Теория информации

Яковлев В.Ю. 051003

Тесты

Вариант 6

1. Столбцовый улучшенный метод.

Шифрование:

Фраза = CRYPTOGRAPHY Дымовое AND DATA SECURITY

Ключ = Crypтестированиеt

C R Y P T (Ключ)

1 3 5 2 4 (Последовательность столбцов)

C

R Y P T

O G

R A P H Y

A N D

D

A T A S

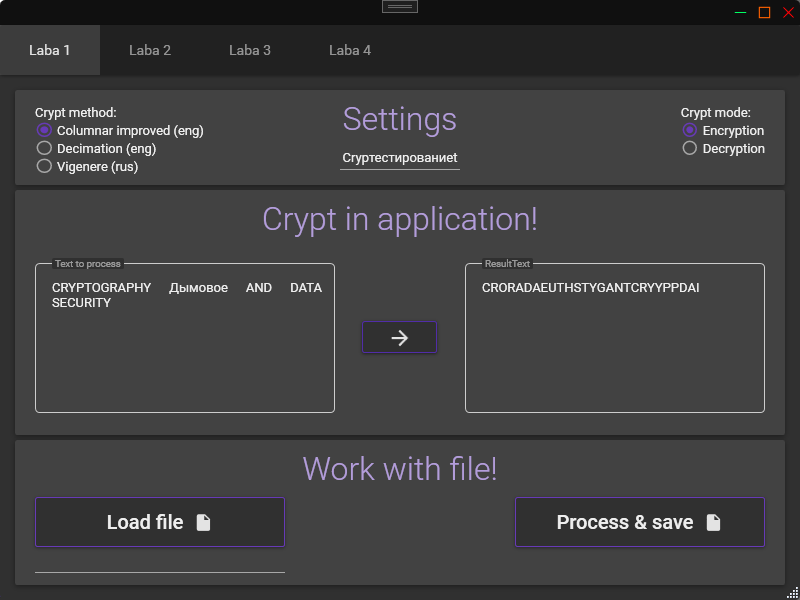
E C

U R I T Y

”CRORADAEU”+”THST”+”YGANTCR”+”YY”+”PPDAI”=

CRORADAEUTHSTYGANTCRYYPPDAI

Шифротекст = CRORADAEUTHSTYGANTCRYYPPDAI



Дешифрование

Шифротекст = CRORADAEUTHSTYGAШИФР?NTCRYYPPDAI

Ключ = CrypЧТО t

Длина шифротекста = 27.

С помощью шифрования бессмысленной строки (длина

длина шифротекста) узнаём кол-во символов в каждом столбце.

C R Y P T (Ключ)

1 3 5 2 4 (Последовательность столбцов)

А

А А А А

А А

А A А А А

A А А

А

А А A А

А А

А А А А А

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

CRORADAEUTHSTYGANTCRYYPPDAI = ”CRORADAEU”(1)+ ”THST”(2)+”YGANTCR”(3)+”YY”(4)+”PPDAI”(5).

Заносим полученные части в столбцы, очерёдность заполнения определяется ключом.

Получаем:

C R Y P T (Ключ)

1 3 5 2 4

C

R Y P T

O G

R A P H Y

A N D

D

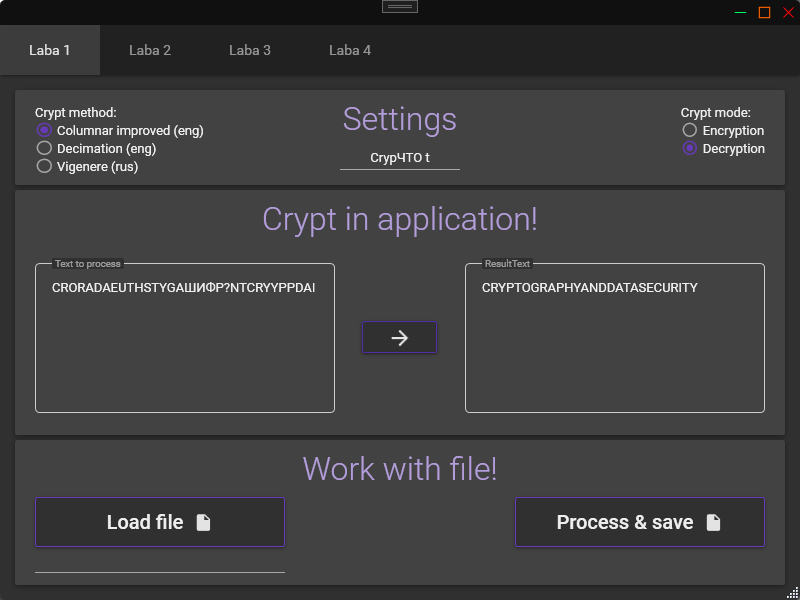
A T A S

E C

U R I T Y

При построчном чтении слева направо получаем исходный текст = CRYPTOGRAPHYANDDATASECURITY.

Фраза = CRYPTOGRAPHYANDDATASECURITY

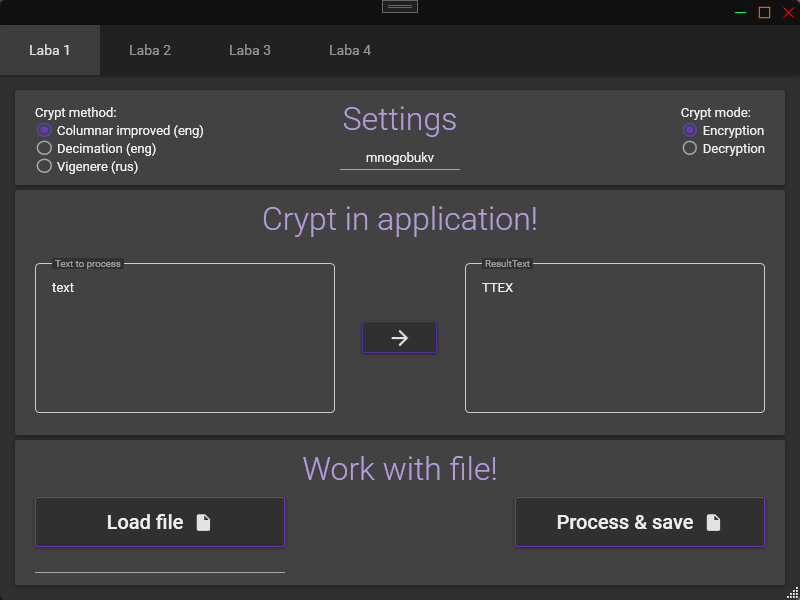


Шифрование с длиной ключа >длины текста

Фраза = text

Ключ = mnogobukv

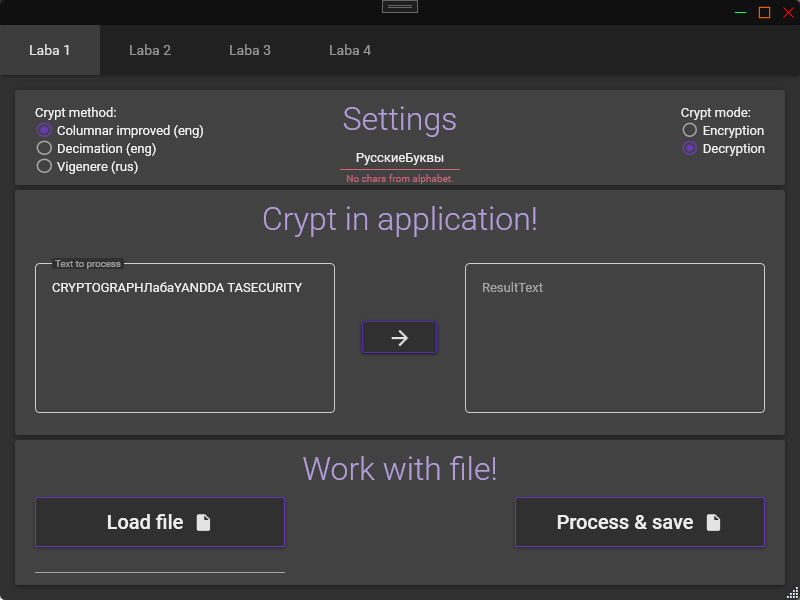
Шифротекст = TTEX



Шифрование при невалидном ключе (ошибка):

Фраза = CRYPTOGRAPHЛабаYANDDA TASECURITY

Ключ = РусскиеБуквы



1. 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 = 3ДD

C R Y P T O G R A P H Y

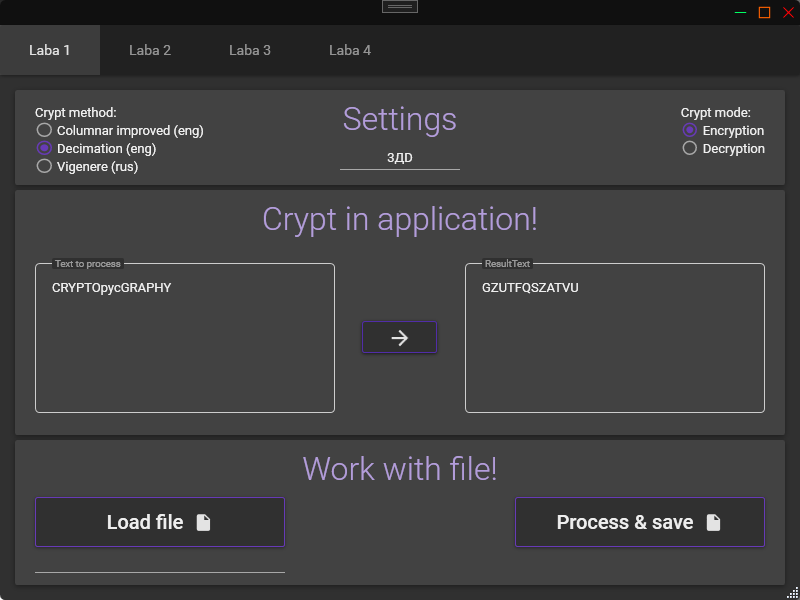
2 17 24 15 19 14 6 17 0 15 7 24

\*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 = 3ДD

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

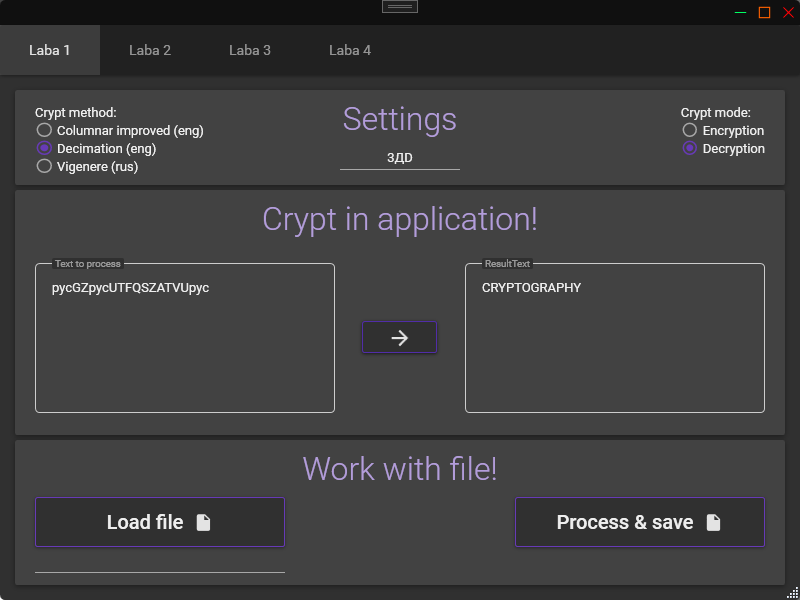
A D G J M P S V Y B E H K N Q T W Z C F I L O R U X

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

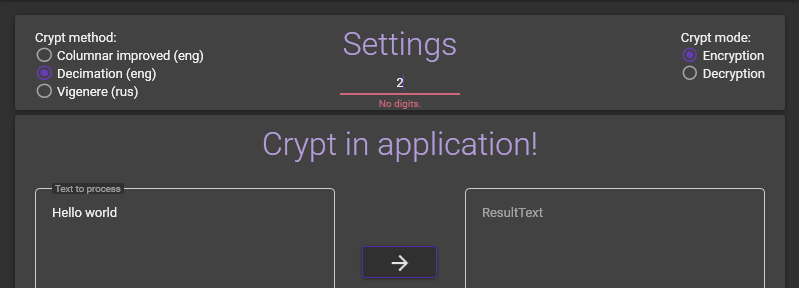
Фраза = CRYPTOGRAPHY



Использование не взаимно простых чисел в ключе (ошибка)

Фраза = Hello World

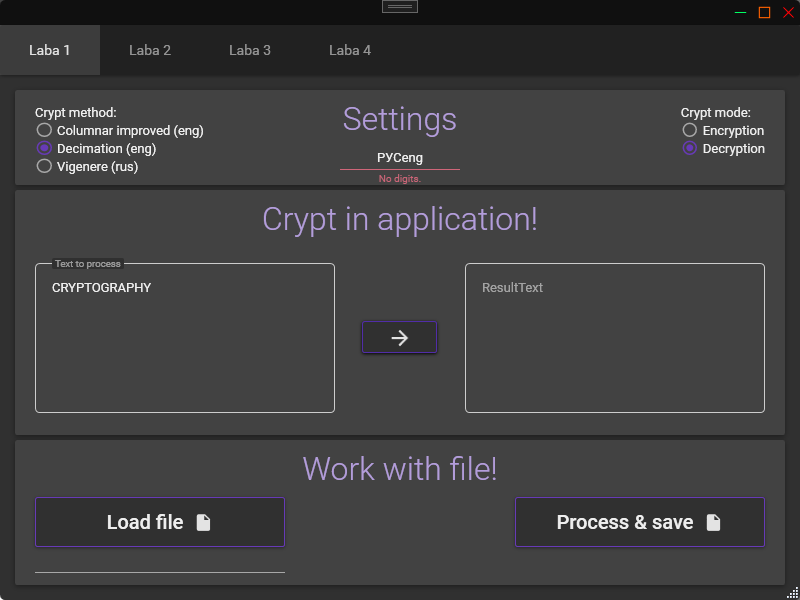
Ключ = 2 (длина алфавита = 26)



Дешифрование при невалидном ключе (ошибка):

Фраза = CRYPTOGRAPHY

Ключ = РУСeng



1. Метод Виженера.



Шифрование:

Фраза = САНКТ-ПЕТЕРБУРГ TETRIS – ГОРОД СВЯТОГО ПЕТРА

Ключ = леSTALINнин

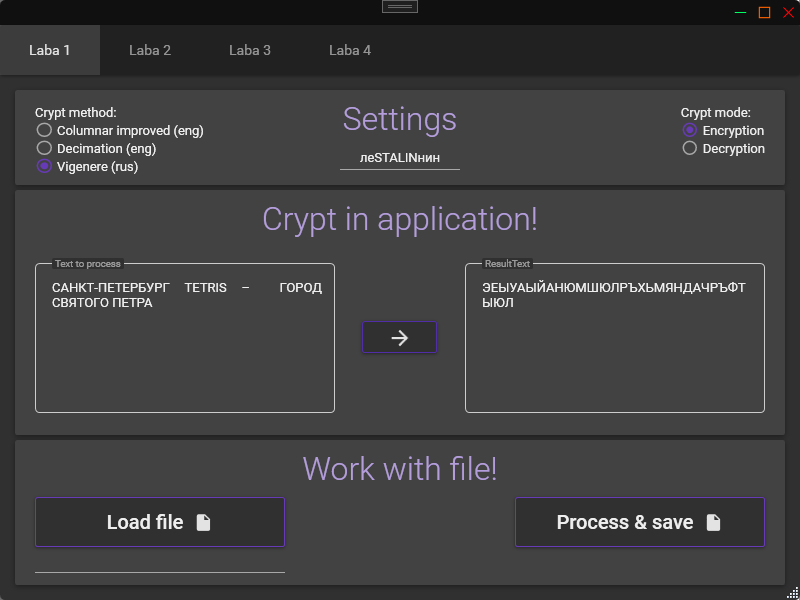
Используя таблицу выше, находим пересечения строки (начинается с символа ключа) и столбца (начинается с символа текста).

САНКТПЕТЕРБУРГГОРОДСВЯТОГОПЕТРА

ЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛ (Ключ)

ЭЕЫУАЫЙАНЮМШЮЛРЪХЬМЯНДАЧРЪФТЫЮЛ

Шифротекст = ЭЕЫУАЫЙАНЮМШЮЛРЪХЬМЯНДАЧРЪФТЫЮЛ



Дешифрование:

Шифротекст = ЭЕЫУАЫЙАНЮМШSSGЮЛРЪХЬМЯНДАЧРЪФТЫЮЛ

Ключ = леSTALINнин

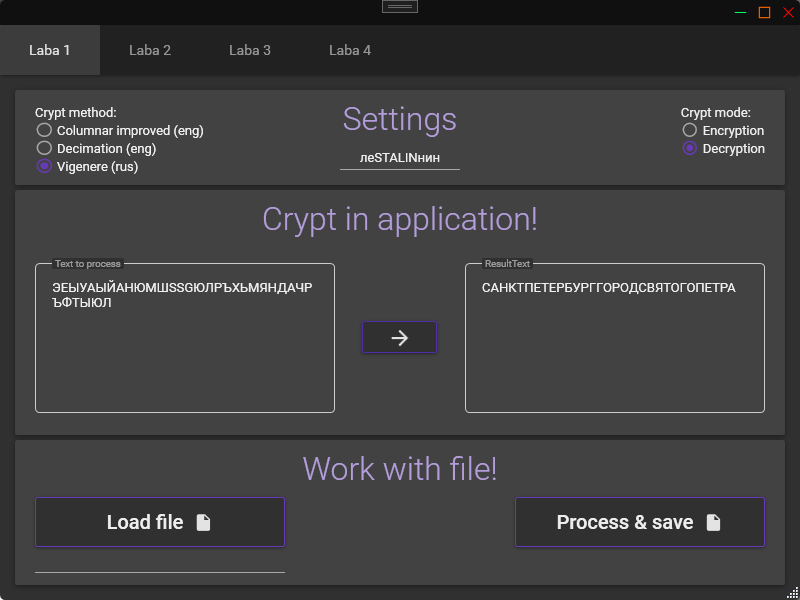
Используя таблицу выше, находим строку по букве ключа, находим букву шифротекста. Верхняя буква является буквой исходного текста.

ЭЕЫУАЫЙАНЮМШЮЛРЪХЬМЯНДАЧРЪФТЫЮЛ

ЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛЕНИНЛ (Ключ)

САНКТПЕТЕРБУРГГОРОДСВЯТОГОПЕТРА

Фраза = САНКТПЕТЕРБУРГГОРОДСВЯТОГОПЕТРА

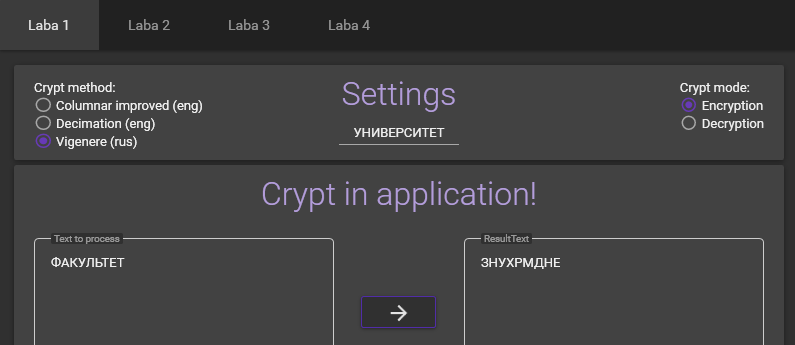


Шифрование при длине ключа > длина текста

Фраза = Факультет

Ключ = Университет

Шифротекст = ЗНУХРМДНЕ



Шифрование при невалидном ключе (ошибка):

Фраза = ЭЕЫУАЫЙАНЮМШSSGЮЛРЪХЬМЯНДАЧРЪФТЫЮЛ

Ключ = STALIN

