

УО «Белорусский государственный университет информатики и
радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1
по предмету «Теория информации»

Вариант 9

Выполнил:

Левкович Н. С.

Гр. 451004

Проверил:

Болтак С. В

Минск 2026

Задание:

Вариант 9.

Написать программу, которая выполняет шифрование и дешифрование текстового файла любого размера, содержащего текст на заданном языке, используя следующие алгоритмы шифрования:

- Шифр Плейфейра, текст на английском языке;
- алгоритм Виженера, прогрессивный ключ, текст на русском языке.

Для всех алгоритмов ключ задается с клавиатуры пользователем.

Программа должна игнорировать все символы, не являющиеся буквами заданного алфавита, и шифровать только текст на заданном языке. Все алгоритмы должны быть реализованы в одной программе. Программа не должна быть написана в консольном режиме. Результат работы программы – зашифрованный/расшифрованный файл/ы. Кроме работы с файлами программа должна предоставлять ввод/вывод шифруемого текста с клавиатуры/на экран.

Шифр Плейфейра

Тесты:

1. Дымовое тестирование

Шифр Плейфейра (англ)

Исходный текст

Ввести открытый текст из файла

Ключ

Получившийся текст

Зашифровать

Дешифровать

Сохранить в файл

Шифр Плейфейра (англ)

Ввести открытый
текст из файла

Исходный текст

MUTOTENWPDOF

Ключ

hELIO

Получившийся текст

PROGRAMXMING

Зашифровать

Дешифровать

Сохранить в файл

Текст: PROGRAMMING

Ключевое слово: HELL

После преобразования текст будет выглядеть так:

PROGRAMXMING

Между повторяющимися символами ‘M’ вставляется пустой символ ‘X’.

Таблица:

H	E	L	A	B
C	D	F	G	I/J
K	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

PR -> MU

OG -> TO

RA -> ET

MX -> NW

MI -> PD

NG -> OF

Шифротекст: MUTOTENWPDOF

2.

Шифр Плейфейра (англ)

Ввести открытый
текст из файла

Исходный текст

CAT

Ключ

MEOW

Получившийся текст

GERZ

Зашифровать

Дешифровать

Сохранить в файл

Шифр Плейфейра (англ)

Ввести открытый
текст из файла

Исходный текст

GERZ

Ключ

MEOW

Получившийся текст

CATX

Зашифровать

Дешифровать

Сохранить в файл

Текст: CAT

Ключ: MEOW

Количество символов нечётное, поэтому в конец будет добавлен 'X'.

Изменённый текст: CATX

Таблица:

M	E	O	W	A
B	C	D	F	G
H	I/J	K	L	N
P	Q	R	S	T
U	V	X	Y	Z

CA -> GE

TX -> RZ

Шифротекст: **GERZ**

3.

Шифр Плейфейра (англ)

Исходный текст
XXXTENTACION

Ключ
DIED

Получившийся текст
YYYYYSGSYHFDPO

Зашифровать Дешифровать Сохранить в файл

Ввести открытый текст из файла

Шифр Плейфейра (англ)

Ввести открытый
текст из файла

Исходный текст

YYYYYSGSYHFDPO

Ключ

DIED

Получившийся текст

XWXWXWXWXTENTACION

Зашифровать

Дешифровать

Сохранить в файл

Текст: XXXTENTACION

Ключ: DIED

Изменённый текст: XXXXXTENTACION

Таблица:

D	I/J	E	A	B
C	F	G	H	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Поскольку ‘X’ используется по умолчанию в качестве пустого символа, то повторение в тексте этих символов провоцируют появление ещё большего количества таких символов, таким образом происходит коллизия.

XX -> YY

XX -> YY

XT -> YS

EN -> GS

TA -> YH

CI -> FD

ON -> PO

Шифротекст: **YYYYYSGSYHFDPO**

После дешифрации полученного шифротекста полученный текст станет ещё длиннее за счет повторяющихся символов ‘Y’.

В итоге текст будет изменён следующим образом:

YXYXYXYXYSGSYHFDPO

YX -> XW

YX -> XW

...

YS -> XT

GS -> EN

YH -> TA

FD -> CI

PO -> ON

В результате получим: **XWXWXWXWTENTACION**

Алгоритм Виженера, прогрессивный ключ

Алфавит языка:

А	1	Й	11	У	21	Э	31
Б	2	К	12	Ф	22	Ю	32
В	3	Л	13	Х	23	Я	33
Г	4	М	14	Ц	24		
Д	5	Н	15	Ч	25		
Е	6	О	16	Ш	26		
Ё	7	П	17	Щ	27		
Ж	8	Р	18	Ь	28		
З	9	С	19	Ы	29		
И	10	Т	20	Ь	30		

Алгоритм Виженера (русск)

Ввести открытый
текст из файла

Исходный текст

коРО00тки1Йз

Ключ

СО00нfk

Получившийся текст

ЭЮЯВГЪЭЫ

Зашифровать

Дешифровать

Сохранить в файл

Алгоритм Виженера (русск)

Ввести открытый
текст из файла

Исходный текст

ЭЮЯВГЪЭЫ

Ключ

СО00нfk

Получившийся текст

КОРОТКИЙ

Зашифровать

Дешифровать

Сохранить в файл

К	О	Р	О	Т	К	И	Й
С	О	Н	Т	П	О	У	Р
Э	Ю	Я	И	Г	Ь	Э	Ы

Шифротекст: ЭЮЯВГЪЭЫ

Недопустимые символы игнорируются как в исходном тексте, так и в ключе.

2.

Алгоритм Виженера (русск)

Ввести открытый
текст из файла

Исходный текст

шёпот

Ключ

МИЛ

Получившийся текст

ЁПЬЭ

Зашифровать

Дешифровать

Сохранить в файл

Алгоритм Виженера (русск)

Ввести открытый
текст из файла

Исходный текст

ЁПЬЭ

Ключ

МИЛ

Получившийся текст

шёпот

Зашифровать

Дешифровать

Сохранить в файл

Ш	Ё	П	О	Т
М	И	Л	Н	Й
Ё	П	Ь	Э	Э

Шифротекст: ЁПЬЭ

3.

Алгоритм Виженера (русск)

Ввести открытый
текст из файла

Исходный текст

ГОЛОС

Ключ

УЛИОЮОИЦ

Получившийся текст

ЧЫХЁЖ

Зашифровать

Дешифровать

Сохранить в файл

Алгоритм Виженера (русск)

Ввести открытый
текст из файла

Исходный текст

ЧЫХЁЖ

Ключ

УЛИОЮОИЦ

Получившийся текст

ГОЛОС

Зашифровать

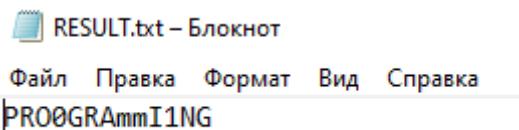
Дешифровать

Сохранить в файл

Г	О	Л	О	С
У	Л	И	Ц	Ф
Ч	Ы	Х	Ё	Ж

Шифротекст: ЧЫХЁЖ

Ввод из файла реализован кнопкой “Ввести открытый текст из файла”:



Шифр Плейфейра (англ)

Исходный текст

PRO0GRAmmI1NG

Сохранение результата в файл реализовано кнопкой “Сохранить в файл”:

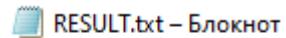
Получившийся текст

QSNHNSYNWNLSN

Зашифровать

Дешифровать

Сохранить в файл



Файл Правка Формат Вид Справка

QSNHNSYNWNLSN