

Міністерство освіти і науки, молоді та спорту України Національний технічний університет України "Київський політехнічний інститут" Фізико-Технічний інститут

Лабораторна робота №1 з Симетричної криптографії

Студент групи ФІ-93

Карловський Володимир Олександрович

Задачі

- 1. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку Н1 та Н2 за безпосереднім означенням. Підрахувати частоти букв та біграм, а також значення Н1 та Н2 на довільно обраному тексті російською мовою достатньої довжини (щонайменше 1Мб), де імовірності замінити відповідними частотами. Також одержати значення Н1 та Н2 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.

Nº1

Для отримання детального результату треба запустити програму (інструкція в README.md) не розміщюю результат тут бо в російському алфавіті 33 літери => 33*33 = 1089 біграм

Короткі результати ентропій:

statByLettersWithSpaces has entropy: 4.462151364016589
statByLettersWithoutSpaces has entropy: 4.462151364016587
statByBigramsWithIntersAndWithoutSpaces has entropy: 4.1453958533961
statByBigramsWithIntersAndWithSpaces has entropy: 3.963214806411822
statByBigramsWithoutIntersAndWithoutSpaces has entropy: 4.145212314083568
statByBigtamsWithoutIntersAndWithSpaces has entropy: 3.90831788858674

Тобто

 $H_{1}=4,46-$ ентропія літер з пробілами і без, очевидно, збігаються $H_{2.1}=4,14-$ ентропія біграм з перетином і без пробілів $H_{2.2}=3,96-$ ентропія біграм з перетином і з пробілами $H_{2.3}=4,14-$ ентропія біграм без перетину і без пробілів

 $H_{_{2.4}} = 3,90 -$ ентропія біграм без перетину і з пробілами

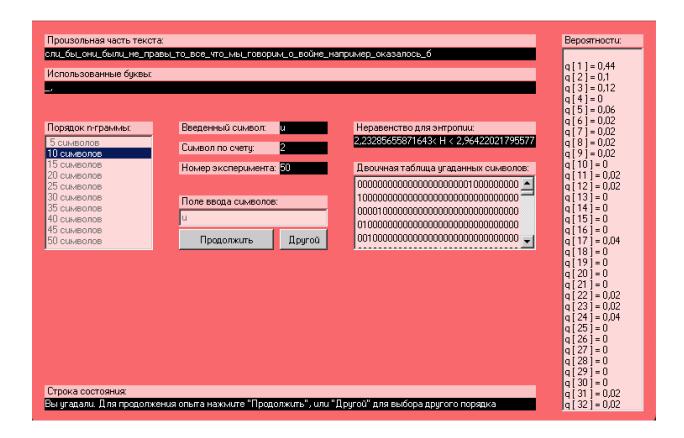
$N^{0}2$

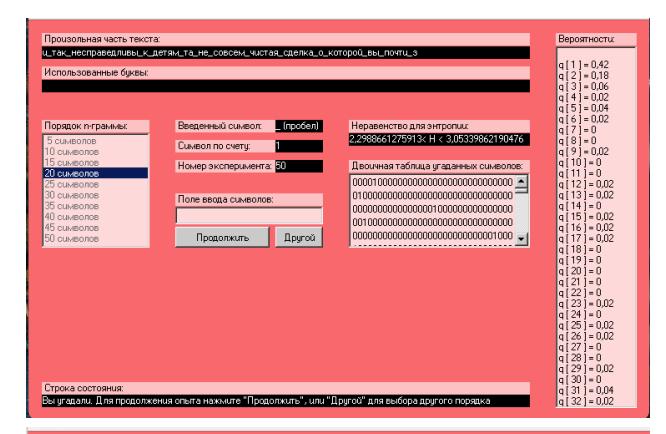
Результати:

$$2,23 < H^{(10)} < 2,96$$

$$2,29 < H^{(20)} < 3,05$$

$$1,71 < H^{(30)} < 2,44$$







№3

$$H_0 = log_2 32 = 5$$

$$H_{inf} \approx H^{(30)}$$

$$H_{inf} \approx H^{(20)}$$

$$H_{inf} \approx H^{(10)}$$

$$H_{inf} \approx H_{2.4}$$

$$R = 0.22$$

$$H_{inf} \approx H_{2.3}$$

$$R = 0.17$$

$$H_{inf} \approx H_{2.2}$$

$$R = 0.20$$

$$H_{inf} \approx H_{2.1}$$

$$R = 0.17$$

$$H_{inf} \approx H_1$$

$$R = 0.10$$