
Front matter

title: "Лабораторная работа №7" subtitle: "Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование" author: "Болотина Александра Сергеевна"

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: 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:

- 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

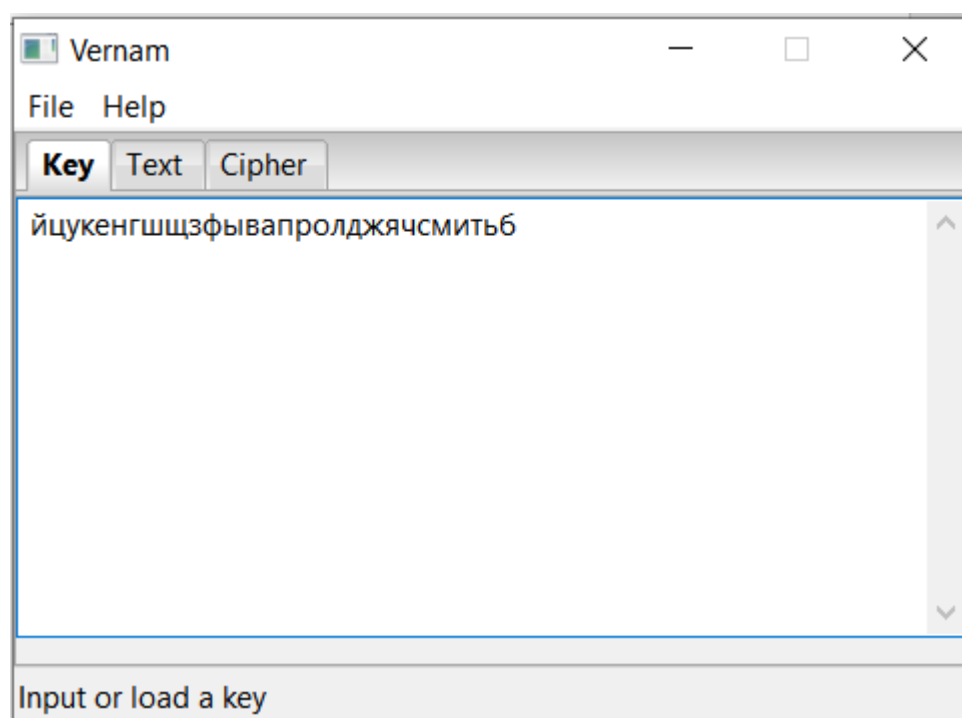
Выполнение лабораторной работы

Программа шифрует и дешифрует сообщения

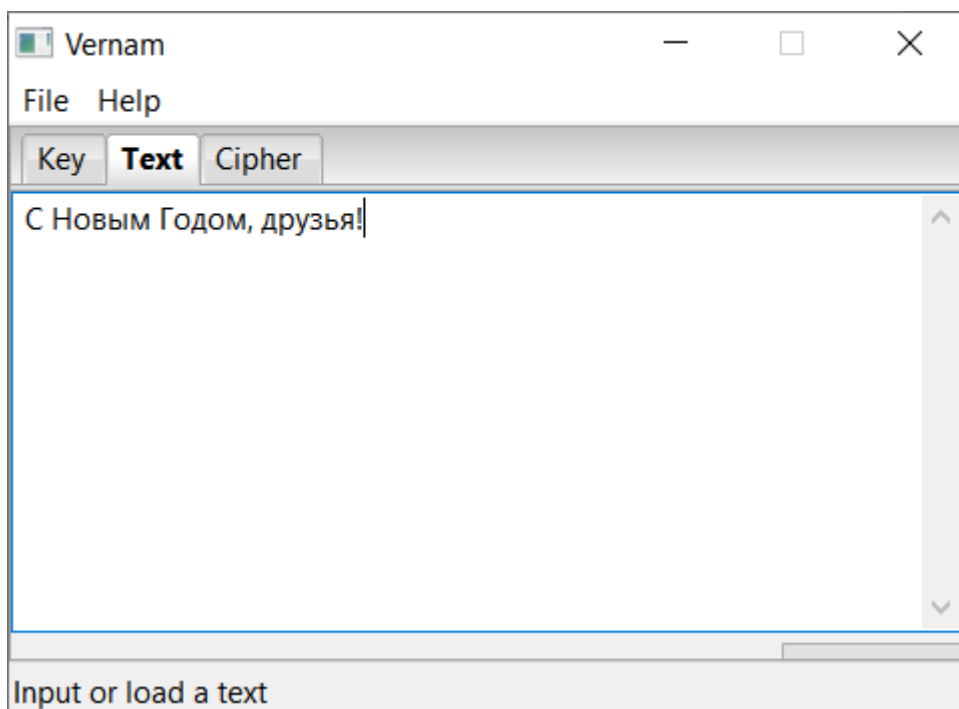
Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

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.

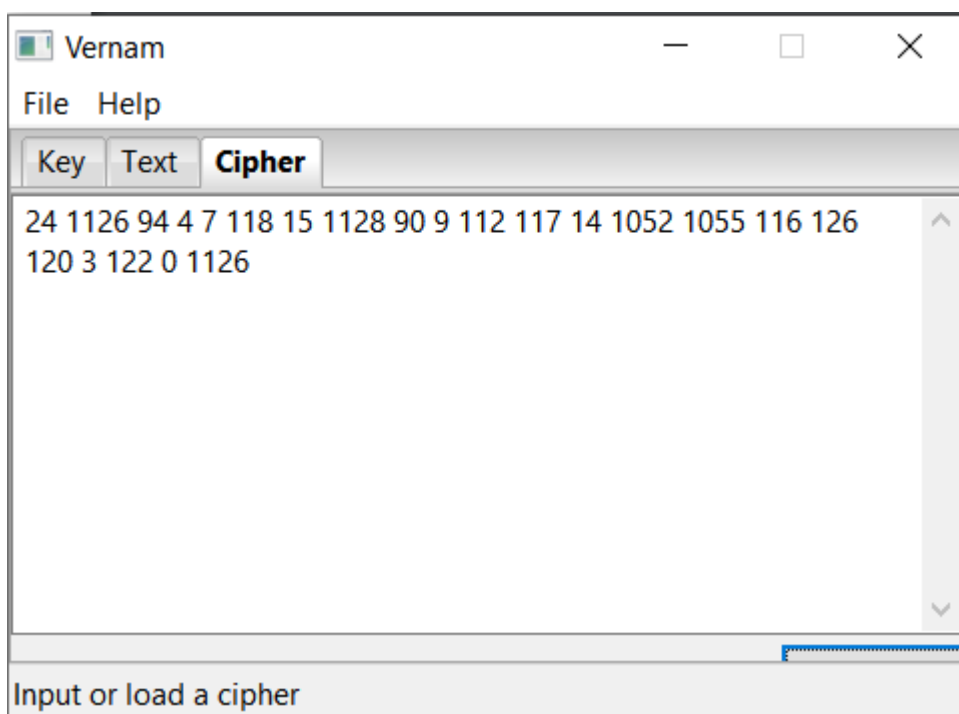
Ключ:



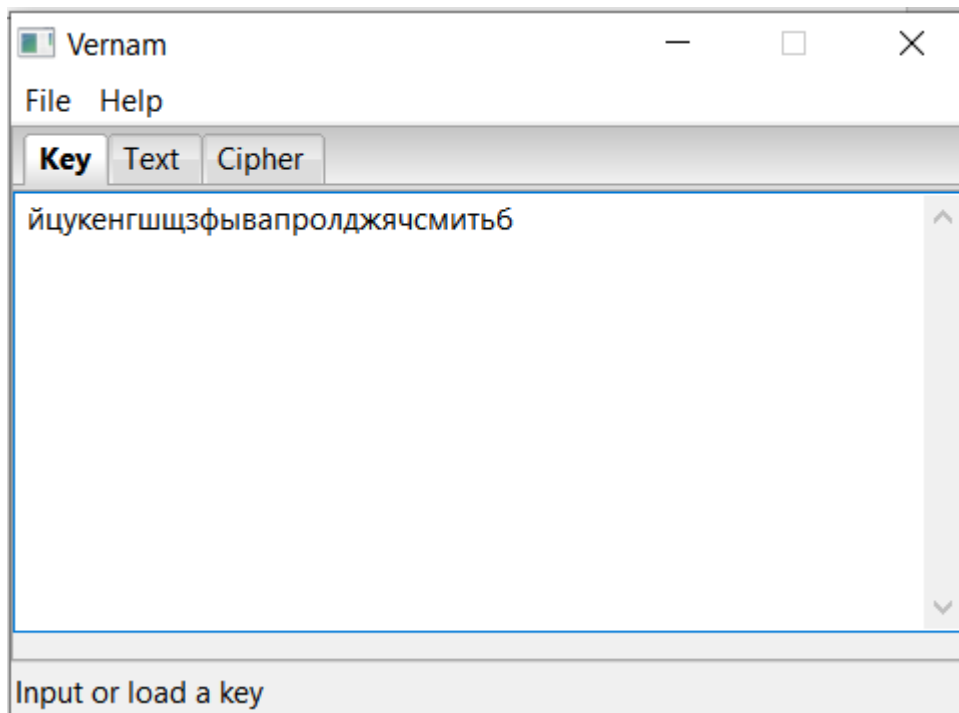
Текст сообщения, которое нужно зашифровать:



Зашифрованное сообщение:



Ключ :



The screenshot shows the Vernam application window with the 'Key' tab selected. The main text area contains the Russian text 'йцукенгшщзфывапролджячсмитьб'. Below the text area is a label 'Input or load a key'.

Vernam

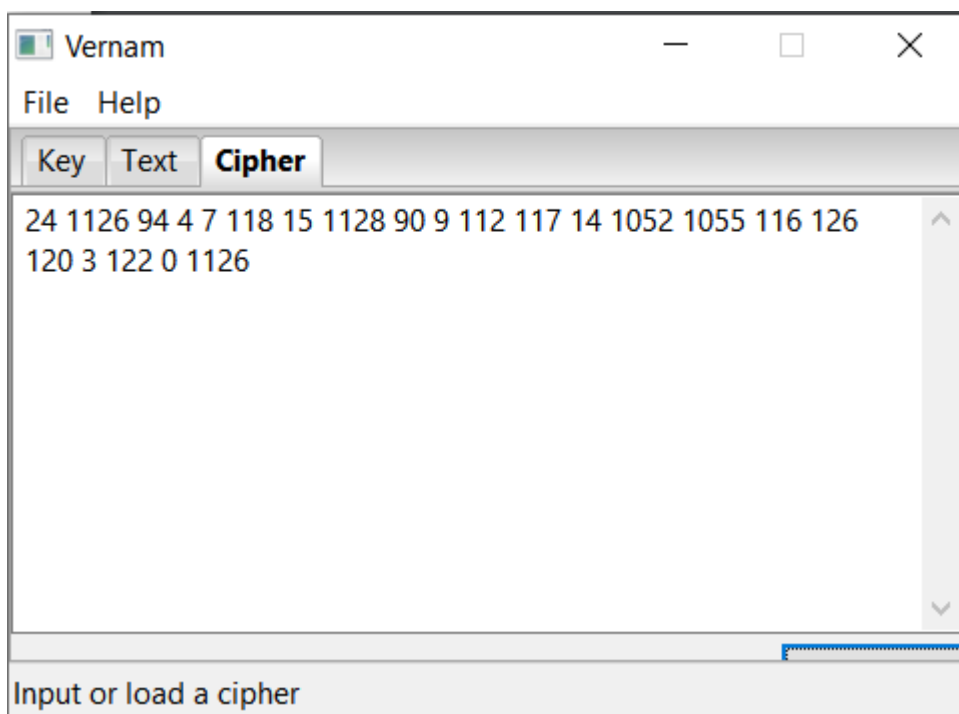
File Help

Key Text Cipher

йцукенгшщзфывапролджячсмитьб

Input or load a key

Текст зашифрованного сообщения:



The screenshot shows the Vernam application window with the 'Cipher' tab selected. The main text area contains the encrypted message '24 1126 94 4 7 118 15 1128 90 9 112 117 14 1052 1055 116 126 120 3 122 0 1126'. Below the text area is a label 'Input or load a cipher'.

Vernam

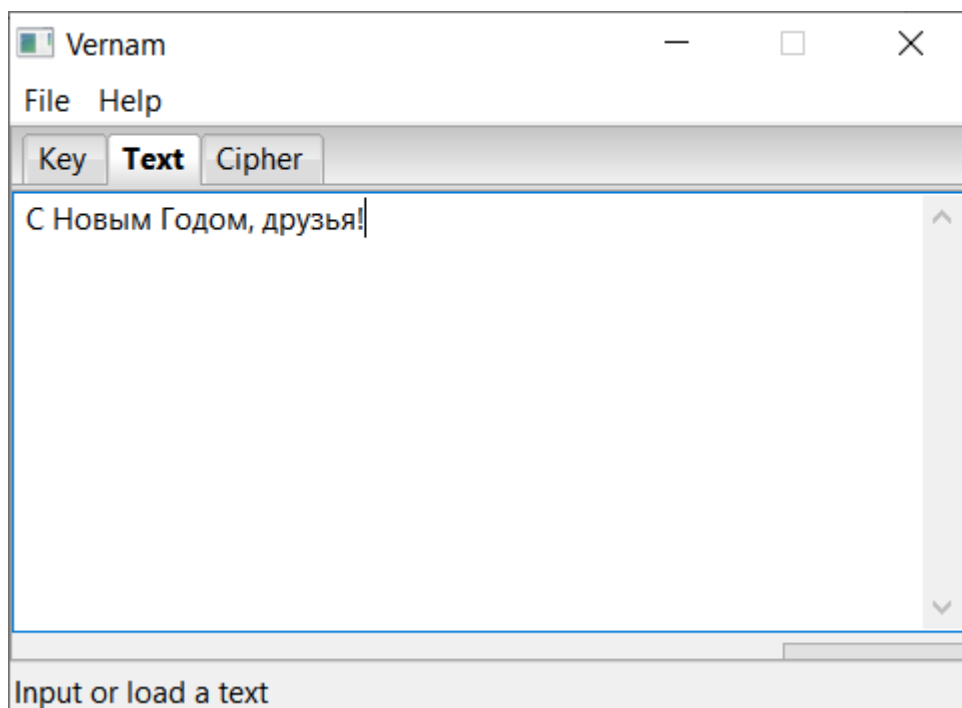
File Help

Key **Cipher** Text

24 1126 94 4 7 118 15 1128 90 9 112 117 14 1052 1055 116 126
120 3 122 0 1126

Input or load a cipher

Расшифрованное сообщение:



Выводы

Я освоила на практике применение режима однократного гаммирования.

Список литературы

1. [Лабораторная работа № 7](#)

::: {#refs} :::