Лабораторная работа №3

Шифрование гаммированием

Тазаева Анастасия Анатольевна

2025-10-04

Содержание I

1. Информация

2. Введение

3. Программный код

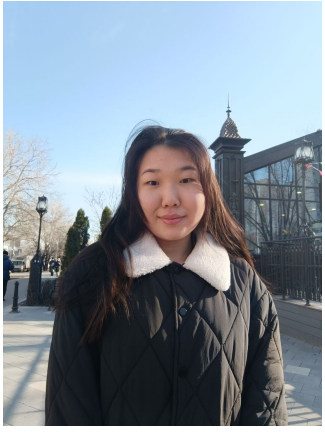
4. Заключение

Раздел 1

1. Информация

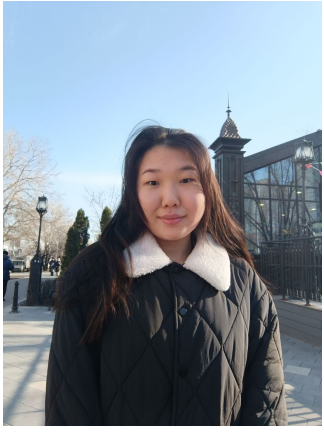
1.1 Докладчик

- Тазаева Анастасия Анатольевна



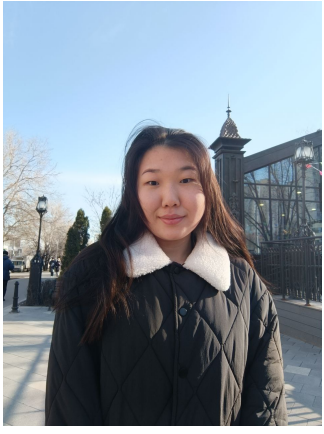
1.1 Докладчик

- Тазаева Анастасия Анатольевна
- студент группы НФИмд-02-25



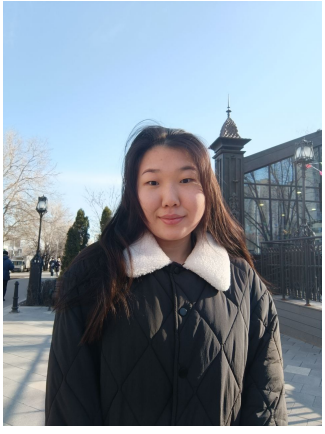
1.1 Докладчик

- Тазаева Анастасия Анатольевна
- студент группы НФИмд-02-25
- Российский университет дружбы народов им. П. Лумумбы



1.1 Докладчик

- Тазаева Анастасия Анатольевна
- студент группы НФИмд-02-25
- Российский университет дружбы народов им. П. Лумумбы
- 1032259385@pfur.ru



Раздел 2

2. Введение

2.1 Цель работы

Ознакомиться с шифрованием гаммированием. Реализовать его.

2.2 Задачи

Реализовать на языке программирования Julia:

1. Шифрование гаммированием.

2.3 Теоретическое введение

Гаммирование - это метод шифрования, при котором символы исходного текста складываются (или иным образом комбинируются) с символами некоторой случайной последовательности, называемой гаммой. *Криптографическая стойкость* данного метода обеспечивается за счёт уникальной, истинно случайной гаммы, длина которой не меньше длины шифруемого сообщения, при этом каждый символ исходного текста преобразуется с помощью соответствующего символа гаммы. Принцип обратимости процесса позволяет восстановить исходный текст путём вычитания той же самой гаммы из зашифрованного сообщения, что делает гаммирование одним из наиболее надежных методов симметричного шифрования при соблюдении всех требований к генерации и использованию гаммы. Основное преимущество метода заключается в том, что при правильном применении (одноразовость гаммы и её истинная случайность) он обеспечивает абсолютную криптостойкость, доказанную математически.

Раздел 3

3. Программный код

3.1 Шифрование гаммированием

```
function gamma_encryption(text, gamma_code)
    # massiv ASCII-kodov kirillicy + simvolov
    alphabet = vcat(1040:1045, 1025, 1046:1071, 32:33, 44, 46
    # println(alphabet)
    # filtryem text, izvestnye simvoly ostautsya
    filtr = filter(x -> findfirst(isequal(Int(only(x))), alph
    #razbivaem text na simvoly
    edited_text = Int.(only.(split(filtr,"")))
    n = length(edited_text)
    #massiv xranit poryadkovyi nomer kajdogo simvola v alfavi
    por_num = [findfirst(isequal(edited_text[i]), alphabet) f
```

3.2 Шифрование гаммированием

```
# propisnye -> zaglavnye
    for i in 1:n
        if por_num[i] > 38
            por_num[i] -= 38
        end
    end
    #rejem na kyso4ki gamma_code, preobrazyija ego v simvolny
    edited_code = [findfirst(isequal(i), alphabet) for i in I
    m = length(edited_code)
    temp = [alphabet[mod(por_num[i]+edited_code[mod(i-1,m)+1]
    result=""
    result*=join(Char.(temp))
    return result
end
```

3.3 Шифрование гаммированием. Результат работы программного кода

```
gamma_encryption("ПРИКАЗ", "ГАММА")
```

```
"УСЦШБЛ"
```

Рисунок 1: Шифрование гаммированием. Пример отработки

Раздел 4

4. Заключение

4.1 Вывод

В ходе лабораторной работы были изучено и реализовано шифрование гаммированием.