

Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

**ЛАБОРАТОРНА РОБОТА №1**

**з дисципліни «Криптографія»**

**«Експериментальна оцінка ентропії на символ джерела відкритого тексту»**

Виконали:

студенти 3 курсу ФТІ

групи ФБ-81

Близнюк Микола та Мишкін Артем

Перевірили:

Чорний О.

Київ – 2020

**Завдання**

**Мета роботи**

Засвоєння понять ентропії на символ джерела та його надлишковості, вивчення та порівняння різних моделей джерела відкритого тексту для наближеного визначення ентропії, набуття практичних навичок щодо оцінки ентропії на символ джерела.

**Порядок виконання роботи**

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

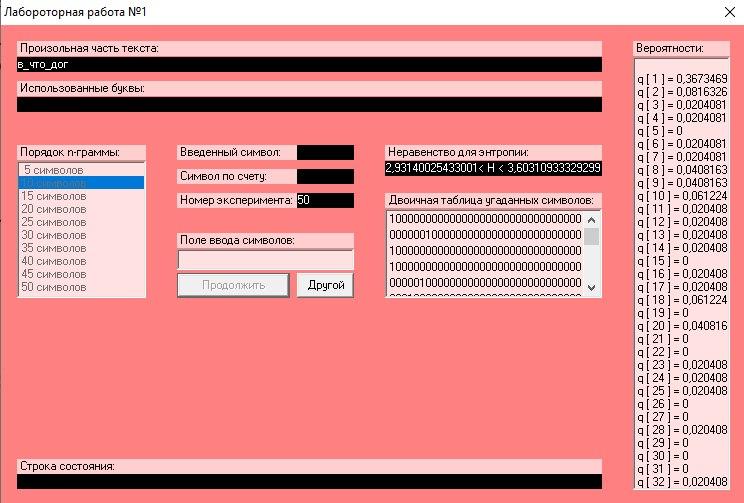
1. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку H1 та H2 за безпосереднім означенням. Підрахувати частоти букв та біграм, а також значення H1 та H2 на довільно обраному тексті російською мовою достатньої довжини (щонайменше 1Мб), де імовірності замінити відповідними частотами. Також одержати значення 1 H та 2 H на тому ж тексті, в якому вилучено всі пробіли.

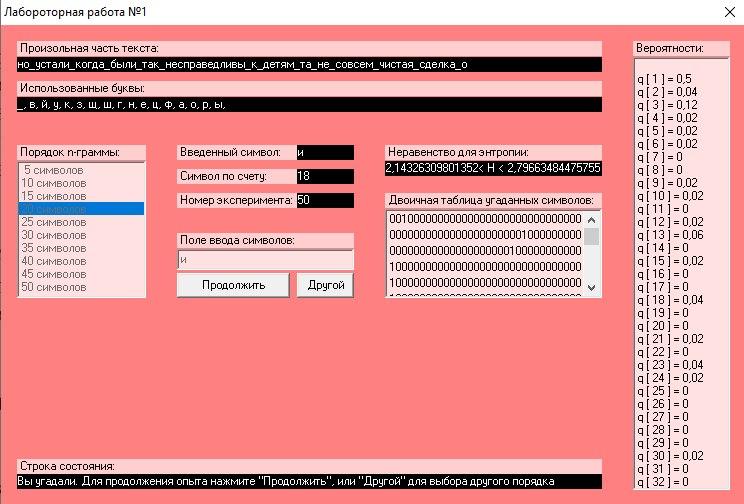
2. За допомогою програми CoolPinkProgram оцінити значення H(10) , H (20), H(30) .

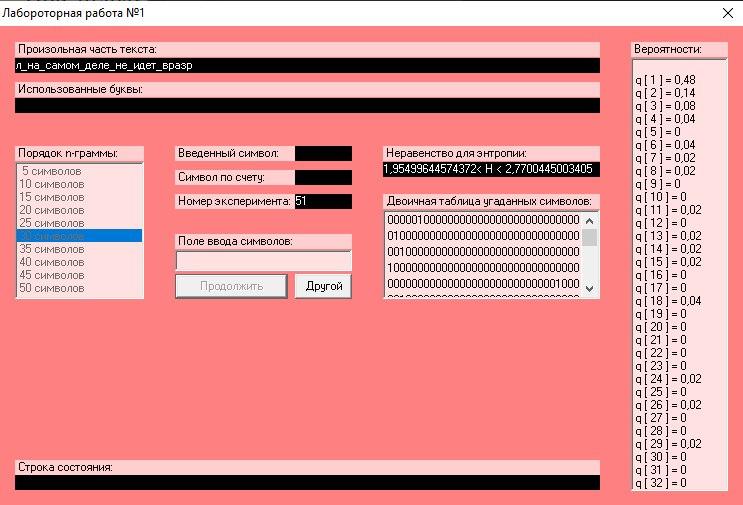
3. Використовуючи отримані значення ентропії, оцінити надлишковість російської мови в різних моделях джерела

**Хід роботи**

|  |  |
| --- | --- |
| Файл | Коментар |
| funcs.py | Включає в себе імпорт потрібних бібліотек та функції |
| main.py | Головний виконуваний файл |
| text.txt | Файл з текстом для аналізу |
| values.txt | Файл з результатами аналізу |

****

****

****

|  |  |  |
| --- | --- | --- |
| Вид тесту | Entropy | Redundancy |
| Монограма (whitespace) | 4.33270764082674 | 0.13345847183465198 |
| Біграма (whitespace) | 3.966574582247116 | 0.2066850835505768 |
| Монограма (no whitespace) | 3.884654462910488 | 0.22306910741790242 |
| Біграма (no whitespace) | 4.154389978943852 | 0.16912200421122958 |

**Висновки**

Під час виконання комп’ютерного практикуму № 1. Ми експериментально оцінили ентропію на символ джерела та надлишковість на прикладі російського алфавіту. Ми порівняли ентропію та надлишковість для монограм і для біграм з пробілом та без нього.