## Министерство образования Республики Беларусь Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей	
Кафедра программного обеспечения информационных т	гехнологий

Тесты к лабораторной работе №1

Проверила: Болтак С. В.

Выполнила: студент гр. 351001 Перова В. Д

# 1. «Столбцовый метод» с одним ключевым словом, текст на русском языке.

#### 1.1 Дымовое тестирование

Тестовая фраза: у многих бывают хобби

Ключевое слово: нелепые

Составим таблицу, используя ключ и тестовую фразу:

Н	Е	Л	Е	П	Ы	Е
5	1	4	2	6	7	3
У	M	Н	О	Γ	И	X
Б	Ы	В	A	Ю	T	X
О	Б	Б	И			

Полученный из таблицы шифротекст: МЫБОАИХХНВБУБОГЮИТ

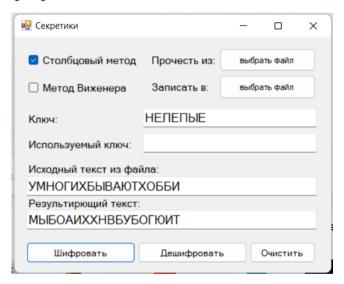


Рисунок 1.1.1 – Шифрование

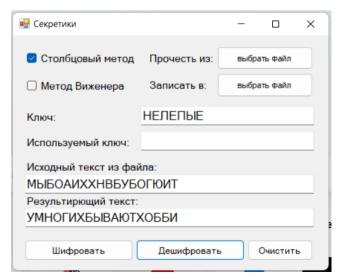


Рисунок 1.1.2 – Дешифрование

#### 1.2 Тестовая фраза заполняет полностью строчки таблицы

Тестовая фраза: рисование картин

Ключевое слово: хобби

Составим таблицу используя ключ и тестовую фразу:

X	О	Б	Б	И
5	4	1	2	3
P	И	С	О	В
A	Н	И	Е	К
A	P	Τ	И	Н

Полученный из таблицы шифротекст: СИТОЕИВКНИНРРАА

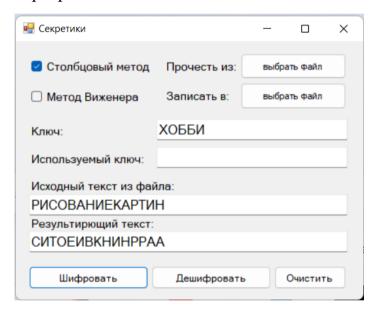


Рисунок 1.2.1 – Шифрование

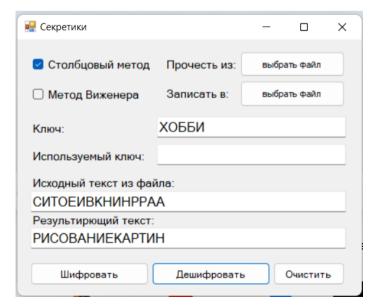


Рисунок 1.2.2 – Дешифрование

#### 1.3 Последняя строка тестовой фразы заполнена не полностью

Тестовая фраза: море и волны

Ключевое слово: картина

Составим таблицу используя тестовую фразу и ключевое слово:

К	A	P	T	И	Н	A
4	1	6	7	3	5	2
M	О	P	Е	И	В	О
Л	Н	Ы				

Полученный из таблицы шифротекст: ОНОИМЛВРЫЕ

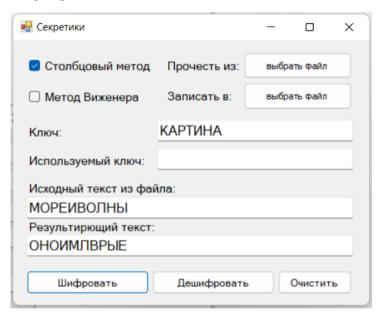


Рисунок 1.3.1 – Шифрование

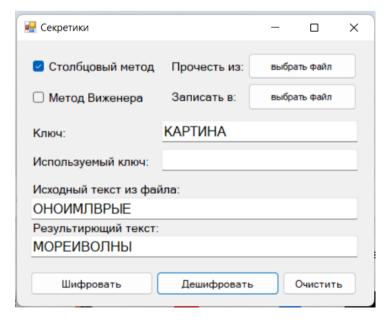


Рисунок 1.3.2 - Дешифрование

#### 1.4 Ломаем на валидных данных

#### Минимальная длина ключа (ключ состоит из одной буквы).

Тестовая фраза: программист

Ключевое слово: а

Составим таблицу используя тестовую фразу и ключевое слово (для удобства таблица записана в строку, а не в столбец):

## A 1 Π P O Γ P A M M И C T

Полученный из таблицы шифротекст: ПРОГРАММИСТ

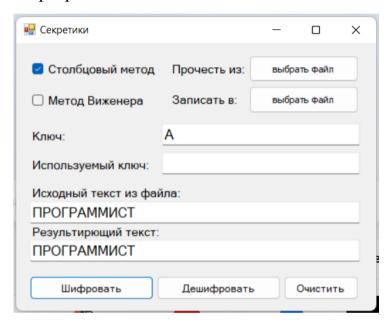


Рисунок 1.4.1 – Шифрование

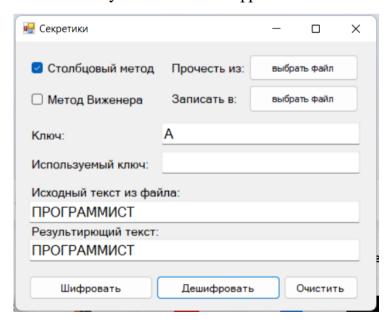


Рисунок 1.4.2 – Дешифрование

# Максимальная длина ключа (ключ имеет длину, превышающую тестовое слово).

Тестовая фраза: слово

Ключевое слово: очень длинный ключ

Составим таблицу используя тестовую фразу и ключевое слово:

О	Ч	Е	Н	Ь	Д	Л	И	Н	Н	Ы	Й	К	Л	Ю	Ч
11	12	2	8	15	1	6	3	9	10	14	4	5	7	16	13
С	Л	О	В	О											

Полученный из таблицы шифротекст: ОВСЛО

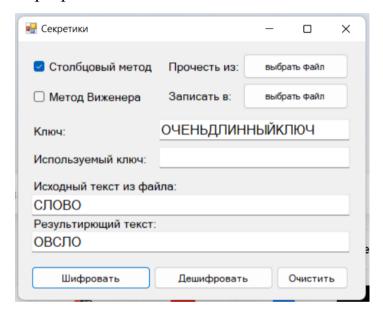


Рисунок 1.4.3 – Шифрование

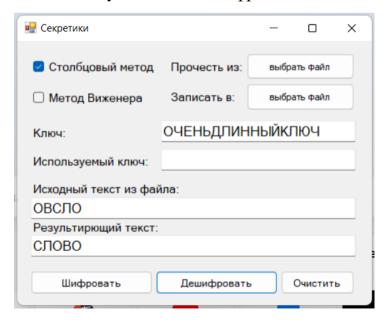


Рисунок 1.4.4 – Дешифрование

#### Ключ с повторяющимися символами.

Тестовая фраза: шифрослово

Ключевое слово: кккллюч

Составим таблицу используя тестовую фразу и ключевое слово:

К	К	К	Л	Л	Ю	Ч
1	2	3	4	5	7	6
Ш	И	Φ	P	О	С	Л
О	В	О				

Полученный из таблицы шифротекст: ШОИВФОРОЛС

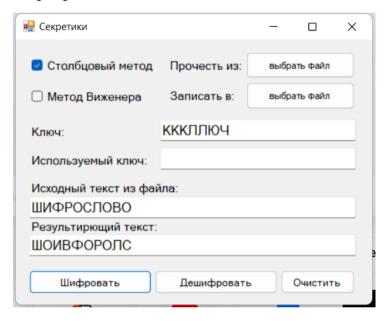


Рисунок 1.4.5 – Шифрование

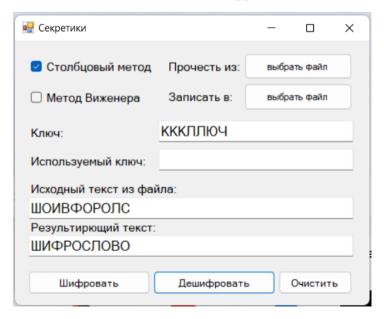


Рисунок 1.4.6 – Дешифрование

#### 1.5 Ломаем на не валидных данных

## Пустой ключ.

Тестовая фраза: программист

Ключевое слово:

Результат работы программы:

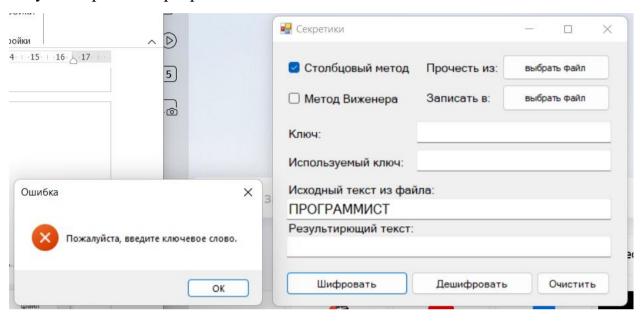


Рисунок 1.4.7 – Шифрование

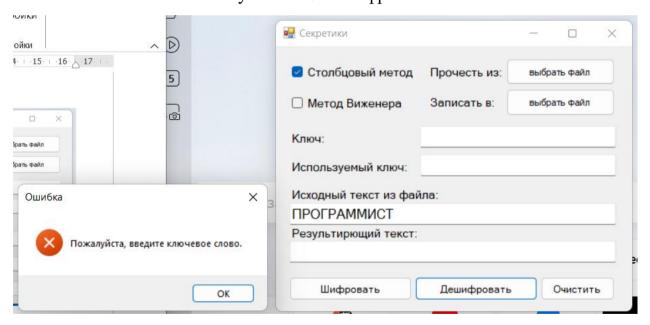


Рисунок 1.4.8 – Дешифрование

Вывод: Программа не начнет выполнять шифрование или дешифрование, пока ячейка ключа не будет заполнена

#### Ключ с недопустимыми значениями.

Тестовая фраза: программист

Ключевое слово: ключ888fg

Составим таблицу используя тестовую фразу и ключевое слово:

К	Л	Ю	Ч
1	2	4	3
П	P	О	Γ
P	A	M	M
И	С	T	

Полученный из таблицы шифротекст: ПРИРАСГМОМТ

Результат работы программы:

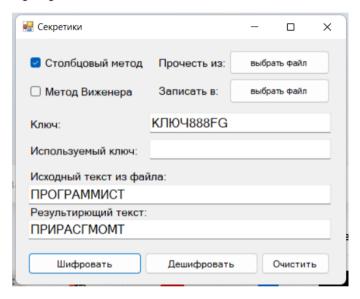


Рисунок 1.4.9 – Шифрование

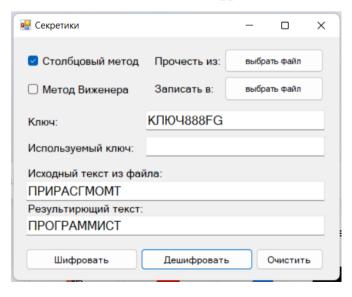


Рисунок 1.4.10 – Дешифрование

Вывод: не валидные данные игнорируются при (де)шифровании.

Тестовая фраза: I have 3 хобби

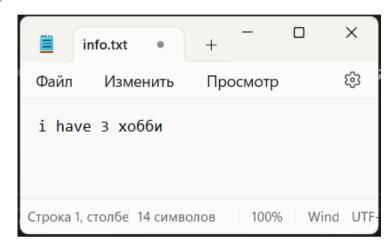
Ключевое слово: круто

Составим таблицу, используя ключ и тестовую фразу:

К	P	У	T	О
1	3	5	4	2
X	О	Б	Б	И

Полученный из таблицы шифротекст: ХИОББ

Содержимое файла:



Результат работы программы:

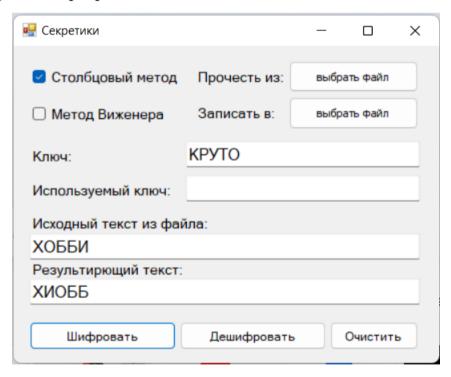


Рисунок 1.4.11 – Шифрование

Вывод: при шифровании, недопустимые значения в исходном тексте игнорируются.

Тестовая фраза (шифротекст): ХИО22БFБ

Ключевое слово: круто

Для дешифрования расставим порядок букв для ключа:

К	P	У	T	О
1	3	5	4	2

Теперь по порядку и подставим наш шифр (игнорируем недопустимые значения):

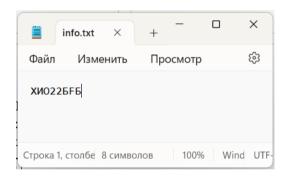
К	О	P	T	У
1	2	3	4	5
X	И	O	Б	Б

Соберем ключ обратно:

К	P	У	T	О
1	3	5	4	2
X	О	Б	Б	И

Полученный из таблицы текст: ХОББИ

Содержимое файла:



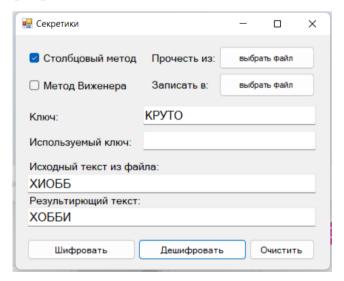


Рисунок 1.4.12 – Дешифрование (недопустимые значения игнорируются)

# 2. Алгоритм Виженера, самогенерирующийся ключ, текст на русском языке

## 2.1 Таблица подстановки для русского языка.

								ı							I																		
В	В	A	P	B	$ \Gamma $	Д	E	Ή	Ж	3	И	Й	K	П	M	Н	0	П	P	С	T	y	Φ	X	ПП	h	Ш	Щ	P	PI	P	Э	NO.
Ю	Ю	К	A	P	В	Ī	Д	田	Ë	Ж	3	И	Й	K	Л	M	Н	0	П	Ь	C	I	y	Φ	X	П	h	П	Щ	P	PI	P	Э
Э	Э	Ю	В	A	P	В	I	Д	E	Ë	Ж	3	И	Й	Х	П	M	Н	0	П	Ь	С	T	У	Φ	X	П	h	П	Щ	Ъ	bI	P
P	P	Э	Ю	В	A	Р	В	Ц	Д	E	Ë	Ж	3	И	Й	K	П	M	Η	0	П	Ь	С	Τ	y	Ф	×	П	h	Ш	Ш	<b>P</b>	PI
PI	PI	q	Э	Ю	В	Α	Р	В	Г	Д	E	Ë	×	3	И	Й	K	П	M	Η	0	П	Ь	С	T	λ	Ф	X	Ц	h	П	Щ	Ъ
<b>P</b>	$\mathbf{q}$	Ιq	q	Э	Ю	К	Α	Р	В	Л	П	Ε	Ë	Ж	3	И	Й	Х	П	М	Η	0	П	d	С	I	V	Ф	X	П	h	$\blacksquare$	Щ
Щ	Ш	$\mathbf{q}$	Iq	q	$\epsilon$	Ю	К	Α	g	В	Л	Д	Э	Ħ	Ж	3	И	Й	К	П	М	Η	0	П	d	Э	L	λ	Ф	X	П	h	Ш
Ш	$\Pi$	Ш	$\mathbf{q}$	PI	q	$\epsilon$	Ю	К	Y	g	В	Γ	П	Ξ	Ë	Ж	8	И	Й	У	Г	М	Η	0	П	ď	С	I	y	Ф	X	Ц	h
Ч	h	Ш	Щ	Ъ	Ы	P	Э	Ю	В	A	Б	В	Γ	Д	E	Ë	Ж	3	И	Й	K	Л	M	Н	0	П	Ь	С	Т	y	Φ	X	Ц
Ц	Ц	h	Ш	Щ	Ъ	PI	P	Э	Ю	В	Α	Б	В	Γ	Д	Е	Ë	Ж	3	И	Й	K	Л	M	Н	0	П	P	С	Τ	y	Φ	X
X	X	Ц	h	Ш	Щ	<b>P</b>	PI	P	Э	Ю	В	A	Р	В	Г	Д	E	Ë	Ж	3	И	Й	K	Л	M	Η	0	П	Ь	С	Τ	У	Φ
Ф	Φ	X	Ц	h	$\Pi$	Щ	P	PI	P	Э	Ю	В	A	Р	В	Γ	Д	Ε	Ë	Ж	3	И	Й	K	Л	M	Н	0	П	Ь	С	Т	y
y	y	Φ	X	Ц	h	Ш	Щ	<b>P</b>	PI	P	Э	Ю	К	A	Р	В	Γ	Д	Е	Ë	Ж	3	И	Й	K	Л	М	Н	0	П	Ь	C	Τ
Т	Τ	y	Φ	X	Ц	h	Ш	Щ	Ъ	PI	P	Э	Ю	К	A	Р	В	Γ	Д	Ε	Ë	Ж	3	И	Й	K	Л	M	Н	0	П	Р	С
С	С	Τ	y	Φ	X	Ц	h	П	Щ	Ъ	PI	b	Э	Ю	В	A	Р	В	Γ	Д	E	Ë	Ж	3	И	Й	Х	Л	M	Н	0	П	Ь
Ь	Ь	С	Τ	y	Φ	X	Ц	h	Ш	Щ	Ъ	PI	P	Э	Ю	К	Α	Р	В	П	Д	Ε	Ë	Ж	3	И	Й	K	Л	M	Η	0	П
П	П	Ь	С	Τ	y	Ф	X	П	h	Ш	Щ	Ъ	PI	P	Э	Ю	В	Α	Б	В	L	Д	E	Ë	Ж	3	И	Й	K	Л	M	Н	0
0	0	П	Ь	С	T	V	Ф	×	Ц	h	Ш	Щ	4	PI	P	9	Ю	К	A	Р	В	Ц	Д	E	Ë	×	3	И	Й	K	Л	M	Н
Η	Н	0	П	Ь	С	L	y	Ф	X	Ц	h	Ш	Ħ	<b>P</b>	PI	Р	Э	Ю	В	Α	Р	В	Г	Д	E	Ή	×	3	И	Й	K	Л	M
M	M	Η	0	П	Ь	C	L	>	Φ	X	Ц	h	Ш	Ш	Ъ	PI	P	Э	Ю	К	A	Р	В	Г	Д	Э	'nП	Ж	3	И	Й	K	Л
Л	Л	M	Н	0	П	Ь	С	П	y	Φ	X	Ц	h	Ш	Ħ	Ъ	PI	P	Э	Ю	К	A	Р	В	Γ	Д	ш	Ë	Ж	3	И	Й	K
К	K	Л	M	Н	0	П	Ь	ပ	Τ	У	Ф	X	П	h	Ħ	Ħ	Ъ	PI	P	Э	Ю	К	Α	Р	В	L	Д	E	Ë	Ж	3	И	Й
Й	Й	K	Л	M	Н	0	П	Ь	С	Τ	y	Φ	X	Ц	h	Ш	Ш	P	PI	q	Э	Ю	В	A	Р	В	Г	Д	Е	Ë	Ж	3	И
И	И	Й	K	Л	M	Η	0	П	Ь	С	Τ	y	Ф	X	Ц	h	Ш	Щ	Ъ	ΡI	P	Э	Ю	К	A	P	В	Γ	Д	E	Ë	×	3
3	3	И	Й	K	Л	M	Н	0	П	Ь	С	Τ	y	Φ	×	П	h	Ш	Щ	<b>P</b>	PI	P	Э	Ю	В	A	Р	В	Γ	Д	E	Ë	Ж
X	Ж	3	И	Й	K	Л	M	Н	0	П	Ь	С	Τ	y	Ф	×	Ц	h	Ш	Ш	<b>P</b>	PI	P	Э	Ю	К	А	Б	В	Г	Д	E	÷П
Ë	Ë	Ж	3	И	Й	K	Л	М	Н	0	П	Р	C	T	V	Ф	X	Ц	h	Ш	Щ	<b>P</b>	Ы	P	Э	Ю	К	A	Р	В	Γ	Д	E
E	E	Ë	Ж	3	И	Й	K	П	M	Η	0	П	Ь	С	Τ	V	Φ	X	Ц	h	Ш	Щ	Ъ	PI	P	Э	Ю	Я	A	Б	В	Γ	Д
Д	Д	E	Ë	Ж	3	И	Й	×	Л	M	Н	0	П	Ь	C	Т	y	Φ	X	Ц	h	Ш	Щ	P	PI	P	Э	Ю	В	A	Р	В	П
L	Γ	Д	Ε	Ë	Ж	3	И	Й	K	Л	M	Н	0	П	Ь	C	Т	y	Φ	×	Ц	h	Ш	Щ	<b>P</b>	PI	P	Э	Ю	В	A	Б	В
В	В	Г	Д	Е	Ë	¥	3	И	Й	K	Л	M	Н	0	П	Ь	С	T	y	Φ	X	Ц	h	Ш	Щ	P	PI	P	Э	Ю	Я	A	Р
P	Р	В	Γ	Д	E	Ë	Ж	33	И	Й	K	Л	M	Н	0	П	Ь	C	Τ	y	Ф	×	Ц	h	Ш	Щ	<b>P</b>	PI	P	Э	Ю	Я	A
A	A	P	В	Г	Д	E	Ë	×	3	И	Й	K	Л	M	Н	0	П	Ь	С	T	y	Φ	X	Ц	h	Ш	Ħ	P	PI	P	Э	Ю	В
	А	Р	В	Γ	Д	E	Ë	×	3	И	Й	K	Л	M	Η	0	П	Ь	С	Τ	y	Ф	X	Ц	h	Ш	Щ	Ъ	Ы	P	Э	Ю	К

#### 2.2 Расчётные формулы

#### **2.2.1** Шифрование (1)

$$C_{i} = (P_{i} + K_{j}) \mod N$$

Сі – Зашифрованный символ на позиции і

Р<sub>і</sub> – Символ тестовой фразы

 $K_i$  — Символ ключа на позиции ј

N – Длина алфавита (в русском составляет 33)

Пример (литературные амбиции, творчество):

#### Русский алфавит:

Α	Б	В	Γ	Д	Ε	Ë	Ж	3	И	Й	К	Л	М	Н	0	П	Р	С	Т	У	Ф	Χ	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

#### Шаги шифрования:

#### 1. Подготовка данных:

Тестовая фраза:

Л	И	T	Е	P	A	T	У	P	Н	Ы	Е	A	M	Б	И	Ц	И	И
12	9	19	5	17	0	19	20	17	13	29	5	0	13	1	9	23	9	9

#### Ключевое слово:

Ī	T	В	О	P	Ч	Е	С	T	В	О	Л	И	T	Е	P	Α	T	У	P
	19	2	15	17	22	5	18	19	2	15	12	9	19	5	17	0	19	20	17

## 2. Применение формулы (1):

$$(12 + 19) \mod 33 = 31$$

$$(9+2) \mod 33 = 11$$

$$(19 + 15) \mod 33 = 1$$

$$(5 + 17) \mod 33 = 22$$

$$(17 + 22) \mod 33 = 6$$

$$(0+5) \mod 33 = 5$$

$$(19 + 18) \mod 33 = 4$$

$$(20 + 19) \mod 33 = 6$$

$$(17 + 2) \mod 33 = 19$$

$$(13 + 15) \mod 33 = 28$$

$$(29 + 12) \mod 33 = 8$$

$$(5+9) \mod 33 = 14$$

$$(0+19) \mod 33 = 19$$

$$(13 + 5) \mod 33 = 18$$

$$(1+17) \mod 33 = 18$$

$$(9+0) \mod 33 = 9$$

$$(23 + 19) \mod 33 = 9$$

$$(9 + 20) \mod 33 = 29$$

$$(9+17) \mod 33 = 26$$

#### 3. Общая таблица с результатом:

символ	Pi	символ	Kj	формула	шифр
фразы		ключа			
Л	12	T	19	31	Ю
И	9	В	2	11	К
Т	19	О	15	1	Б
Е	5	P	17	22	Ч
Р	17	Ч	22	6	3
Α	0	Е	5	5	Е
Т	19	С	18	4	Д
У	20	T	19	6	Ë
Р	17	В	2	19	T
Н	13	O	15	28	Ь
Ы	28	Л	12	7	Ж
Е	5	И	9	14	Н
Α	0	T	19	19	T
М	13	Е	5	18	C
Б	1	P	17	18	C
И	9	A	0	9	И
Ц	23	T	19	9	И
И	9	У	20	29	Ь
И	9	P	17	26	Щ

## 4. Результат:

Зашифрованный текст: ЮКБХЗЕДЁТЬЖНТССИИЬЩ

#### 2.2.2 Дешифрование (2)

$$P_{i} = (C_{i} - K_{i} + N) \mod N$$

Сі – Зашифрованный символ на позиции і

Р<sub>і</sub> – Символ тестовой фразы

K<sub>i</sub> – Символ ключа на позиции ј

N – Длина алфавита (в русском составляет 33)

Пример (литературные амбиции, творчество):

#### Русский алфавит:

Α	Б	В	Γ	Д	Е	Ë	Ж	3	И	Й	К	Л	М	I	0	П	Р	С	Т	У	Ф	Χ	Д	Д	Е	E	Ъ	Ы	Ф	$\mathbf{\Theta}$	Э	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

#### Шаги шифрования:

#### 1. Подготовка данных:

#### Зашифрованная фраза:

Ю	К	Б	Χ	3	Ε	Д	Ë	Т	Ь	Ж	Н	T	С	С	И	И	Ь	Щ
31	11	1	22	6	5	4	6	19	28	8	14	19	18	18	9	9	29	26

#### Ключевое слово:

Т	В	0	Р	Ч	Е	С	Т	В	0	Ю	К	Б	Χ	3	Ε	Д	Ë	Т
19	2	15	17	22	5	18	19	2	15	29	11	1	22	8	5	4	6	19

## 2. Применение формулы (1):

$$(31 - 19 + 33) \mod 33 = 12$$

$$(11 - 2 + 33) \mod 33 = 9$$

$$(1-15+33) \mod 33 = 19$$

$$(22 - 17 + 33) \mod 33 = 5$$

$$(6-22+33) \mod 33 = 17$$

$$(5 - 5 + 33) \mod 33 = 0$$

$$(4-18+33) \mod 33 = 19$$

$$(6 - 19 + 33) \mod 33 = 20$$

$$(19 - 2 + 33) \mod 33 = 17$$

$$(29 - 15 + 33) \mod 33 = 14$$

Так как мы используем самогенерирующий ключ, то после того, как мы закончили расшифровывать исходный ключ, мы используем часть расшифрованного текста для его продолжения.

$$(7-12+33) \mod 33 = 28$$

$$(14 - 9 + 33) \mod 33 = 5$$

$$(19-19+33) \mod 33=0$$

$$(18 - 5 + 33) \mod 33 = 13$$

$$(18-17+33) \mod 33 = 1$$

$$(9 - 0 + 33) \mod 33 = 9$$

$$(9 - 19 + 33) \mod 33 = 23$$

$$(29 - 20 + 33) \mod 33 = 9$$

$$(26 - 17 + 33) \mod 33 = 9$$

## 3. Общая таблица с результатом:

символ фразы	Pi	символ ключа	Kj	формула	фраза
Ю	31	Т	19	12	Л
К	11	В	2	9	И
Б	1	0	15	19	T
Х	22	Р	17	5	E
3	6	Ч	22	17	Р
Е	5	Е	5	0	Α
Д	4	С	18	19	Т
Ë	6	Т	19	20	У
Т	19	В	2	17	Р
Ь	29	0	15	14	Н
Ж	7	Л	12	28	Ы
Н	14	И	9	5	E
Т	19	Т	19	0	Α
С	18	E	5	13	М
С	18	Р	17	1	Б
И	9	Α	0	9	И
И	9	Т	19	23	Ц
Ь	29	У	20	9	И
Щ	26	Р	17	9	И

#### 4. Результат:

Расшифрованный текст: ЛИТЕРАТУРНЫЕ АМБИЦИИ

#### 2.3 Дымовое тестирование

Тестовая фраза: литературные амбиции

Ключевое слово: творчество

Сгенерированный ключ: ТВОРЧЕСТВОЛИТЕРАТУР

Составим таблицу, используя ключ и тестовую фразу:

Л	И	Т	Е	P	A	T	У	P	Н	Ы	Е	A	M	Б	И	Ц	И	И
T	В	О	P	Ч	Е	С	T	В	О	Л	И	T	Е	P	A	T	У	P
Ю	К	Б	Ч	3	Е	Д	Ë	T	Ь	Ж	Н	T	С	С	И	И	Ь	Щ

Полученный из таблицы шифротекст: ЮКБХЗЕДЁТЬЖНТССИИЬЩ

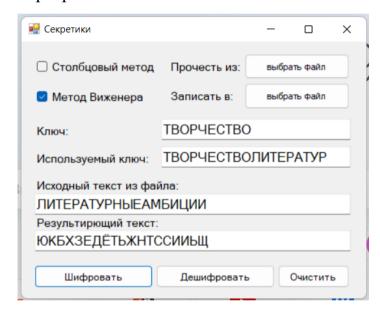


Рисунок 2.3.1 – Шифрование

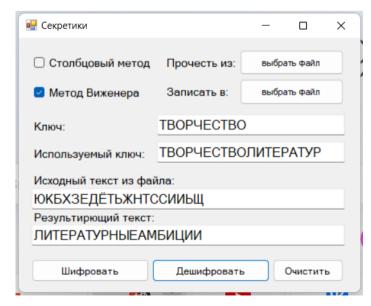


Рисунок 2.3.1 – Дешифрование

### 2.4 Ломаем на валидных данных (тестовая фраза, содержащая букву Ё)

Тестовая фраза: ёж и ёлка

Ключевое слово: иголка

Сгенерированное слово: ИГОЛКАЁ

Составим таблицу, используя ключ и тестовую фразу:

Ë	Ж	И	Ë	Л	К	A
И	Γ	О	Л	К	A	Ë
О	Й	Ч	С	Ц	К	Ë

Полученный из таблицы шифротекст: ОЙЧСЦКЁ

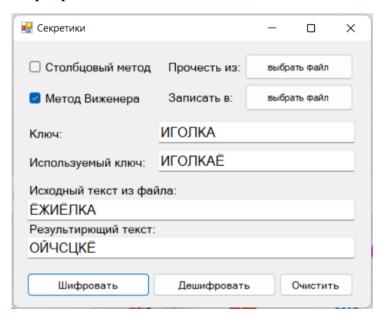


Рисунок 2.4.1 – Шифрование

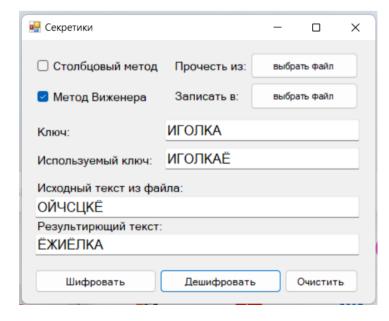


Рисунок 2.4.2 – Дешифрование

## 2.5 Ломаем на не валидных данных (ключ содержит недопустимые значения)

Тестовая фраза: несколько значений

Ключевое слово: **fчис9ло** 

Сгенерированное слово: ЧИСЛОНЕСКОЛЬКОЗНА

Составим таблицу, используя ключ и тестовую фразу:

Н	Е	C	К	О	Л	Ь	К	О	3	Н	A	Ч	Е	Н	И	Й
Ч	И	С	Л	О	Н	Е	С	К	О	Л	Ь	К	О	3	Н	Α
Е	Н	Γ	Ц	Э	Щ	Б	Ь	Щ	Ц	Щ	Ь	В	У	Χ	Ц	Й

Полученный из таблицы шифротекст: ЕНГЦЭЩБЬЩЦЩЬВУХЦЙ

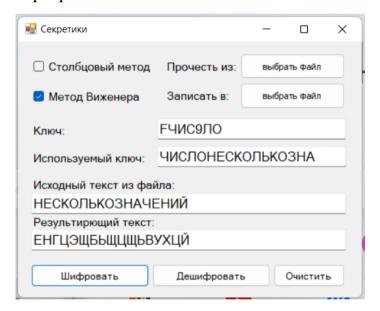


Рисунок 2.5.1 – Шифрование

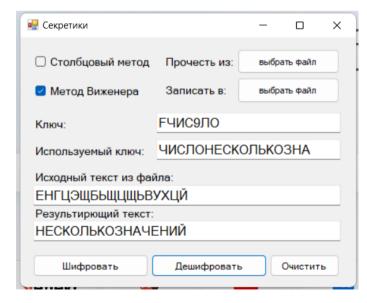


Рисунок 2.5.2 – Дешифрование