

Лабораторная работа №1

Статистические свойства открытых текстов

Цели работы:

- 1) Получить представление о статистических свойствах открытых текстов.
- 2) Понять, как влияет на статистические свойства текстов их представление в компьютере.
- 3) Научиться создавать программы, которые реализуют простейшие шифрпреобразования.

Продолжительность: 4 часа

Теоретические сведения.

Шифр простой замены – шифр, при котором каждый знак открытого текста заменяется по ключевой подстановке на знак шифрованного текста.

Шифр вертикальной перестановки – шифр, при котором открытый текст записывается построчно слева - направо в прямоугольную рамку, с заранее оговоренным числом столбцов, столбцы переписываются в другую рамку переставленные по ключу, шифрованный текст считывается из рамки построчно слева - направо.

Лабораторное задание

1. Свойства текстов

Таблица 1

Номер варианта	Задание
Чётный	Создать файл программой Microsoft Word с расширением *.doc, содержащий текст “Veni, vidi, vici”. Создать программу на языке C++, определяющую его длину в байтах.
Нечётный	Создать файл программой Microsoft Word с расширением *.doc, содержащий текст “Пришёл, увидел, победил”. Создать программу на языке C++, определяющую его длину в байтах.

Таблица 2

Номер варианта	Задание
Чётный	Создать программу на языке C++, подсчитывающую частоту появления каждого байта в произвольном файле.
Нечётный	Создать программу на языке C++, подсчитывающую относительные частоты появления каждого байта в произвольном файле.

2. Криптопреобразование

Таблица 3

Номер варианта	Задание
Нечётный	Создать программу на языке C++, реализующую простую замену каждого байта для произвольного дискового файла. Ключ – подстановку порядка 256, вводить из отдельного файла с именем «key.txt». Программа должна иметь два режима: шифрование и расшифрование.
Чётный	Создать программу на языке C++, реализующую шифр вертикальной перестановки для произвольного дискового файла (число столбцов для шифра вертикальной перестановки – 5). В случае, если длина файла не кратна 5, дописывать его символами z. Ключ – подстановку порядка 5, вводить из отдельного файла с именем «key.txt». Программа должна иметь два режима: шифрование и расшифрование.

Приложение. Пример программы с вводом из указанного двоичного файла и выводом в двоичный файл “test”

```
#include <iostream>
#include <fstream>
using namespace std;

int main(int argc, char* argv[]){
    cout<<"Input filename.\n";
    char str[1024];
    cin>>str;

    ifstream in(str, ios::in | ios::binary);
```

```
if (!in) {
    cout << "Cannot open file.\n";
    return 1;
}

ofstream out("test", ios::out | ios::binary);
if (!out) {
    cout << "Cannot open file.\n";
    return 1;
}

char ch;
int per[256];
int i;

for (i=0;i<256;i++) per[i]=i;

while (in) {
    in.read(&ch,1);
    if(in.fail()){
        if(!in.eof()) {cout<<"Input error\n";break;}
        else break;
    }
    out.put((char)per[ch]);
    cout << ch;
}

in.close();
out.close();

getchar();
return 0;
}
```