

Теория информации
Яковлев В.Ю. 051003
Тесты
Вариант 6

1. Столбцовый улучшенный метод.

Шифрование:

Фраза = CRYPTOGRAPHY Дымовое AND DATA SECURITY

Ключ = Скрытестированиет

С R Y P T (Ключ)

1 3 5 2 4 (Последовательность столбцов)

С

R Y P T

O G

R A P H Y

A N D

D

A T A S

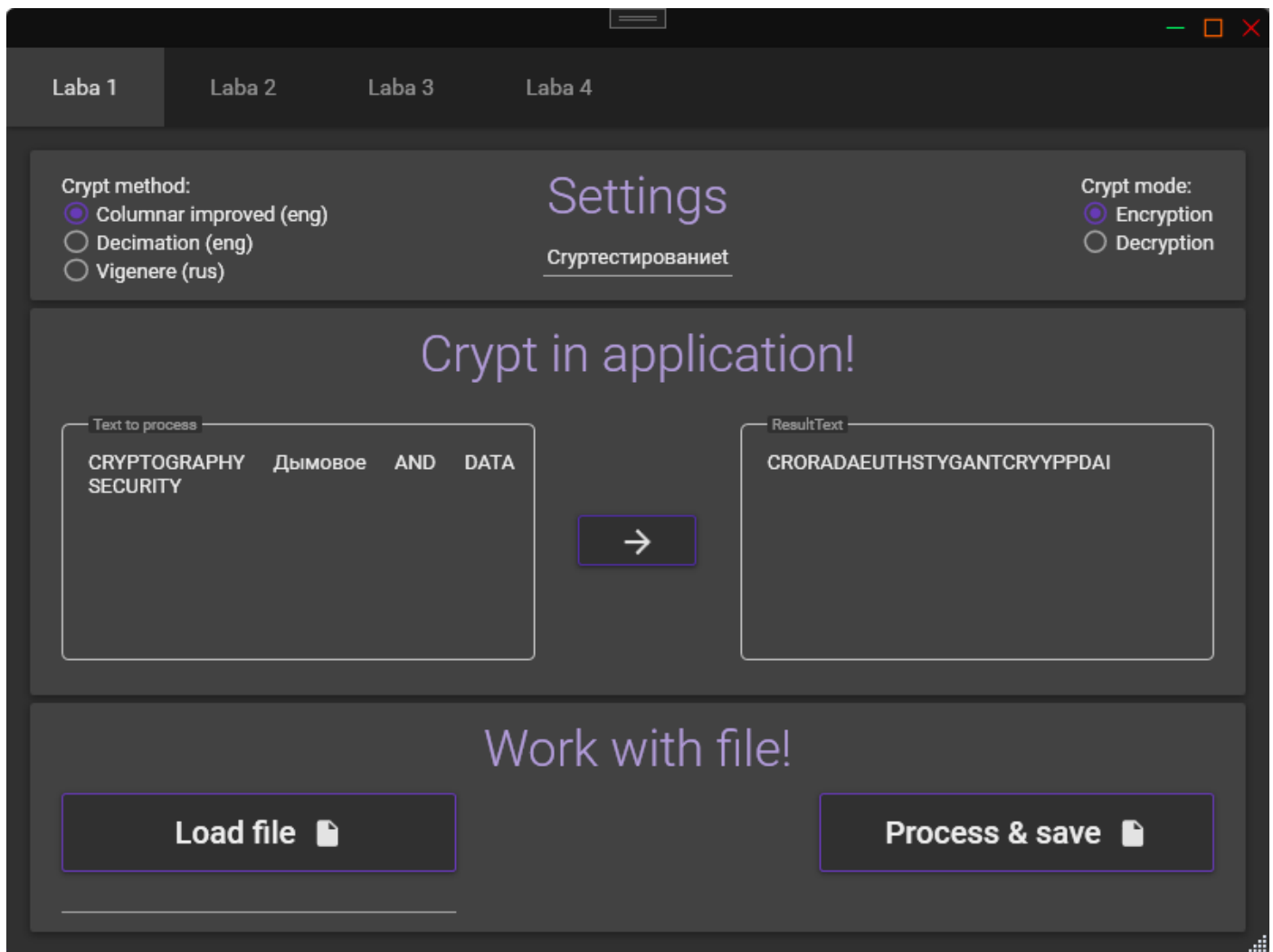
E C

U R I T Y

"CRORADAEU"+"THST"+"YGANTCR"+"YY"+"PPDAI"=

CRORADAEUTHSTYGANTCRYYPPDAI

Шифротекст = CRORADAEUTHSTYGANTCRYYPPDAI



Дешифрование

Шифротекст = CRORADAEUTHSTYGAШИФР?NTCRYPPDAI

Ключ = СrypЧТО t

Длина шифротекста = 27.

С помощью шифрования бессмысленной строки (длина длина шифротекста) узнаём кол-во символов в каждом столбце.

С	Р	У	Р	Т	(Ключ)
1	3	5	2	4	(Последовательность столбцов)
А					
А	А	А	А		
А	А				
А	А	А	А	А	
А	А	А			
А					
А	А	А	А	А	
А	А				
А	А	А	А	А	

Так шифротекст разбивается на 5 частей (столбцов), которые были при шифровании:

CRORADAEUTHSTYGANTCRYYPDAI = "CRORADAEU" (1) + "THST" (2) + "YGANTCR" (3) + "YY" (4) + "PPDAI" (5) .

Заносим полученные части в столбцы, очередность заполнения определяется ключом.

Получаем:

С R Y P T (Ключ)

1 3 5 2 4

С

R Y P T

O G

R A P H Y

A N D

D

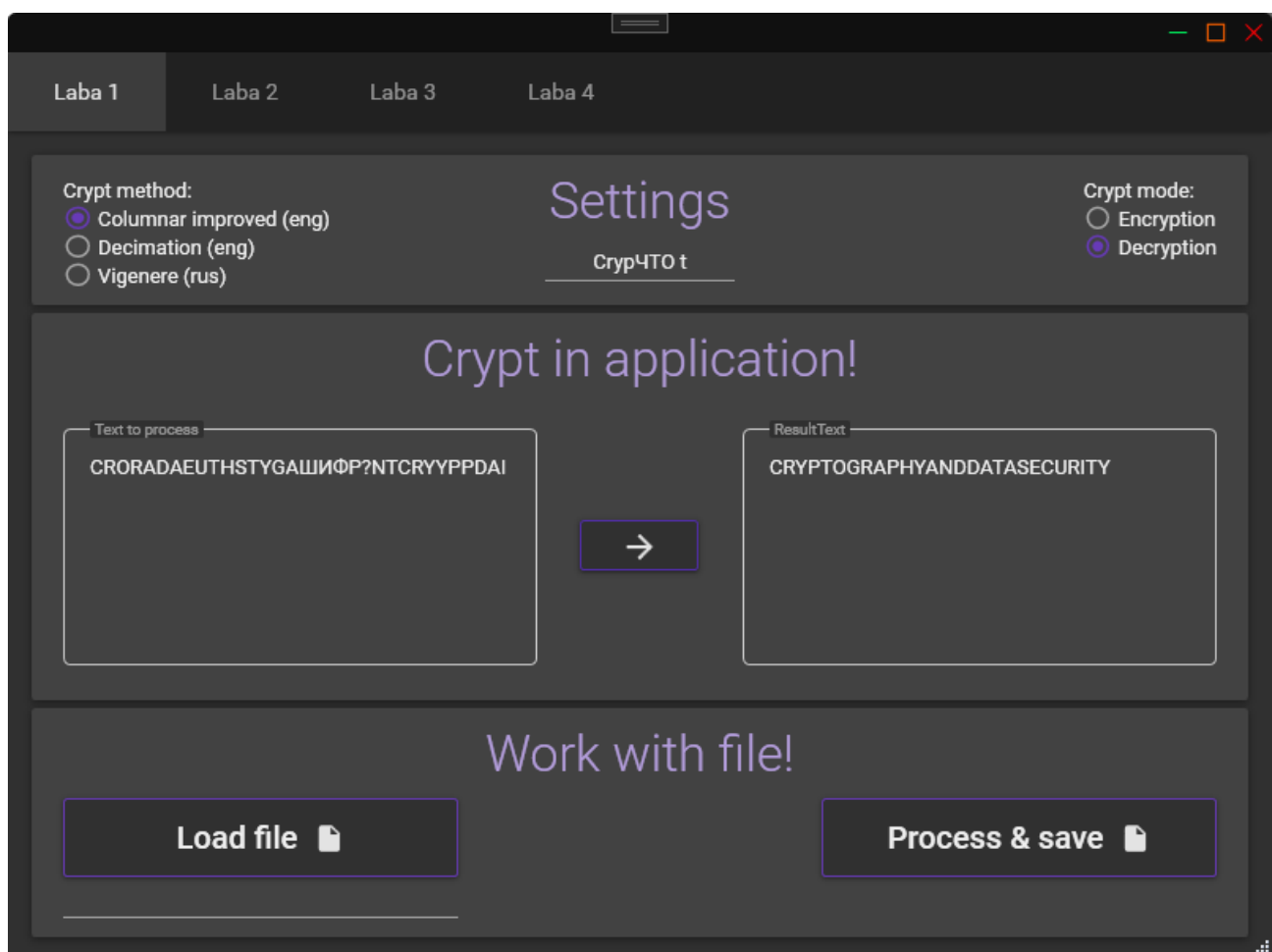
A T A S

E C

U R I T Y

При построчном чтении слева направо получаем исходный текст = CRYPTOGRAPHYANDDATASECURITY.

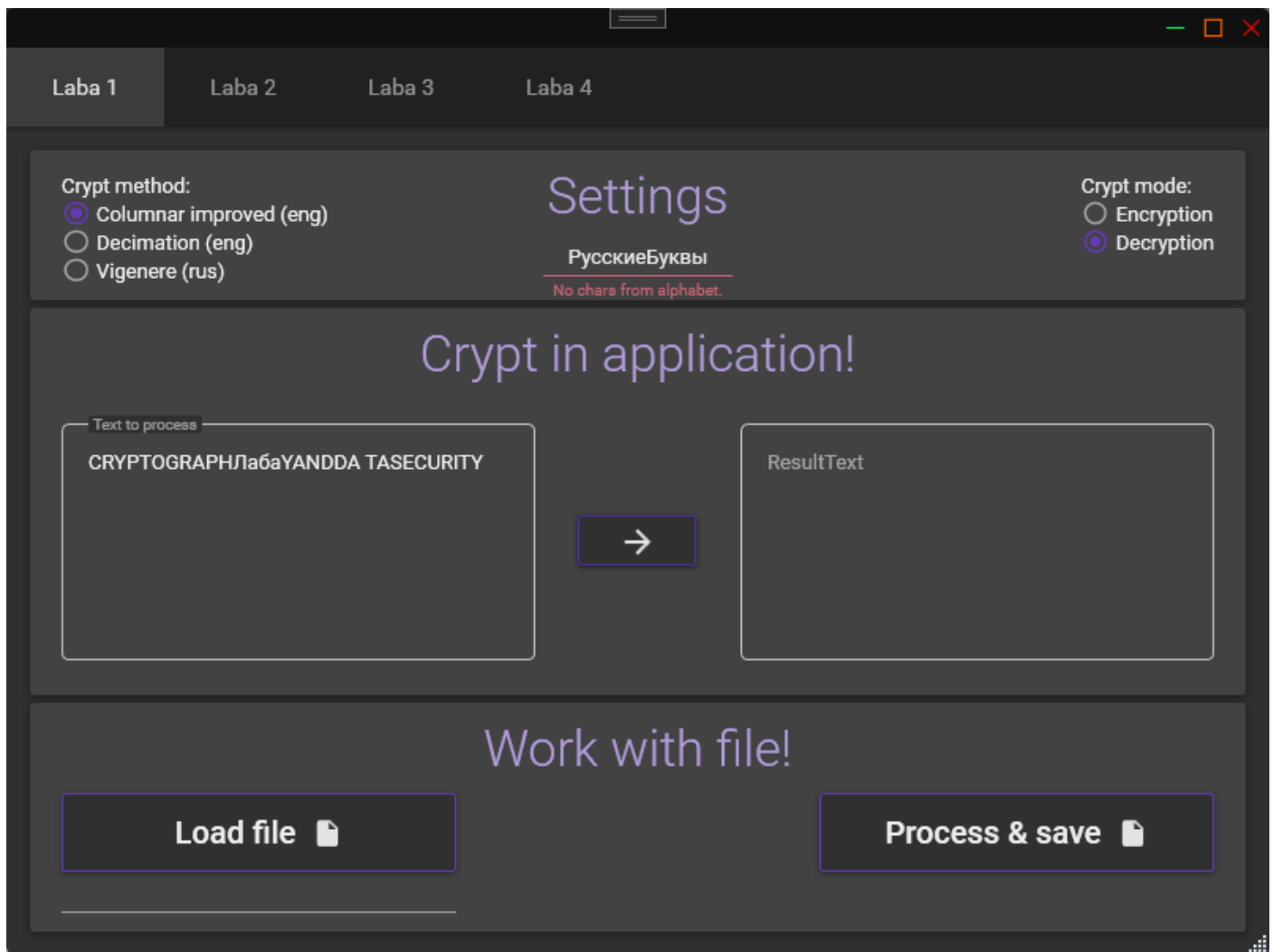
Фраза = CRYPTOGRAPHYANDDATASECURITY



Шифрование с длиной ключа >длины текста
Фраза = text
Ключ = mnogobukv
Шифротекст = TTEX

The screenshot shows a software application window with a dark theme. At the top, there are four tabs labeled 'Laba 1', 'Laba 2', 'Laba 3', and 'Laba 4', with 'Laba 1' being the active tab. The main content area is divided into three sections. The top section, titled 'Settings', contains 'Crypt method' options: 'Columnar improved (eng)' (selected), 'Decimation (eng)', and 'Vigenere (rus)'. It also shows the key 'mnogobukv' and 'Crypt mode' options: 'Encryption' (selected) and 'Decryption'. The middle section, titled 'Crypt in application!', features two text input fields. The left field, labeled 'Text to process', contains the text 'text'. The right field, labeled 'ResultText', contains the encrypted text 'TTEX'. A right-pointing arrow button is positioned between these two fields. The bottom section, titled 'Work with file!', contains two buttons: 'Load file' and 'Process & save', each accompanied by a file icon. The application window has standard Windows-style window controls (minimize, maximize, close) in the top right corner.

Шифрование при невалидном ключе (ошибка):
Фраза = CRYPTOGRAPHЛабаYANDDA TASECURITY
Ключ = РусскиеБуквы



2. Метод децимаций.

Английский алфавит:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
19	20	21	22	23	24	25												
T	U	V	W	X	Y	Z												

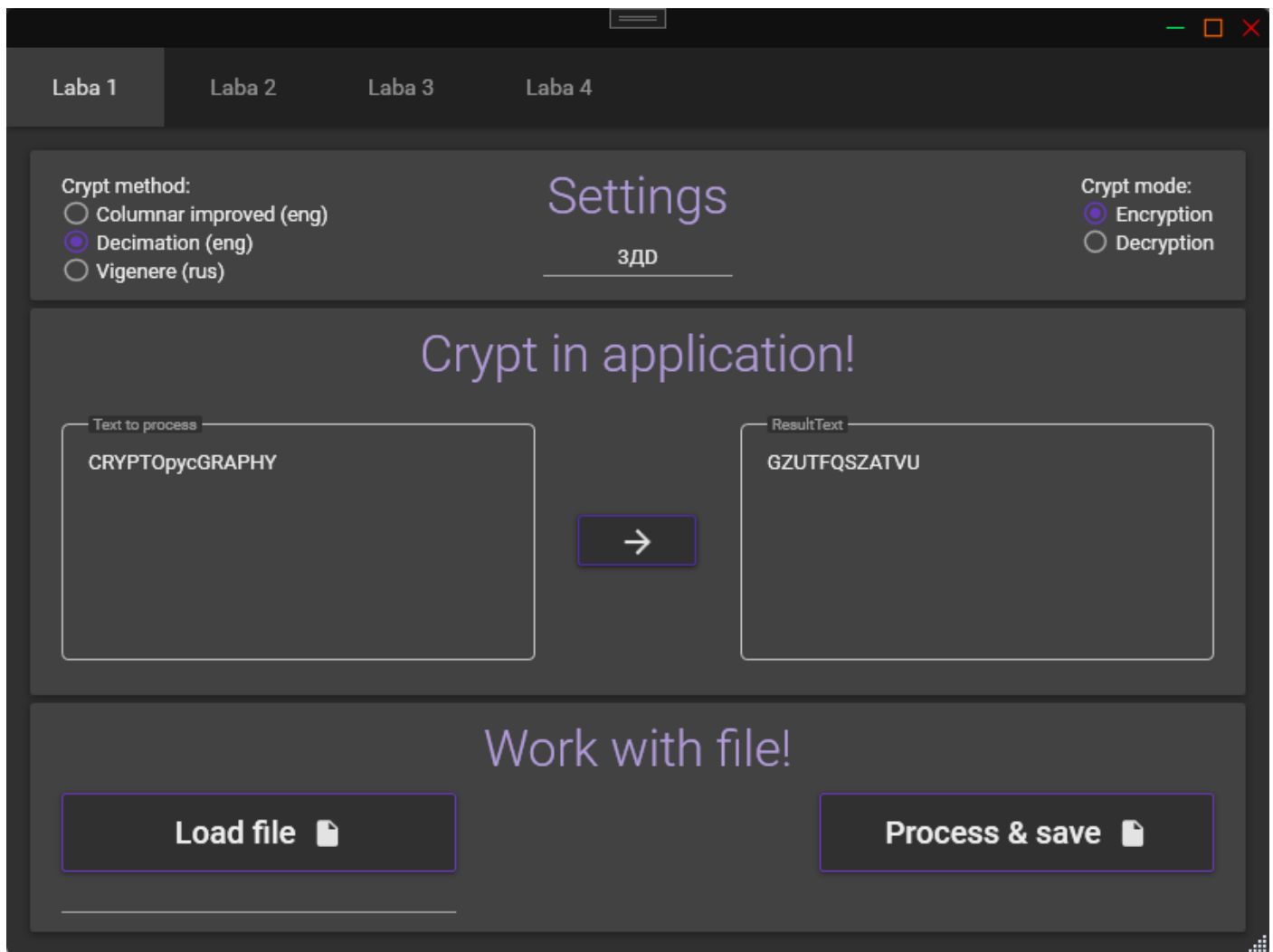
Шифрование:

Фраза = CRYPTOрусGRAPHY

Ключ = 3ДД

C	R	Y	P	T	O	G	R	A	P	H	Y
2	17	24	15	19	14	6	17	0	15	7	24
						*3%26					
6	25	20	19	5	16	18	25	0	19	21	20
G	Z	U	T	F	Q	S	Z	A	T	V	U

Шифротекст = GZUTFQSZATVU



Дешифрование:

Шифротекст = русGZрусUTFQSZATVUрус

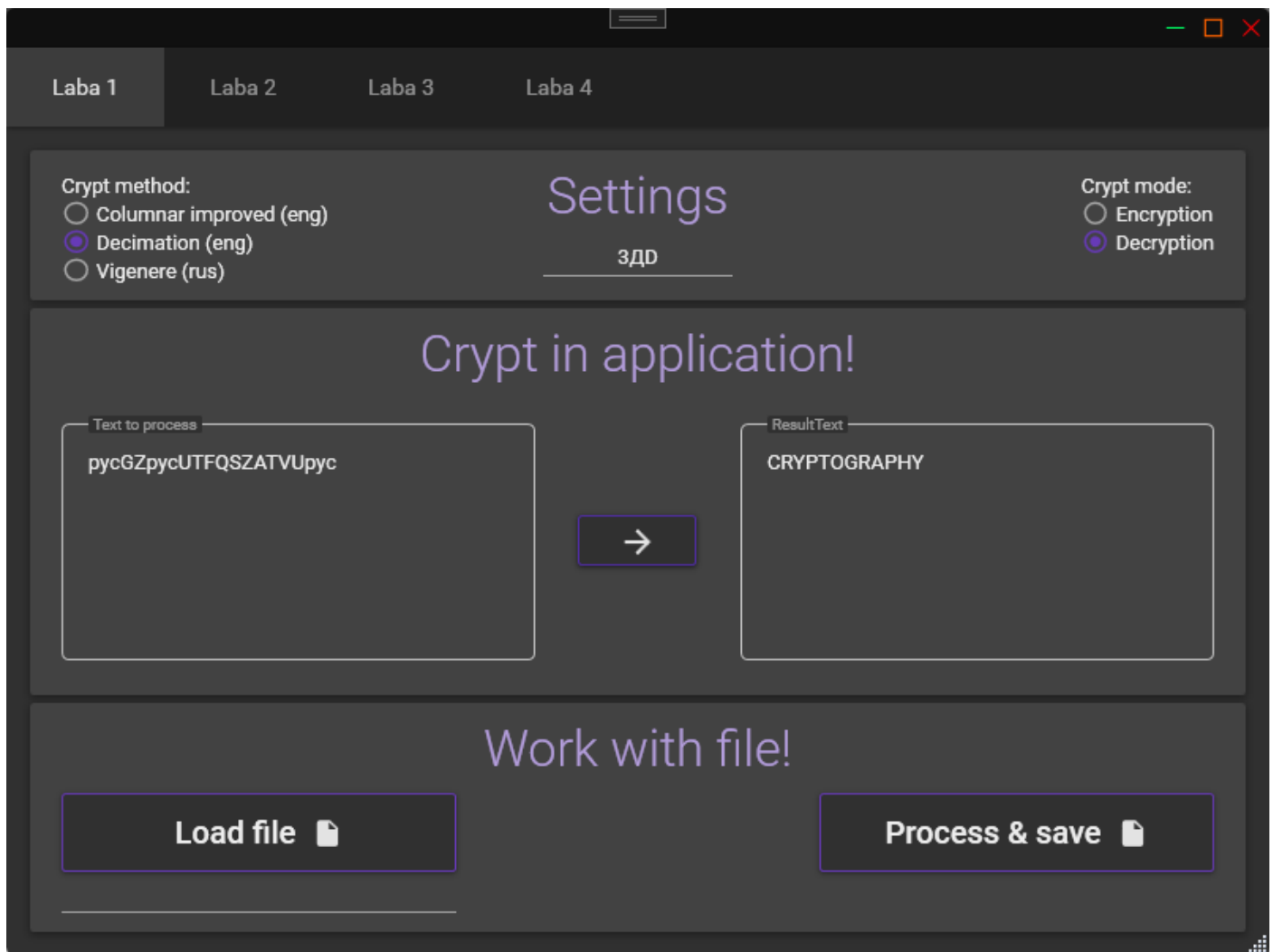
Ключ = 3DD

Зашифрованный английский алфавит (для ключа 3):

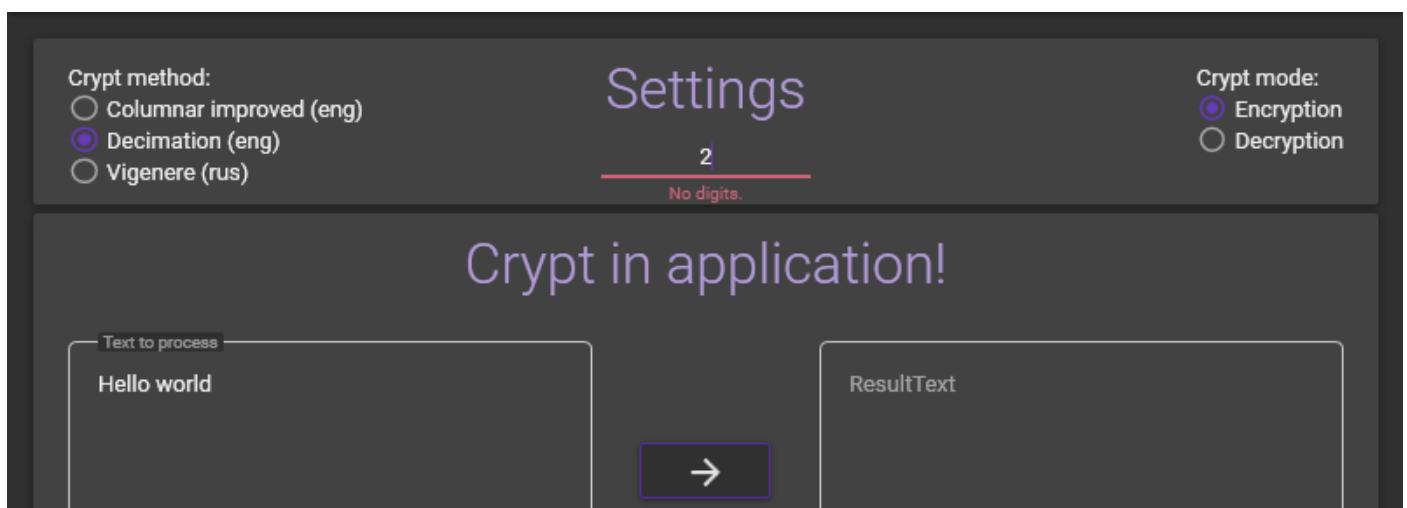
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X

Шифротекст = GZUTFQSZATVU. Заменяем символы шифротекста на символы из оригинального алфавита по таблице выше.

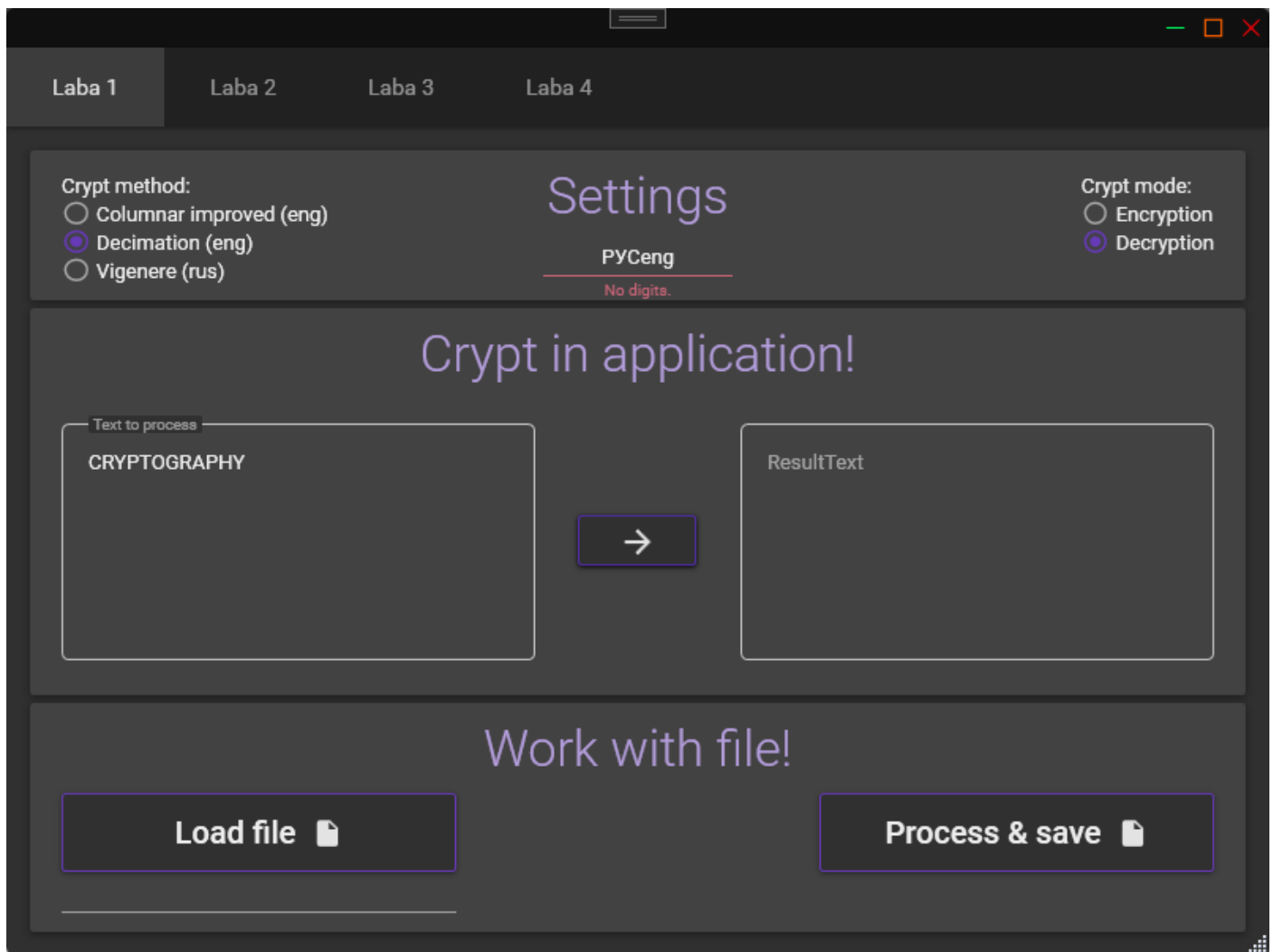
G Z U T F Q S Z A T V U
C R Y P T O G R A P H Y
Фраза = CRYPTOGRAPHY



Использование не взаимно простых чисел в ключе (ошибка)
Фраза = Hello World
Ключ = 2 (длина алфавита = 26)



Дешифрование при невалидном ключе (ошибка):
Фраза = CRYPTOGRAPHY
Ключ = РУСeng



3. Метод Виженера.

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	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
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	
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		
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			
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				
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					
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						
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							
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								
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									
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я										
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я											
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я												
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я													
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я														
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я															
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																	
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																		
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																			
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																				
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																					
Х	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																						
Ц	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																							
Ч	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																								
Ш	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я																									
Щ	Щ	Ъ	Ы	Ь	Э	Ю	Я																										
Ъ	Ъ	Ы	Ь	Э	Ю	Я																											
Ы	Ы	Ь	Э	Ю	Я																												
Ь	Ь	Э	Ю	Я																													
Э	Э	Ю	Я																														
Ю	Ю	Я																															
Я	Я																																

Шифрование:

Фраза = САНКТ-ПЕТЕРБУРГ TETRIS – ГОРОД СВЯТОГО ПЕТРА

Ключ = леSTALINнин

Используя таблицу выше, находим пересечения строки (начинается с символа ключа) и столбца (начинается с символа текста).

САНКТПЕТЕРБУРГГГОРОДСВЯТОГОПЕТРА

ЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛ (Ключ)

ЭЕЫУАЫЙАНЮМШЮЛРЪХЪМЯНДАЧРЪФТЫЮЛ

Шифротекст = ЭЕЫУАЫЙАНЮМШЮЛРЪХЪМЯНДАЧРЪФТЫЮЛ

The screenshot shows a web application with a dark theme. At the top, there are four tabs labeled 'Laba 1', 'Laba 2', 'Laba 3', and 'Laba 4'. The main content area is divided into two sections. The top section is titled 'Settings' and contains two groups of radio buttons. On the left, 'Crypt method:' has three options: 'Columnar improved (eng)', 'Decimation (eng)', and 'Vigenere (rus)' (which is selected). On the right, 'Crypt mode:' has two options: 'Encryption' (selected) and 'Decryption'. Below the settings, there is a large heading 'Crypt in application!'. Under this heading, there are two text input fields. The left field, labeled 'Text to process', contains the text 'САНКТ-ПЕТЕРБУРГ TETRIS – ГОРОД СВЯТОГО ПЕТРА'. The right field, labeled 'ResultText', contains the encrypted text 'ЭЕЫУАЫЙАНЮМШЮЛРЪХЪМЯНДАЧРЪФТЫЮЛ'. A blue arrow button points from the left field to the right field. Below this section, there is another heading 'Work with file!'. Under this heading, there are two buttons: 'Load file' with a file icon and 'Process & save' with a file icon. A horizontal line is visible below the 'Load file' button.

Дешифрование:

Шифротекст = ЭЕЫУАЫЙАНЮМШSSGYЛРЪХЪМЯНДАЧРЪФТЫЮЛ

Ключ = леSTALINнин

Используя таблицу выше, находим строку по букве ключа, находим букву шифротекста. Верхняя буква является буквой исходного текста.

ЭЕЫУАЫЙАНЮМШЮЛРЪХЪМЯНДАЧРЪФТЫЮЛ

ЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛ (Ключ)

САНКТПЕТЕРБУРГГГОРОДСВЯТОГОПЕТРА

Фраза = САНКТПЕТЕРБУРГГОРОДСВЯТОГОПЕТРА

Lab 1 Lab 2 Lab 3 Lab 4

Crypt method:

- ☐ Columnar improved (eng)
- ☐ Decimation (eng)
- ☒ Vigenere (rus)

Settings

леSTALINнин

Crypt mode:

- ☐ Encryption
- ☒ Decryption

Crypt in application!

Text to process

ЭБЫУАЫЙАНИОМШISSGYLPРЪХЪМЯНДАЧР
ЪФТЫЮЛ

ResultText

САНКТПЕТЕРБУРГГОРОДСВЯТОГОПЕТРА

Work with file!

Load file

Process & save

Шифрование при длине ключа > длина текста

Фраза = Факультет

Ключ = Университет

Шифротекст = ЗНУХРМДНЕ

Lab 1 Lab 2 Lab 3 Lab 4

Crypt method:

- ☐ Columnar improved (eng)
- ☐ Decimation (eng)
- ☒ Vigenere (rus)

Settings

УНИВЕРСИТЕТ

Crypt mode:

- ☒ Encryption
- ☐ Decryption

Crypt in application!

Text to process

ФАКУЛЬТЕТ

ResultText

ЗНУХРМДНЕ

Work with file!

Load file

Process & save

Шифрование при невалидном ключе (ошибка):
Фраза = ЭЕЫУАЫЙАНЮМШSSGЮЛРЪХЪМЯНДАЧРЪФТЫЮЛ
Ключ = STALIN

Laba 1Laba 2Laba 3Laba 4

Crypt method:

☐ Columnar improved (eng)☐ Decimation (eng)☒ Vigenere (rus)

Settings

STALIN

No chars from alphabet.

Crypt mode:

☐ Encryption☒ Decryption

Crypt in application!


Text to process

ЭЕЫУАЫЙАНЮМШSSGЮЛРЪХЪМЯНДАЧРЪФТЫЮЛ

→

ResultText

Work with file!

Load file 

Process & save 