Лабораторная работа №2

Шифры перестановки

Кубасов В.Ю.

Вводная часть

Актуальность

- Шифры перестановки используются до сих пор
- Перестановочные алгоритмы лежат в основе современного шифрования

Цели и задачи

- Ознакомиться с перестановочными и многоалфавитными шифрами
- Реализовать предложенные шифры

Выполнение работы

Маршрутные шифры

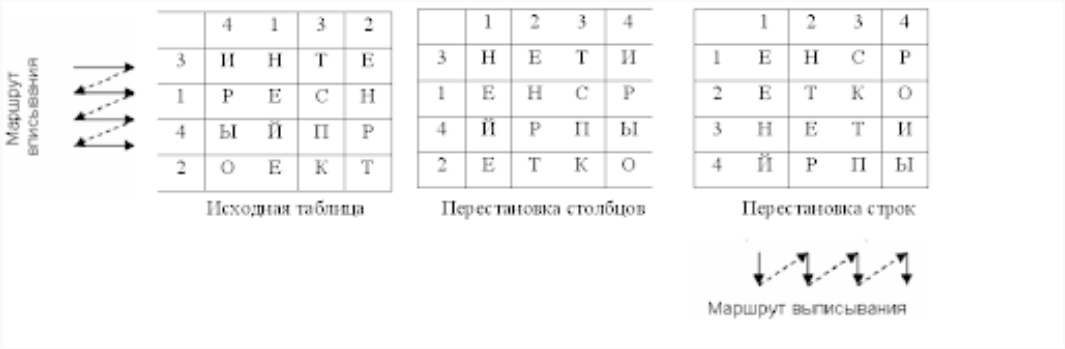

Рис. 1: Маршрутный шифр

Маршрутные шифры

```
println("Введите пароль");
pass = lowercase(readline());
sortedPass = join(sort(collect(pass)));

numberOfColumn = [];
lengthOfPass = length(pass);

for i in 1:2:length(sortedPass) * 2
    push!(numberOfColumn, (Int64)
      ((findfirst(sortedPass[i], pass) - 1) / 2 + 1));
end;
```

Маршрутные шифры

```
println("Строку к шифрованию (без пробелов и других символов кроме кириллицы)
rawString = lowercase(readline());

encodedString = "";

numberOfRaws = ceil(length(rawString) / lengthOfPass);

while length(rawString) < (numberOfRaws * lengthOfPass)
    global rawString *= 'a'; # заглушка для количества символов
end;
```

Маршрутные шифры

```
for i in numberOfColumn
    current = i;
    while (current <= length(rawString))
        global encodedString *= rawString[2 * current - 1];
        current += lengthOfPass;
    end;
end;

println(encodedString);
```

Шифр Виженера

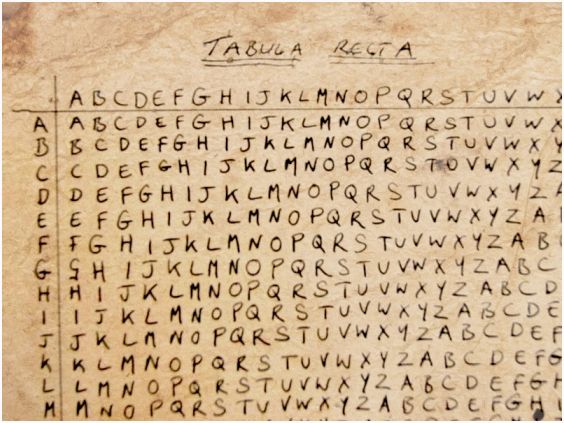

Рис. 2: Рис. 2 Шифр Виженера

Шифр Виженера

```
const abcStart = codepoint('а');
const abcEnd = codepoint('я');

println("Введите пароль");
pass = lowercase(readline());

# Работает при условии только кириллицы, без других символов
println("Введите строку для шифрования");
rawString = lowercase(readline());

encodedString = "";
```

Шифр Виженера

```
while (length(pass) < length(rawString))
    global pass *= pass;
end;

for i in 1:2:2 * length(rawString)
    global encodedString *= (Char)(abcStart - 1 +
        mod(codepoint(rawString[i]) +
            codepoint(pass[i]) - 2 * abcStart + 1, abcEnd - abcStart));
end;

println(encodedString);
```

Выводы

Выводы

1. Познакомились с многоалфавитными шифрами и шифрами перестановок
2. Реализовали маршрутный шифр и шифр Виженера