
Front matter

title: "Лабораторная работа №8" subtitle: "Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом" author: "Болотина Александра Сергеевна"

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: false # 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

Выполнение лабораторной работы

Программа шифрует и дешифрует сообщения

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 P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 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.

Листинг программы:

```
#Импортируем необходимые библиотеки
import random as rnd
import string as str

#Пишем небоходимые функции

def create_key(size=10, chars=str.ascii_letters + str.digits):
    return ''.join(rnd.choice(chars) for _ in range(size))


def hexadical_form(s):
    return ''.join("{:02x}".format(ord(c)) for c in s)


def gamming(fst_text, sec_text):
    fst_text_ascii = [ord(i) for i in fst_text]
    sec_text_ascii = [ord(i) for i in sec_text]
    return ''.join(chr(s^k) for s,k in zip(fst_text_ascii,sec_text_ascii))

#Выполним шифрование
P1, P2 = 'example', 'hello world'
print(f'original texts: {P1}, {P2}')
key=create_key(len(P1))

print('Key for encoding:', create_key(len(P1)))
print('Hexadecimal key for encoding:', hexadical_form(key))
print('Ciphertext for plaintext 1 and the key:', gamming(P1, key))
print('Ciphertext for plaintext 2 and the key:', gamming(P2, key))
print('The result of the gamming of two ciphers and the source text:')
```

```
print(gamming(gamming(P1, key)+gamming(P2, key), P1))
print(gamming(gamming(P1, key)+gamming(P2, key), P2))
```

Результаты выполнения:

```
original texts: example, hello world
Key for encoding: 5DBNmdn
Hexadecimal key for encoding: 584f5335794e77
Ciphertext for plaintext 1 and the key: =72X    "
Ciphertext for plaintext 2 and the key: 0*?Yn
The result of the gamming of two ciphers and the source text:
XOS5yNw
UR^4fe_XS=
```

Выводы

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Список литературы

1. Лабораторная работа № 8

::: {#refs} :::