**Front matter**

title: "Лабораторная работа №8" subtitle: "Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом" author: "Аникин Константин Сергеевич"

**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 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.

**Теоретическое введение**

Есть 3 вида разрешений. Они определяют права пользователя на 3 действия: чтение, запись и выполнение. В Linux эти действия обозначаются вот так:

• r — read (чтение) — право просматривать содержимое файла;

• w — write (запись) — право изменять содержимое файла;

• x — execute (выполнение) — право запускать файл, если это программа или скрипт.

У каждого файла есть 3 группы пользователей, для которых можно устанавливать права доступа.

• owner (владелец) — отдельный человек, который владеет файлом. Обычно это тот, кто создал файл, но

владельцем можно сделать и кого-то другого.

• group (группа) — пользователи с общими заданными правами.

• others (другие) — все остальные пользователи, не относящиеся к группе и не являющиеся владельцами.

Более подробно о правах доступа см. в [@codecheck:page].

**Выполнение лабораторной работы**

Код программы представлен на рис. @fig:1, @fig:2 и @fig:3. На первом изображении - вспомогательные функции, создающие словари перевода текста в числа и переводящие hex-ключи в числа. На втором изображении - функции, способные закодировать текст по ключу и находящие раскодированный текст по закодированным и одному раскодированному. На третьем изображении - примеры работы функций.

Вспомогательные функции{#fig:1}

Криптографические функции{#fig:2}

Пример работы функций{#fig:3}

**Выводы**

Работа выполнена полностью.

**Список литературы{.unnumbered}**

::: {#refs} :::