# Лабораторная работа №1

Исследование частотных свойств шифра простой замены

В работе используется программа “ALFAVIT”, позволяющая провести частотный анализ открытого и зашифрованного текста в рамках русского алфавита. Текст необходимо набирать в “ Блокноте”, либо ввести из заранее подготовленного файла.

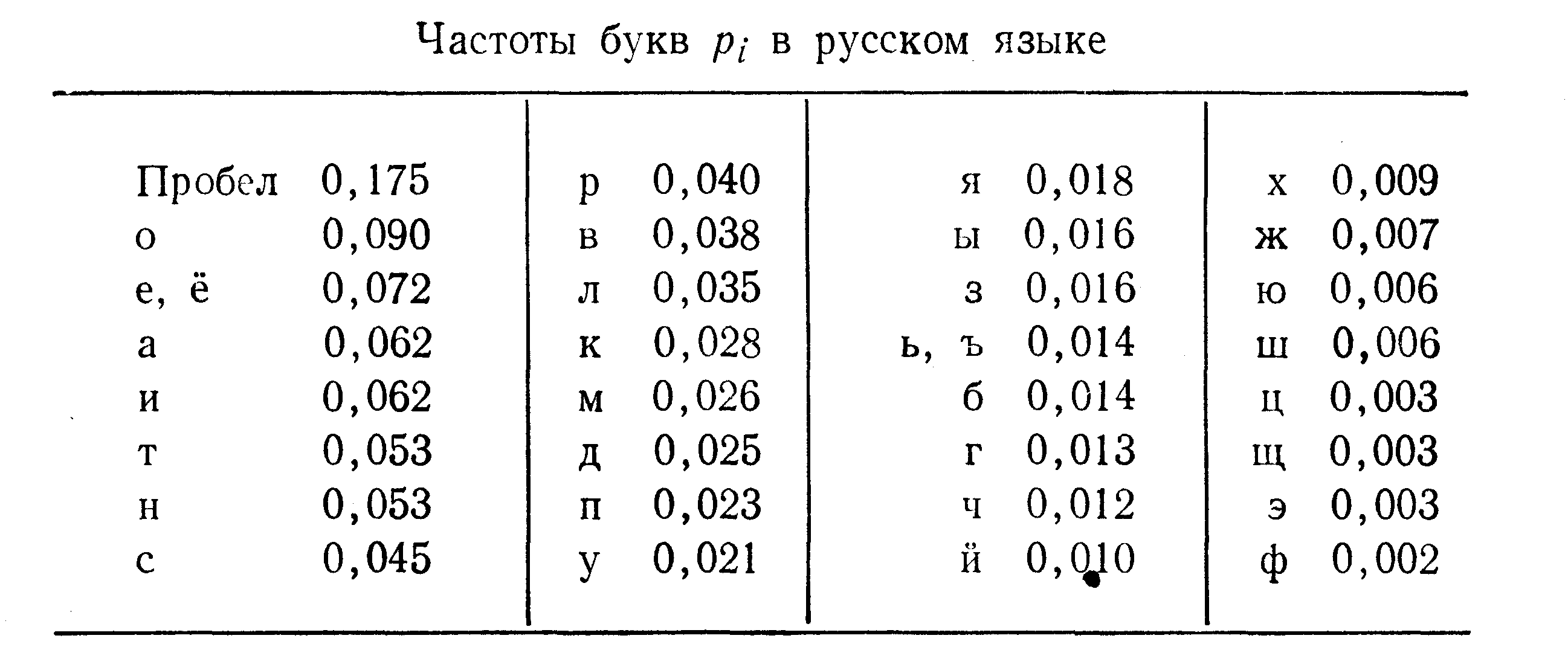
Опция «Посчитать» производит анализ текста, определяет количество букв и строит диаграмму распределения числа букв по алфавиту.

Опция «Зашифровать» производит преобразование исходного текста по алгоритму одноалфавитного шифра простой замены (система шифрования Цезаря) с ключом К = 3÷15 (опция «Сдвиг»).

Опция «H» предназначена для подсчета информационной энтропии как открытого, так и зашифрованного текста.

**Рабочее задание.**

1. Набрать текст (или ввести в“ALFAVIT” из файла) в “ Блокноте” (порядка 100 букв), исключить пробелы, знаки препинания и заменить заглавные буквы на строчные.
2. Провести анализ текста (опции «Посчитать» и «H»), выделить и зафиксировать наиболее информативные признаки (3-4 наибольших значения и их положение относительно друг друга) полученного распределения.
3. Для значения КЕ = (N+3)mod11+2, где N – номер по списку в группе, зашифровать текст и вновь провести анализ. Сравнить полученные результаты.
4. Построить вариационный ряд (упорядочить буквы по убыванию вероятности), сравнить с распределением частот русского языка :



1. Расшифровать предлагаемый текст СN (N- номер по списку группы), используя наиболее вероятное распределение частот появления букв в тексте на русском языке (пробел в программе ALFAVIT исключен из анализа).
2. Используя результаты п.5, определить ключ расшифрования KD.
3. Открыть пакет "Математика" и прочитать (ReadList) первые 10 букв из файла п.1.
4. С помощью функции FromCharacterCode перевести коды ASCII в символы.
5. Создать строку, содержащую первые пять символов русского алфавита и с помощью функции ToCharacterCode определить коды представления русского алфавита.
6. Перевести символы вектора п.7 из кодов ASCII в UNICOD и вновь вывести с помощью FromCharacterCode (см. Character Codes в системе документации Wolfram Mathematica).
7. Используя пример (шаблон) для латинского алфавита сформировать программу, реализующую шифр Цезаря для русского алфавита с вводом данных из файла. С помощью функции ToCharacterCode и FromCharacterCode пакета "Математика", преобразующих символы в ASCII коды и обратно ( код буквы a-97, код буквы b-98 и т.д.), можно задать шифр Цезаря с помощью следующей функции:

CaesarCipher[plaintext\_, key\_]:=

FromCharacterCode[ Mod[ ToCharacterCode[plaintext] - 97 +key, 26] + 97]

## Пример использования:

## CaesarCipher[plaintext\_, key\_]:= FromCharacterCode[ Mod[ ToCharacterCode[plaintext] - 97 +key, 26] + 97]

plaintext="typehereyourplaintextinsmallletters";

key=24;

## CaesarCipher[plaintext,key]

## rwncfcpcwmspnjyglrcvrglqkyjjjcrrcpq

1. Реализовать расшифровку заданного в п.5 файла CN методом силовой атаки (использовать первые 40 символов текста).

Пример для латинского алфавита : ciphertext="yhaklwpnw";

## Table[CaesarCipher[ciphertext,-key],{key,1,26}].

## Разработать программный модуль шифрования текста системой афинных подстановок.

14. Разработать программный модуль шифрования текста системой Цезаря с ключевым словом.

15. Построить три совмещенные по вертикали диаграммы распределения символов текста из п1:

* исходный открытый текст;
* текст, зашифрованный с помощью основного алгоритма Цезаря на ключе КЕ = (N+3)mod11+2;

## текст, зашифрованный на произвольном ключе с помощью системой афинных подстановок;

* текст, зашифрованный на произвольном ключе с помощью системы Цезаря с ключевым словом..