УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1

по предмету «Теория информации»

Вариант 9

Выполнил:

Левкович Н. С.

Гр. 451004

Проверил:

Болтак С. В

Минск 2026

Задание:

Вариант 9.

Написать программу, которая выполняет шифрование и дешифрование текстового файла любого размера, содержащего текст на заданном языке, используя следующие алгоритмы шифрования:

- **Шифр Плейфейра**, текст на английском языке;
- алгоритм **Виженера**, **прогрессивный ключ**, текст на русском языке.

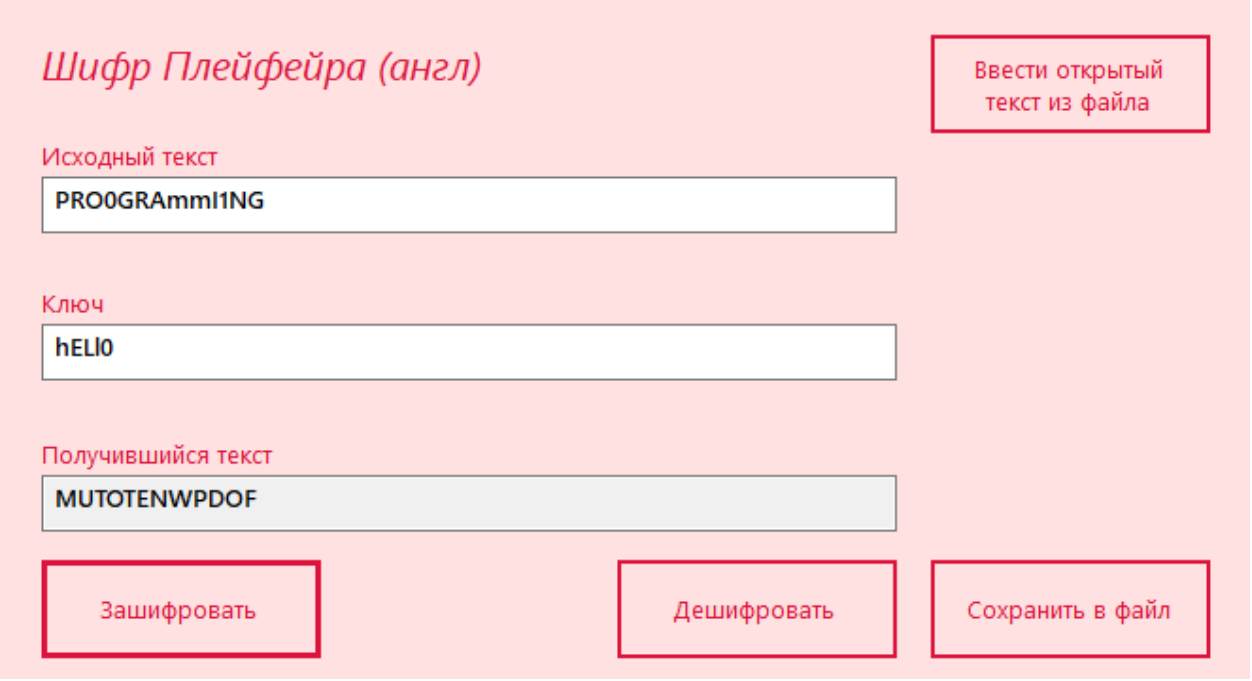
Для всех алгоритмов ключ задается с клавиатуры пользователем.

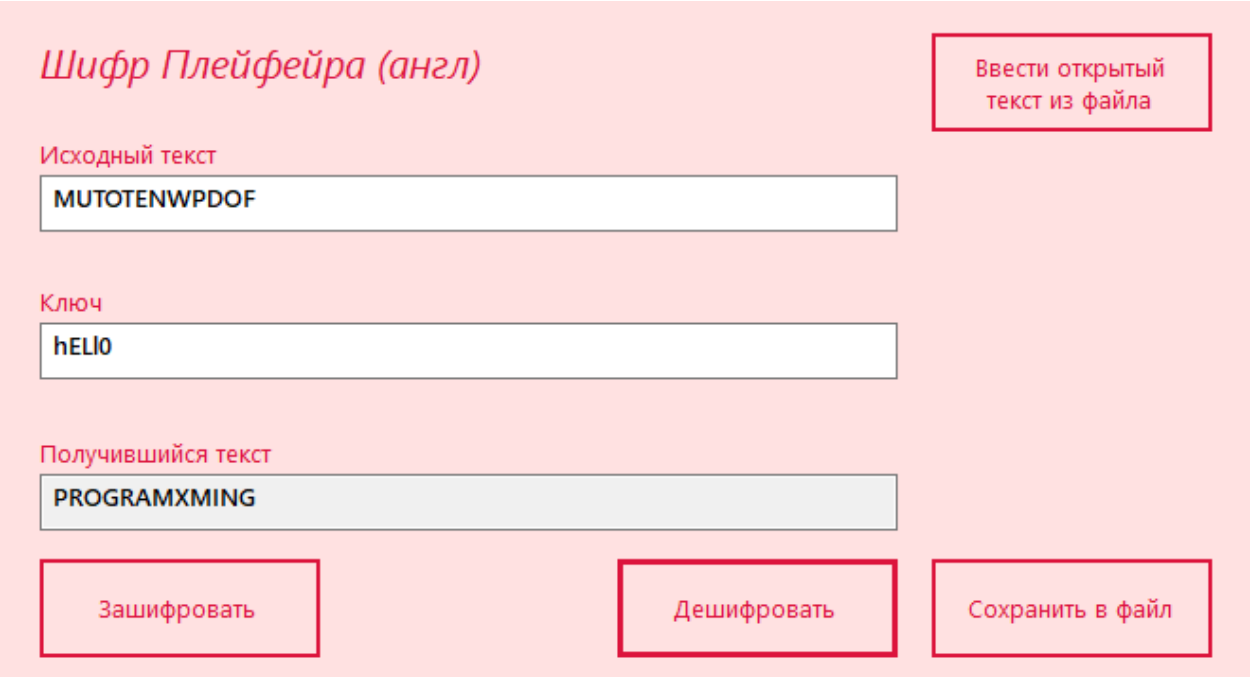
Программа должна игнорировать все символы, не являющиеся буквами заданного алфавита, и шифровать только текст на заданном языке. Все алгоритмы должны быть реализованы в одной программе. Программа не должна быть написана в консольном режиме. Результат работы программы – зашифрованный/расшифрованный файл/ы. Кроме работы с файлами программа должна предоставлять ввод/вывод шифруемого текста с клавиатуры/на экран.

Шифр Плейфейра

Тесты:

1. Дымовое тестирование





Текст: PROGRAMMING
Ключевое слово: HELL

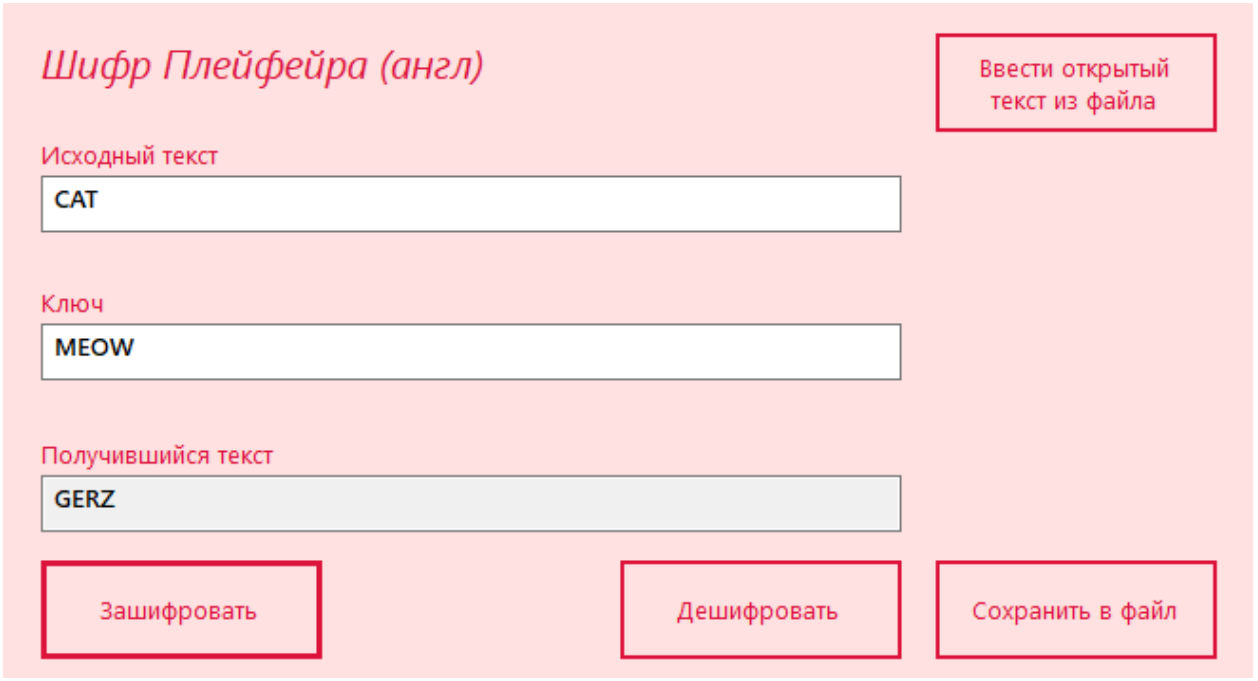
После преобразования текст будет выглядеть так:
PROGRAMXMING
Между повторяющимися символами ‘M’ вставляется пустой символ ‘X’.

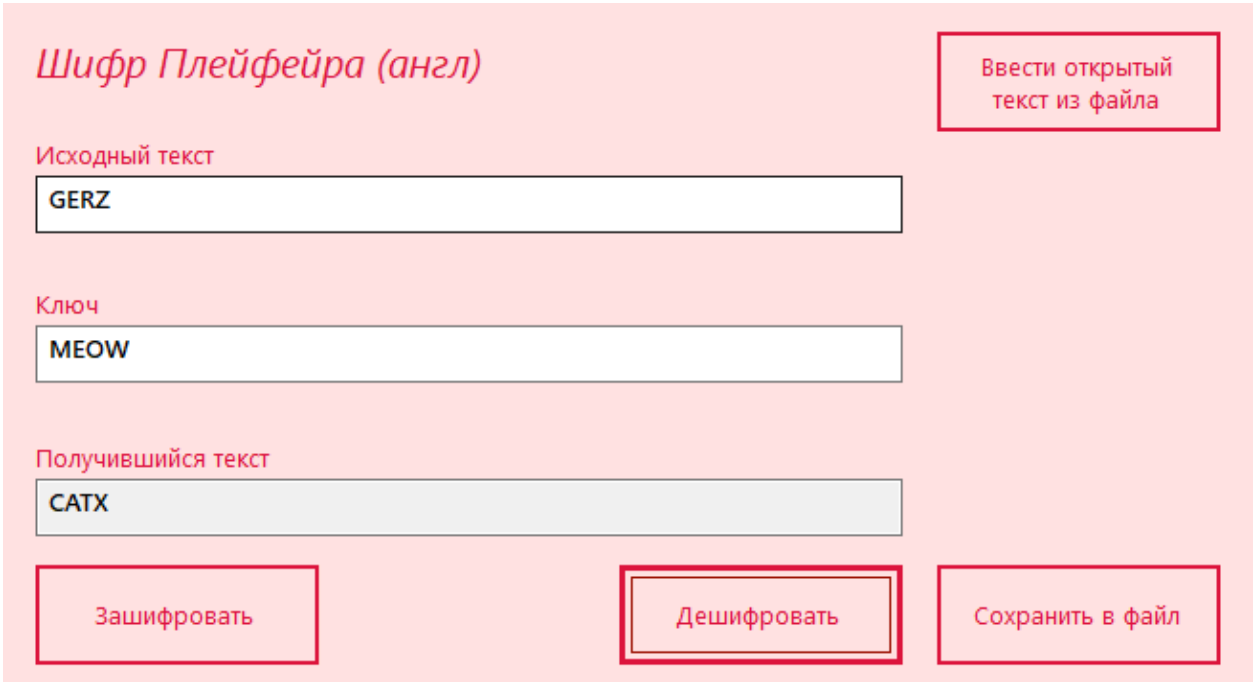
Таблица:

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

PR -> MU
OG -> TO
RA -> ET
MX -> NW
MI -> PD
NG -> OF
Шифротекст: **MUTOTENWPDOF**

2.





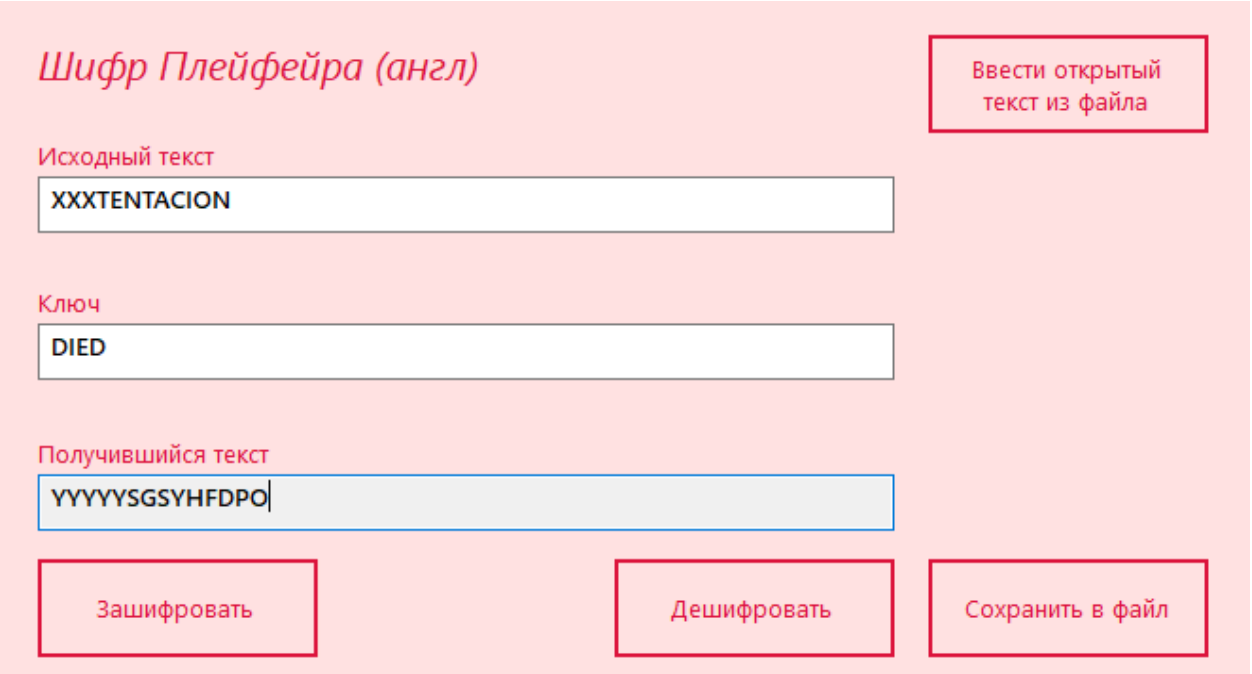
Текст: CAT
Ключ: MEOW
Количество символов нечётное, поэтому в конец будет добавлен ‘X’.
Изменённый текст: CATX

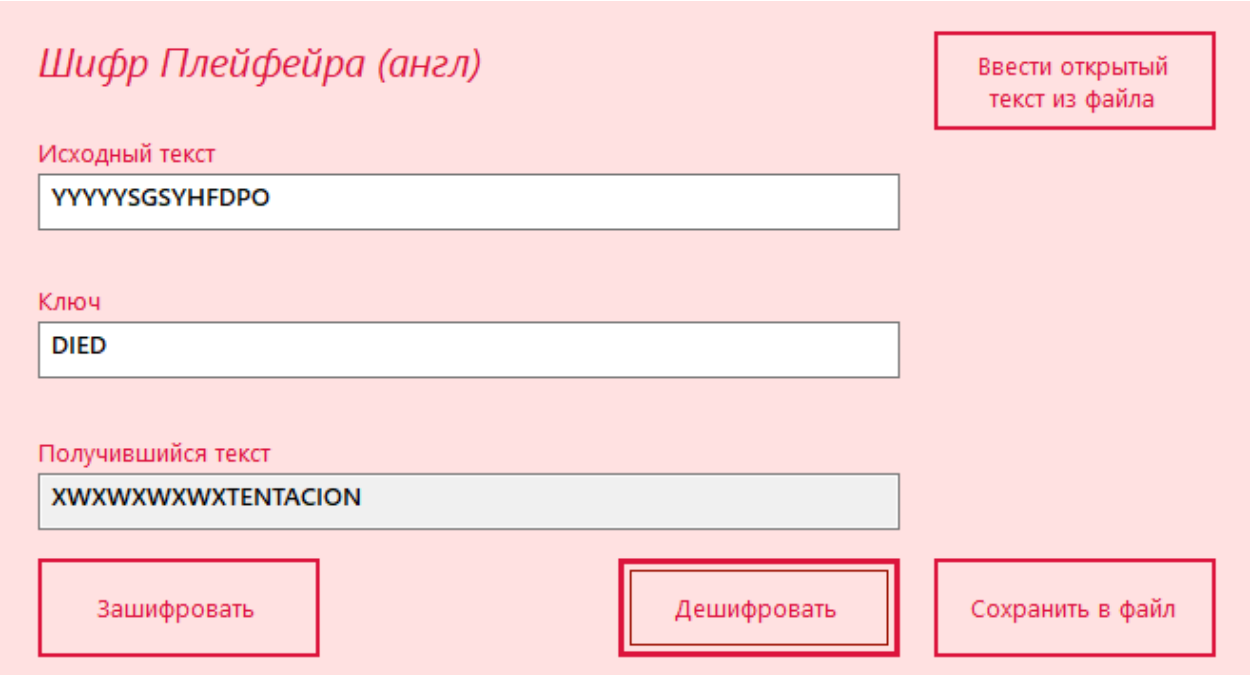
Таблица:

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

CA -> GE
TX -> RZ
Шифротекст: **GERZ**

3.





Текст: XXXTENTACION
Ключ: DIED
Изменённый текст: XXXXXTENTACION
Таблица:

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

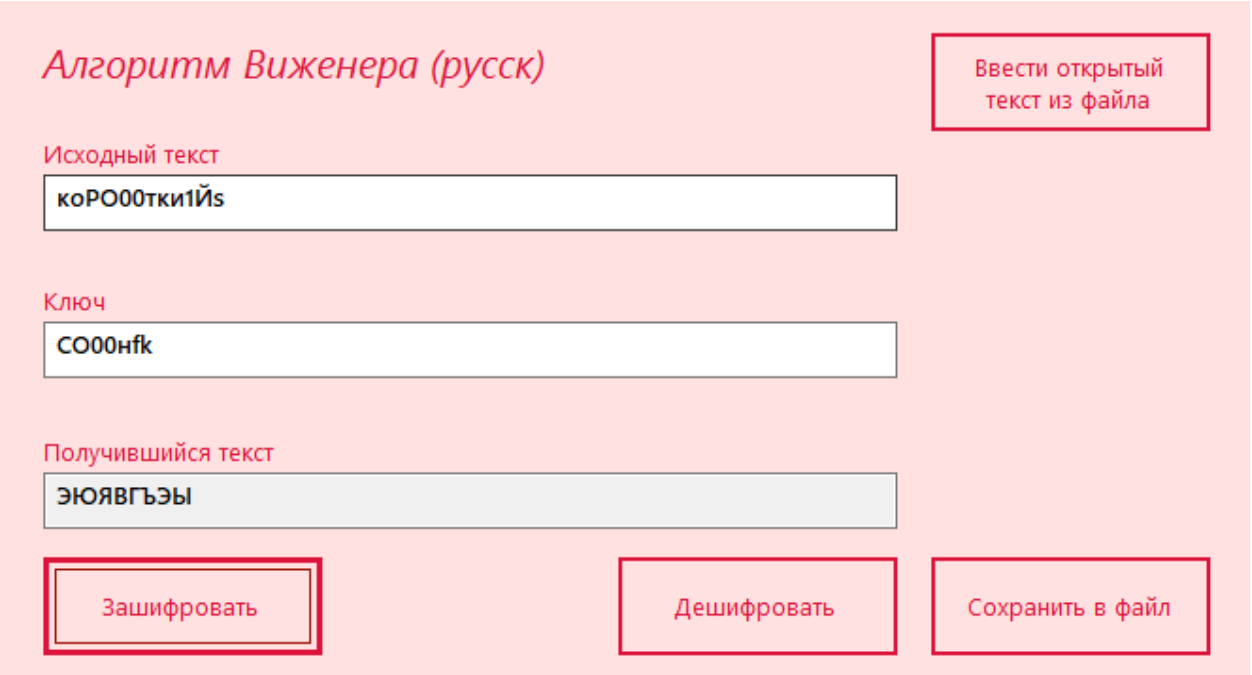
Поскольку ‘X’ используется по умолчанию в качестве пустого символа, то повторение в тексте этих символов провоцируют появление ещё большего количества таких символов, таким образом происходит коллизия.
XX -> YY
XX -> YY
XT -> YS
EN -> GS
TA -> YH
CI -> FD
ON -> PO

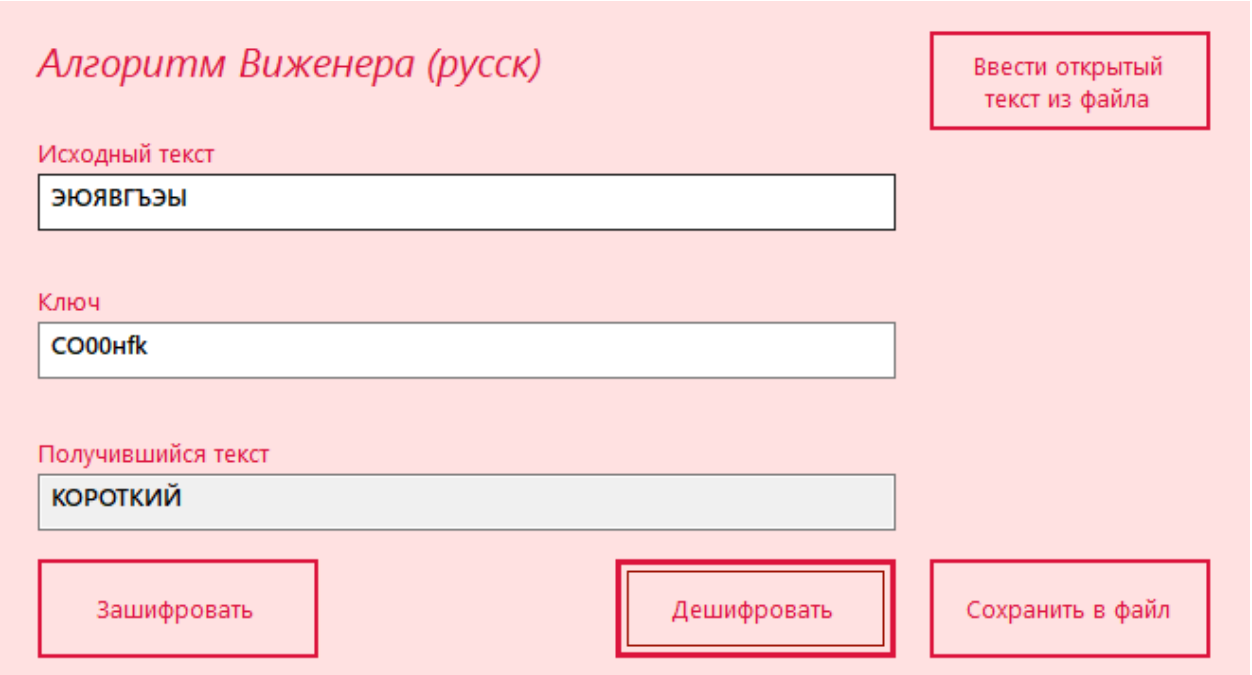
Шифротекст: **YYYYYSGSYHFDPO**
После дешифрации полученного шифротекста полученный текст станет ещё длиннее за счет повторяющихся символов ‘Y’.
В итоге текст будет изменён следующим образом:
YXYXYXYXYSGSYHFDPO
YX -> XW
YX -> XW
…
YS -> XT
GS -> EN
YH -> TA
FD -> CI
PO -> ON
В результате получим: **XWXWXWXWXTENTACION**

Алгоритм Виженера, прогрессивный ключ

Алфавит языка:

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



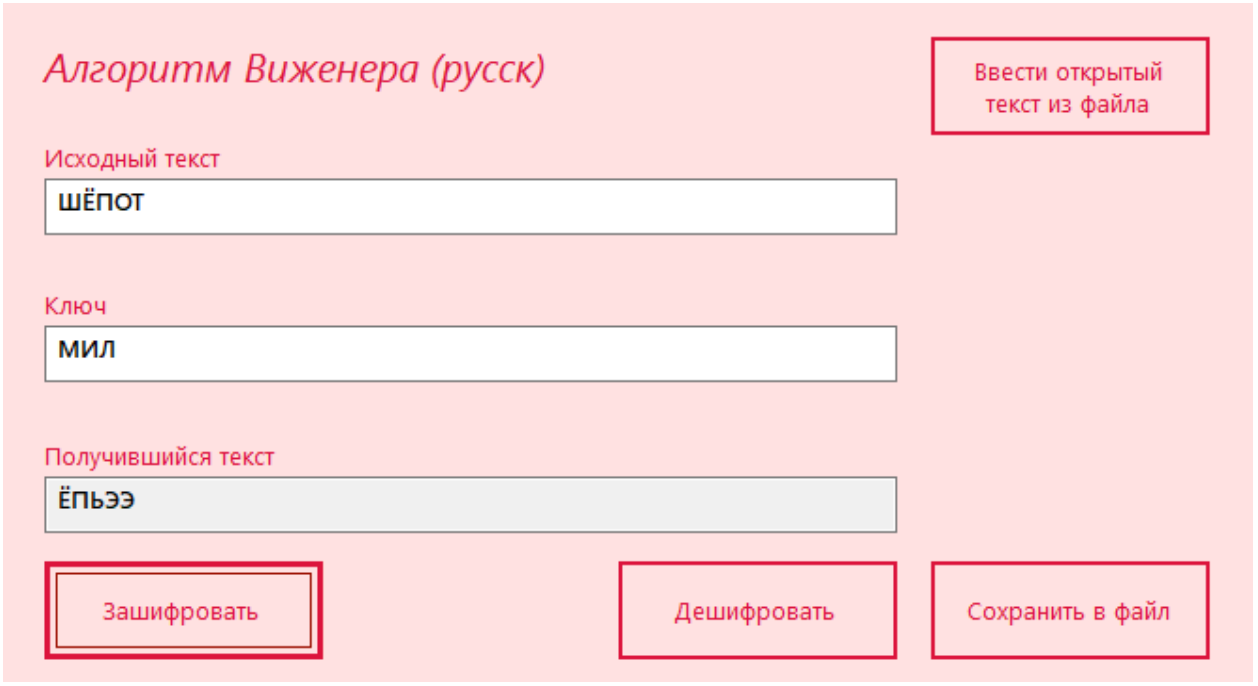


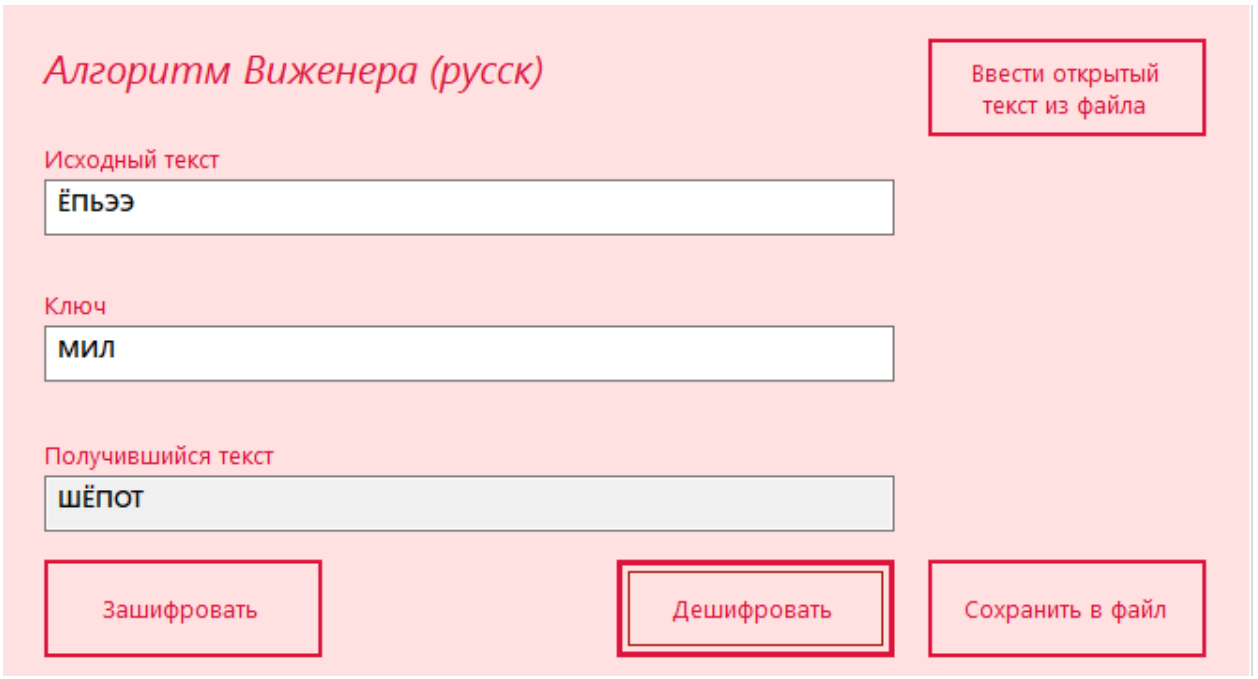
К	О	Р	О	Т	К	И	Й
С	О	Н	Т	П	О	У	Р
Э	Ю	Я	И	Г	Ъ	Э	Ы

Шифротекст: **ЭЮЯВГЪЭЫ**

Недопустимые символы игнорируются как в исходном тексте, так и в ключе.

2.

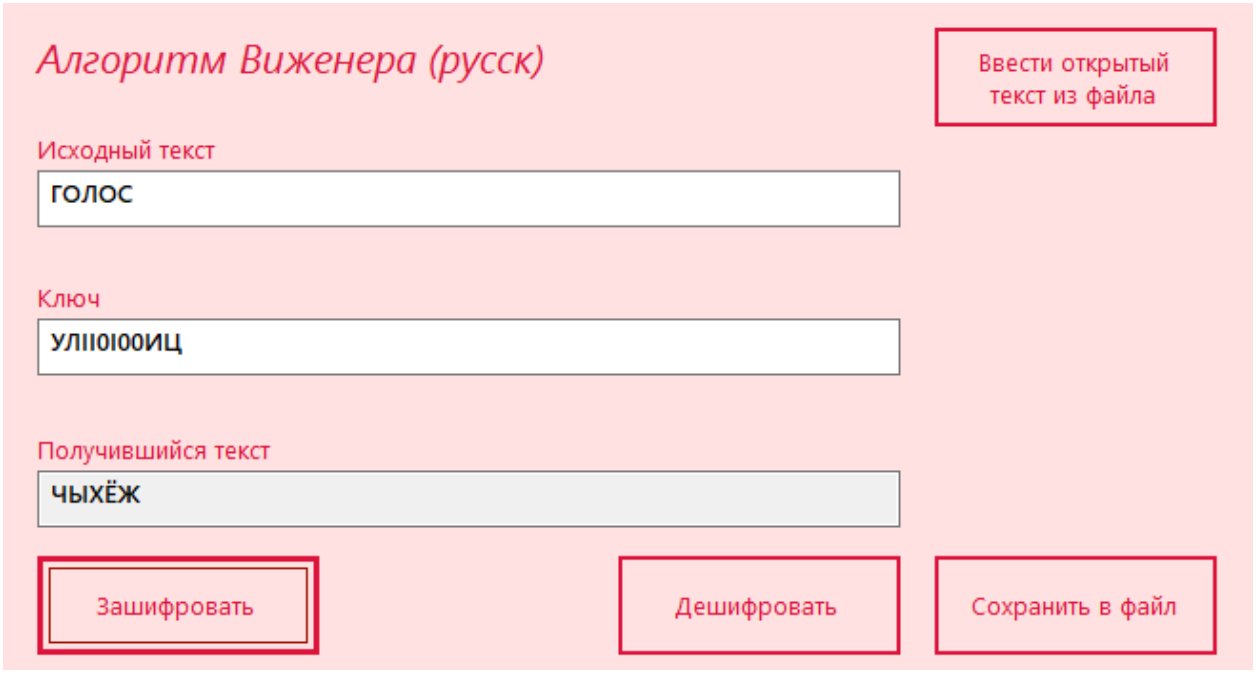


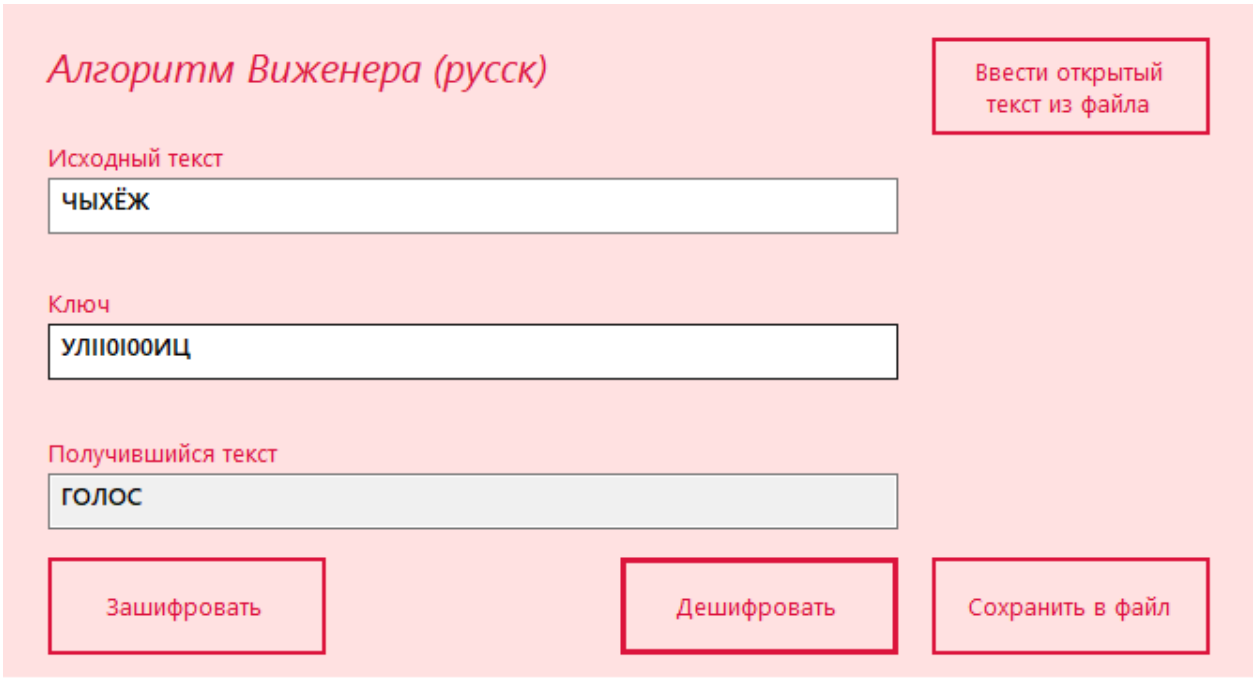


Ш	Ё	П	О	Т
М	И	Л	Н	Й
Ё	П	Ь	Э	Э

Шифротекст: **ЁПЬЭЭ**

3.

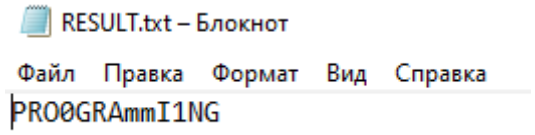


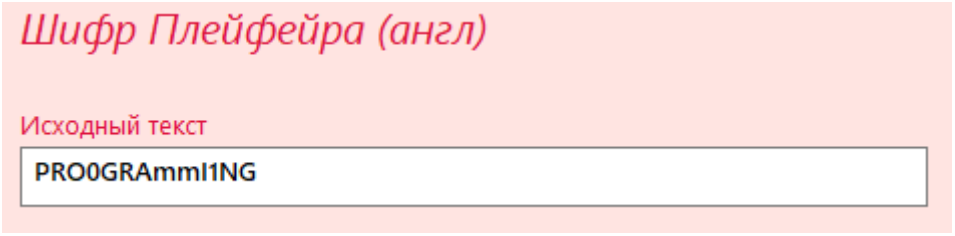


Г	О	Л	О	С
У	Л	И	Ц	Ф
Ч	Ы	Х	Ё	Ж

Шифротекст: **ЧЫХЁЖ**

Ввод из файла реализован кнопкой “Ввести открытый текст из файла”:





Сохранение результата в файл реализовано кнопкой “Сохранить в файл”: