Отчёт по лабораторной работе №1 Математические основы защиты информации и информационной безопасности

Шифры простой замены

Выполнил: Махорин Иван Сергеевич,
НФИмд-02-21, 1032259380

Содержание

Список иллюстраций

1 Цель работы

Изучить шифры простой замены и научиться их реализовывать.

2 Выполнение лабораторной работы

2.1 Реализация шифра Цезаря с произвольным ключом K

Шифр Цезаря — это древнейший шифр подстановки, в котором каждая буква исходного текста заменяется другой буквой, сдвинутой на фиксированное число позиций в алфавите. Этот метод очень прост: например, при сдвиге на 3, А становится Г, Б — Д и так далее. Для восстановления исходного текста нужно сдвинуть буквы в обратном направлении.

Выполним реализацию этого алгоритма на языке Julia (рис. 2.1):

```julia
# Шифр Цезаря с произвольным ключом K
function caesar_cipher(text::String, k::Int)::String
    # Создание массива символов русского алфавита (без ё)
    alphabet = collect("абвгдежзийклмнопрстуфхцчшщъыьэюя")
    # Инициализация пустой строки для результата
    result = ""

    # Итерация по каждому символу в тексте, приведенному к нижнему регистру
    for char in lowercase(text)
        # Поиск индекса символа в алфавите
        idx = findfirst(isequal(char), alphabet)
        # Если символ найден в алфавите (т.е. это буква)
        if idx !== nothing
            # Вычисление нового индекса с учетом сдвига k и цикличности алфавита
            new_idx = (idx - 1 + k) % length(alphabet) + 1
            # Добавление зашифрованного символа к результату
            result *= string(alphabet[new_idx])
        else
            # Если символ не из алфавита (пробел, знак препинания), добавляем без изменений
            result *= char
        end
    end

    # Возврат полученной зашифрованной строки
    return result
end
```

Рис. 2.1: Реализация шифра цезаря с произвольным ключом K

Проверим работу алгоритма (рис. 2.2):

```julia
# Тестирование шифра Цезаря
println(caesar_cipher("привет", 4))
```

```
уфмжйц
```

Рис. 2.2: Проверка

2.2 Реализация шифра Атбаш

Шифр Атбаш — это простейший шифр замены, в котором буквы алфавита заменяются в обратном порядке: первая буква становится последней, вторая — предпоследней и так далее. Например, A становится Z, B — Y, а C — X. Этот метод изначально применялся для еврейского алфавита, откуда и получил свое название от первых букв «алеф» и «тав»:

Выполним реализацию этого алгоритма на языке Julia (рис. 2.3):

```julia
# Шифр Атбаш
function atbash_cipher(text::String)::String
    # Создание массива символов русского алфавита (без ё)
    alphabet = collect("абвгдежзийклмнопрстуфхцчшщъыьэюя ")
    # Инициализация пустой строки для результата
    result = ""

    # Итерация по каждому символу в тексте в нижнем регистре
    for char in lowercase(text)
        # Поиск индекса символа в алфавите
        idx = findfirst(isequal(char), alphabet)
        # Если символ найден в алфавите (т.е. это буква)
        if idx !== nothing
            # Вычисление индекса симметричного символа (от конца алфавита)
            result *= string(alphabet[end - idx + 1])
        else
            # Если символ не из алфавита, добавляем без изменений
            result *= char
        end
    end

    # Возврат результата
    return result
end
```

Рис. 2.3: Реализация шифра Атбаш

Проверим работу алгоритма (рис. 2.4):

```
# Тестирование шифра Атбаш
println(atbash_cipher("привет"))
```

```
сршюыо
```

Рис. 2.4: Проверка

3 Список литературы. Библиография

[1] Julia: https://docs.julialang.org/en/v1/