Отчёт по лабораторной работе 3

МОЗИиИБ

Папикян Гагик Тигранович

Содержание

[1 Цель работы 1](#_Toc88923289)

[2 Задание 1](#_Toc88923290)

[3 Теоретическое введение 1](#_Toc88923291)

[3.1 Шифрование гаммированием 1](#_Toc88923292)

[3.2 Шифрование конечной гаммой 2](#_Toc88923293)

[4 Выполнение лабораторной работы 2](#_Toc88923294)

[5 Выводы 3](#_Toc88923295)

# 1 Цель работы

Познакомиться с принципом шифрования через гаммирование, посредством реализации алгоритма шифрования с конечной гаммой

# 2 Задание

1. Реализовать алгоритм шифрования конечной гаммой

# 3 Теоретическое введение

## 3.1 Шифрование гаммированием

Гамми́рование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле.

## 3.2 Шифрование конечной гаммой

Шифрование конечной гаммой использует определеный ключ маленькой длины, и циклическим его повторением получает гамму, равную по длине входному сообщению

# 4 Выполнение лабораторной работы

Был написан следующий скрипт на javascript

const alphabet = 'qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM !'  
const reversedAlphabet = alphabet.split('').reverse().join('')  
  
function gammaCipher(msg, gamma, decode = false){  
 const swappedAlphabet = decode ? reversedAlphabet : alphabet  
 const fullGamma = gamma.repeat(Math.ceil(msg.length / gamma.length))  
  
 const msgCodes = msg.split('').map(char=>swappedAlphabet.indexOf(char))  
 const fullGammaCodes = fullGamma.split('').map(char=>alphabet.indexOf(char))  
  
 const resCodes = msgCodes.map((msgCode, idx)   
 => (msgCode+fullGammaCodes[idx])%alphabet.length)  
 const res = resCodes.map( code=>swappedAlphabet[code] ).join('')  
  
 return res  
}  
  
const key = 'pass'  
const msg = 'hello there!'  
const encoded = gammaCipher(msg, key)   
const decoded = gammaCipher(encoded, key, true)  
  
console.log( `  
key = ${key}, msg = ${msg},   
encoded = ${encoded}  
decoded = ${decoded}  
` )

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

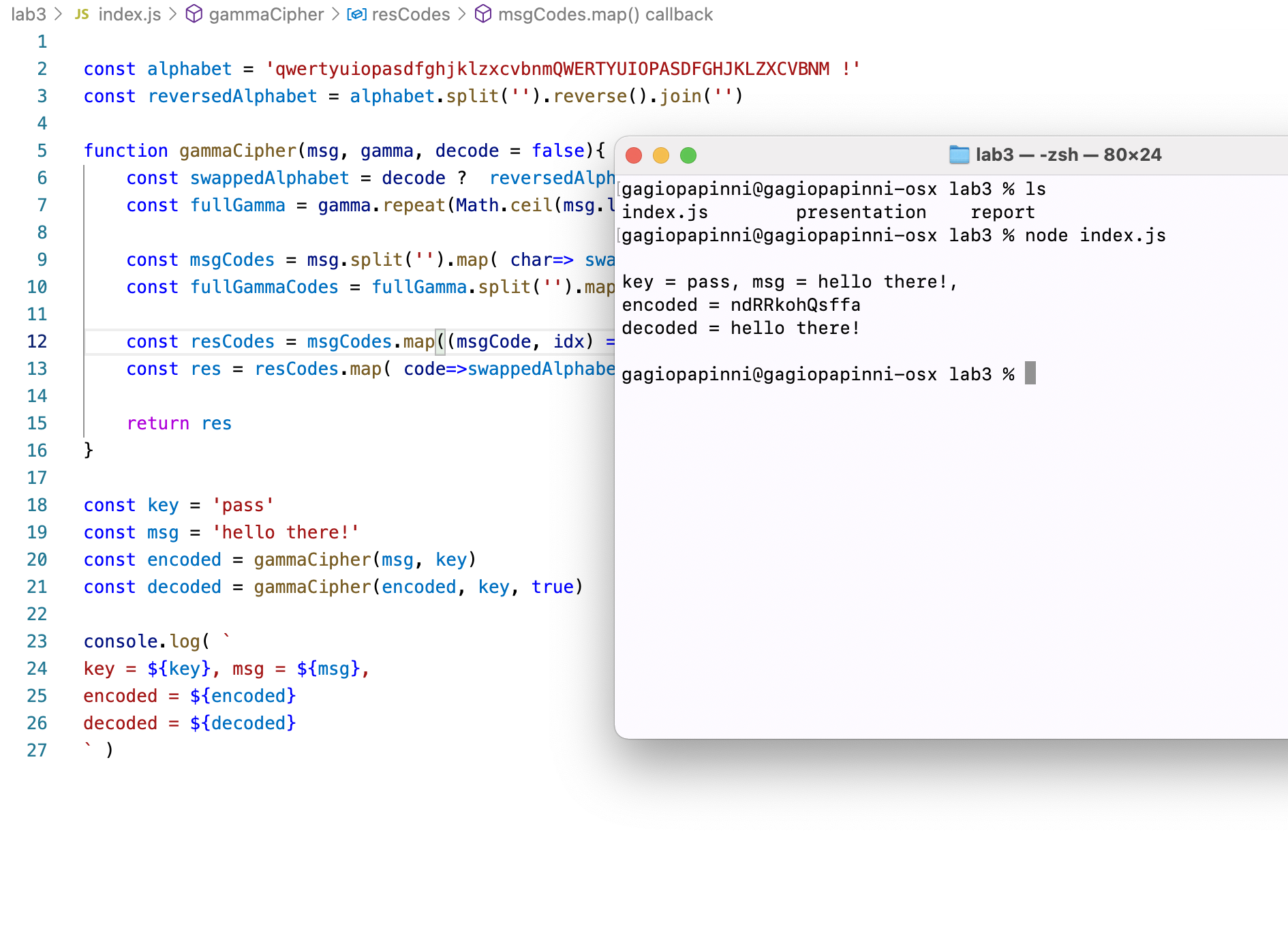


Figure 1: Выполнение лабораторной работы

# 5 Выводы

Был реализован алгоритм шифрования конечной гаммой  
Был использован фиксированный алфавит, состоящий из символов  
“qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM !”

На рисунке 4.1 в окне терминала было показано, как текст “hello there!” зашифровывается и расшифровывается реализованным алгоритмом