Защита лабораторной работы №3

Шифрование гаммированием

Бармина Ольга

10 Октября 2024

Российский университет дружбы народов, Москва, Россия

Цель выполнения лабораторной работы

- Освоение шифрования гаммированием
- Программная реализация алгоритма ширования гаммированием конечной гаммой

Теоретические сведения

Гаммирование - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, то есть псевдослучайной последовательности (ПСП) с выходом генератора G. Псевдослучайная последовательность по своим статистическим свойствам неотличима от случайной последовательности, но является детерминированной, то есть известен алгоритм ее формирования.

Результат выполнения лабораторной работы

Результат выполнения лабораторной работы

Алгоритм поиска зашифрованного текста на основе принципа формирования шифрования гаммирования:

```
function gen_key(m, pas)
    m = lowercase(replace(m, " " => ""))
    pas = lowercase(replace(pas, " " => ""))
    pas = collect(pas)
    if length(m) == length(pas)
        return pas
    else
        for i in 1:(length(m) - length(pas))
            push!(pas, pas[(i-1) % length(pas) + 1])
        end
    end
    return pas
end
```

Рис. 1: Генерация ключа

Результат выполнения лабораторной работы

Пример шифрования:

```
function gamma(text, pas)
    alphabet = collect("абвгдежзийклмнопрстуфхцчшщъыьэюя")
    pas = gen_key(text, pas)
    text = collect(text)

    res = ""
    for i in 1:length(text)
        c = (Int(text[i]) + Int(pas[i]) - 2 * Int('a') + 2) % 31
        res *= alphabet[c]
    end
    return res
end
```

```
gamma (generic function with 1 method)
```

```
gamma("приказ", "гамма")
```

```
"усхчбл"
```

Рис. 2: Реализация шифрования

Выводы

1. Изучили шифрование гаммированием
2. Реализовали алгоритм шифрования гаммированием конечной гаммой на языке Julia