УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Тесты к лабораторной работе № 1

по предмету «Теория информации»

Вариант 8

Выполнил:

Гузаев Е.Д.

гр. 351003

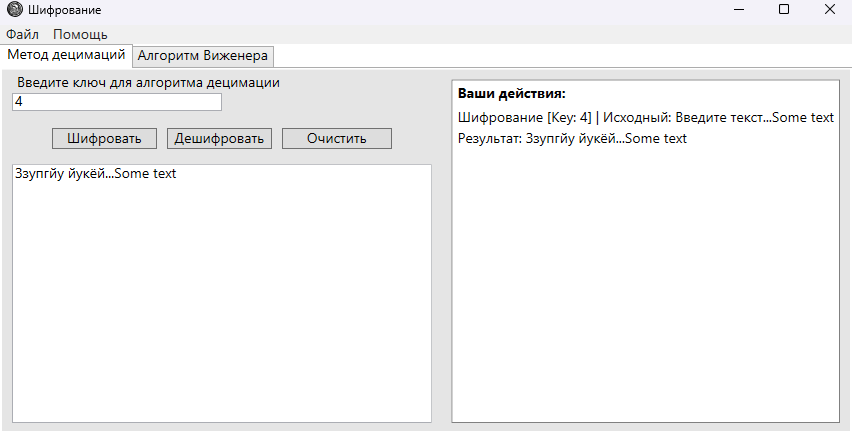
Проверила:

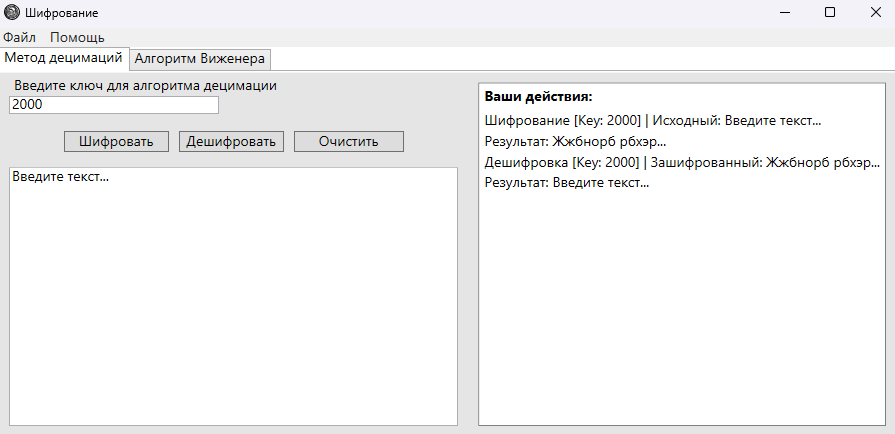
Болтак С.В.

Минск, 2025

**Метод децимаций**

*Дымовое тестирование:*

*Ломаем на валидных данных:*

**

Для шифрования методом децимаций по формуле  
  c = (a ⋅ k) mod n

при условии, что:  
 • n = 33  (русский алфавит без пробела – 33 символа),  
 • k = 2000.

Заметим, что сначала удобно привести ключ к остатку от деления на 33:  
  2000 mod 33 = 20

То есть эквивалентное преобразование выглядит как:  
  c = (a ⋅ 20) mod 33,  
где a – номер буквы исходного алфавита, нумеруемого от 0 до 32.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Исходная буква | Индекс | Вычисление | Результат (индекс) | Зашифрованная буква |
| А | 0 | 20 \* 0 mod 33 = 0 | 0 | А |  |
| Б | 1 | 20 \* 1 mod 33 = 20 | 20 | У |  |
| В | 2 | 20 \* 2 mod 33 = 7 | 7 | Ж |  |
| Г | 3 | 20 \* 3 mod 33 = 27 | 27 | Ъ |  |
| Д | 4 | 20 \* 4 mod 33 = 14 | 14 | Н |  |
| Е | 5 | 20 \* 5 mod 33 = 1 | 1 | Б |  |
| Ё | 6 | 20 \* 6 mod 33 = 21 | 21 | Ф |  |
| Ж | 7 | 20 \* 7 mod 33 = 8 | 8 | З |  |
| З | 8 | 20 \* 8 mod 33 = 28 | 28 | Ы |  |
| И | 9 | 20 \* 9 mod 33 = 15 | 15 | О |  |
| Й | 10 | 20 \* 10 mod 33 = 2 | 2 | В |  |
| К | 11 | 20 \* 11 mod 33 = 22 | 22 | Х |  |
| Л | 12 | 20 \* 12 mod 33 = 9 | 9 | И |  |
| М | 13 | 20 \* 13 mod 33 = 29 | 29 | Ь |  |
| Н | 14 | 20 \* 14 mod 33 = 16 | 16 | П |  |
| О | 15 | 20 \* 15 mod 33 = 3 | 3 | Г |  |
| П | 16 | 20 \* 16 mod 33 = 23 | 23 | Ц |  |
| Р | 17 | 20 \* 17 mod 33 = 10 | 10 | Й |  |
| С | 18 | 20 \* 18 mod 33 = 30 | 30 | Э |  |
| Т | 19 | 20 \* 19 mod 33 = 17 | 17 | Р |  |
| У | 20 | 20 \* 20 mod 33 = 4 | 4 | Д |  |
| Ф | 21 | 20 \* 21 mod 33 = 24 | 24 | Ч |  |
| Х | 22 | 20 \* 22 mod 33 = 11 | 11 | К |  |
| Ц | 23 | 20 \* 23 mod 33 = 31 | 31 | Ю |  |
| Ч | 24 | 20 \* 24 mod 33 = 18 | 18 | С |  |
| Ш | 25 | 20 \* 25 mod 33 = 5 | 5 | Е |  |
| Щ | 26 | 20 \* 26 mod 33 = 25 | 25 | Ш |  |
| Ъ | 27 | 20 \* 27 mod 33 = 12 | 12 | Л |  |
| Ы | 28 | 20 \* 28 mod 33 = 32 | 32 | Я |  |
| Ь | 29 | 20 \* 29 mod 33 = 19 | 19 | Т |  |
| Э | 30 | 20 \* 30 mod 33 = 6 | 6 | Ё |  |
| Ю | 31 | 20 \* 31 mod 33 = 26 | 26 | Щ |  |
| Я | 32 | 20 \* 32 mod 33 = 13 | 13 | М |  |
|  |  |  |  |  |  |

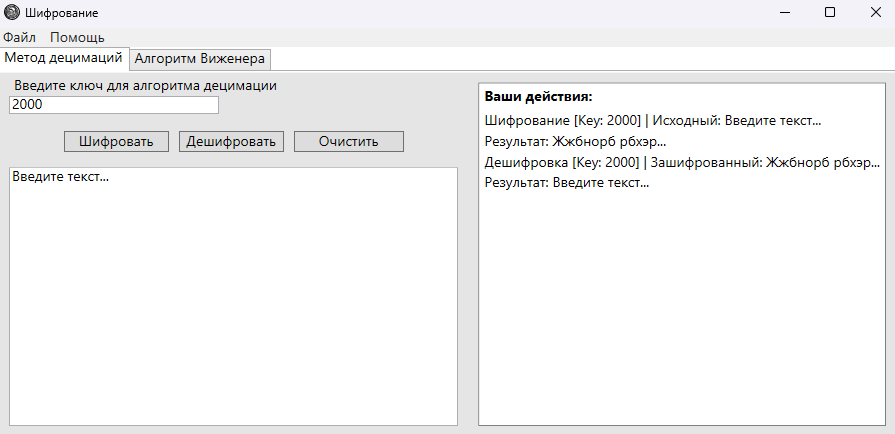
Таким образом, для исходного текста «Введите текст...» при использовании данного метода шифрования каждая буква будет заменена согласно указанной таблице (при этом символы, отсутствующие в алфавите, например, пробел и знаки препинания, остаются без изменений).

**Исходный текст:**

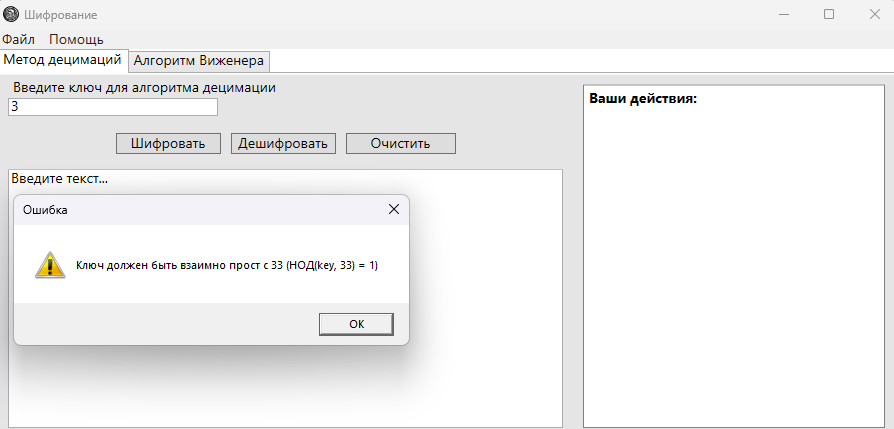
Введите текст…

**Расшифрованный текст:**

Жжбнорб рбхэр…



*Ломаем на не валидных данных:*



**Шифр Виженера, самогенерирующийся ключ**

*Дымовое тестирование: Показываем, что программа работает.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 |

Таблица преобразований для русского алфавита

Исходный текст:

Введите текст…

Ключ:

Ключ

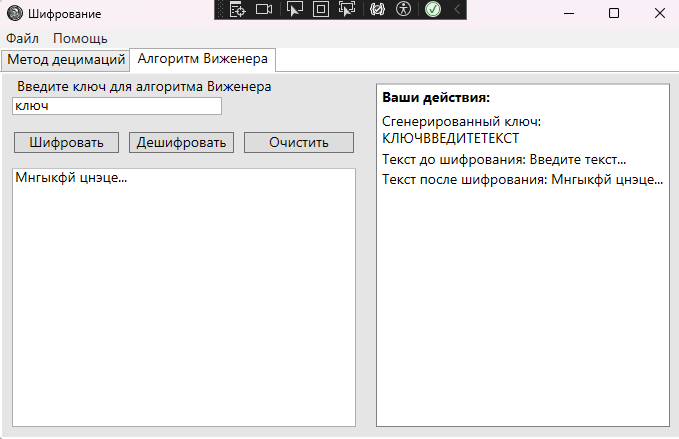
Сгенерированный ключ:

КЛЮЧВВЕДИТЕТЕКСТ

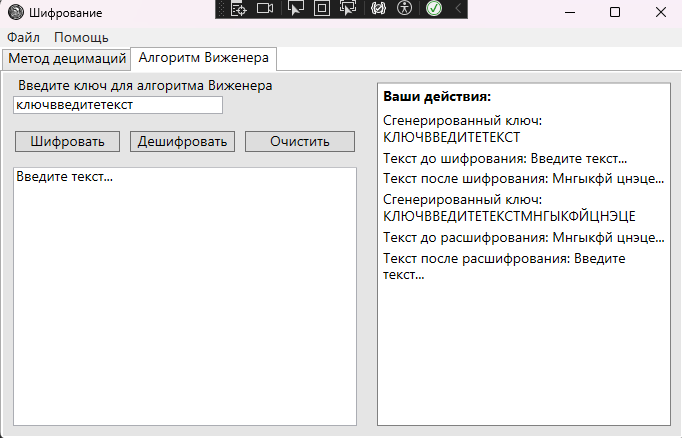
Зашифрованный текст:

Мнгыкфй цнэце…

Результат работы программы:



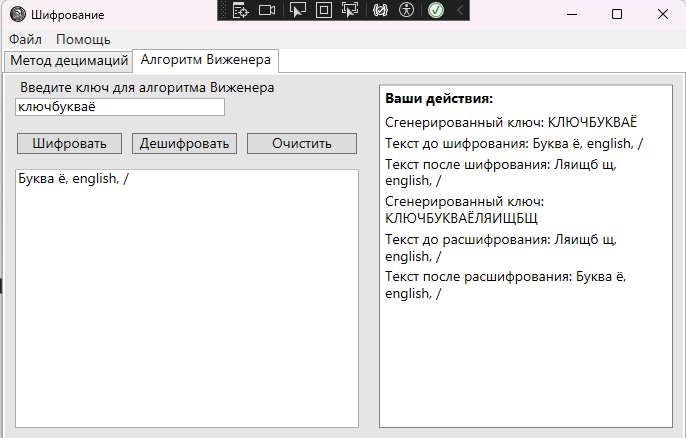
Пример шифрования



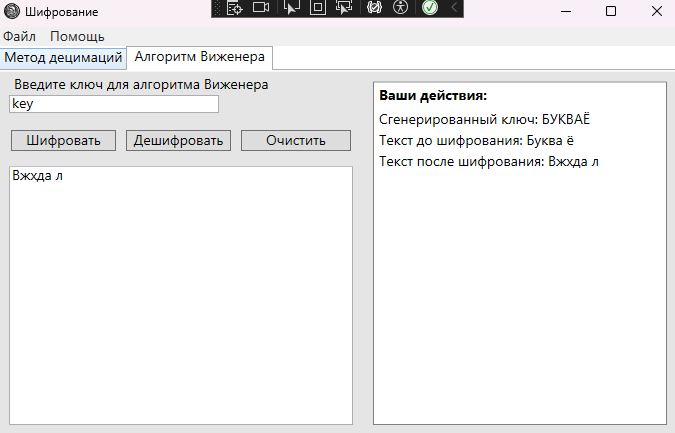
Пример дешифровки

*Ломаем на валидных данных:*

Все вышеизложенное проделываем для тестовой фразы, содержащей букву Ё.

**

*Ломаем на не валидных данных:*

****