Отчёт по лабораторной работе 2

МОЗИиИБ

Папикян Гагик Тигранович

Содержание

[1 Цель работы 1](#_Toc88336993)

[2 Задание 1](#_Toc88336994)

[3 Теоретическое введение 1](#_Toc88336995)

[3.1 Шифры перестановки 1](#_Toc88336996)

[3.2 Шифр вертикальной перестановки 2](#_Toc88336997)

[3.3 Шифр «поворотная решётка» 2](#_Toc88336998)

[3.4 Шифр двойной перестановки 3](#_Toc88336999)

[4 Выполнение лабораторной работы 3](#_Toc88337000)

[5 Выводы 4](#_Toc88337001)

# 1 Цель работы

Познакомиться с простейшими алгоритмами шифрования данных, посредством реализации алгоритмов шифрования на основе перестановок

# 2 Задание

1. Реализовать Маршрутное шифрование
2. Реализовать шифрование с помощю решеток
3. Реализовать шифрование на основе таблицы Виженера

# 3 Теоретическое введение

## 3.1 Шифры перестановки

Шифр перестано́вки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы. В классической криптографии шифры перестановки можно разделить на два класса:

Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз. Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз. В качестве альтернативы шифрам перестановки можно рассматривать подстановочные шифры. В них элементы текста не меняют свою последовательность, а изменяются сами.

## 3.2 Шифр вертикальной перестановки

Широкое распространение получила разновидность маршрутной перестановки — вертикальная перестановка. В этом шифре также используется прямоугольная таблица, в которую сообщение записывается по строкам слева направо. Выписывается шифрограмма по вертикалям, при этом столбцы выбираются в порядке, определяемом ключом.

## 3.3 Шифр «поворотная решётка»

Решётка Кардано В 1550 году итальянский математик Джероламо Кардано (1501—1576) в книге «О тонкостях» предложил новую технику шифрования сообщений — решётку.

Изначально решётка Кардано представляла собой трафарет с отверстиями, в которые записывали буквы, слоги или слова сообщения. Затем трафарет убирали, а свободное место заполняли более или менее осмысленным текстом. Такой метод сокрытия информации относится к стеганографии.

Позднее был предложен шифр «поворотная решётка» — первый транспозиционный (геометрический) шифр. Несмотря на то, что существует большая разница между изначальным предложением Кардано и шифром «поворотная решётка», методы шифрования, основанные на трафаретах, принято называть «решётками Кардано».

Четыре позиции решётки Для шифрования и дешифрования с помощью данного шифра изготовляется трафарет с вырезанными ячейками. При наложении трафарета на таблицу того же размера четырьмя возможными способами, его вырезы полностью должны покрывать все клетки таблицы ровно по одному разу.

При шифровании трафарет накладывают на таблицу. В видимые ячейки по определённому маршруту вписывают буквы открытого текста. Далее трафарет переворачивают три раза, каждый раз проделывая операцию заполнения.

Шифрограмму выписывают из получившейся таблицы по определённому маршруту. Ключом являются трафарет, маршрут вписывания и порядок поворотов.

Данный метод шифрования использовался для передачи секретной информации нидерландскими правителями в 1740-х годах. Во время Первой мировой войны армия кайзера Вильгельма использовала шифр «поворотная решётка». Немцы использовали решётки разных размеров, однако очень недолго (четыре месяца), к огромному разочарованию французских криптоаналитиков, которые только-только начали подбирать к ним ключи. Для решёток разных размеров французы придумали собственные кодовые имена: Анна (25 букв), Берта (36 букв), Дора (64 буквы) и Эмиль (81 буква).

## 3.4 Шифр двойной перестановки

При шифровании шифром двойной перестановки в таблицу по определённому маршруту записывается текст, затем переставляются столбцы и строки. Далее по определённому маршруту выписывается шифрограмма.

Ключом к шифру являются размер таблицы, маршруты вписывания и выписывания, порядки перестановки столбцов и строк. Если маршруты являются фиксированными величинами, то количество ключей равно n!m!, где n и m — количество строк и столбцов в таблице.

# 4 Выполнение лабораторной работы

Был написан следующий скрипт на javascript, который реализует маршрутное шифрование

function pathCipher (msg, key = 'password'){  
 const n = key.length  
 const m = Math.ceil(msg.length / n)  
 const completedMsg = msg + 'a'.repeat( m\*n - msg.length )  
  
 const sortedKey = key.split('').map((char,idx)=>[char,idx])  
 .sort((a,b)=>a[0] > b[0])  
 const getCol = (idx) => {  
 let res = ''  
 for(let i = 0;i<m;i++){  
 res+=completedMsg[idx + i\*n ]  
 }  
 return res  
 }  
  
 let res = ''  
 for(let [\_, idx] of sortedKey){  
 res+=getCol(idx)  
 }  
 return res  
}  
  
console.log(pathCipher('нельзянедооцениватьпротивника', 'пароль')) //еенпнзоатаьовокннеьвлдирияцтиa

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

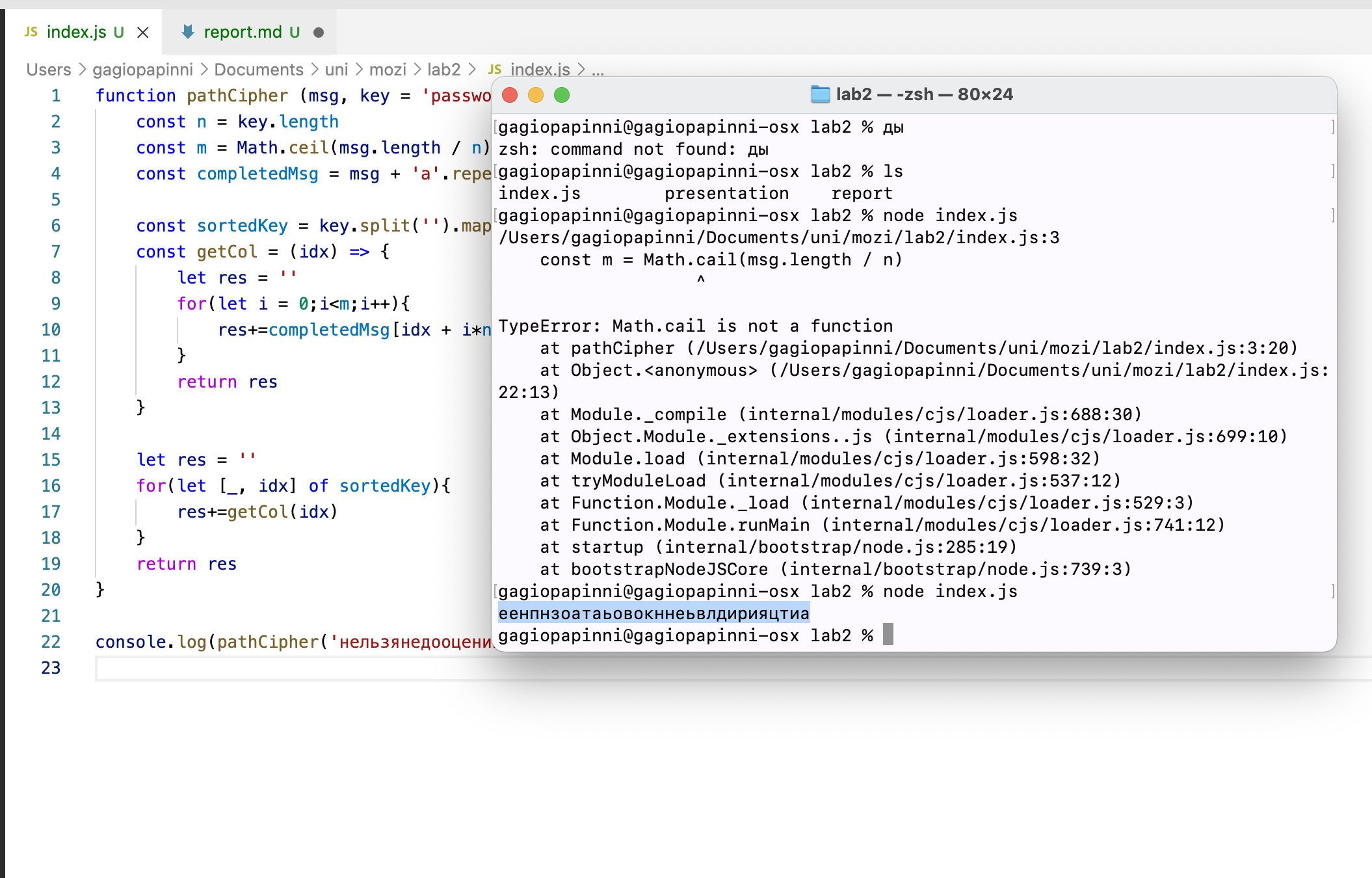


Figure 1: Выполнение лабораторной работы

# 5 Выводы

Был реализован алгоритм саршрутного цифрования с произвольным ключом Было показано на рисунке 4.1, что при входных данных, приведенных в файле лабораторной работы, получаем ожидаемый результат, следовательно алгоритм работает корректно