Отчёт по лабораторной работе 1

МОЗИиИБ

Папикян Гагик Тигранович

Содержание

[1 Цель работы 1](#_Toc87895840)

[2 Задание 1](#_Toc87895841)

[3 Теоретическое введение 1](#_Toc87895842)

[3.1 Принцип работы симметричных алгоритмов 1](#_Toc87895843)

[3.2 Шифр Цезаря 2](#_Toc87895844)

[3.3 Шифр Атба́ш 2](#_Toc87895845)

[4 Выполнение лабораторной работы 2](#_Toc87895846)

[5 Выводы 4](#_Toc87895847)

# 1 Цель работы

Познакомиться с простейшими алгоритмами шифрования данных, посредством реализации шифра Цезаря и Атбаш

# 2 Задание

1. Реализовать шифр Цезаря с ключом К
2. Реализовать шифр Атбаш

# 3 Теоретическое введение

## 3.1 Принцип работы симметричных алгоритмов

В целом симметричным считается любой шифр, использующий один и тот же секретный ключ для шифрования и расшифровки.

Например, если алгоритм предполагает замену букв числами, то и у отправителя сообщения, и у его получателя должна быть одна и та же таблица соответствия букв и чисел: первый с ее помощью шифрует сообщения, а второй — расшифровывает.

Однако такие простейшие шифры легко взломать — например, зная частотность разных букв в языке, можно соотносить самые часто встречающиеся буквы с самыми многочисленными числами или символами в коде, пока не удастся получить осмысленные слова. С использованием компьютерных технологий такая задача стала занимать настолько мало времени, что использование подобных алгоритмов утратило всякий смысл.

## 3.2 Шифр Цезаря

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 вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского полководца 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, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

## 3.3 Шифр Атба́ш

Атба́ш — простой шифр подстановки для алфавитного письма. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n-i+1, где n — число букв в алфавите. Ниже даны примеры для английского, русского и еврейского алфавитов:

# 4 Выполнение лабораторной работы

Был написан следующий скрипт на javascript

//Caesar Cipher  
//UTF  
//[a-z] 97-122  
//[A-Z] 65-90  
const alphabet = "! abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"  
  
function CaesarEncode( msg, k = 1){  
 let res = ''  
 for(let char of msg){  
 let code = alphabet.indexOf(char)  
 res += alphabet[ (code+k)%alphabet.length ]  
 }  
 return res  
}  
  
function CaesarDecode( msg, k = 1){  
 let res = ''  
 for(let char of msg){  
 let code = [...alphabet].reverse().indexOf(char)  
 res += [...alphabet].reverse()[ (code+k)%alphabet.length ]  
 }  
 return res  
}  
  
//Atbash Cipher  
function AtbashEncodeDecode( msg ){  
 let res = ''  
 for(let char of msg){  
 let code = alphabet.indexOf(char)  
 res += [...alphabet].reverse()[ code ]  
 }  
 return res  
}  
  
const k = 55  
const text = 'Hey There!'  
console.log(`  
Caesar Cipher:  
text=${text}  
k=${k}  
encoded=${CaesarEncode( text, k )}  
decoded=${ CaesarDecode( CaesarEncode( text, k ), k)}  
  
Atbash Cipher:  
text=${text}  
encoded=${AtbashEncodeDecode( text )}  
decoded=${ AtbashEncodeDecode( AtbashEncodeDecode( text ))}  
  
`)

Результат исполнения скрипта приведен на рисунке 1 (рис. 1)

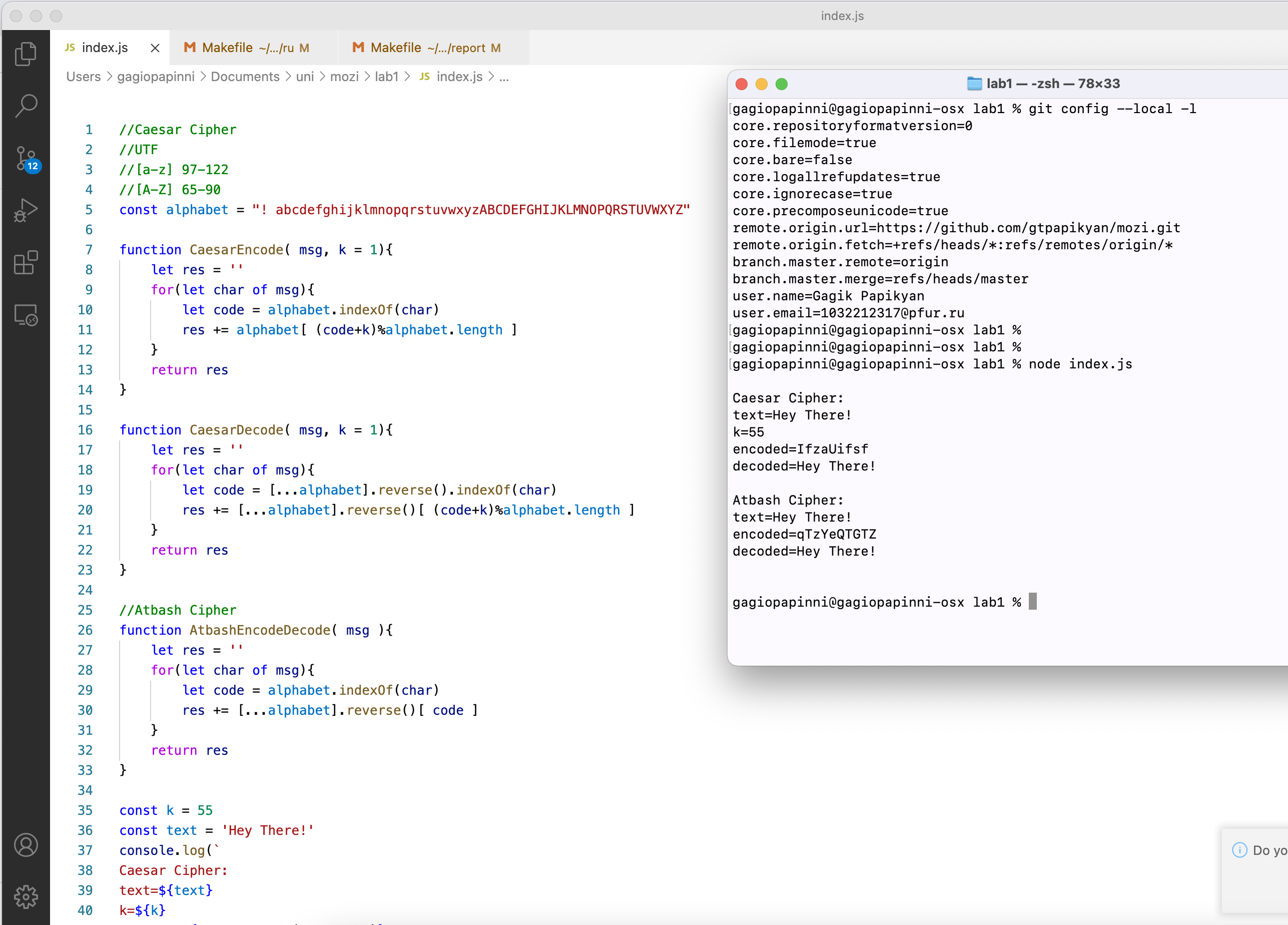


Figure 1: Выполнение лабораторной работы

# 5 Выводы

Был реализован Шифр Цезаря с произвольным ключом и Шифр Атбаша Был использован фиксированный алфавит, состоящий из символов “! abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ”

На рисунке 4.1 в окне терминала было показано, как текст “Hey There!” зашифровывается и расшифровывается сначала алгоритмом Цезаря, потом Атбаш