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

## КРИПТОГРАФІЯ

Комп'ютерний практикум №1 Експериментальна оцінка ентропії на символ джерела відкритого тексту Варіант 1

> Виконала: Студентка 3 курсу Групи ФБ-01 Маковська М. В.

**Мета:** 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

#### Постановка задачі:

- 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 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  $\mathbf{H}^{(10)}$  ,  $\mathbf{H}^{(20)}$  ,  $\mathbf{H}^{(30)}$
- 3. Використовуючи отримані значення ентропії, оцінити надлишковість російської мови в різних моделях джерела.

## Хід роботи

Для подальшої роботи з текстом було обрано "Таємні думки кобзаря" Т. Шевченка (російською мовою)

### Отримані результати для тексту з пробілами:

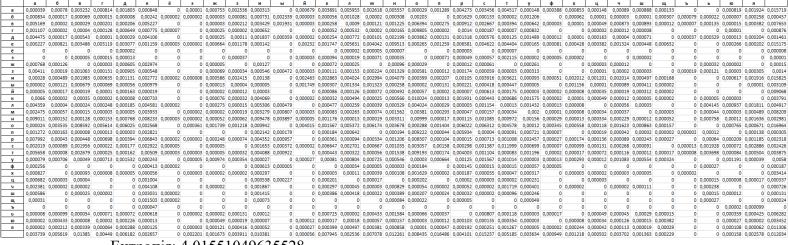
Частота букв:

'ë'	0.000034	'я'	0.017743
'ъ'	0.000167	'y'	0.021872
'φ'	0.001987	'n'	0.024327
'ə'	0.002605	'A'	0.024679
'щ'	0.002755	'm'	0.02776
'ц'	0.003552	'k'	0.031542
'ю'	0.005857	' <b>л</b> '	0.035305
'ш'	0.007176	'в'	0.04025
'x'	0.007198	'p'	0.042085
'ж'	0.007372	'T'	0.045212
'й'	0.011375	'c'	0.047214
'ь'	0.012433	'H'	0.056367
'4'	0.012843	'и'	0.061689
'a'	0.01294	'a'	0.065299
'ы'	0.012945	'e'	0.073366
'6'	0.014152	'o'	0.092209
'r'	0.017298	**	0.160392

Ентропія: 4.378468487047604

Надлишковість: 0.13936108750594567

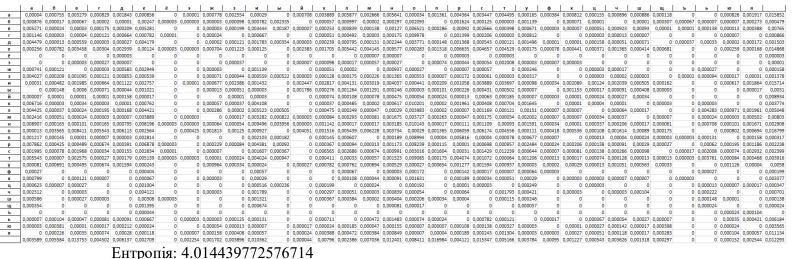
Частота біграм Н1:



Ентропія: 4.01551049635528

Надлишковість: 0.21070470258837437

# Частота біграм Н2:



Ентропія: 4.014439772576714

Надлишковість: 0.2109151658019599

Отримані результати для тексту без пробілів:

Частота букв:

0.00004	'я'	0.021132
0.000199	'y'	0.026051
0.002366	'n'	0.028975
0.003103	'д'	0.029394
0.003281	'm'	0.033063
0.00423	'k'	0.037568
0.006976	'л'	0.042049
0.008547	'в'	0.047939
0.008573	'p'	0.050125
0.00878	'T'	0.053849
0.013548	'c'	0.056233
0.014808	'H'	0.067135
0.015296	'и'	0.073474
0.015412	'a'	0.077773
0.015418	'e'	0.087381
0.016855	'o'	0.109824
0.020602		
	0.000199 0.002366 0.003103 0.003281 0.00423 0.006976 0.008547 0.00878 0.013548 0.014808 0.015296 0.015412 0.015418 0.016855	0.000199 'y' 0.002366 'n' 0.003103 'A' 0.003281 'M' 0.00423 'K' 0.006976 'л' 0.008547 'B' 0.008573 'p' 0.00878 'T' 0.013548 'c' 0.014808 'H' 0.015296 'M' 0.015412 'a' 0.016855 'o'

Ентропія: 4.458284802695269

Надлишковість: 0.12367226222343031

# Частота біграм Н1:

	a	6	8	r	Д	e	ë	9	ж	3	И	ы	й	K	Л	M	н	0	n	р	c	T	У	ф	x	ц	ч	ш	щ	ъ	ь	ю	я
a	0,00065	0,00166	0,0057	0,00154	0,00283	0,00134	0	0,00031	0,00107	0,00346	0,00185	0	0,00083	0,0056	0,00738	0,00397	0,00799	0,00119	0,00368	0,00566	0,00591	0,0061	0,00059	0,00061	0,00112	0,00021	0,00147	0,00123	0,00019	0	C	0,00099	0,00266
6	0,00101	2,6E-05	9,4E-05	2,2E-05	2,4E-05	0,00289	2E-06	7,4E-05	4E-06	0,0001	0,00092	0,00279	4E-06	7,8E-05	0,00127	3,2E-05	0,00039	0,00246	3,6E-05	0,00195	0,00032	4E-06	0,00145	0	7,4E-05	1,4E-05	0,00001	1,4E-05	0,00037	9,4E-05	2,6E-05	8E-06	0,00031
В	0,00643	0,00027	0,00056	0,00099	0,0006	0,00635	0	0,00029	9,2E-05	0,00046	0,00445	0,0023	6E-06	0,00095	0,00123	0,00057	0,00201	0,0082	0,00133	0,00145	0,00413	0,00087	0,00099	4,4E-05	0,00007	0,00011	0,00134	0,00112	1,6E-05	8E-06	0,00016	0,00003	0,00051
r	0,00135	4,2E-05	0,00015	0,00018	0,00083	0,00093	8E-06	0	4,4E-05	0,00003	0,00085	0	0	0,00012	0,00065	0,00005	0,00025	0,01176	0,00012	0,0017	0,00033	3,2E-05	0,00102	0,00001	8E-06	4E-06	3,8E-05	6,8E-05	0	0	C	1,2E-05	1,2E-05
А	0,00541	8,8E-05	0,00081	0,00006	7,4E-05	0,00497	0	0,00003	5,8E-05	0,00019	0,00228	0,00043	2E-06	0,0004	0,00095	0,0002	0,00277	0,00466	0,00025	0,00171	0,00087	0,0002	0,00182	3,4E-05	2,2E-05	0,0002	7,8E-05	9,4E-05	. 0	4,4E-05	0,00039	0,00002	0,00029
e	0,00062	0,00171	0,00601	0,00421	0,0044	0,00164	4E-06	0,00025	0,00095	0,00208	0,0014	0	0,00277	0,00283	0,00698	0,00564	0,01284	0,0014	0,00364	0,00827	0,00755	0,00584	0,00068	0,00022	0,00069	0,0005	0,00199	0,00069	0,00078	0	C	0,00034	0,00046
ë	0	2E-06	2E-06	2E-06	2E-06	0	0	0	0	0	0	0	0	2E-06	2E-06	6E-06	8E-06	0	0	4E-06	0	8E-06	0	0	0	0	0	0	. 0	. 0	C	0	2E-06
	2E-06	0		1,8E-05	1,6E-05	0	0	0	0	4,4E-05	4E-06	0	4E-06	0,00011	2,2E-05	8,4E-05	4,4E-05	0	8,4E-05	5,8E-05	6,8E-05	0,00252	2E-06	8E-06	2E-06	0	0	2E-06	0	0	C	0	0
ж	0,00092	0,00016	1,4E-05	8E-06	0,00073	0,00355	0	6E-06	8E-06	6E-06	0,00153	0	0	0,00009	0,00003	4E-06	0,00118	4,4E-05	1,8E-05	1,8E-05	9,4E-05	6E-06	0,00031	0	2E-06	4E-06	1,6E-05	0	. 0	. 0	3,8E-05	2E-06	2E-06
3	0,00495	0,00028	0,00142	0,0002	0,00117	0,00068	0	4,2E-05	0,00009	7,4E-05	0,00069	0,00056	4E-06	0,00025	0,00021	0,0004	0,00173	0,00077	0,00023	0,00026	0,00023	7,4E-05	0,00043	1,2E-05	1,4E-05	1,8E-05	0,00005	1,8E-05	. 0	2,2E-05	0,00014	3,8E-05	0,00037
И	0,00072	0,00132	0,00418	0,0012	0,00234	0,00367	2E-06	0,00029	0,00085	0,00339	0,0028	0	0,00294	0,00437	0,00512	0,00445	0,00649	0,00162	0,00245	0,0018	0,00634	0,00512	0,00052	0,00015	0,00265	0,00148	0,00282	0,00074	0,00021	. 0	0	0,00075	0,00268
ы	0,00012	0,00029	0,00117	0,00017	0,00021	0,00125	0	5,8E-05	0,00003	0,00016	0,00039	0	0,00208	0,00055	0,00164	0,0017	0,00068	0,00022	0,00054	0,00036	0,00084	0,00067	0,00008	1,6E-05	0,00141	0,00003	0,00017	0,00051	2E-06	0	C	2E-06	9,8E-05
й	0,00034	0,00046	0,00083	0,00038	0,00072	0,00014	0	0,00012	0,00023	0,0003	0,00083	0	4E-06	0,00078	0,00039	0,00064	0,0013	0,00052	0,00125	0,00048	0,00192	0,00052	0,00022	9,2E-05	9,8E-05	0,00011	0,00025	0,00052	6E-06	0	0	1,4E-05	0,00012
K	0,00796	0,00025	0,00076	0,00016	0,00017	0,00095	0	8,6E-05	0,00014	0,00015	0,00521	0	2E-06	0,0003	0,00069	0,00025	0,00113	0,01218	0,00042	0,00242	0,00097	0,00095	0,00196	2,2E-05	4,6E-05	7,4E-05	0,00016	3,8E-05	0,00001	. 0	6E-06	2,2E-05	0,00011
Л	0,00529	0,00022	0,00066	0,00037	0,0004	0,00572	2E-06	0,00006	0,00037	0,00013	0,00671	0,00057	0	0,00092	0,00039	0,00054	0,00088	0,0051	0,00059	8,2E-05	0,00195	0,00029	0,00193	5,6E-05	2,8E-05	0,00001	0,00024	6,6E-05	6E-06	. 0	0,00494	0,00112	0,00244
M	0,00328						0	8,8E-05	0,00016	0,0003	0,00473	0,00096																	3,4E-05			1,6E-05	
н	0,0109	0,0004	0,00051	0,00029	0,00104	0,00985	4E-06	2,2E-05	8,4E-05	0,00014	0,01165	0,00464	6E-06	0,00156	5,2E-05	0,00019	0,00418	0,0121	0,00049	0,00021	0,00162	0,00126	0,00196	5,8E-05	3,4E-05	0,00041	0,00032	0,00003	7,6E-05	. 0	0,0009	0,00014	0,002
0	0,00029							0,00064																			0,0025			. 0		0,00093	
п	0,00156	0,00021	4,6E-05	4,6E-05	1,4E-05	0,00337	0	4E-06	0	2E-06	0,00257	0,00021	0	0,00026	0,00078	0,00001	0,00024	0,011	8,2E-05	0,00707	8,2E-05	0,00012	0,00088	0,00001	0	2,2E-05	5,4E-05	0,00003	4E-06		0,00014		0,00017
р	0,00969						2E-06	4,8E-05	0,00031	0,00016	0,00548	0,00114															0,00017					0,00025	
С	0,00248						6E-06	6,6E-05	4,2E-05	5,4E-05	0,00205	0,00044	2E-06	0,00813	0,00328	0,00099	0,00157	0,00373	0,0022	0,00043	0,00187	0,01443	0,0009	3,4E-05	0,00014	0,00019	0,00035	0,00019	7,2E-05	1,6E-05	0,0023	8,8E-05	0,00345
T	0,00687							0,00011																						0,00001			
y				0,00101			0	0,00008																		3,2E-05			0,0004			0,00143	
ф		8E-06				0,00049	2E-06	0		1,4E-05		6E-06									0,00002					0		2E-06				1,8E-05	
X	0,00107							0,00005				0	0											1,8E-05	0,00005		8,8E-05					4E-06	
ц	0,00084							2E-06			0,00068										3,2E-05				4E-06							0,00001	
ч	0,00285						0	6E-06	0,00001	-,	-,	0	0	0,00042							0,00024						-,	-,	1,2E-05		0,00028		
ш	0,0007		4,6E-05			0,00361	2E-06	0			0,0017	0		0,00047	0,0005						1,4E-05					1,2E-05	2E-06	_	_			1,4E-05	0
щ	0,00037	0	2E-06	2E-06		0,00179	2E-06	0	0	0	0,00087	0		0	0	2E-06	0,0001	2,6E-05	0,00001	8E-06	2E-06	0	5,8E-05		0	0	0	0	0	0	3,2E-05		0
ъ	0	0	0	0		5,6E-05	0		0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		2,4E-05	
b	0,00017							0,00014	-	,	_	0																	2,8E-05			0,00044	
ю	0,00011							6,2E-05																					0,00046			0,00004	
Я	0,00023	0,00066	0,00192	0,00046	0,00082	0,00041	0	0,00017	0,00029	0,0009	0,001	0	3,8E-05	0,00128	0,00078	0,00099	0,00246	0,00076	0,00156	0,00057	0,00174	0,00197	0,00033	0,00009	0,00039	8,8E-05	0,00037	0,00011	0,00035	0	0	0,00013	0,00029
							4	1.5	10.1	0.0	050	000	_																				

Ентропія: 4.154249679568825

Надлишковість: 0.18343390228127132

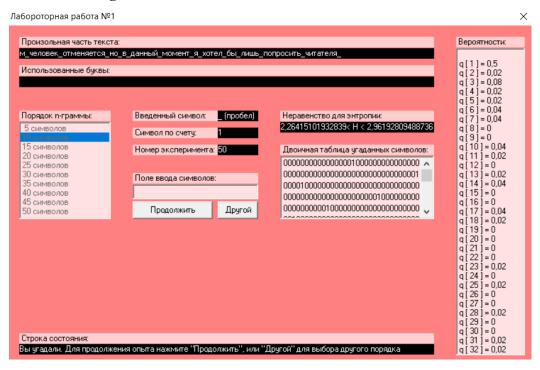
# Частота біграм Н2:

								-																									
	a	6	В	r	д	e	ë	9	ж	3	И	ы	й	K	л	м	н	0	п	р	С	т	y	ф	x	ц	ч	ш	щ	ъ	ь	ю	я
a	0,00067	0,00161	0,00569	0,00157	0,00277	0,00132	0	0,00028	0,00107	0,00343	0,00183	0	0,00082	0,00554	0,00727	0,00414	0,0079	0,00126	0,00364	0,00567	0,00608	0,00611	0,00049	0,00054	0,00115	0,00019	0,00152	0,00123	0,00018	0	0	0,00097	0,00252
6	0,00098	3,6E-05	8,8E-05	2,4E-05	0,00002	0,00284	0	7,2E-05	4E-06	5,6E-05	0,00084	0,00274	4E-06	8,8E-05	0,00124	3,6E-05	0,00042	0,00228	3,6E-05	0,00207	0,00029	4E-06	0,00138	0	7,2E-05	1,6E-05	1,2E-05	1,6E-05	0,00035	8,8E-05	2,8E-05	4E-06	0,00029
В	0,00637	0,00027	0,0005	0,00099	0,00059	0,00642	0	0,0003	9,6E-05	0,00045	0,00463	0,00233	4E-06	0,00096	0,00116	0,00058	0,00201	0,00825	0,00128	0,00145	0,00432	0,00089	0,00097	5,2E-05	0,00008	0,0001	0,00128	0,00112	2,8E-05	8E-06	0,00016	4,8E-05	0,00049
r	0,0013	5,2E-05	0,00015	0,00019	0,00076	0,00104	4E-06	0	5,2E-05	0,00002	0,00088	0	0	0,00014	0,00059	4,8E-05	0,00025	0,01185	0,00013	0,00169	0,00036	0,00004	0,001	0	1,2E-05	0	3,2E-05	7,2E-05	0	0	0	1,2E-05	8E-06
д	0,00556	0,00011	0,00083	0,00006	7,2E-05	0,00505	0	1,6E-05	4,8E-05	0,00017	0,00239	0,00043	0	0,00039	0,00088	0,00021	0,00273	0,0046	0,00029	0,00186	0,00088	0,00023	0,00181	2,8E-05	2,4E-05	0,00022	0,0001	0,00013	0	3,6E-05	0,0004	0,00002	0,00032
e	0,00064	0,00178	0,00608	0,00419	0,00449	0,0016	4E-06	0,00031	0,00104	0,00212	0,00136	0	0,00287	0,0028	0,00707	0,00563	0,01271	0,00138	0,00367	0,00841	0,00739	0,00586	0,00068	0,0002	0,00076	0,00047	0,00201	0,00073	0,00073	0	0	0,00036	0,00045
ë	0	0	0	0	4E-06	0	0	0	0	0	0	0	0	4E-06	0	8E-06	8E-06	0	0	4E-06	0	1,2E-05	0	0	0	0	0	0	0	0	0	0	0
9	0	0	8E-06	1,2E-05	2,4E-05	0	0	0	0	3,6E-05	4E-06	0	4E-06	9,6E-05	3,2E-05	0,00008	2,8E-05	0	0,00006	0,00004	7,6E-05	0,00251	0	1,2E-05	4E-06	0	0	4E-06	0	0	0	0	0
ж	0,00095	0,00015	1,2E-05	8E-06	0,00069	0,00354	0	8E-06	0	0	0,00149	0	0	9,2E-05	3,6E-05	0	0,0012	0,00004	1,2E-05	1,6E-05	8,4E-05	0	0,00031	0	0	4E-06	0,00002	0	0	0	3,6E-05	4E-06	0
3	0,00485	0,00029	0,00138	0,00023	0,00122	0,0007	0	4,8E-05	0,0001	8,8E-05	0,00065	0,00054	8E-06	0,00024	0,00022	0,00038	0,00165	0,00078	0,00019	0,0003	0,00025	0,0001	0,00042	8E-06	0,00002	0,00002	2,4E-05	1,6E-05	0	2,8E-05			
И				0,00108			0	0,00024	0,00081	0,00336	0,00277	0	0,00297	0,0044	0,00514	0,00444	0,00624	0,00162	0,00244	0,00174	0,00633	0,00512	0,00053	0,00018	0,00265	0,00146	0,00283	0,00075	0,00023	0	0	0,00076	
ы	0,00014	0,00025	0,00117	0,00019	0,00017	0,00124	0	5,6E-05	0,00004	0,00017	0,00041	0	0,00214	0,00055	0,00167	0,0017	0,00071	0,00021	0,00054	0,00039	0,00081	0,00071	0,00006	1,6E-05	0,00138	2,8E-05	0,00016	0,00046	0	0	0	4E-06	0,00012
й	0,00033	0,00046	0,00077	0,00043	0,00071	0,00014	0	0,00014	0,00023	0,00029	0,00081	0		0,00076																0		1,6E-05	
К	0,008	0,00027	0,00074	0,00021	0,00016	0,00092	0	8,8E-05	0,00014	0,00018	0,00524	0	0	0,00031	0,00062	0,00029	0,00109	0,01225	0,00043	0,00258	0,00096	0,00095	0,00204	0,00002	0,00006	7,6E-05	0,00016	4,8E-05	1,6E-05	0		1,2E-05	
л	0,00531						4E-06	6,4E-05	0,00038	0,00012	0,0067	0,00063	0	0,00092	0,0004	0,00058	0,00096												8E-06		0,00484		
м	0,00344										0,00474			0,00056											8,8E-05						7,2E-05		0,00074
н	0,01093	0,00046	0,00059	0,00031	0,00102	0,00974	4E-06	2,4E-05	0,0001	0,00012	0,01171	0,00468	0	0,00163	6,8E-05	0,0002	0,00432	0,01201	0,00057	0,00021	0,00169	0,00128	0,00208	0,00008	0,00002	0,0004	0,00031	3,6E-05	7,6E-05	0		0,00014	
0	0,00034						0	0,00067		0,00199			0,00478	0,00269	0,0068										0,00084	0,00023	0,00248	0,00119	0,0002	0		0,00098	
п	0,00159	0,00024	6,4E-05	0,00004	1,2E-05	0,0033	0	4E-06	0	4E-06	0,00271	0,00017	0	0,00031	0,0007	8E-06	0,00026	0,01108	8,4E-05	0,0069	5,6E-05	0,00012	0,00089	1,6E-05	0	2,8E-05	5,6E-05	0,00004	4E-06	4E-06	8,8E-05	0	0,00014
р	0,00977	0,00063	0,00084	0,00079	0,00053	0,00803	4E-06	4,8E-05	0,00025	0,00014	0,00554	0,00113	4E-06	0,00061	0,00015	0,00046	0,00155	0,01018	0,00044	6,8E-05	0,00113	0,0013	0,00295	7,2E-05	0,00025	0,0002	0,00018	0,00033	0,00004	0	0,0008	0,00025	0,00141
С	0,00251										0,002			0,00786																		0,00008	
T	0,00675										0,00535			0,00079																8E-06		7,6E-05	
У	0,00032									0,00053				0,00128													0,00151	0,00077		0		0,00135	0,00017
ф	0,00031	8E-06	-		4E-06		0			-	0,00082	1,2E-05		4E-06			-							-		0	0	0	4E-06		2,8E-05	_	0
x				0,0002			0	6,4E-05		0,00012		0		0,00021															4E-06	4E-06	0		0,00006
ц	0,00085						0	0			0,00069	0,0003		0,00027			5,6E-05						0,00028	0			1,2E-05		0				
ч	0,00282								1,2E-05	0,00002		0		0,00043													1,2E-05	0,00016	8E-06		0,00024	0	8E-06
W	0,00069		5,6E-05		1,6E-05		4E-06	0	0		0,00166	0		0,00048							-			0	0		0	0	0			1,6E-05	0
щ	0,00042		4E-06	4E-06		0,00179	0	0	0	0	0,00089	0	0		0	0	0,0001			1,2E-05	0		8,8E-05	0	0	0	0	0	0		2,4E-05		0
ъ	0	0	0	0		7,2E-05	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		2,8E-05	
ь	0,00018									0,00041		0		0,00118																0		0,00043	
ю	0,00008									0,00011			-,	0,00024	-,										4,8E-05					0		0,00004	
Я	0,00024	0,00071	0,00198	0,00043	0,00084	0,00041	0	0,00017	0,0003	0,00102	0,00106	0	4,8E-05	0,00136	0,0007	0,00095	0,00246	0,00073	0,00161	0,00055	0,00179	0,00206	0,00036	0,00011	0,00038	0,00012	0,00037	8,8E-05	0,00038	0	0	0,00012	0,00025
				т	_		• ,		105	100	70.40	100	100																				

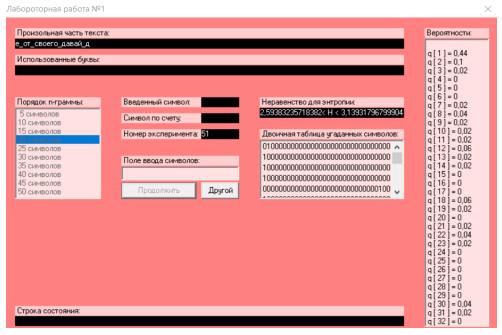
Ентропія: 4.1540726784296265

Надлишковість: 0.18346869391409937

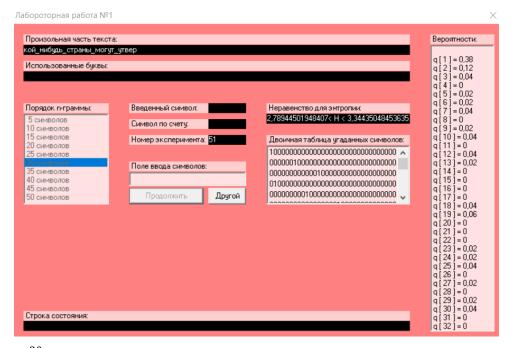
## Робота з CoolPinkProgram



 $2.26415 < H^{10} < 2.96192$ 



# $2.59383 < H^{20} < 3.13931$



 $2.78944 < H^{30} < 3.34435$ 

#### Висновки:

У ході виконання роботи, я навчилась вимірювати частоти повторювання символів та біграм у тексті, визначати ентропію і надлишковість мови. Також помітила, що у тексті без пробілів ентропія більша, ніж у тексті з пробілами. Тому перед шифруванням усі пробіли варто видаляти.