

Министерство образования Республики Беларусь

Учреждение образования
**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ**

Факультет компьютерных систем и сетей
Кафедра программного обеспечения информационных технологий

ОТЧЕТ

по лабораторной работе
на тему:

КРИПТОАНАЛИЗ МЕТОДОВ ПРОСТОЙ ПОДСТАНОВКИ

Выполнил
Студент гр. 051007

Н. А. Захаренко

Проверил

Асс. С.В. Болтак

Минск, 2022

1. Задание

1.1 Постановка задачи

Вариант 5.

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

- перестановочный шифр: «**столбцовый метод**» с одним ключевым словом, текст на английском языке;

- два подстановочных шифра - алгоритм **Виженера**, **прогрессивный ключ**, текст на русском языке. **Метод децимаций** текст на английском 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.

1.2 Тесты и скриншоты

Столбцовый метод:

Входная строка: **CRYPTOGRAPHY AND DATA SECURITY**

Ключ: **CRYPT**

Результат: **CONDETPANARR GYA CYTP DSIYRATU**

C		R	Y	P	T
1		3	5	2	4
C		R	Y	P	T
O		G	R	A	P
H		Y	A	N	D
D		A	T	A	S
E		C	U	R	I
T		Y			

lab01_TL_051007

FileColumn method

Lab01

CRYPTOGRAPHY AND DATA SECURITY

COHDETPANARR GYA CYTP DSIYRATU

CRYPT

Encrypt

lab01_TL_051007

FileColumn method

Lab01

COHDETPANARR GYA CYTP DSIYRATU

CRYPTOGRAPHY AND DATA SECURITY

CRYPT

Decrypt

Входная строка: **TEXT**
Ключ: **SUPERLONGKEY**
Результат: **TXTE**

S	U	P	E	R	L	O	N	G	K	E	Y
10	11	8	1	9	5	7	6	3	4	2	12
T	E	X	T								
Результат: TXTE											

Входная строка: **YES**
Ключ: **A**
Результат: **YES**

A
1
Y
E
S
Результат: YES

Входная строка: **GARЬ AGE!**
Ключ: **КЕШY2**
Результат: **AGGЬ ARE!**

K	E	Ш	Y	2
2	1	-	3	-
G	A	-	R	-
A	G	-	E	-
Результат: AGGЬ ARE!				

lab01_TI_051007

File

Lab01

Column method

GARЬ AGE!

AGGЬ ARE!

КЕШY2

Encrypt

Входная строка: **abcde**
Ключ: **edcba**
Результат: **edcba**

e	d	c	b	a
5	4	3	2	1
a	b	c	d	e

Метод Виженера:

Буквы исходного текста																																			
	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я		
Буквы ключа	А	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
	Б	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
	В	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
	Г	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
	Д	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
	Е	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
	Ё	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё
	Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж
	З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З
	И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И
	Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
	К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К
	Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
	М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
	Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
	О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
	П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
	Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р
	С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
	Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
	У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
	Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
	Х	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
	Ц	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
	Ч	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
	Ш	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Щ	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	
Ъ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	
Ы	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	
Ь	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	
Э	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	
Ю	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	
Я	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я		

Входная строка: Исходный текст
Ключ: Ключ (Прогрессивный ключ: КЛЮЧ|ЛМЯШ|МНАЩ|Н)
Результат: УЭУЁПЪВ ЯТККА

Входная строка: Ёжик
Ключ: ё(Прогрессивный ключ: ёжзи)
Результат: ЛНРУ

lab01_TI_051007

File Vinegere method

Lab01

Исходный текст

УЭУЁПЪЪВ ЯТККА

Ключ

Encrypt

lab01_TI_051007

File Vinegere method

Lab01

УЭУЁПЪЪВ ЯТККА

ИСХОДНЫЙ ТЕКСТ

Ключ

Decrypt

Входная строка: **САНКТ-ПЕТЕРБУРГ – ГОРОД СВЯТОГО ПЕТРА**
Ключ: **ленин**

Результат: **ЭЕЫУА-ЬКБОЯОЪАН – ТЭШЯП ВСЗДЫФЯ ЩЧАГС**

Входная строка: **ЁЛКИ ЗЕЛЁНЫЕ В ЛЕСУ**
Ключ: **ЛЕС**

Результат: СРЪХ НЧЩМБЙМ Ц ЫНЖД

lab01_TI_051007

File

Lab01

Vingere method

ЁЛКИ ЗЕЛЁНЫЕ В ЛЕСУ

СРЪХ НЧЩМБЙМ Ц ЫНЖД

ЛЕС

Encrypt

Входная строка: ЁЛRVФКИ ЗЕ!!ЛЁНЫЕ В ЛЕ@СУ!

Ключ: ЛWE_C2

Результат: СРRVФЪХ_НЧ!!ЩМБЙМ Ц ЫН@ЖД!

Метод Децимации:

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	13	14	15	16	17	18	19	20	21	22	23	24	25

Входная строка: **Cryptography**

Ключ: **3**

Результат: **Gzutfqszatvu**

$G = (\text{POS}('C') * 3) \bmod 26 = 2 * 3 \bmod 26 = 6 \bmod 26 = 16$
 $z = (\text{POS}('r') * 3) \bmod 26 = 17 * 3 \bmod 26 = 51 \bmod 26 = 25$
 $u = (\text{POS}('y') * 3) \bmod 26 = 24 * 3 \bmod 26 = 72 \bmod 26 = 20$
 $t = (\text{POS}('p') * 3) \bmod 26 = 15 * 3 \bmod 26 = 45 \bmod 26 = 19$
 $f = (\text{POS}('t') * 3) \bmod 26 = 19 * 3 \bmod 26 = 57 \bmod 26 = 5$
 $q = (\text{POS}('o') * 3) \bmod 26 = 14 * 3 \bmod 26 = 42 \bmod 26 = 16$
 $s = (\text{POS}('g') * 3) \bmod 26 = 6 * 3 \bmod 26 = 18 \bmod 26 = 18$
 $z = (\text{POS}('r') * 3) \bmod 26 = 17 * 3 \bmod 26 = 51 \bmod 26 = 25$
 $a = (\text{POS}('a') * 3) \bmod 26 = 0 * 3 \bmod 26 = 0 \bmod 26 = 0$
 $t = (\text{POS}('p') * 3) \bmod 26 = 15 * 3 \bmod 26 = 45 \bmod 26 = 19$
 $v = (\text{POS}('h') * 3) \bmod 26 = 7 * 3 \bmod 26 = 21 \bmod 26 = 21$
 $u = (\text{POS}('y') * 3) \bmod 26 = 24 * 3 \bmod 26 = 72 \bmod 26 = 20$

lab01_TI_051007

File

Decimation method

Lab01

Cryptography

Gzutfqszatvu

3

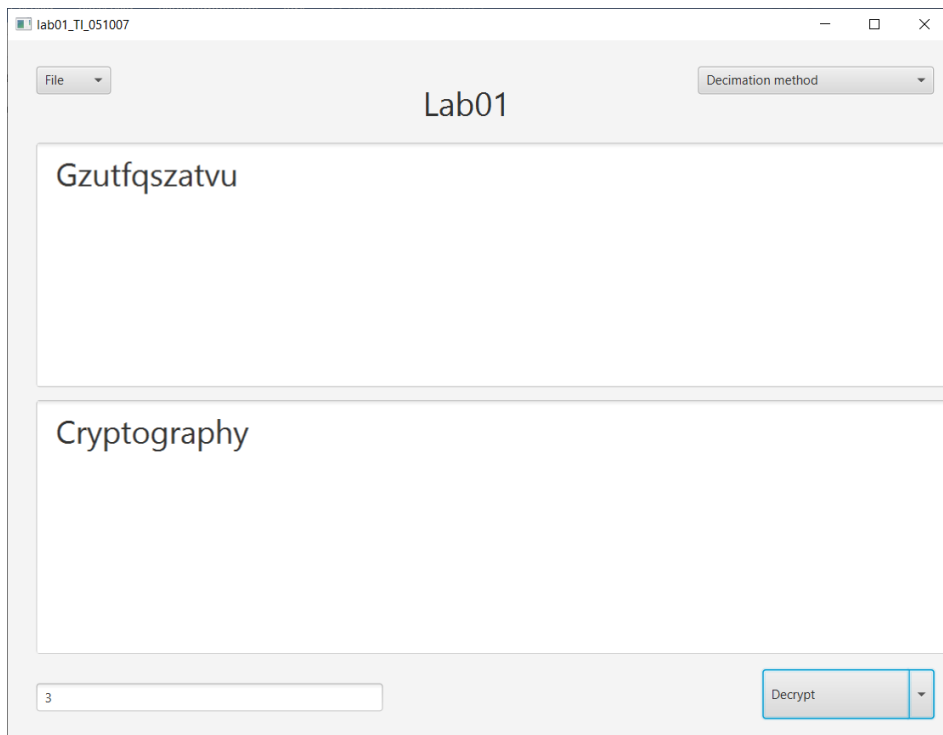
Encrypt

Входная строка: **Text!**

Ключ: **0**

Результат: **Aaaa!**

$(\text{<Любой символ>} * 0) \% 26 = 0 = A$



Входная строка: **ABC**

Ключ: **5**

Результат: **AFK**

$$(0(A) * 5) \% 26 = 0(A)$$

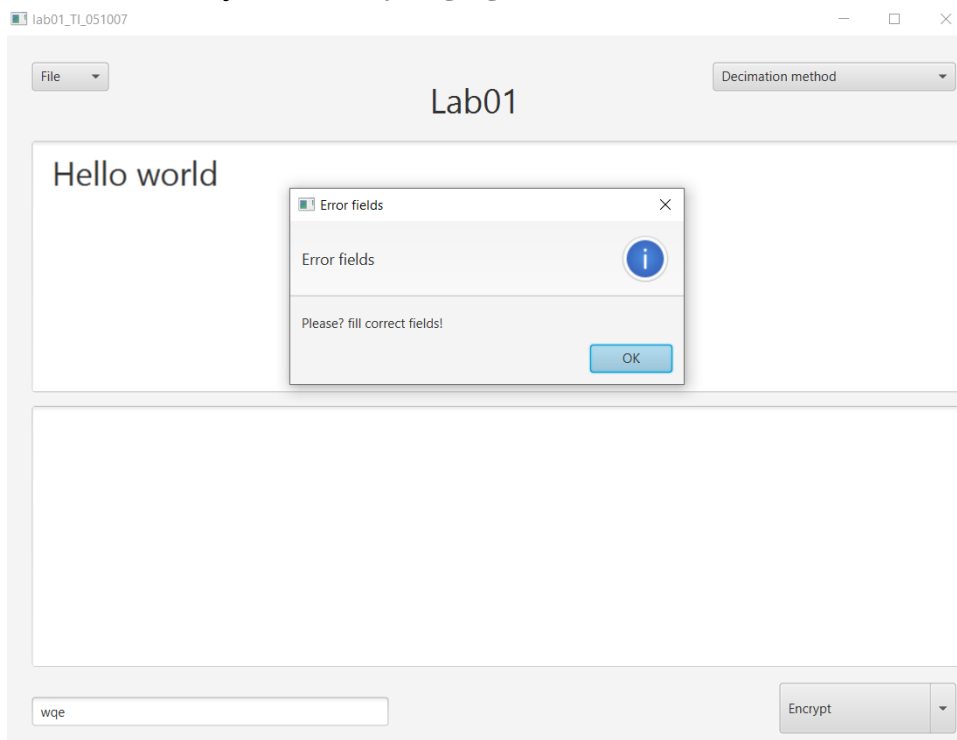
$$(1(B) * 5) \% 26 = 5(F)$$

$$(2(C) * 5) \% 26 = 10(K)$$

Входная строка: **Hello world**

Ключ: **45**

Результат: **Dybbg cglbf**



Входная строка: **Hel123lo woБ3rld!**

Ключ: **45**

Результат: **Dyb123bg cgБ3lbf!**

lab01_TI_051007

File

Lab01

Decimation method

Hel123lo woБ3rld!

Dyb123bg cgБ3lbf!

45

Encrypt

lab01_TI_051007

File

Lab01

Decimation method

Dyb123bg cgБ3lbf!

Hel123lo woБ3rld!

45

Decrypt