Лабораторная работа №2

Математические основы защиты информации и информационной безопасности

Данилова Анастасия Сергеевна

Содержание

Цель работы

Изучить шифры перестановки и реализовать их на языке программирования Julia.

Задание

Реализовать шифры перестановки:

- маршрутное шифрование

- шифрование с помощью решеток

- таблица Виженера

Теоретическое введение

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Важным требованием является равенство длин ключа и исходного текста.

Маршрутное шифрование

Маршрутное шифрование — это способ шифрования, изобретённый французским математиком и криптографом Франсуа Виетом.

Суть метода:

1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной произведению m и n.
2. Блок вписывается построчно в таблицу размерности m × n. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ шифра.

Чаще всего буквы выписывают по столбцам, которые упорядочиваются в соответствии с паролем.

Шифрование с помощью решеток

Шифрование с помощью решёток — это способ шифрования, предложенный в 1881 году австрийским криптографом Эдуардом Флейснером.

Процесс шифрования происходит следующим образом:

1. Выбирается натуральное число k > 1, и квадрат размерности k×k построчно заполняется числами 1, 2, …, k.
2. Квадрат поворачивается по часовой стрелке на 90° и размещается вплотную к предыдущему квадрату. Аналогичные действия совершаются ещё два раза, так чтобы в результате из четырёх малых квадратов образовался один большой с длиной стороны 2k.
3. Далее из большого квадрата вырезаются клетки с числами от 1 до k^2, для каждого числа одна клетка.
4. Сделанная решётка (квадрат с прорезями) накладывается на чистый квадрат 2k × 2k, и в прорези по строчкам (то есть слева направо и сверху вниз) вписываются первые буквы открытого текста.
5. Затем решётка поворачивается на 90° по часовой стрелке и накладывается на частично заполненный квадрат, вписывание продолжается.
6. После третьего поворота, наложения и вписывания все клетки квадрата будут заполнены. Правило выбора прорезей гарантирует, что при заполнении квадрата буква на букву никогда не попадёт.
7. Из заполненного квадрата буквы можно выписать по столбцам, выбрав подходящий пароль.

Таблица Виженера

Шифрование с помощью таблицы Виженера основано на том, что каждая буква в исходном шифруемом тексте сдвигается по алфавиту не на фиксированное, а на переменное количество символов. Величина сдвига каждой буквы задаётся ключом (паролем) — секретным словом или фразой, которая используется для шифрования и расшифровки.

Для шифрования используется так называемый «квадрат Виженера» — таблица, где в каждой строке алфавит сдвигается на одну позицию вправо. Например, если взять строку с первой буквой ключа и столбец с первой буквой исходного текста, то на их пересечении будет первая буква зашифрованного сообщения. Затем процедура повторяется для всех остальных пар букв ключа и исходного сообщения по очереди.

Выполнение лабораторной работы

Маршрутное шифрование

```
function route_sh(message, key)
    message = replace(uppercase(message), " " => "")
    rows = ceil(Int, length(message)/length(key))
    cols = length(key)

    matrix = Matrix{Char}(undef, row, cols)
    index = 1
    for j in 1:cols
        for i in 1:rows
            if index <= length(message)
                matrix[i, j] = message[index]
                index += 1
            else
                matrix[i, j] = " "
            end
        end
    end
    indkey = sortperm(collect(key))
    newtext = ""
    for j in indkey
        for i in 1:rows
            newtext *= string(matrix[i, j])
        end
    end

    return newtext
end

print("Введите текст: ")
text = readline()
print("Ключ: ")
key = readline()
```

```
  Activating project at `C:\Users\nastd\.julia\environments\v1.8`
Введите текст: hello world
Ключ: posts
Зашифрованный текст: LLHEOWLDOR
```

Результат

Шифрование с помощью решеток

```julia
function grid_sh(message::AbstractString, key::AbstractString)
    message = uppercase(message)
    key = uppercase(key)
    table_size = ceil(Int, sqrt(length(message)))
    message = message * " "^((table_size * table_size) - length(message))

    key_inds = Dict(char => i for (i, char) in enumerate(key))
    sorted_key = sort(collect(key))

    table = reshape(collect(message), table_size, table_size)

    new_message = ""
    for char in sorted_key
        for j in 1:table_size
            for i in 1:table_size
                if table[i, j] == char
                    new_message *= char
                end
            end
        end
    end

    return new_message
end
print("Введите исходное сообщение: ")
text = readline()
print("Введите ключ: ")
key = readline()
new_message = grid_sh(text, key)
println("зашифрованное: $new_message")
```

```
  Activating project at `C:\Users\nastd\.julia\environments\v1.8`
Введите текст: hello world
Ключ: tables
Зашифрованный текст: ELLL
  Terminal will be reused by tasks, press any key to close it.
```

Результат

Таблица Виженера

```julia
function vigenere(text::AbstractString, key::AbstractString)
    text = replace(uppercase(text), " " => "")
    key = uppercase(key)
    key_length = length(key)
    new_text = Char[]

    for (i, letter) in enumerate(text)
        shift = Int(key[mod1(i, key_length)]) - Int('A') + 1
        n_letter = shift_cipher(letter, shift)
        push!(new_text, n_letter)
    end
    return join(new_text)
end

function shift_cipher(letter::Char, shift::Int)
    if 'A' <= letter <= 'Z'
        encr = Char(((Int(letter) - Int('A') + shift) % 26) + Int('A'))
        return encr
    else
        return letter
    end
end

print("Введите текст: ")
text = readline()
print("Ключ: ")
key = readline()
newtext = vigenere(text, key)
println("Зашифрованный текст: $newtext")
```

```
  Activating project at `C:\Users\nastd\.julia\environments\v1.8`
Введите текст: hello world
Ключ: vignere
Зашифрованный текст: DNSZTOTNUK
  Terminal will be reused by tasks, press any key to close it.
```

Результат

Выводы

Мы изучили 3 шифра перестановки и реализовали их на языке программирования Julia.

Список литературы

1. Mathematics // Julia URL: https://docs.julialang.org/en/v1/base/math/