Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЕТ
к лабораторной работе №2
на тему

ШИФР ЦЕЗАРЯ. ШИФР ВИЖЕНЕРА

Выполнил:
студент гр. 253504
Носкович П.Н.

Проверил:
Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Шифр – система обратимых преобразований, зависящая от некоторого секретного параметра (ключа) и предназначенная для обеспечения секретности передаваемой информации.

Цель данной лабораторной работы заключается в изучении теоретических сведений по работе Шифра Цезаря и Шифра Виженера и разработки программы, шифрующей и дешифрующей информацию с помощью данных шифров.

1 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря – один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря – это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 4 А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

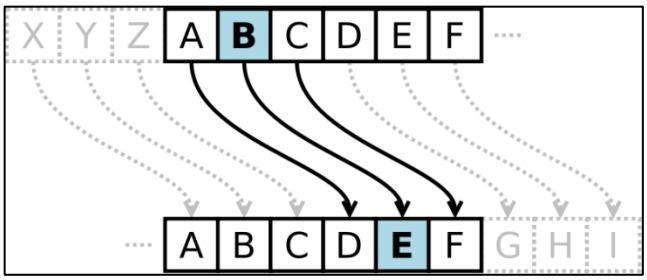

Рисунок 1 – Шифр Цезаря

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики: $y = (x + k) \mod n$, $x = (y - k + n) \mod n$,

где x – символ открытого текста, y – символ шифрованного текста, n – мощность алфавита, а k – ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая *tabula recta* или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет такой вид: *ATTACKATDAWN*

Человек, посылающий сообщение, записывает ключевое слово («*LEMON*») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста: *LEMONLEMONLE*

Первый символ исходного текста A зашифрован последовательностью *L*, которая является первым символом ключа. Первый символ *L* шифрованного текста находится на пересечении строки *L* и столбца *A* в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста *X* получается на пересечении строки *E* и столбца *T*. Остальная часть исходного текста шифруется подобным способом.

Исходный текст: *ATTACKATDAWN*; Ключ: *LEMONLEMONLE*; Зашифрованный текст: *LXFOPVEFRNHR*.

	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

Рисунок 2 – Квадрат Виженера

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если — количество букв в алфавите, — буквы открытого текста, — буквы ключа, то шифрование Виженера можно записать следующим образом:

И расшифровывание:

В компьютере такая операция соответствует сложению кодов *ASCII* символов сообщения и ключа по некоторому модулю. Кажется, что если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Это действительно так, если ее менять чаще, например, от слова, к слову. Но составление таких таблиц, представляющих собой латинские квадраты.

2 РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ ПРОГРАММЫ

В результате разработки программы было создано консольное приложение, осуществляющее шифровку и дешифровку информации из файлов по заданным ключам.

На рисунке 2.1 представлена блок-схема алгоритма для работы с шифром Цезаря.

На рисунке 2.2 представлена блок-схема алгоритма для работы с шифром Виженера.

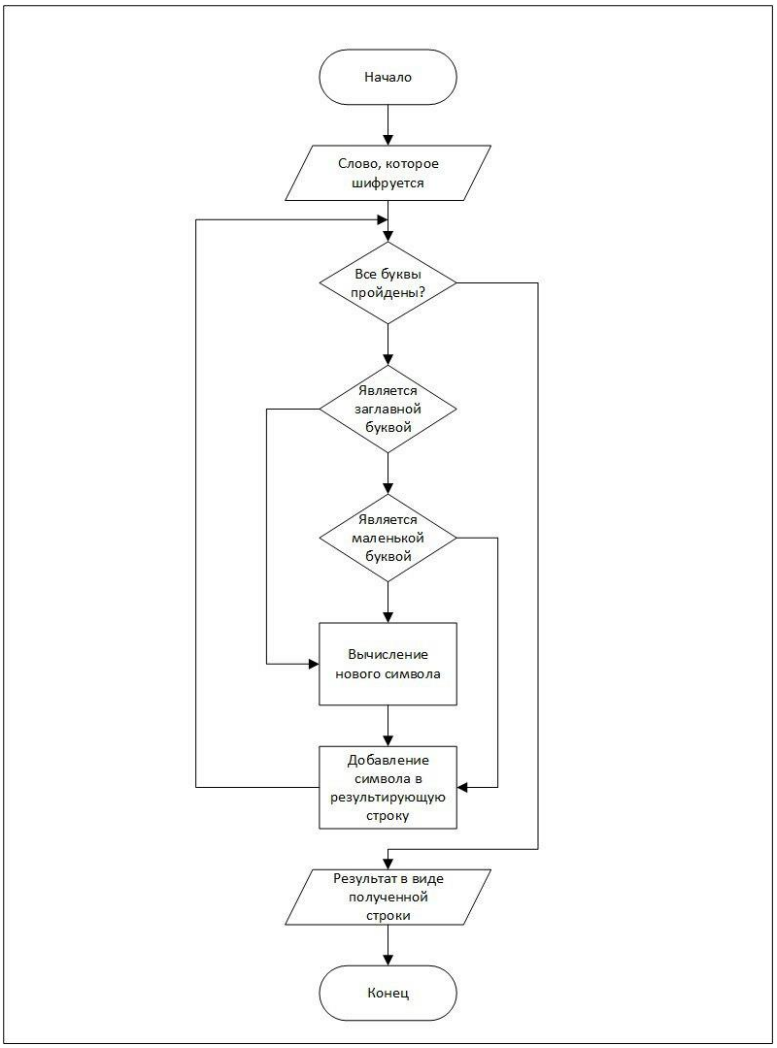

Рисунок 2.1 – Блок-схема алгоритма для работы с шифром Цезаря

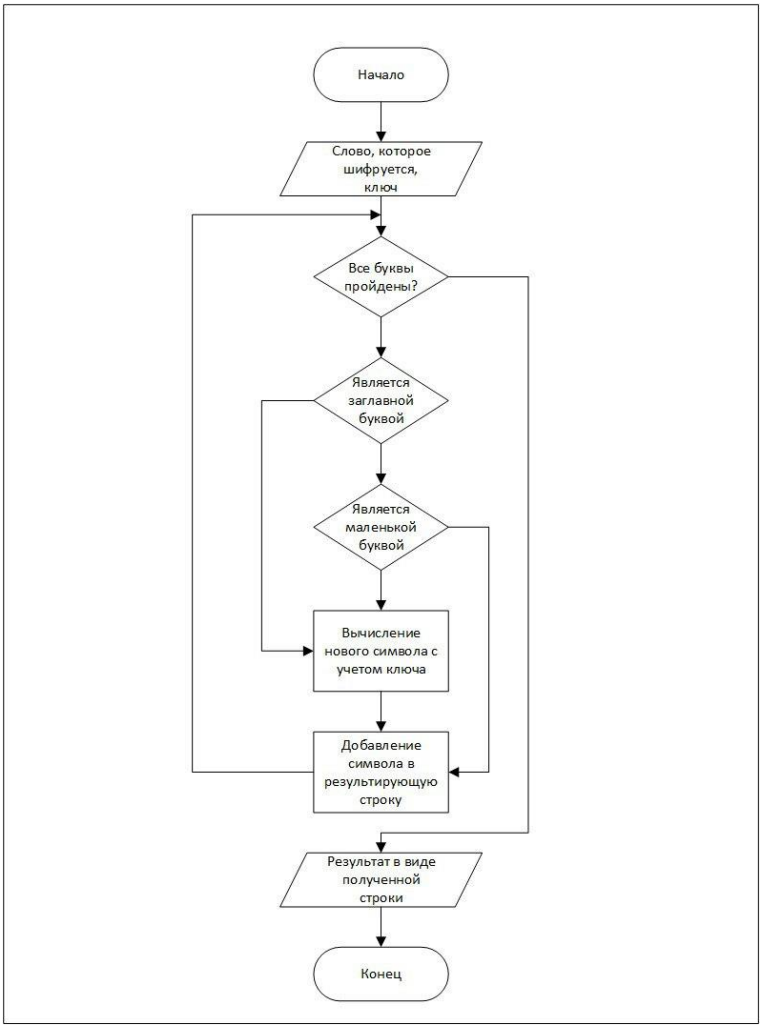

Рисунок 2.2 – Блок-схема алгоритма для работы с шифром Виженера

Результат выполнения программы изображён на рисунке 2.3.

```
Введите текст для обработки: polina полина
Выберите действие (1 - Зашифровать, 2 - Расшифровать): 1
Выберите метод шифрования (1 - Цезарь, 2 - Виженер): 1
Введите ключ для шифра Цезаря (целое число): 22

Зашифрованный текст:   lkhejw едбюгц

PS D:\6 сем\ИСОБ\lab2> python main.py
Введите текст для обработки: lkhejw едбюгц
Выберите действие (1 - Зашифровать, 2 - Расшифровать): 2
Выберите метод расшифрования (1 - Цезарь, 2 - Виженер): 1
Введите ключ для шифра Цезаря (целое число): 22

Расшифрованный текст:   polina полина
```

Рисунок 2.3 – Результат программы

ПРИЛОЖЕНИЕ А
(обязательное)
Исходный код программы

main.py

```
def caesar_cipher(text, shift, encrypt=True):
    result = ''
    for char in text:
        if char.isalpha():
            if 'а' <= char <= 'я' or 'А' <= char <= 'Я':
                start = ord('а') if char.islower() else ord('А')
                alphabet_size = 32
            else:
                start = ord('a') if char.islower() else ord('A')
                alphabet_size = 26

            shifted_char = chr((ord(char) - start + (shift if encrypt else -
shift)) % alphabet_size + start)
        elif char.isdigit():
            shifted_char = str((int(char) + (shift if encrypt else -shift)) %
10)
        else:
            shifted_char = char  # Не изменяем пробелы и знаки препинания
        result += shifted_char
    return result

def vigenere_cipher(text, key, encrypt=True):
    result = ''
    key_len = len(key)
    key_index = 0

    for char in text:
        if char.isalpha():
            if 'а' <= char <= 'я' or 'А' <= char <= 'Я':
                start = ord('а') if char.islower() else ord('А')
                alphabet_size = 32
            else:
                start = ord('a') if char.islower() else ord('A')
                alphabet_size = 26
            key_char = key[key_index % key_len].lower()
            if 'а' <= key_char <= 'я':
                shift = ord(key_char) - ord('а')
            else:
                shift = ord(key_char) - ord('a')

            # Для расшифровки мы используем отрицательный сдвиг
            shifted_char = chr((ord(char) - start - (shift if encrypt else -
shift)) % alphabet_size + start)
            key_index += 1
        else:
            shifted_char = char  # Не изменяем пробелы и знаки препинания
        result += shifted_char
    return result

def get_valid_choice(prompt, valid_choices):
    while True:
        choice = input(prompt)
        if choice in valid_choices:
            return choice
        else:
            print(f"Ошибка! Введите одно из значений: {',
'.join(valid_choices)}")
```

```
def get_valid_int_input(prompt):
    while True:
        try:
            value = int(input(prompt))
            return value
        except ValueError:
            print("Ошибка! Пожалуйста, введите целое число.")

def get_valid_string_input(prompt):
    while True:
        value = input(prompt).strip()
        if value:  # Убедимся, что строка не пустая
            return value
        else:
            print("Ошибка! Пожалуйста, введите не пустую строку.")

def main():
    input_text = get_valid_string_input("Введите текст для обработки: ")

    action_choice = get_valid_choice("Выберите действие (1 - Зашифровать, 2 -
Расшифровать): ", ["1", "2"])

    if action_choice == "1":
        cipher_choice = get_valid_choice("Выберите метод шифрования (1 -
Цезарь, 2 - Виженер): ", ["1", "2"])

        if cipher_choice == "1":
            key = get_valid_int_input("Введите ключ для шифра Цезаря (целое
число): ")
            ciphered_text = caesar_cipher(input_text, key)
            print("\nЗашифрованный текст:   " + ciphered_text + '\n')
        elif cipher_choice == "2":
            key = get_valid_string_input("Введите ключ для шифра Виженера
(строка): ")
            ciphered_text = vigenere_cipher(input_text, key)
            print("\nЗашифрованный текст:   " + ciphered_text + '\n')

    elif action_choice == "2":
        cipher_choice = get_valid_choice("Выберите метод расшифрования (1 -
Цезарь, 2 - Виженер): ", ["1", "2"])

        if cipher_choice == "1":
            key = get_valid_int_input("Введите ключ для шифра Цезаря (целое
число): ")
            deciphered_text = caesar_cipher(input_text, key, encrypt=False)
            print("\nРасшифрованный текст:   " + deciphered_text + '\n')
        elif cipher_choice == "2":
            key = get_valid_string_input("Введите ключ для шифра Виженера
(строка): ")
            deciphered_text = vigenere_cipher(input_text, key, encrypt=False)
            print("\nРасшифрованный текст:   " + deciphered_text + '\n')

if __name__ == "__main__":
    main()
```