**ТЕСТЫ К ЛАБОРАТОРНОЙ РАБОТЕ №1**

**ВАРИАНТ №11**

*Стрижак Вероника., гр. 351001*

*Шифр Плейфера с 4 шифрующими таблицами, английский язык.*

Тест №1.1 – Дымовое тестирование

Исходный текст: Sunsets are truly beautiful things

Ключ для таблицы 1: Inspiration

Ключ для таблицы 2: Discovery

Ключ для таблицы 3: Adventure

Ключ для таблицы 4: Understanding

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

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

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

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

Зашифрованный текст: **DVDUFUSRCNADLQTIGUMCSFLQYGIABB**

Дешифрованный текст (при исходном ключе): **SUNSETSARETRULYBEAUTIFULTHINGS**

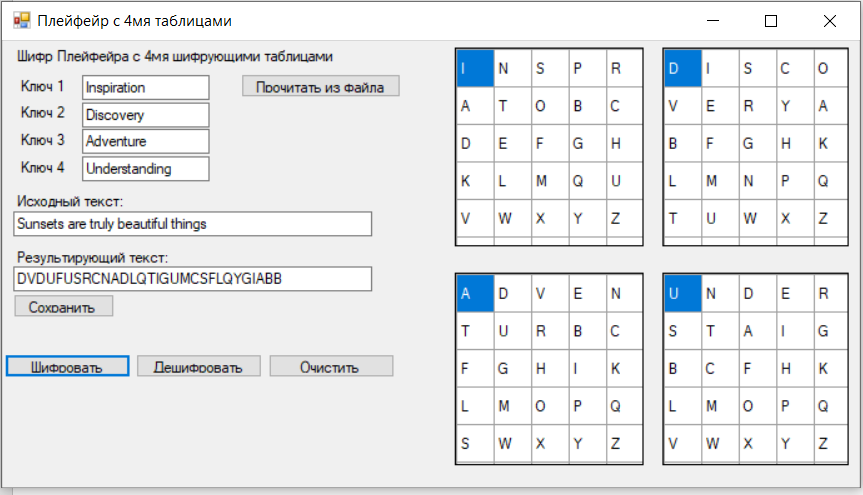


Рис. 1.1.1 – Результат работы шифрования

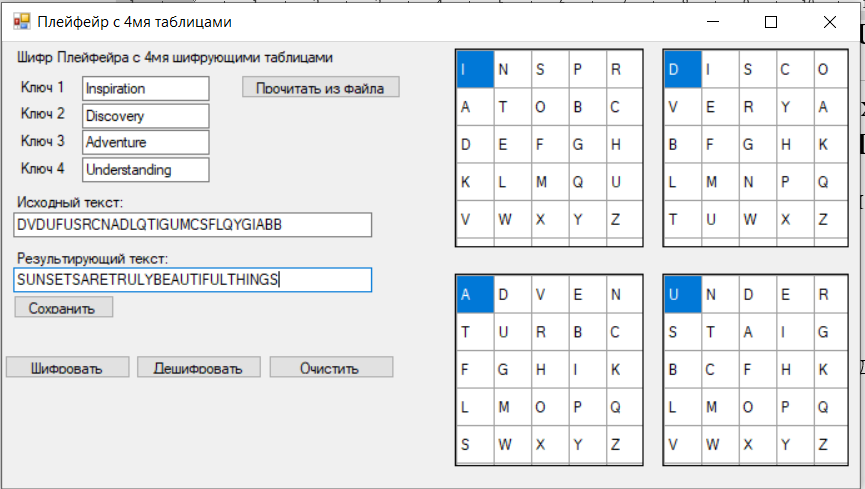


Рис. 1.1.2 – Результат работы дешифрования

Тест №2.1 – Ломаем на валидных данных. Длинный текст с нечетным количеством символов

*Шифр Плейфера с 4 шифрующими таблицами, английский язык.*

Исходный текст: Sharks are ocean predators

Ключ для таблицы 1: Reproduction

Ключ для таблицы 2: environment

Ключ для таблицы 3: Thermoregulation

Ключ для таблицы 4: Carcharhiniformes

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

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

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

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

Зашифрованный текст: **QMFTKIFTVGBGCOVEVNGFVRPZ**

Дешифрованный текст (при исходном ключе): **SHARKSAREOCEANPREDATORSX**

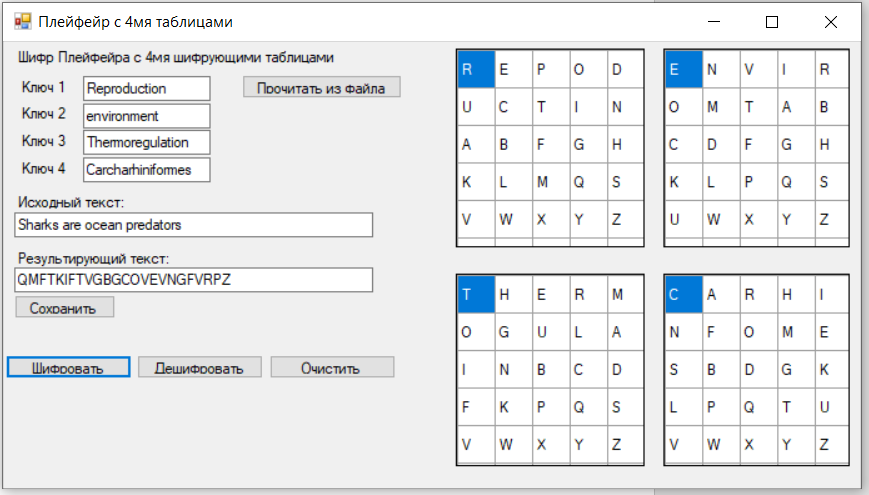


Рис. 2.1.1 – Результат работы шифрования

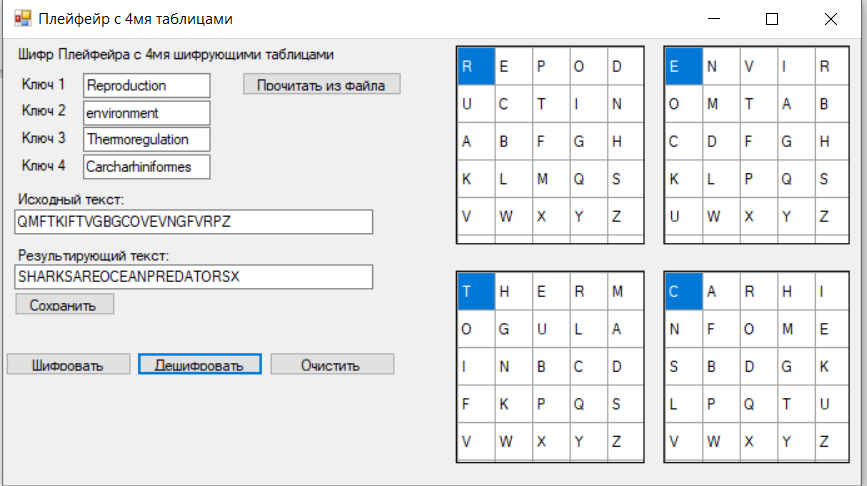
****

Рис. 2.1.2 – Результат работы дешифрования

Тест №2.2 – Ломаем на валидных данных. Длинный текст с четным количеством символов. Встречаются 2 одинаковые буквы подряд

Исходный текст: **I need a book to read before bed**

Ключ для таблицы 1: cinema

Ключ для таблицы 2: cloud

Ключ для таблицы 3: luxvisage

Ключ для таблицы 4: relouis

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

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

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

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

Зашифрованный текст: **LNLVEGFUNHSVQUACBUFVQUBUEW**

Дешифрованный текст (при исходном ключе): **INEEDABOOKTOREADBEFOREBEDX**

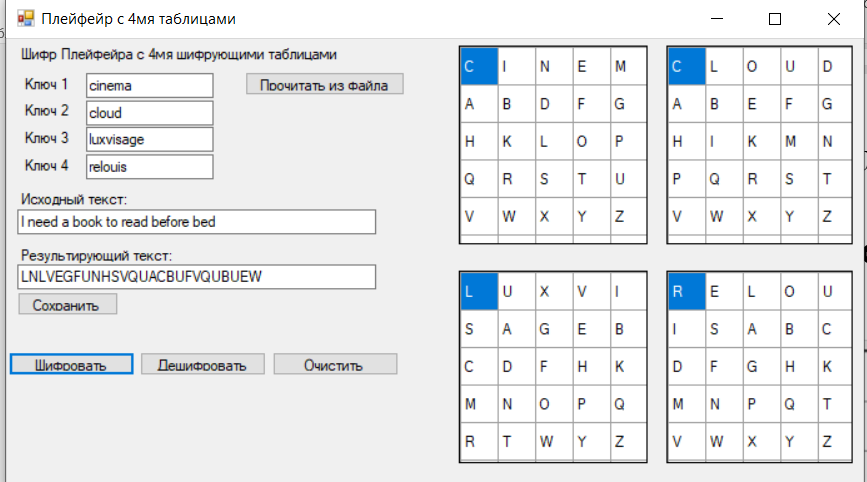


Рис. 2.2.1 – Результат работы шифрования

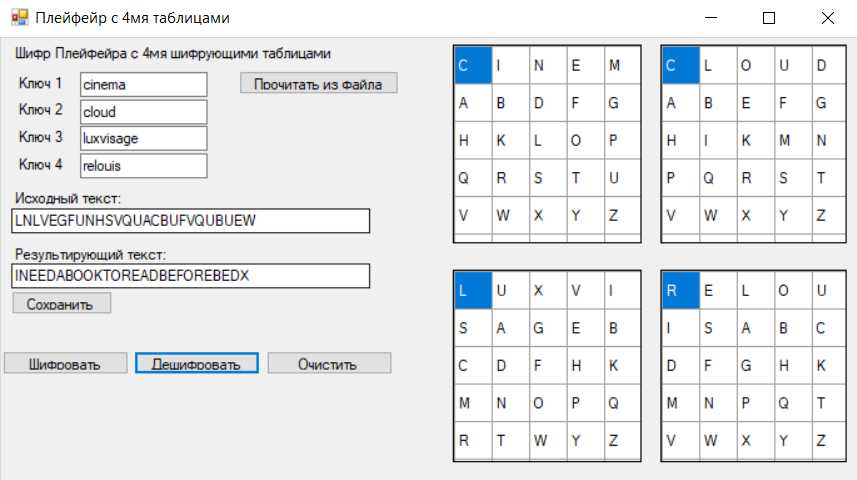


Рис. 2.2.2 – Результат работы дешифрования

Тест №3.1 – Ломаем на невалидных данных. В тексте присутствуюет буква J. При вводе ключа используется буква J

Исходный текст: **Jumping over the lazy dog felt joyful**

Ключ для таблицы 1: january

Ключ для таблицы 2: cryptography

Ключ для таблицы 3: jewelry

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

Ключ для таблицы 4: women

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

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

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

Зашифрованный текст: **CTLNTIEEXETSIWDDXZGLKABMWFQUDTFZ**

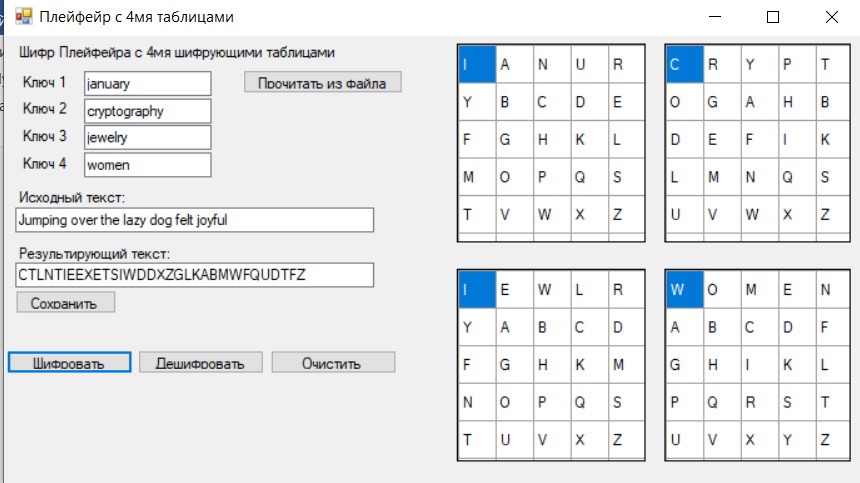
Дешифрованный текст (при исходном ключе): **IUMPINGOVERTHELAZYDOGFELTIOYFULX** 

Рис. 3.1.1 – Результат работы шифрования

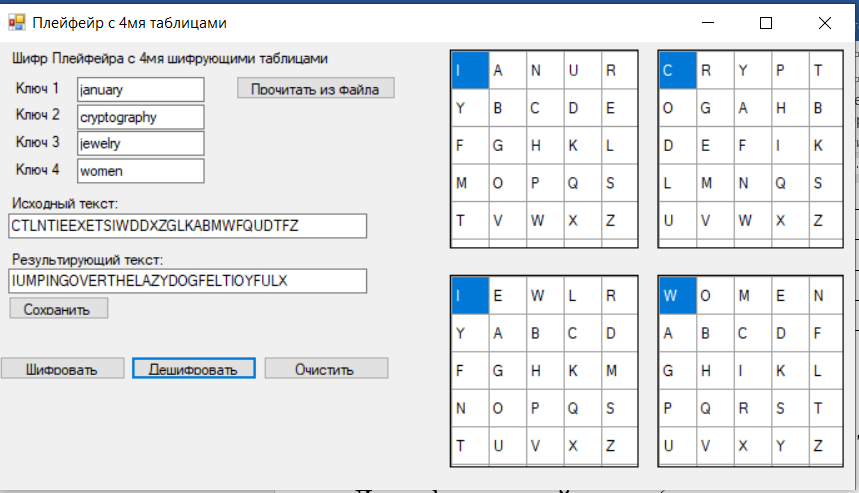


Рис. 3.1.2 – Результат работы дешифрования

Тест №3.2 – Ломаем на невалидных данных. В тексте присутствуют символы, не соответствующие английскому алфавиту. При вводе ключа используются недопустимые символы

Исходный текст: **Jumимpi4ng ove2r the lazyва dog f0elt joy3ful**

Ключ для таблицы 1: janu345ary

Ключ для таблицы 2: cryщидиьtography

Ключ для таблицы 3: jewelryммм

Ключ для таблицы 4: wo23тлпmen

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

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

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

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

Зашифрованный текст: **CTLNTIEEXETSIWDDXZGLKABMWFQUDTFZ**

Дешифрованный текст (при исходном ключе): **IUMPINGOVERTHELAZYDOGFELTIOYFULX**

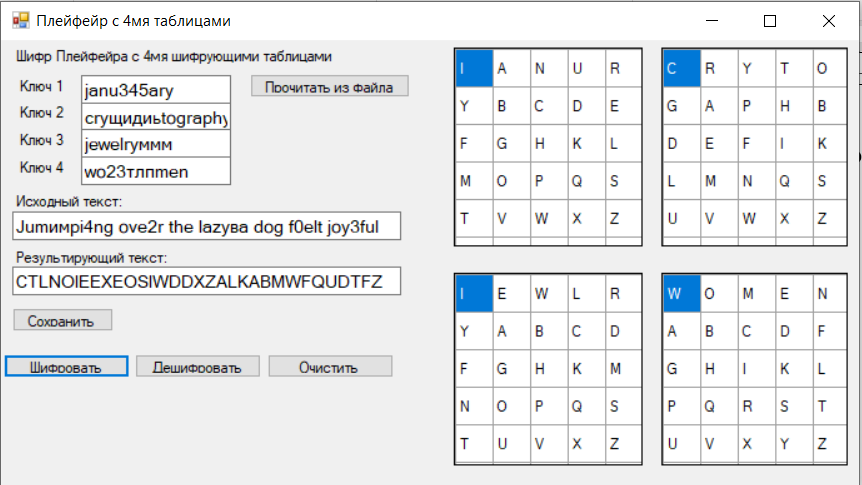


Рис. 3.2.1 – Результат работы шифрования

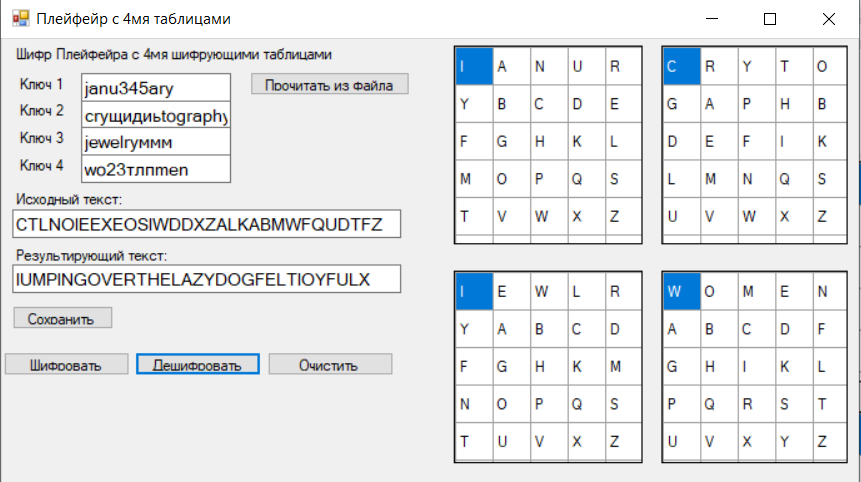


Рис. 3.2.2 – Результат работы дешифрования

*Алгоритм Виженера, прямой ключ, русский язык.*

**Таблица Виженера для русского языка:**

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

**Формула для шифрования (c\_j):**

Cj= (mj + kj) mod  n

**Формула для расшифровки (m\_j):**

Mj = (cj – k j+ n) mod  n

cj=(mj+kj)modn

 n — количество букв в алфавите (например, для русского алфавита n = 33)

 mj — порядковый номер буквы открытого текста

 kj — порядковый номер буквы ключа

 cj — порядковый номер буквы шифртекста

Тест №1 – Дымовое тестирование

Исходный текст: **пухленький тюленьчик**

Ключ: **льдина**

[**Таблица Виженера**](#_Таблица_Виженера_для)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **П** | **У** | **Х** | **Л** | **Е** | **Н** | **Ь** | **К** | **И** | **Й** | **Т** | **Ю** | **Л** | **Е** | **Н** | **Ь** | **Ч** | **И** | **К** |
| **Л** | **Ь** | **Д** | **И** | **Н** | **А** | **Л** | **Ь** | **Д** | **И** | **Н** | **А** | **Л** | **Ь** | **Д** | **И** | **Н** | **А** | **Л** |
| **Ы** | **П** | **Щ** | **Ф** | **Т** | **Н** | **З** | **Ж** | **М** | **Т** | **А** | **Ю** | **Ч** | **Б** | **С** | **Е** | **Е** | **И** | **Ц** |

Зашифрованный текст: **ЫПЩФТНЗЖМТАЮЧБСЕЕИЦ**

Дешифрованный текст (при исходном ключе): **ПУХЛЕНЬКИЙТЮЛЕНЬЧИК**

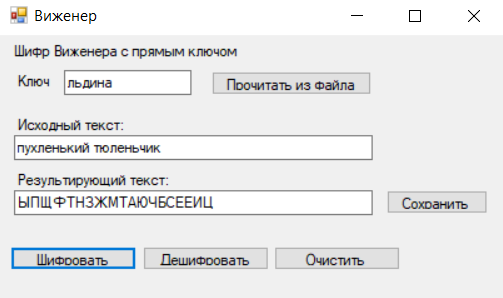


Рис. 1.1 – Результат работы шифрования

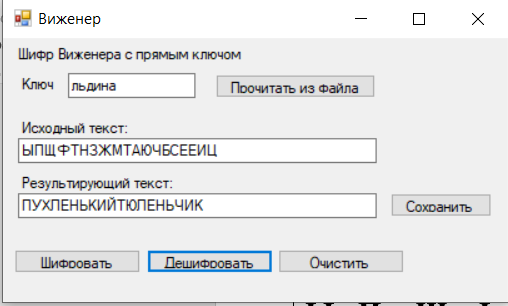


Рис. 1.2 – Результат работы дешифрования

Тест №2 – Ломаем на валидных данных (присутствует буква ё)

Открытый текст: **Ёжик жил у ёлки**

Ключ: **иголка**

[**Таблица Виженера**](#_Таблица_Виженера_для)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ё** | **Ж** | **И** | **К** | **Ж** | **И** | **Л** | **У** | **Ё** | **Л** | **К** | **И** |
| **И** | **Г** | **О** | **Л** | **К** | **А** | **И** | **Г** | **О** | **Л** | **К** | **А** |
| **О** | **Й** | **Ч** | **Ц** | **С** | **И** | **Ф** | **Ц** | **Ф** | **Ч** | **Х** | **И** |

Зашифрованный текст: **ОЙЧЦСИФЦФЧХИ**

Дешифрованный текст (при исходном ключе): **ЁЖИКЖИЛУЁЛКИ**

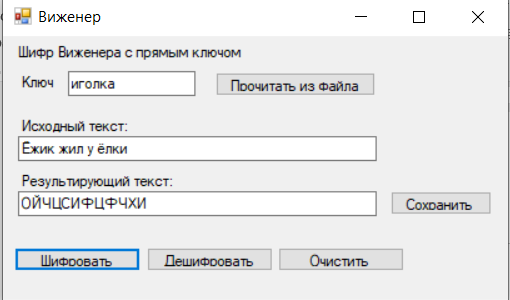
****

Рис. 2.1 – Результат работы шифрования

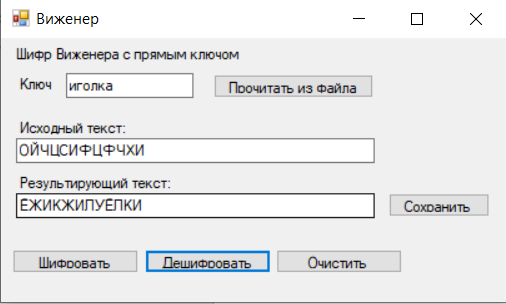


Рис. 2.2 – Результат работы дешифрования

Тест №3 – Ломаем на невалидных данных

Открытый текст: **Ёж343ик ж5fffил у ёлк12и**

Ключ: **иго345qлка**

[**Таблица Виженера**](#_Таблица_Виженера_для)

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ё** | **Ж** | **И** | **К** | **Ж** | **И** | **Л** | **У** | **Ё** | **Л** | **К** | **И** |
| **И** | **Г** | **О** | **Л** | **К** | **А** | **И** | **Г** | **О** | **Л** | **К** | **А** |
| **О** | **Й** | **Ч** | **Ц** | **С** | **И** | **Ф** | **Ц** | **Ф** | **Ч** | **Х** | **И** |

Зашифрованный текст: **ОЙЧЦСИФЦФЧХИ**

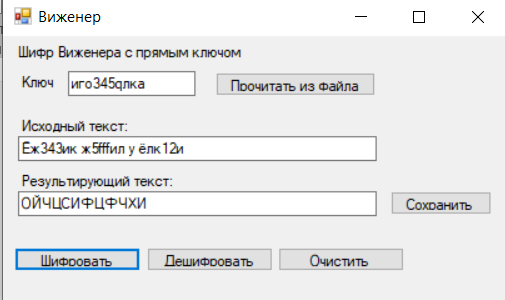
****Дешифрованный текст (при исходном ключе): **ЁЖИКЖИЛУЁЛКИ**

Рис. 3.1 – Результат работы шифрования

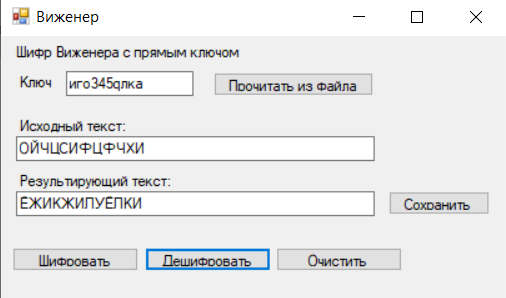


Рис. 3.2 – Результат работы дешифрования

Тест №4 – Ломаем на валидных данных. Длина ключа больше длины текста

Открытый текст: **утро**

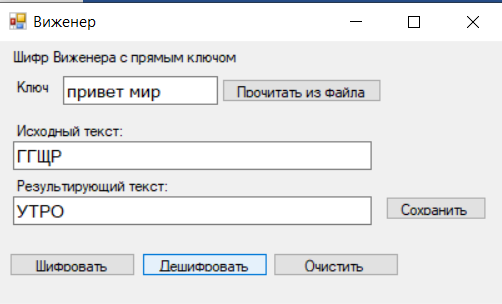
Ключ: **привет мир**

[**Таблица Виженера**](#_Таблица_Виженера_для)

|  |  |  |  |
| --- | --- | --- | --- |
| **У** | **Т** | **Р** | **О** |
| **П** | **Р** | **И** | **В** |
| **Г** | **Г** | **Щ** | **Р** |

Зашифрованный текст: **ГГЩР**

Дешифрованный текст (при исходном ключе): **УТРО**



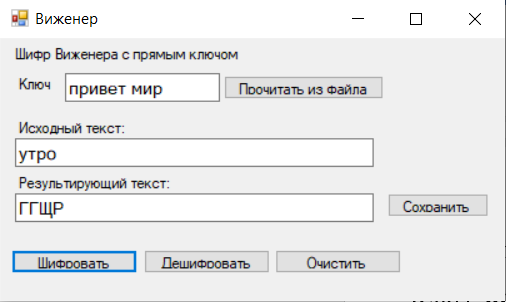
 Рис. 4.1 – Результат работы шифрования

Рис. 4.2 – Результат работы дешифрования