

Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

Лабораторная работа №1 по дисциплине
«Информационные сети. Основы безопасности»

Выполнил:

студент группы 753502

Василюк В.И.

Проверил:

Протьюко М.И.

Введение

В данной лабораторной работе необходимо реализовать программные средства шифрования и дешифрования текстовых файлов при помощи Шифра Цезаря, (шифра сдвига, кода Цезаря) и шифра Виженера.

1. Шифр Цезаря

Шифр Цезаря – один из наиболее простых и широко известных алгоритмов шифрования текстовых данных. Этот метод назван в честь римского полководца Гая Юлия Цезаря, который применял шифр для личной переписки с подчиненными.

Алгоритм шифрования Цезаря заключается в замене каждого символа входящего сообщения на символ, который находится на некотором константном расстоянии с правой или левой стороны. Расстояние при этом называют – *ключом*.

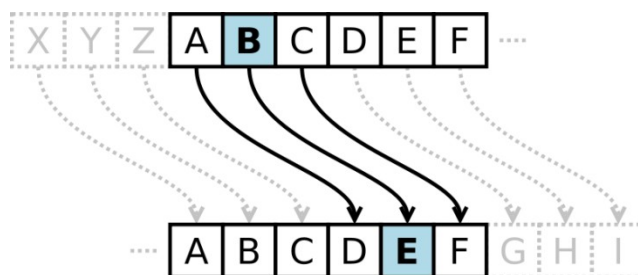


Рис.1(шифр Цезаря)

Например для ключа 5 получаем последовательность:

- Русский алфавит:
 - 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
- Шифр:
 - 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

То есть А заменяем на Е, Б на Ё, и т. д.

Математически шифр Цезаря можно описать следующими формулами:

- $Encrypt(m_n) = (Q + m_n + k) \% Q;$

- $Decrypt(c_n) = (Q + c_n - k) \% Q$.

где m - открытый текст, k - ключ шифрования, Q - количество символов в алфавите, c - зашифрованный текст.

2. Шифр Виженера

Шифр Виженера – алгоритм шифрования текстовых данных с помощью ключевого слова. Шифрование Виженера можно представить как несколько шифров Цезаря с различными ключами. Проще всего шифры представить в виде таблицы, для английского алфавита мы получим 26 строк шифра Цезаря, в каждой строке сдвиг на единицу больше предыдущей:

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

Математически шифр Виженера можно описать следующими формулами:

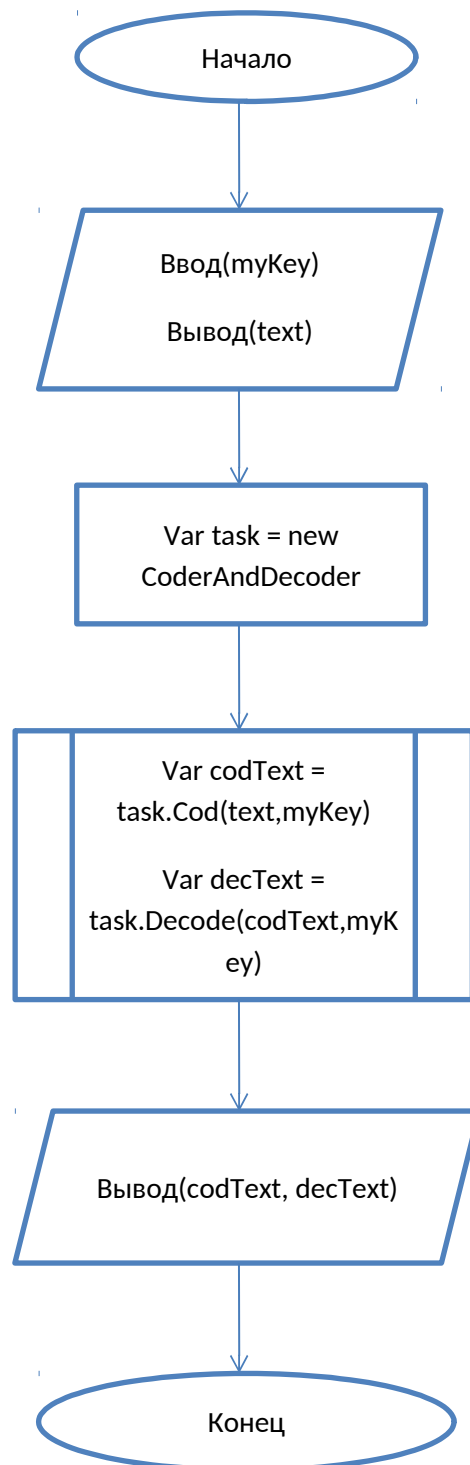
- $Encrypt(m_n) = (Q + m_n + k_n) \% Q$;
- $Decrypt(c_n) = (Q + c_n - k_n) \% Q$.

где t_n - позиция символа открытого текста, k_n - позиция символа ключа шифрования, Q - количество символов в алфавите, c_n - позиция символа зашифрованного текста.

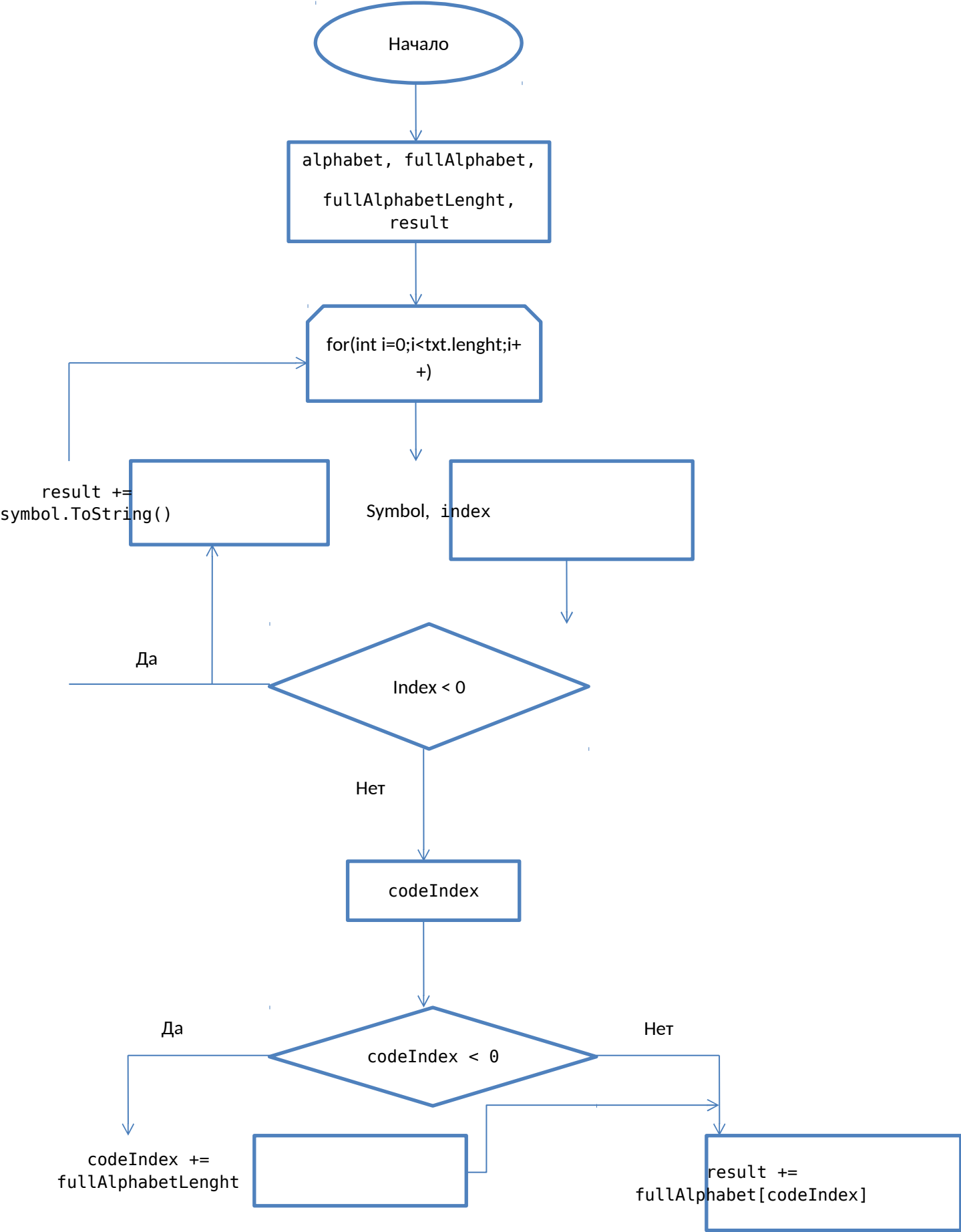
Блок-схема

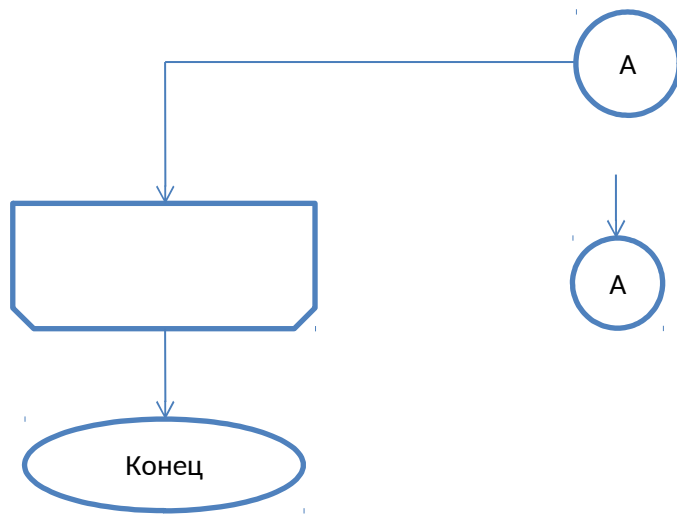
1. Шифр Цезаря

Program.cs:



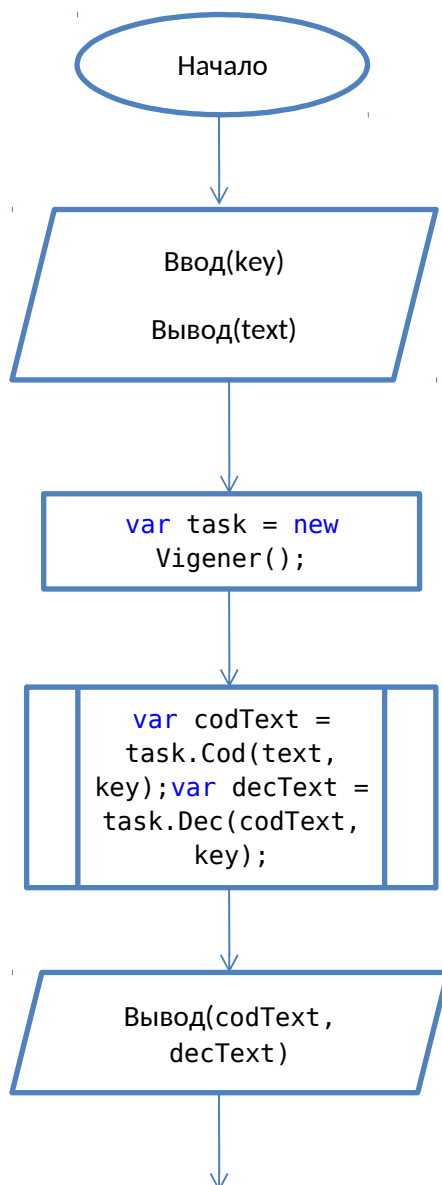
CoderAndDecoder.cs:



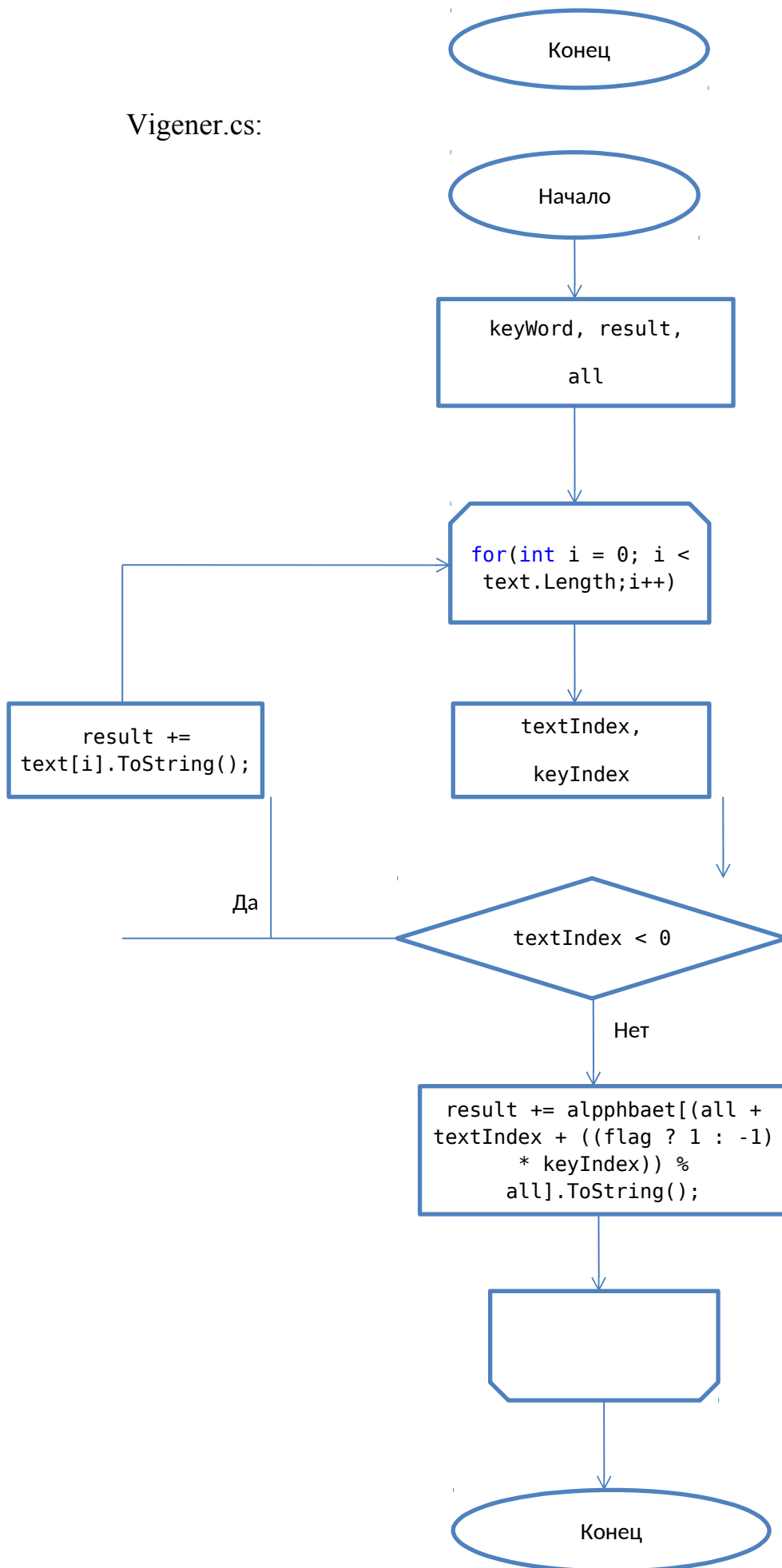


2. Шифр Виженера

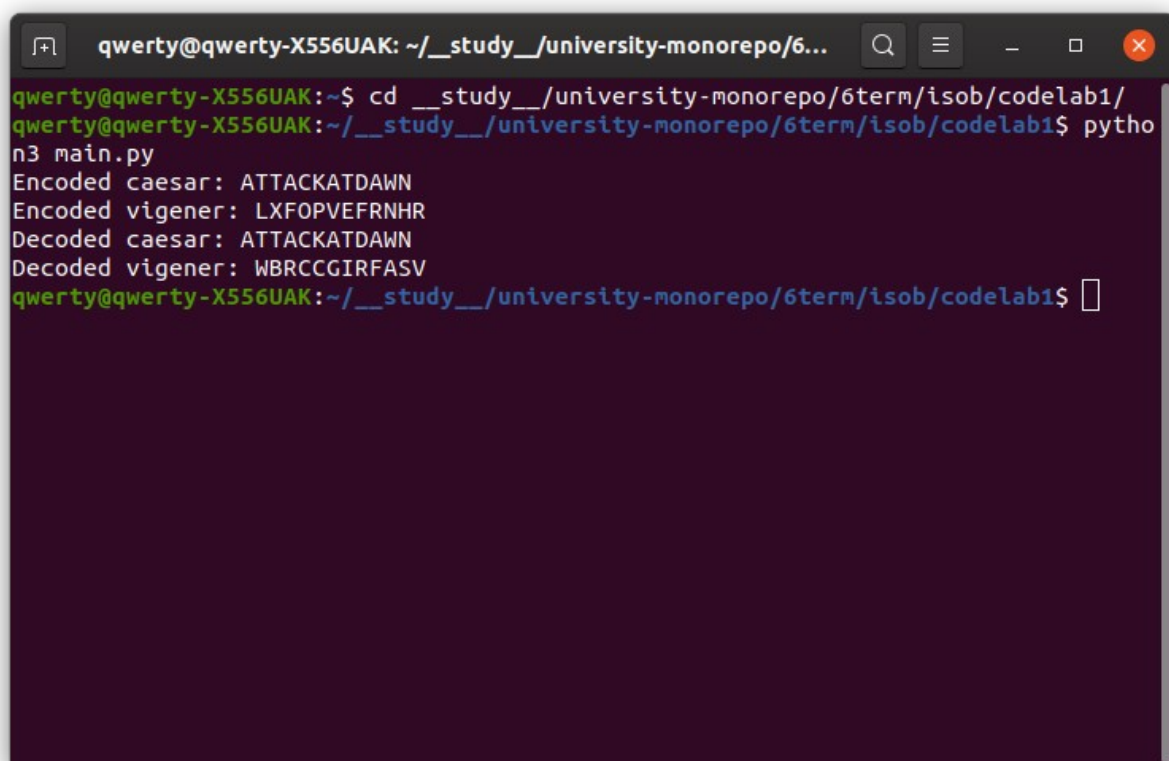
Main.cs:



Vigener.cs:



Демонстрация работы программы

A terminal window with a dark purple background and white text. The window title bar shows the user 'qwerty' on a machine named 'qwerty-X556UAK' at the directory '~/__study__/university-monorepo/6...'. The terminal content shows a sequence of commands and their outputs: a 'cd' command to change to a specific directory, followed by a 'python3 main.py' command. The program outputs four lines: 'Encoded caesar: ATTACKATDAWN', 'Encoded vigenere: LXFOPVEFRNHR', 'Decoded caesar: ATTACKATDAWN', and 'Decoded vigenere: WBRCCGIRFASV'. The prompt returns to the shell.

```
qwerty@qwerty-X556UAK: ~/__study__/university-monorepo/6...  
qwerty@qwerty-X556UAK:~$ cd __study__/university-monorepo/6term/isob/codelab1/  
qwerty@qwerty-X556UAK:~/__study__/university-monorepo/6term/isob/codelab1$ python3 main.py  
Encoded caesar: ATTACKATDAWN  
Encoded vigenere: LXFOPVEFRNHR  
Decoded caesar: ATTACKATDAWN  
Decoded vigenere: WBRCCGIRFASV  
qwerty@qwerty-X556UAK:~/__study__/university-monorepo/6term/isob/codelab1$
```

Программный код

main.py:

```
from caesar import Caesar
from vigenere import Vigenere

if __name__ == "__main__":
    text = "ATTACKATDAWN"
    key_caesar = 3
    key_vigenere = "LEMON"
    encoded_caesar = Caesar.code(text, key_caesar)
    encoded_vigenere = Vigenere.code(text, key_vigenere)
    print("Encoded caesar:", encoded_caesar)
    print("Encoded vigenere:", encoded_vigenere)
    print("Decoded caesar:", Caesar.code(encoded_caesar,
key_caesar))
    print("Decoded vigenere:", Vigenere.code(encoded_vigenere,
key_vigenere))
```

caesar.py:

```
class Caesar:
    @staticmethod
    def code_and_dec(text, key):
        alphabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"
        result = ""
        for char in text:
            index = alphabet.find(char.upper())
            if index < 0:
                result += char
            else:
                code_index = (index + key) % len(alphabet)
                if code_index < 0:
                    code_index += len(alphabet)
                if char.islower():
                    result += result[code_index].lower()
                else:
```

```

        result += alphabet[code_index]
    return result

    @staticmethod
    def code(text, key):
        return Caesar.code_and_dec(text, key)

    @staticmethod
    def decode(text, key):
        return Caesar.code_and_dec(text, -key)

```

vigener.py:

```

class Vigenere:
    @staticmethod
    def get_key(text, length):
        temp = text
        while len(temp) < length:
            temp += text
        return temp[:length]

    @staticmethod
    def code_and_dec(text, key, flag):
        alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
        password = Vigenere.get_key(key, len(text))
        result = ""
        q = len(alphabet)

        index = 0

        for char in text:
            text_index = alphabet.find(char.upper())
            key_index = alphabet.find(password[index].upper())
            if text_index < 0:
                result += char
            else:
                result += alphabet[(q + text_index + flag *
key_index) % q]
            index += 1
        return result

    @staticmethod
    def code(text, key):
        return Vigenere.code_and_dec(text, key, 1)

    @staticmethod
    def decode(text, key):

```

```
return Vigenere.code_and_dec(text, key, -1)
```

Вывод

В ходе данной лабораторной работы я научился шифровать и дешифровывать данные при помощи шифра Цезаря и шифра Виженера. На мой взгляд, оба шифра очень примитивны и не пригодны для использования в повседневной жизни, т.к. могут быть легко дешифрованы.