

**Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут**

Криптографія

Лабораторна робота №1.

Виконав:
студент гр. ФБ-94
Резніченко Н. І.
Белоцький. Д. О.

Київ – 2021

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

Entropy:

Letters with spaces entropy: 4.446592

Letters without spaces entropy: 4.446592

Entropy for crossed bgramms with spaces: 5.187000

Entropy for uncrossed bgramms with spaces: 2.891708

Entropy for crossed bgramms without spaces: 4.629763

Entropy for uncrossed bgramms without spaces: 2.564196

Letters with spaces count:

п: 23449.000000 ч: 15073.000000

ю: 4672.000000 я: 17941.000000

ы: 13933.000000 о: 97745.000000

ж: 9531.000000 к: 28479.000000

б: 14863.000000 и: 61333.000000

ц: 2540.000000 г: 14090.000000

х: 7542.000000 а: 67791.000000

м: 26714.000000 с: 44101.000000

л: 39430.000000 р: 35509.000000

з: 13563.000000 д: 27316.000000

ь: 20115.000000 щ: 2600.000000

е: 72365.000000 ш: 7378.000000

т: 55096.000000 ф: 826.000000

в: 38403.000000 у: 25696.000000

н: 54457.000000 й: 8347.000000

э: 2739.000000

Letters without spaces count:

щ: 2600.000000 н: 54457.000000 а:

67791.000000 э: 2739.000000

г: 14090.000000 х: 7542.000000

ы: 13933.000000 м: 26714.000000

ь: 20115.000000 ч: 15073.000000

о: 97745.000000 п: 23449.000000

т: 55096.000000 у: 25696.000000

ж: 9531.000000 ц: 2540.000000

б: 14863.000000 ф: 826.000000

ю: 4672.000000 р: 35509.000000

й: 8347.000000 к: 28479.000000

д: 27316.000000 с: 44101.000000

е: 72365.000000 я: 17941.000000

з: 13563.000000 в: 38403.000000

и: 61333.000000 л: 39430.000000

ш: 7378.000000

Letters frequency with spaces:

о: 0.114504 е: 0.084773

а: 0.079414 и: 0.071849

т: 0.064543 н: 0.063794

с: 0.051662 л: 0.046191

в: 0.044988 р: 0.041597

к: 0.033362 д: 0.032000

м: 0.031294 у: 0.030102

п: 0.027470 ь: 0.023564

я: 0.021017 ч: 0.017657

б: 0.017411 г: 0.016506

ы: 0.016322 з: 0.015888

ж: 0.011165 й: 0.009778

х: 0.008835 ш: 0.008643

ю: 0.005473 э: 0.003209

щ: 0.003046 ц: 0.002976

ф: 0.000968

Letters frequency without spaces:

о: 0.114504 е: 0.084773

а: 0.079414 и: 0.071849

т: 0.064543 н: 0.063794

с: 0.051662 л: 0.046191

в: 0.044988 р: 0.041597

к: 0.033362 д: 0.032000

м: 0.031294 у: 0.030102

п: 0.027470 б: 0.023564

я: 0.021017 ч: 0.017657

б: 0.017411 г: 0.016506

ы: 0.016322 з: 0.015888

ж: 0.011165 й: 0.009778

х: 0.008835 ш: 0.008643

ю: 0.005473 э: 0.003209

щ: 0.003046 ц: 0.002976

ф: 0.000968

CoolPinkProgram

$H(10) = 4,465, R = 0.107 (10.7\%)$

Произвольная часть текста:
ию_только

Использованные буквы:

Порядок n-граммы:
5 символов
10 символов
15 символов
20 символов
25 символов
30 символов
35 символов
40 символов
45 символов
50 символов

Введенный символ:

Символ по счету:

Номер эксперимента: 51

Поле ввода символов:

Продолжить

Другой

Неравенство для энтропии:
4.78595441501199< H < 4.15856293964492

Двоичная таблица угаданных символов:
000000000000010000000000000000
00000000000000000000000001000000
000000000000000000000000000001000
000000000000000000000000000000000
00000100000000000000000000000000

Вероятности:
q[1] = 0.08
q[2] = 0
q[3] = 0
q[4] = 0.04
q[5] = 0.04
q[6] = 0.16
q[7] = 0.04
q[8] = 0
q[9] = 0
q[10] = 0
q[11] = 0
q[12] = 0
q[13] = 0.08
q[14] = 0.04
q[15] = 0.04
q[16] = 0
q[17] = 0
q[18] = 0.02
q[19] = 0.06
q[20] = 0.04
q[21] = 0.04
q[22] = 0
q[23] = 0.04
q[24] = 0.02
q[25] = 0.02
q[26] = 0.04
q[27] = 0.02
q[28] = 0.06
q[29] = 0.04
q[30] = 0
q[31] = 0.02
q[32] = 0.06

Строка состояния:

$H(20) = 4,731, R = 0.053 (5.3\%)$

Произвольная часть текста:
_знает_его_инстинкт

Использованные буквы:

Порядок n-граммы:
5 символов
10 символов
15 символов
20 символов
25 символов
30 символов
35 символов
40 символов
45 символов
50 символов

Введенный символ:

Символ по счету:

Номер эксперимента: 51

Поле ввода символов:

Продолжить

Другой

Неравенство для энтропии:
4.90913820838391< H < 4.55326968951511

Двоичная таблица угаданных символов:
00000001000000000000000000000000
00000000000000000000000001000000
00000000000000000000000000000000
000000000000000000000000000000001
0000000000000000000000000100000000

Вероятности:
q[1] = 0.02
q[2] = 0.06
q[3] = 0.04
q[4] = 0.04
q[5] = 0.04
q[6] = 0.02
q[7] = 0.02
q[8] = 0.08
q[9] = 0.06
q[10] = 0
q[11] = 0.02
q[12] = 0.04
q[13] = 0
q[14] = 0.02
q[15] = 0
q[16] = 0.02
q[17] = 0.04
q[18] = 0.02
q[19] = 0.06
q[20] = 0
q[21] = 0.06
q[22] = 0.04
q[23] = 0.02
q[24] = 0.02
q[25] = 0
q[26] = 0.04
q[27] = 0.04
q[28] = 0.06
q[29] = 0.06
q[30] = 0
q[31] = 0.02
q[32] = 0.04

Строка состояния:

H(30) = 4,17, R = 0.166 (16.6%)

[illegible]

Висновки: При виконанні лабораторної роботи ми засвоїли поняття ентропії на символ джерела та надлишковості та навчилися їх вимірювати, набули навичок щодо їх оцінки.