Отчёт по лабораторной работе №1

Шифр простой замены

Сырцов Александр НФИмд-02-23

Содержание

Список иллюстраций

Цель работы

Создание программы для шифрования методом простой замены

Теоретические сведения

Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. Он является моноалфавитным, то есть имеет подстановочный тип, где каждая буква в открытом тексте заменяется на другую букву, смещенную на определенное количество позиций в алфавите.

Шифр Цезаря называется так благодаря Юлию Цезарю, который использовал его со сдвигом 3, чтобы защищать военные сообщения. Несмотря на то, что Цезарь считается первым зафиксированным человеком, использующим эту схему, другие шифры подстановки, как известно, использовались и раньше.

Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Пример шифрования со сдвигом 5:

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер п/п	12	18	10	17	20	16	4	18	1	22	10	33
Номер п/п +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное

приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

```
y = (x + k) mod n
x = (y - k + n) mod n
```

где: x — символ открытого текста, y — символ шифрованного текста, n — мощность алфавита, k — ключ.

Шифр Атбаш

Шифр простой замены Атбаш использовался для еврейского алфавита и оттуда же получил свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю. (алеф(первая буква) заменяется на тау(последнюю), бет(вторая) заменяется на шин(предпоследняя) из этих сочетаний шифр и получил свое название).

Шифр Атбаш для английского алфавита:

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

Правило шифрования состоит в замене i-й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите. # Выполнение работы

Реализация шифра Цезаря

```
#include <iostream>
#include <optional>
```

```
struct str
{
    char* symbols = nullptr;
    size_t len = 0;
};

struct CeasarCode
{
    str key;
    size_t position = 0;

    str encode(str line)
    {
        str code{new char[line.len+1], line.len};

        for(size_t i = 0; i < line.len; i++)
        {
            if((size_t)(line.symbols[i]) < this->position || (size_t)(line.symbol
            {
                code.symbols[i] = line.symbols[i];
                continue;
            }
            code.symbols[i] = key.symbols[(size_t)line.symbols[i]-this->position]
        }
        return code;
    }
};
```

```
void main()
{
    CeasarCode cc;
    str exmpl;
    str code;

    cc.key.symbols = "QWERTY";
    cc.key.len = 6;
    cc.position = (size_t)'a'+4;

    exmpl.symbols = "abcdefghijklmnopqrstuvwxyz";
    exmpl.len = 26;

    code = cc.encode(exmpl);

    std::cout << code.symbols;
}
```

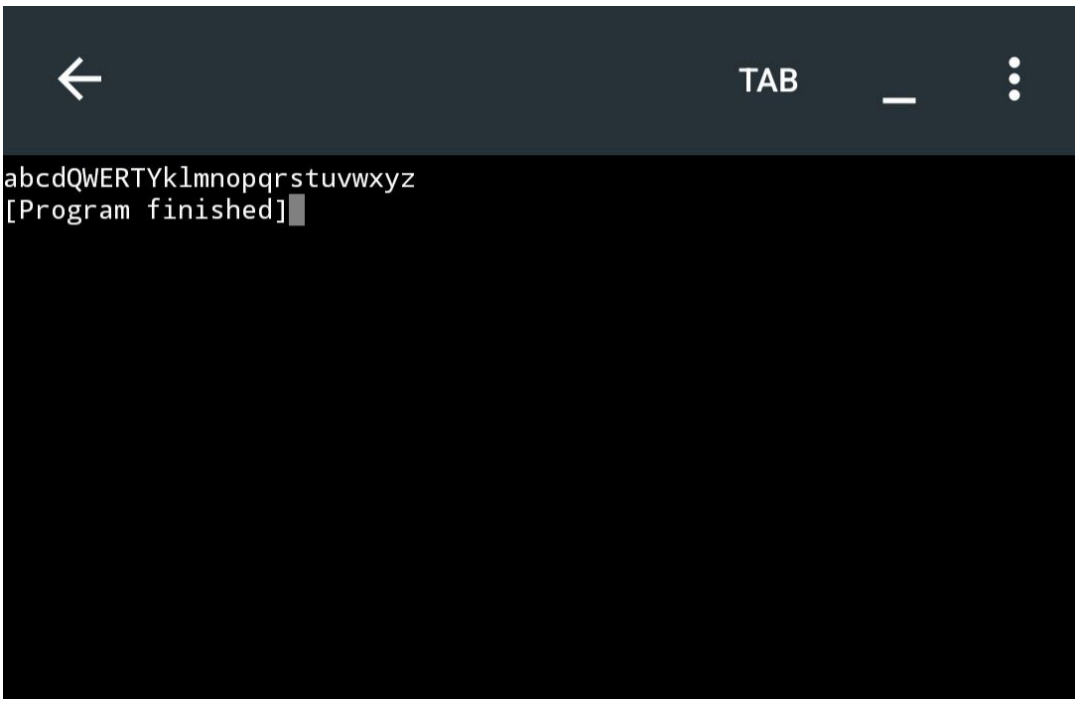

Рис. 1: Результат работы алгоритма цезаря

Реализация шифра Атбаш

```
#include <iostream>

char* reverse_char_ord(const char* word, size_t len)
{
    auto code = new char[len];

    for(size_t i = 0; i < len; i++)
    {
        code[i] = ((size_t)'z'-((size_t)word[i]-(size_t)'a'));
    }
    return code;
}
```

```
void main()
{
    std::cout << reverse_char_ord("abcd", 4);
}
```

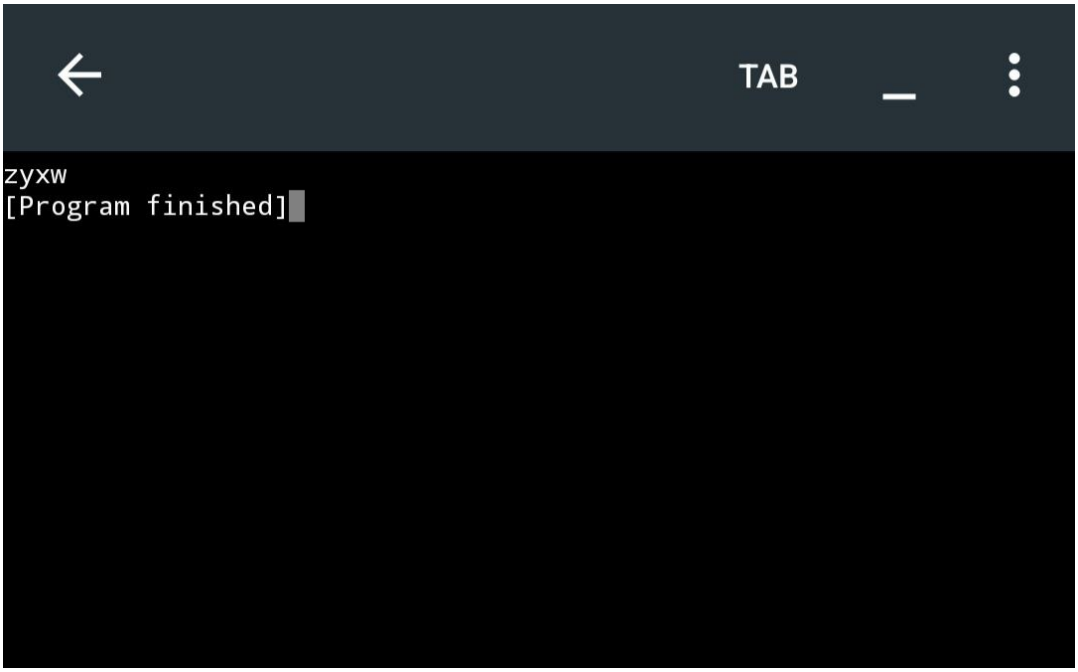

Рис. 2: Результат работы алгоритма Атбаш

Вывод

Я освоил шифрование методом простой замены и реализовал программу для шифрования.