 new\_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))  
 return new\_text  
  
t1 = 'С Новым Годом, друзья!'  
key = generate\_key\_hex(t1)  
en\_t1 = en\_de\_crypt(t1, key)  
de\_t1 = en\_de\_crypt(en\_t1, key)  
  
t2 = "У Слона домов, огого!!"  
en\_t2 = en\_de\_crypt(t2, key)  
de\_t2 = en\_de\_crypt(en\_t2, key)  
  
print('Открытый текст: ', t1, "\nКлюч: ", key, '\nШифротекст: ', en\_t1, '\nИсходный текст: ', de\_t1,)  
print('Открытый текст: ', t2, "\nКлюч: ", key, '\nШифротекст: ', en\_t2, '\nИсходный текст: ', de\_t2,)  
  
r = en\_de\_crypt(en\_t2, en\_t1) #С1^C2  
print('Расшифровать второй текст, зная первый: ', en\_de\_crypt(t1, r))  
print('Расшифровать первый текст, зная второй: ', en\_de\_crypt(t2, r))

# Ответы на контрольные вопросы

1. Как, зная один из текстов ($P\_1$ или $P\_2$), определить другой, не зная при этом ключа? - Для определения другого текста ($P\_2$) можно просто взять зашифрованные тексты $C\_1 ⊕ C\_2$, далее применить XOR к ним и к известному тексту: $C\_1 ⊕ C\_2 ⊕ P\_1 = P\_2$.
2. Что будет при повторном использовании ключа при шифровании текста? - При повторном использовании ключа мы получим дешифрованный текст.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? - Режим шифрования однократного гаммирования одним ключом двух открытых текстов осуществляется путем XOR-ирования каждого бита первого текста с соответствующим битом ключа или второго текста.
4. Перечислите недостатки шифрования одним ключом двух открытых текстов - Недостатки шифрования одним ключом двух открытых текстов включают возможность раскрытия ключа или текстов при известном открытом тексте.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов - Преимущества шифрования одним ключом двух открытых текстов включают использование одного ключа для зашифрования нескольких сообщений без необходимости создания нового ключа и выделения на него памяти.

# Выводы

В ходе лабораторной работы были освоины на практике навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы{.unnumbered}

::: {#refs} :::