

Лабораторная работа №3

Тема: Шифрование гаммированием

Выполнила: Исламова Сания Маратовна

Группа: НПИМд-01-24

Студ.билет: 1132249576

Задача лабораторной работы:

Реализовать алгоритм шифрования гаммированием конечной гаммой

Описание хода выполнения лабораторной работы:

Создаём массив русских букв алфавита для шифрования

```
a = collect("абвгдеёжзийклмнопрстуфхцчщъыьэюя")
```

Бесконечный цикл меню

```
while true
```

Запрос команды и приведение к нижнему регистру

```
print("Ш/Р/В:"); c = lowercase(readline())
```

Выход из программы, если команда "в". Пропуск итерации, если команда не "ш" или "р".

```
c == "в" && break; c in ["ш", "р"] || continue
```

Ввод текста

```
print("Текст:"); t = filter(x -> x in a, collect(lowercase(readline())))
```

Ввод гаммы

```
print("Гамма:"); g = filter(x -> x in a, collect(lowercase(readline())))
```

Проверка, что текст и гамма не пустые

```
length(t) == 0 && length(g) == 0 && (println("Ошибка"); continue)
```

Преобразование текста и гаммы в числовые коды

```
tn = [findfirst(==(x), a) for x in t]
```

```
gn = [findfirst(==(x), a) for x in g]
```

На шифрование/расшифрование циклическое применение гаммы

```
r = [c == "ш" ? (tn[i] + gn[(i-1)%length(gn)+1] - 1) % 33 + 1 : (tn[i] - gn[(i-1)%length(gn)+1] + 32) % 33 + 1 for i in 1:length(tn)]
```

Преобразование числовых кодов обратно в буквы и вывод результата

```
println("Результат: $(join([a[n] for n in r]))")
```

```
end
```

Код реализации алгоритма шифрования гаммированием конечной гаммой выглядит следующим образом:

```
C: > Users > 4eka0 > Downloads > Lab03.jl > ...
1  a = collect("абвгдеёжзийклмнопрстуфхцчшщъыьэюя")
2
3  while true
4
5      print("Ш/Р/В: "); c = lowercase(readline())
6
7      c == "в" && break; c in ["ш", "р"] || continue
8
9      print("Текст: "); t = filter(x -> x in a, collect(lowercase(readline())))
10     print("Гамма: "); g = filter(x -> x in a, collect(lowercase(readline())))
11
12     length(t) == 0 && length(g) == 0 && (println("Ошибка"); continue)
13     tn = [findfirst(==(x), a) for x in t]
14     gn = [findfirst(==(x), a) for x in g]
15     r = [c == "ш" ? (tn[i] + gn[(i-1)%length(gn)+1] - 1) % 33 + 1 :
16           (tn[i] - gn[(i-1)%length(gn)+1] + 32) % 33 + 1 for i in 1:length(tn)]
17
18     println("Результат: $(join([a[n] for n in r]))")
19 end
20
```

Результат работы алгоритма и шифрования слов различными гаммами:

```
ПРОБЛЕМЫ  ВЫХОДНЫЕ ДАННЫЕ  КОНСОЛЬ ОТЛАДКИ  ТЕРМИНАЛ  ПОРТЫ

Ш/Р/В: Ш

Ш/Р/В: Ш
Ш/Р/В: Ш
Текст: Лабораторная работа
Текст: Лабораторная работа
Гамма: мир
Гамма: мир
Результат: щйттьсашвыйрюйттьс
Результат: щйттьсашвыйрюйттьс
Ш/Р/В: Ш
Текст: математическое моделирование
Гамма: криптография
Результат: шсьхапцышыкыццячфпсьдлащьо
Ш/Р/В: 
```