УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1

по предмету «Теория информации»

Вариант 5

Выполнил:

Матюшенко А.Д.

Проверил:

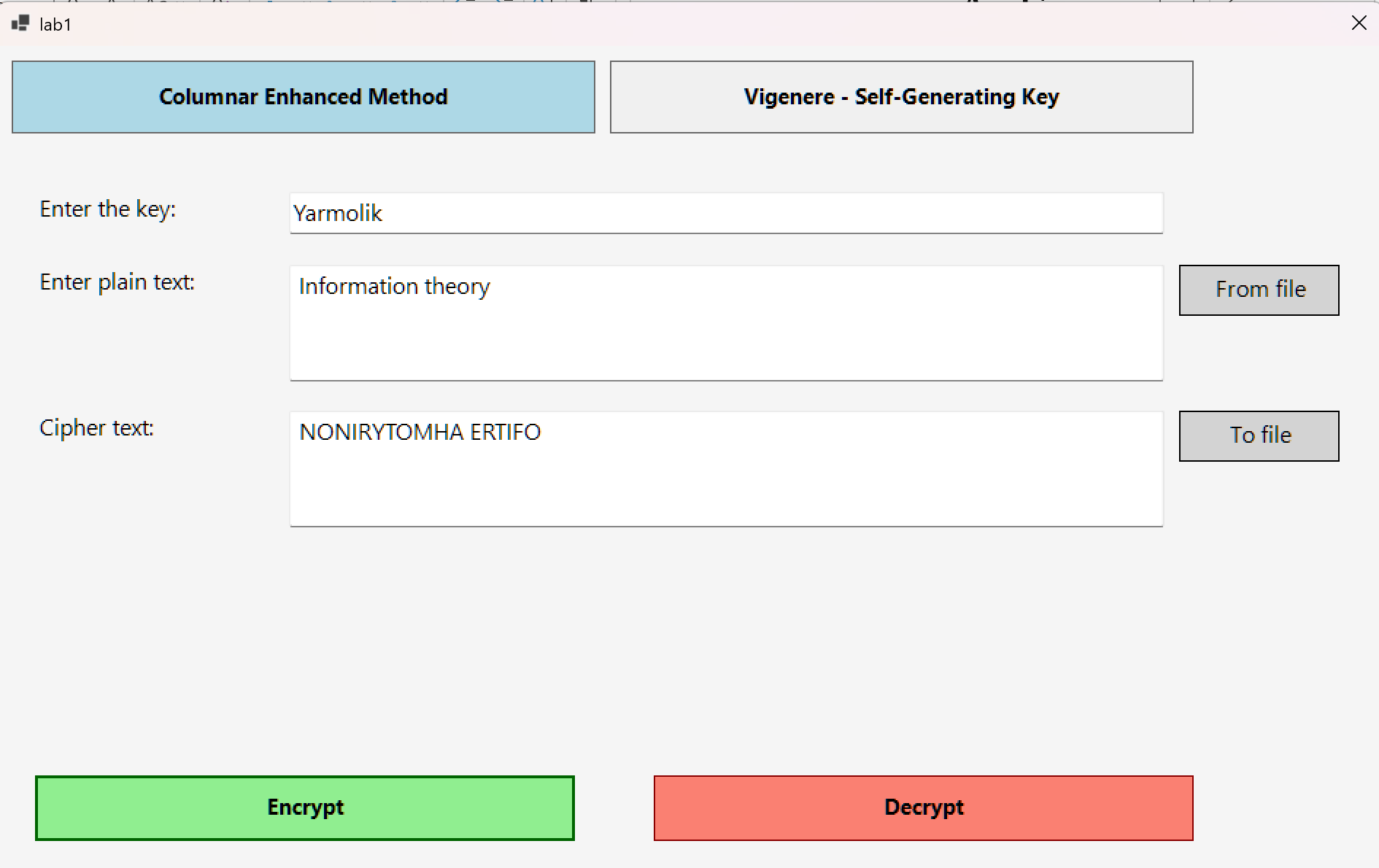
Болтак С.В.

Группа 351001

Минск 2025

**Алгоритм улучшенный столбцовый, текст на англиском языке.**

Интерфейс приложения при выборе шифрования улучшенным столбцовым

****

Тест 1

Кейс: случайная фраза (последняя строчка заполнена полностью)

Сообщение: Information theory

Ключ: Yarmolik

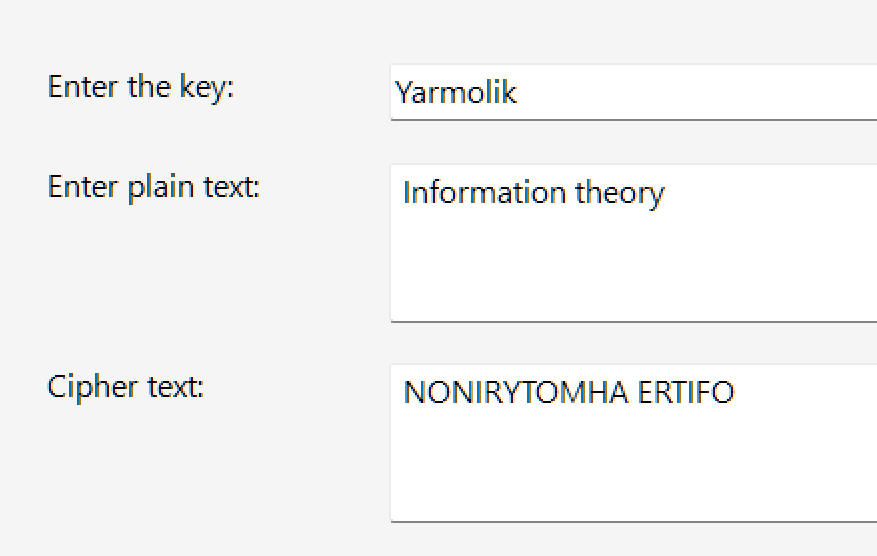
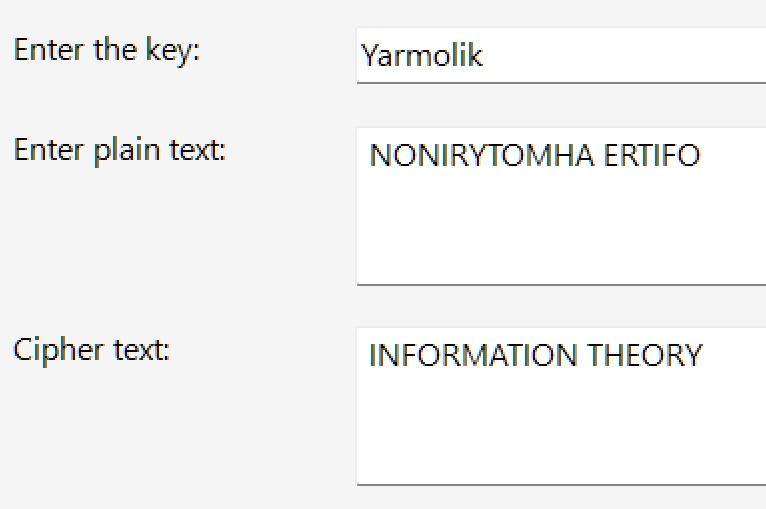
Y A R M O L I K

8 1 7 5 6 4 2 3

I N

F O R M A T I

O N T H E O R Y

Тест 2

Кейс: случайная фраза (последняя строчка не заполнена полностью)

Сообщение: Information theorium

Ключ: Yarmolik

Y A R M O L I K

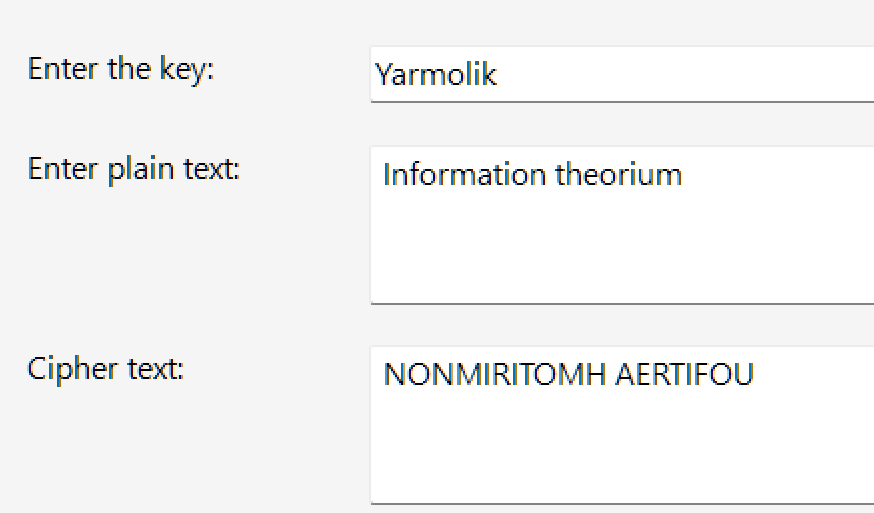
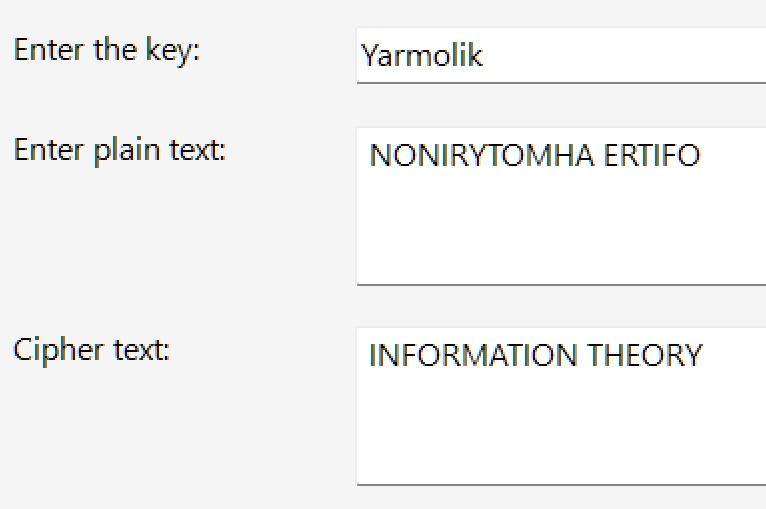
8 1 7 5 6 4 2 3

I N

F O R M A T I

O N T H E O R I

U M

Тест 3

Кейс: лишние символы в фразе и ключе (в ключе отбрасываются, в фразе остаются на местах в исходном виде)

Сообщение: INF123ORMATION THE23ORI

Ключ: Yarmolikтоп

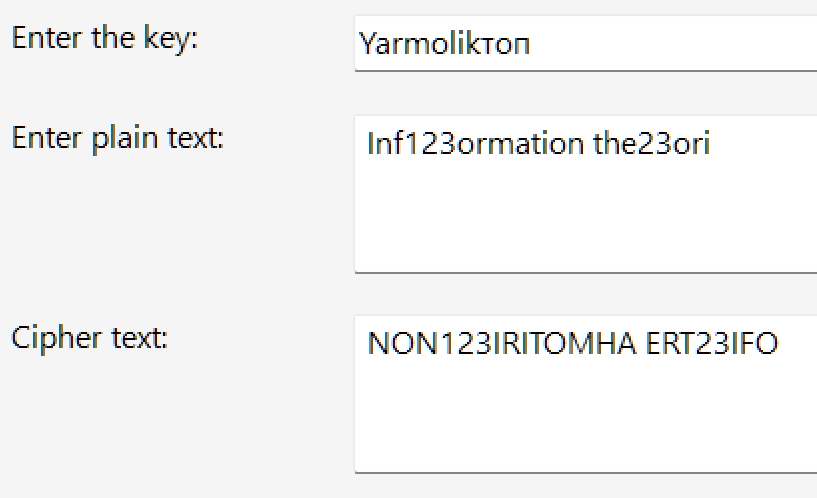
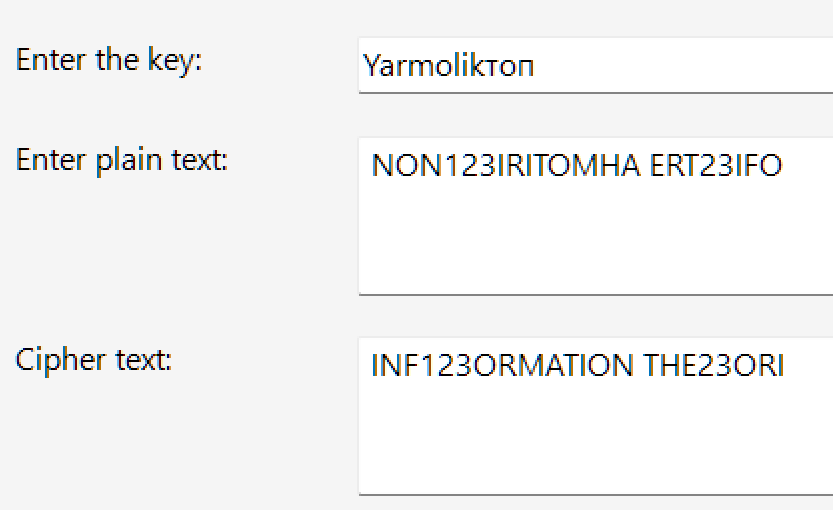
Y A R M O L I K

8 1 7 5 6 4 2 3

I N

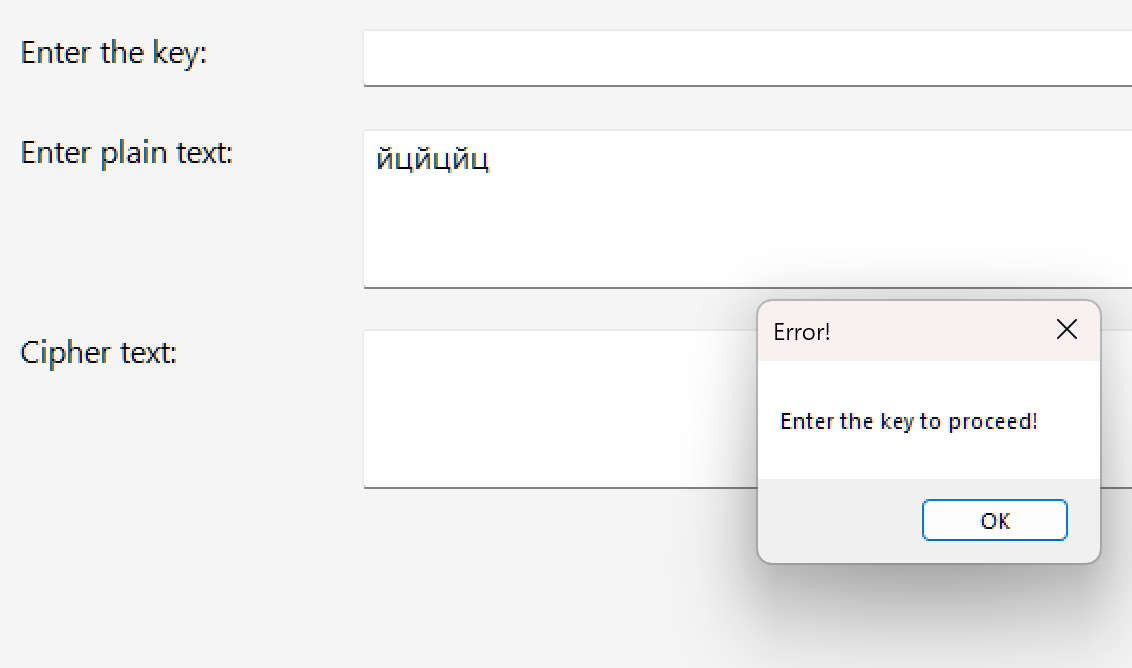
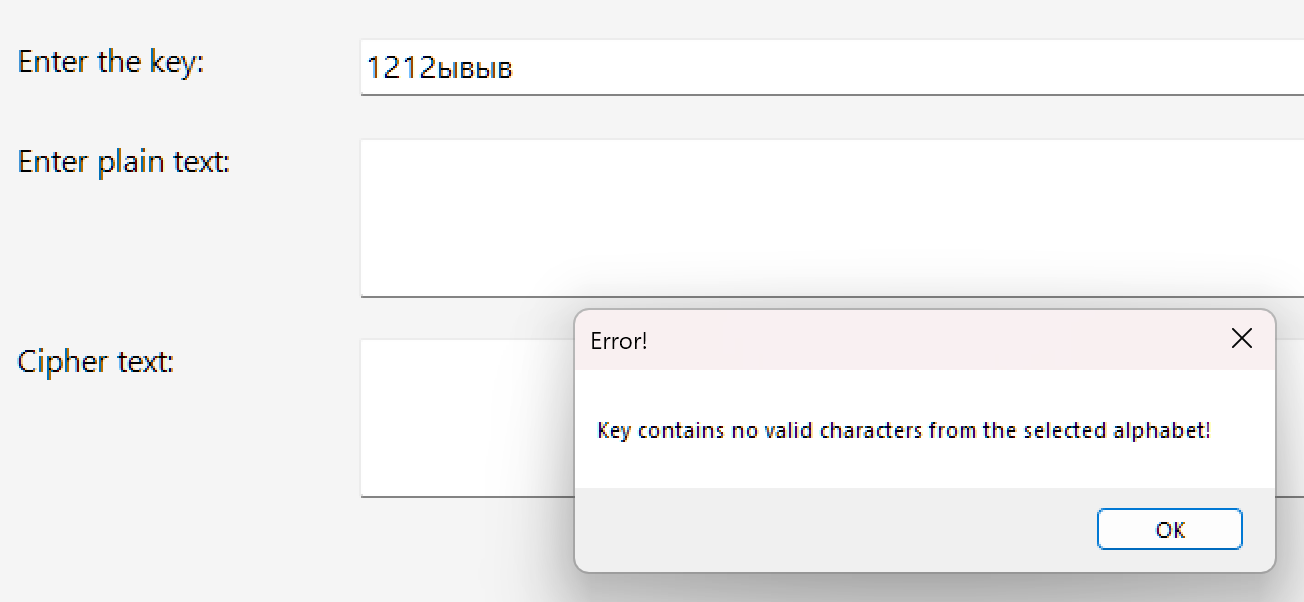
F O R M A T I

O N T H E O R I

Тест 4

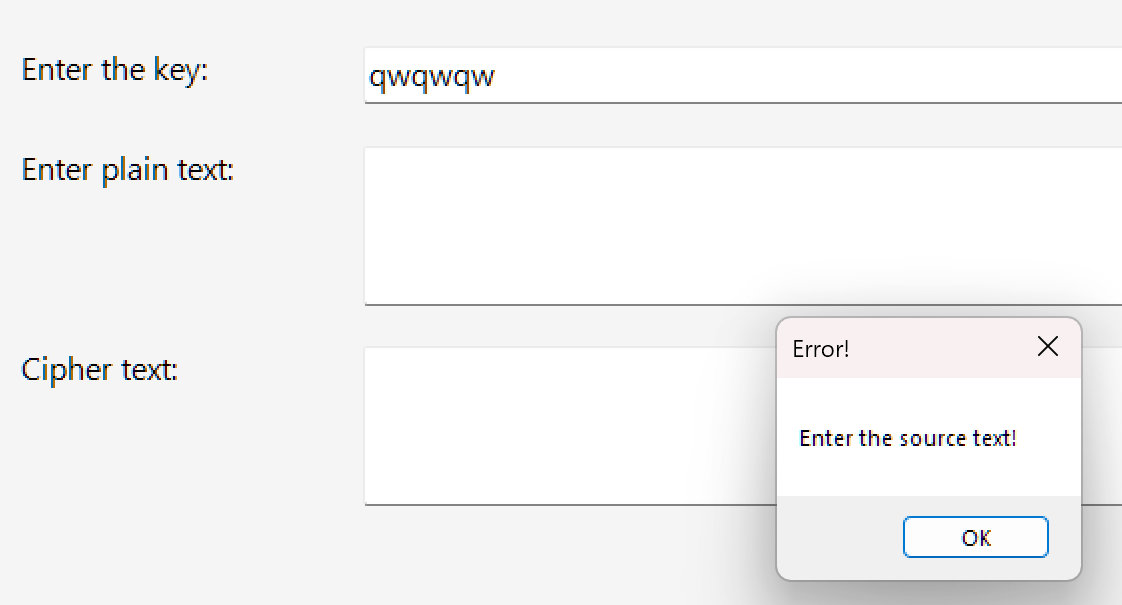
Кейс: пустой ключ или без символов алфавита

Тест 5

Кейс: пустой текст сообщения

Сообщение:



Тест 6

Кейс: ключ из символов с одинаковым порядком

Сообщение: Information theorium

Ключ: aaaaaaaaa

A A A A A A A A A

1 2 3 4 5 6 7 8 9

I

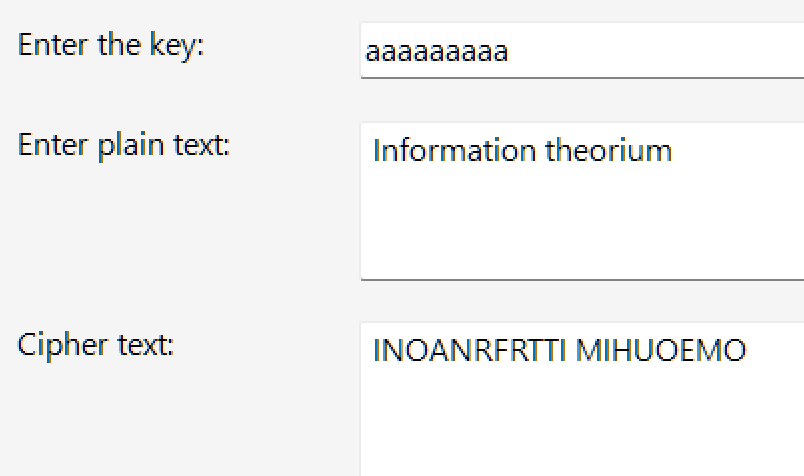
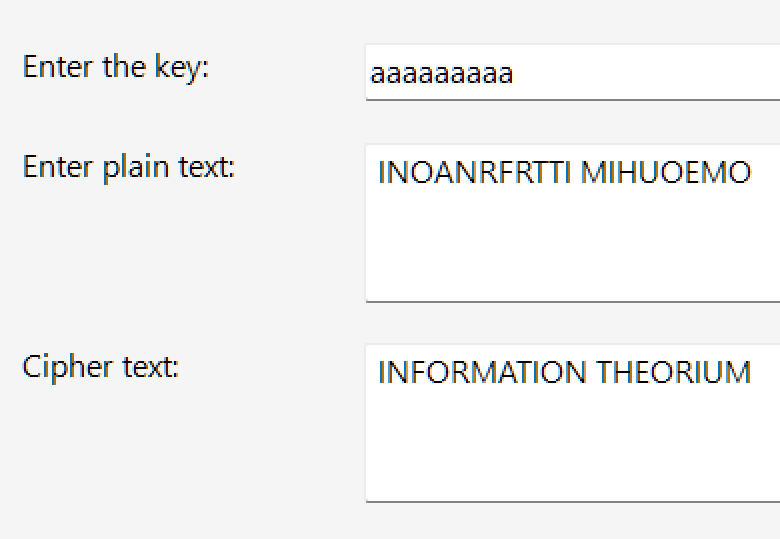
N F

O R M

A T I O

N T H E O

R I U M

Тест 7

Кейс: длинный ключ

Сообщение: Hello crypto

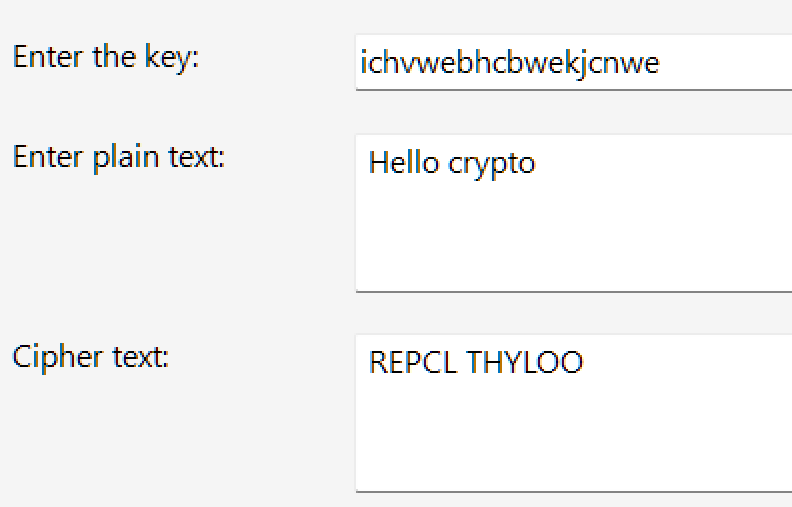
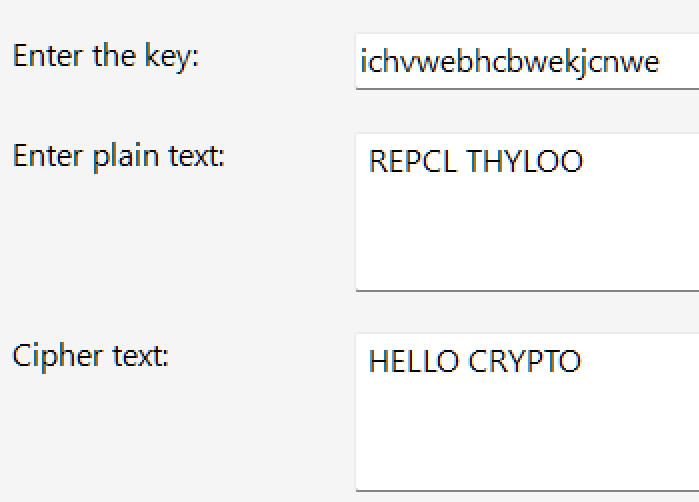
Ключ: ichvwebhcbwekjcnwe

I C H V W E B H C B W E K J C N W E

11 3 9 15 16 6 1 10 4 2 17 7 13 12 5 14 18 8

H E L L O C R

Y P T O

Тест 8

Кейс: короткий ключ, длинное сообщение

Сообщение: cjwoiejfojwejfwjejoewkonw

Ключ: cat

C A T

2 1 3

J I

F

W F E

E O

C

W O J

O J

J

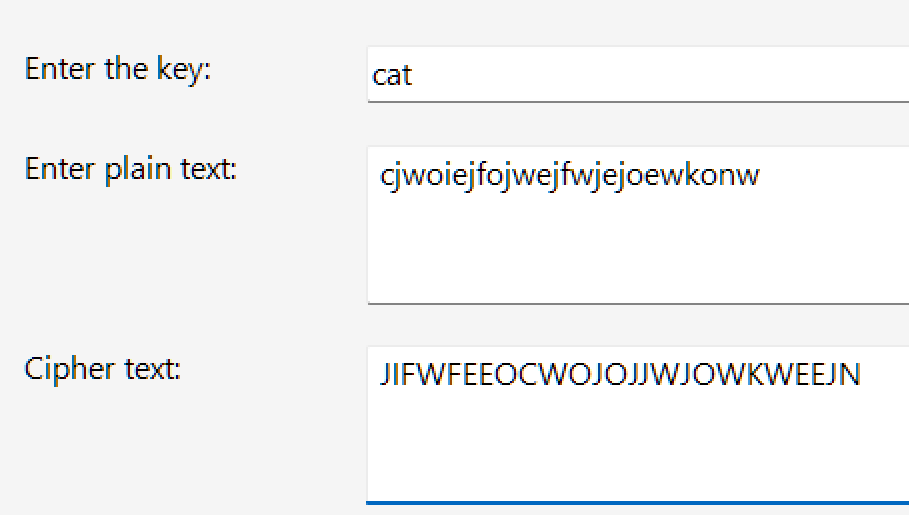
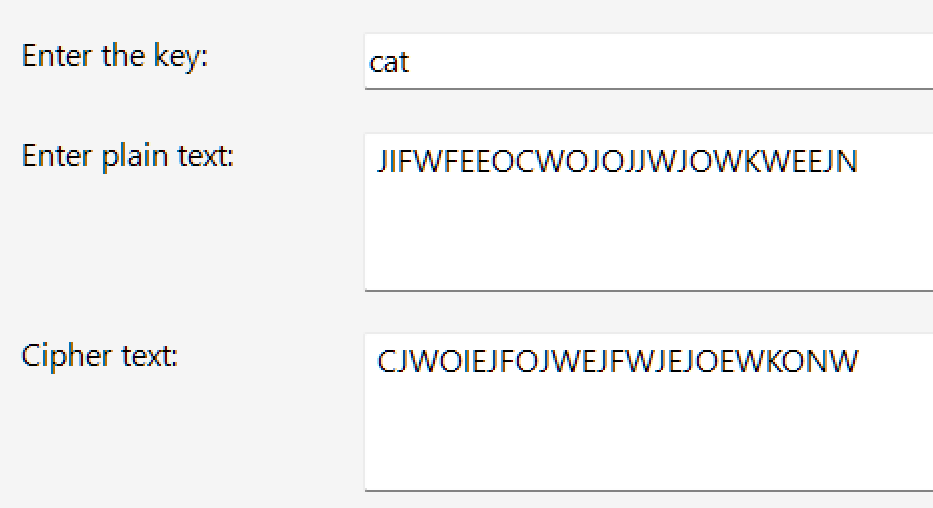
W J O

W K

W

E E J

N

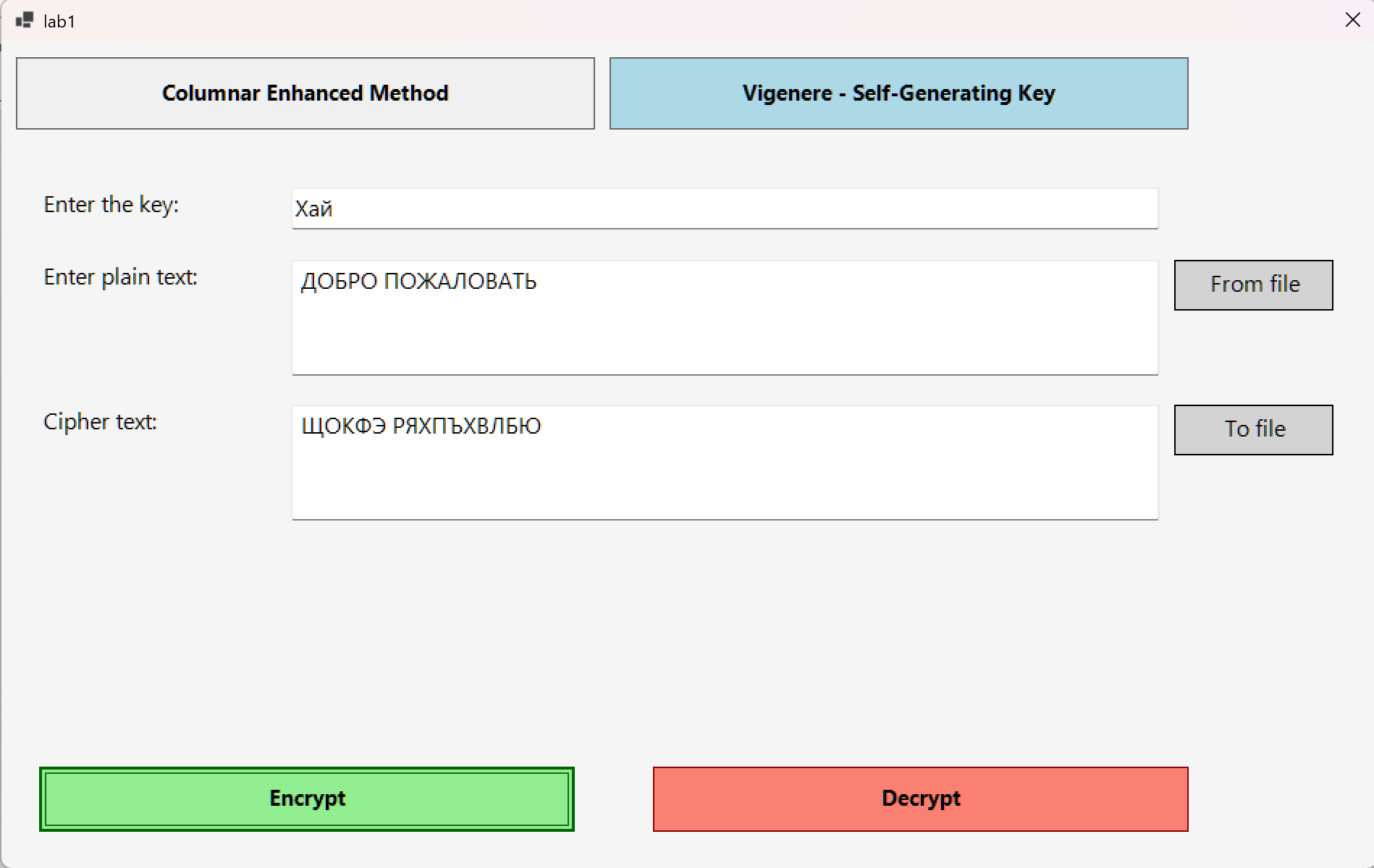
 

**Алгоритм Виженера, самогенерирующийся ключ, текст на русском языке.**

Таблица для шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \* | 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 | А |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |

Интерфейс приложения при выборе шифрования Виженера



Тест 1

Кейс: случайная фраза

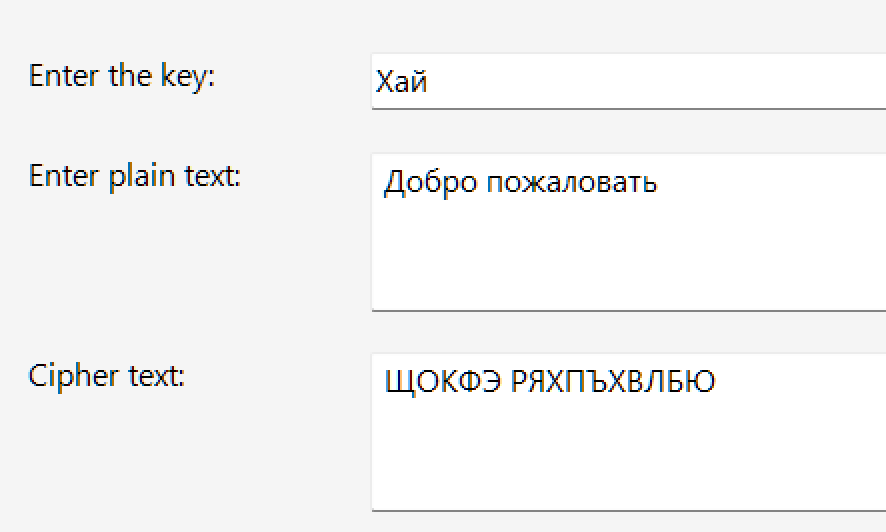
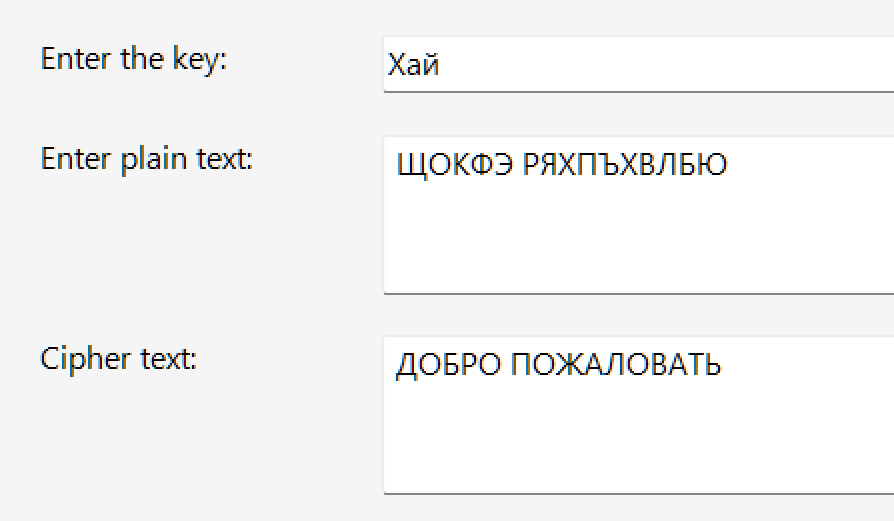
Сообщение: Добро пожаловать

Ключ: Хай

Д О Б Р О П О Ж А Л О В А Т Ь

Х А Й Д О Б Р О П О Ж А Л О В

Щ О К Ф Э Р Я Х П Ъ Х В Л Б Ю

Тест 2

Кейс: Ё, короткий ключ и лишний символ не из алфавита (просто остается в исходном виде)

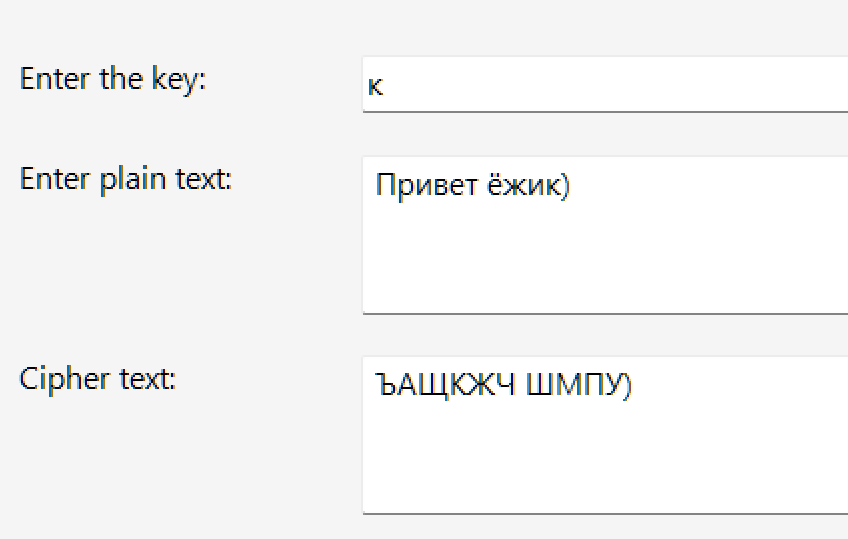
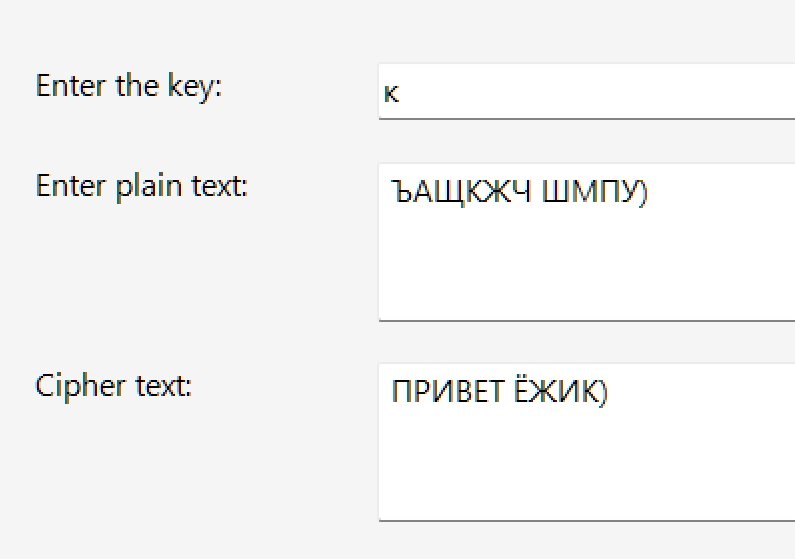
Сообщение: Привет ёжик)

Ключ: к

П Р И В Е Т Ё Ж И К

К П Р И В Е Т Ё Ж И

Ъ А Щ К Ж Ч Ш М П У

Тест 3

Кейс: фраза и ключ с символами не из алфавита

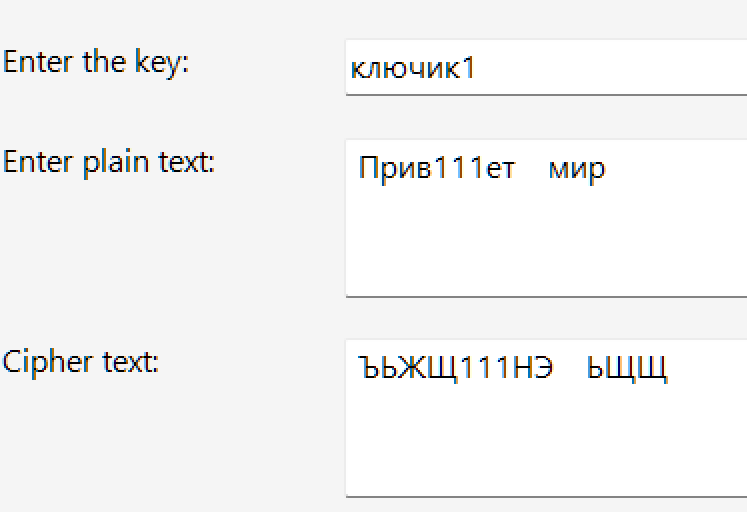
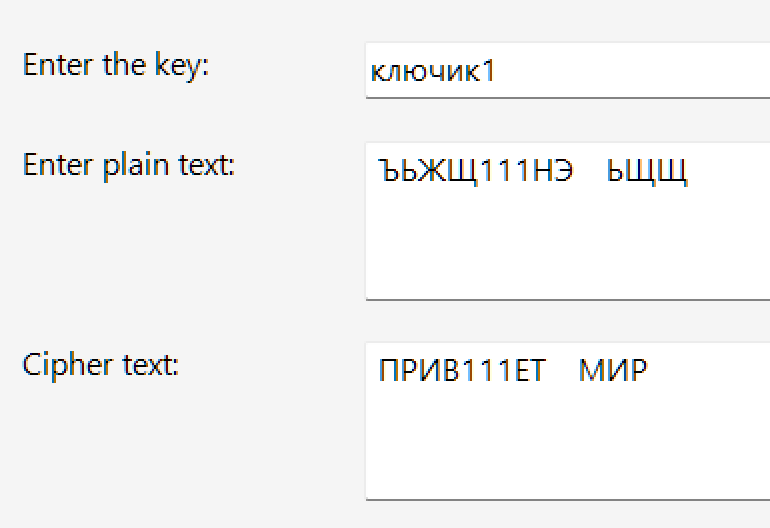
Сообщение: Прив111ет мир

Ключ: ключик1

П Р И В Е Т М И Р

К Л Ю Ч И К П Р И

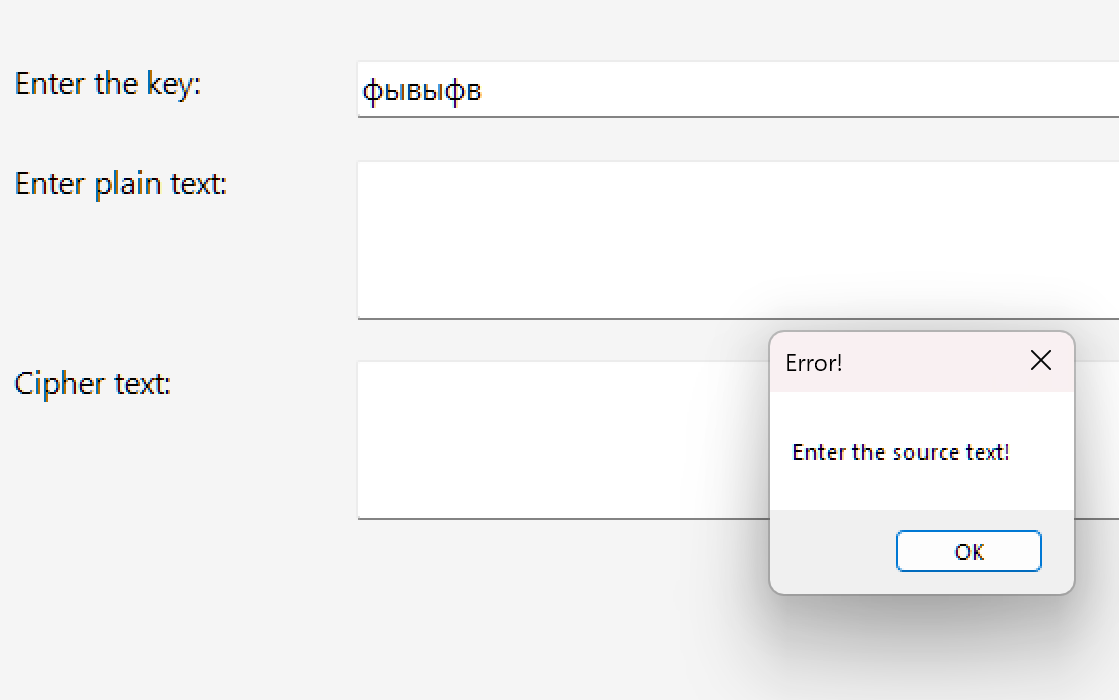
Ъ Ь Ж Щ Н Э Ь Щ Щ

Тест 4

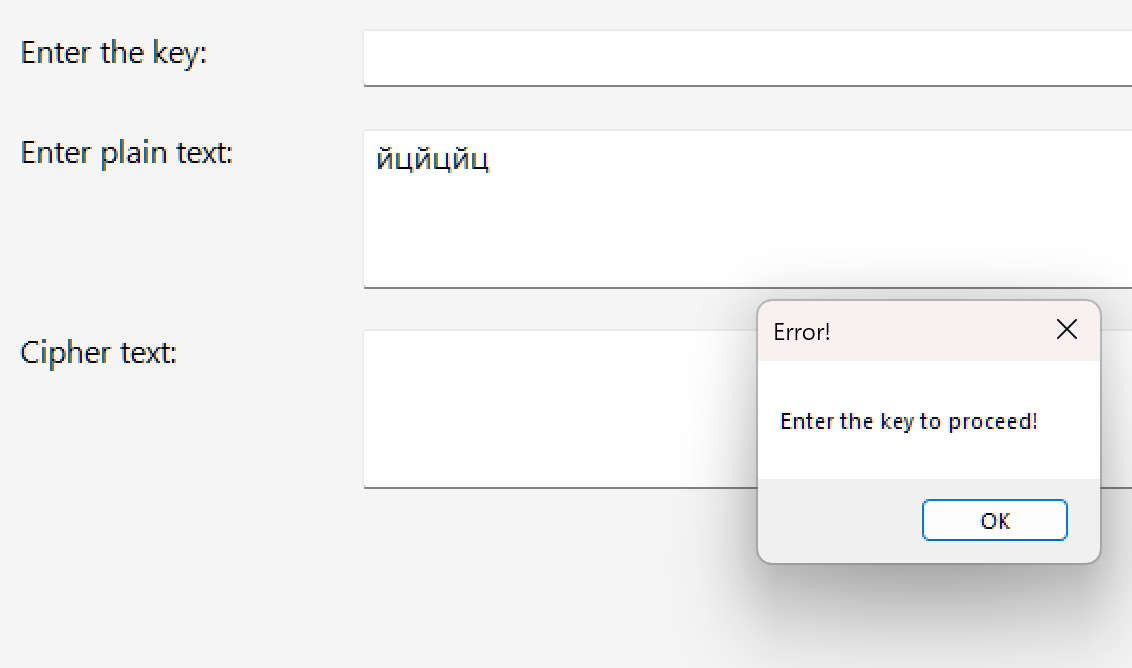
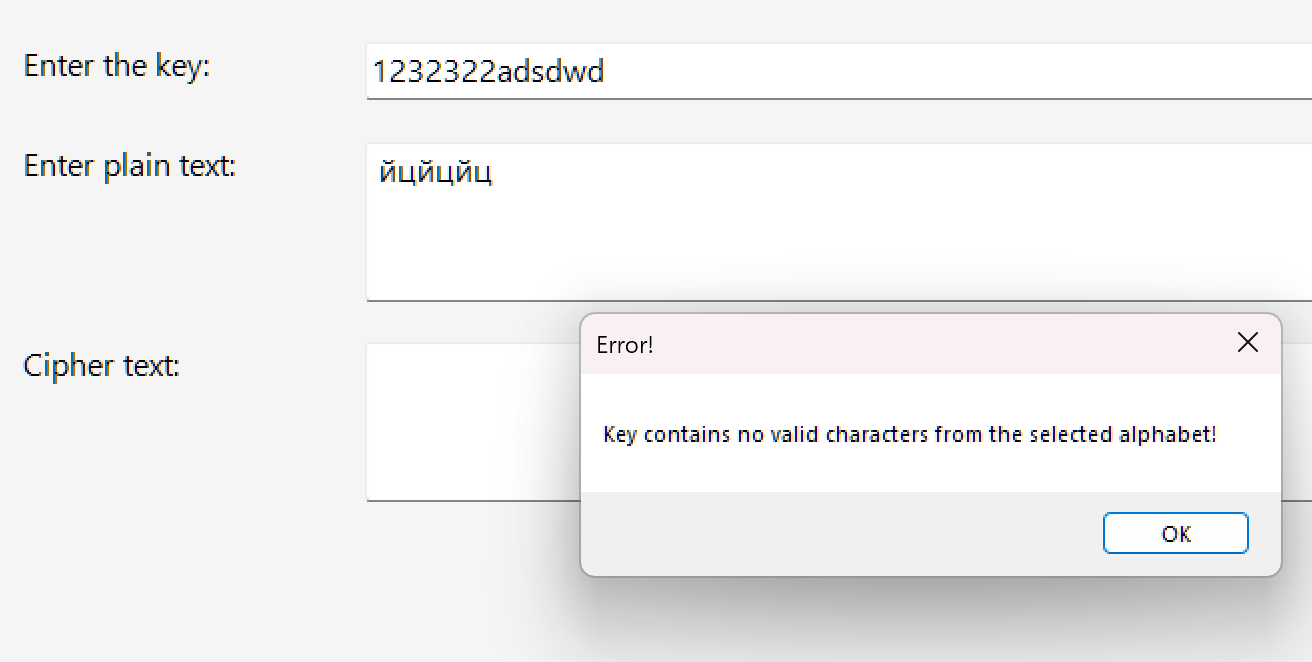
Кейс: пустой текст сообщения

Сообщение:



Тест 5

Кейс: пустой ключ или без символов алфавита

Тест 6

Кейс: длинный ключ и фраза

Сообщение: составляем таблицу, которая будет содержать весь алфавит заданного языка и номер каждой буквы.

Ключ: записываем преобразованную тестовую фразу, а под ней ключевое слово, повторяющееся столько раз, сколько необходимо.

С О С Т А В Л Я Е М Т А Б Л И Ц У К О Т О Р А Я Б У Д Е Т С О Д Е Р Ж А Т Ь В Е С Ь А Л Ф А В И Т З А Д А Н Н О Г О Я З Ы К А И Н О М Е Р К А Ж Д О Й Б У К В Ы

З А П И С Ы В А Е М П Р Е О Б Р А З О В А Н Н У Ю Т Е С Т О В У Ю Ф Р А З У А П О Д Н Е Й К Л Ю Ч Е В О Е С Л О В О П О В Т О Р Я Ю Щ Е Е С Я С Т О Л Ь К О Р А

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

