Лабораторная работа №1

Шифры простой замены

Кубасов В.Ю., ст.б. 1132249516

12 сентября 2024

Вводная часть

Цели и задачи

Цель работы:
Ознакомиться с элементарными методами шифрования на примере шифров простой замены

Задачаи работы:

- Реализовать шифр Цезаря
- Реализовать шифр Атбаш

Теоретическое введение

Теоретическое введение

Шифр подстано́вки — это метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым правилом

Реализация

Шифр Цезаря

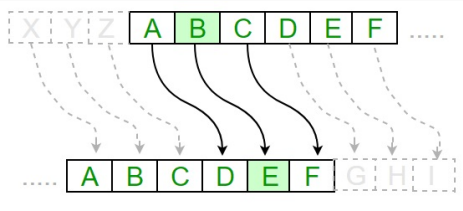

Рис. 1: Шифр Цезаря

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее . Величину *сдвига* можно рассматривать как ключ шифрования.

Шифр Цезаря

```
function gimmePassword()
    println("Введите смещение");

    offset = parse(Int64, readline());
    trueOffset = mod(offset, smallZOrd - smallAOrd + 1);
    rawPassword = "";

    for i in smallAOrd:1:smallZOrd
        rawPassword = rawPassword * (Char)(i);
    end;

    password = rawPassword[trueOffset + 1:length(rawPassword)]
         * rawPassword[1:trueOffset];
    return password;
```

Шифр Атбаш

Исходный текст	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Зашифрованный текст	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Исходный текст	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Зашифрованный текст	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б	А

Исходный текст	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Зашифрованный текст	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Рис. 2: Шифр Атбаш

Шифр Атбаш основан на *инверсии* алфавита: первая буква заменяется последней, вторая — предпоследней и так далее. В английском алфавите A меняется на Z, B на Y и так далее.

Шифр Атбаш

```
function gimmePassword()
    rawPassword = "";

    for i in smallAOrd:1:smallZOrd
        rawPassword = rawPassword * (Char)(i);
    end;

    password = reverse(rawPassword * ' ');

    return password;
end;
```

Вывод

Вывод

- Изучили элементарные виды шифрования, такие как алфавитные подстановки.
- Реализовали шифры алфавитных подстановок на примере шифра Цезаря и Атбаш.