КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ, ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Лабораторна робота №4

З дисципліни «Захист інформації у комп'ютерних системах»

«Дослідження частотних характеристик української мови»

Виконав
Юрченко П. А.
Студент 4 курсу СА

Київ 2024

Мета: дослідити вірогіднісні параметри появи літер української мови для різних типів текстів. Аналіз найбільш імовірних літер, біграм та триграм для використання в частотному криптоаналізі.

Хід роботи

1. Знаходження відносної частоти появи літер українського алфавіту

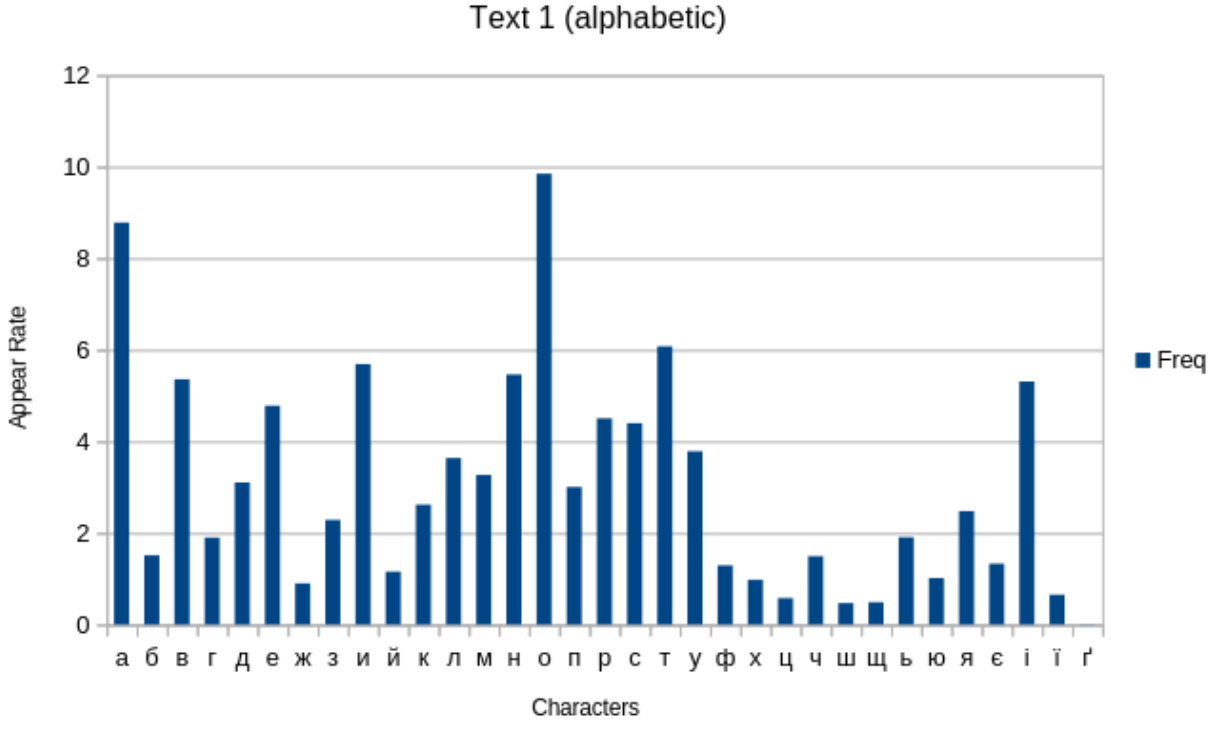
Створіть програму (будь-якою зручною для вас мовою), яка в якості аргументів приймає перелік текстових файлів, та аналізуючи їх вміст обраховує частоти появи літер українського алфавіту. Для спрощення аналізу з тексту виключаються всі знаки пунктуації окрім “пробілу”.

Для аналізу відносної частоти появи літер в українській мові було використано текст переказу “Фауста” та перша глава “Життєвої філософії кота Мура” (приблизно 20к символів кожен).

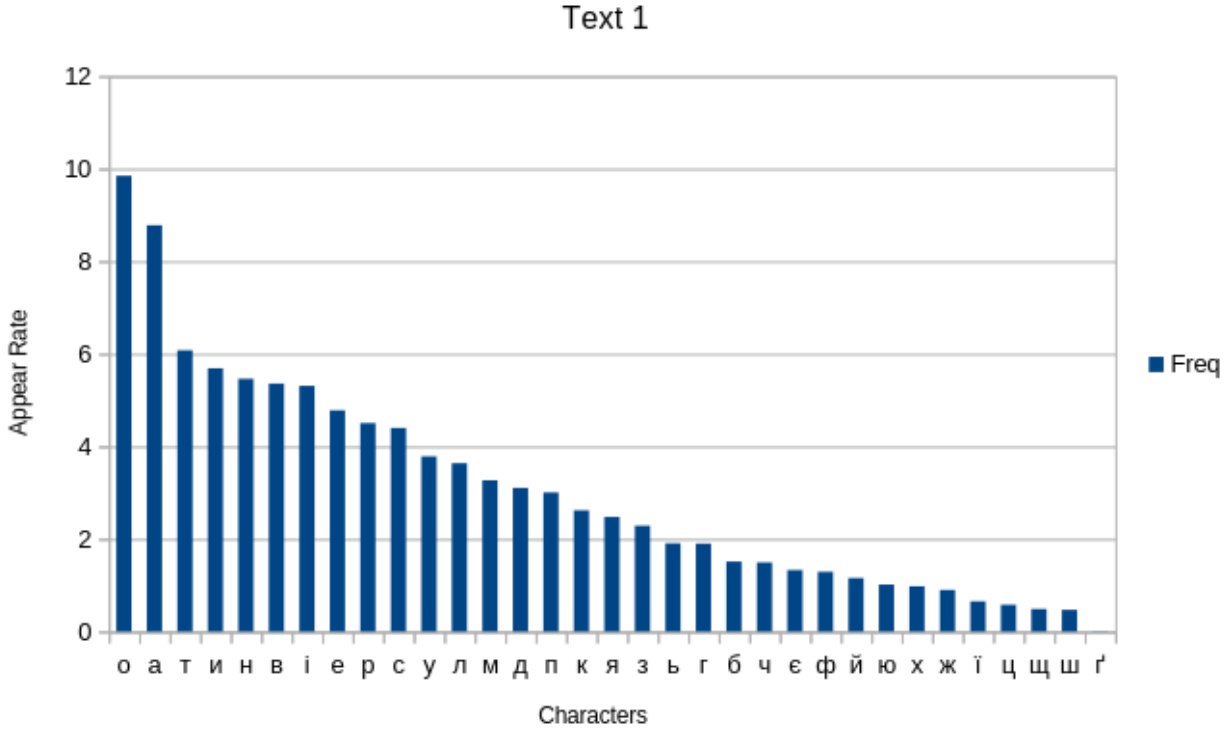
Код для проведення аналізу був написаний на JavaScript.

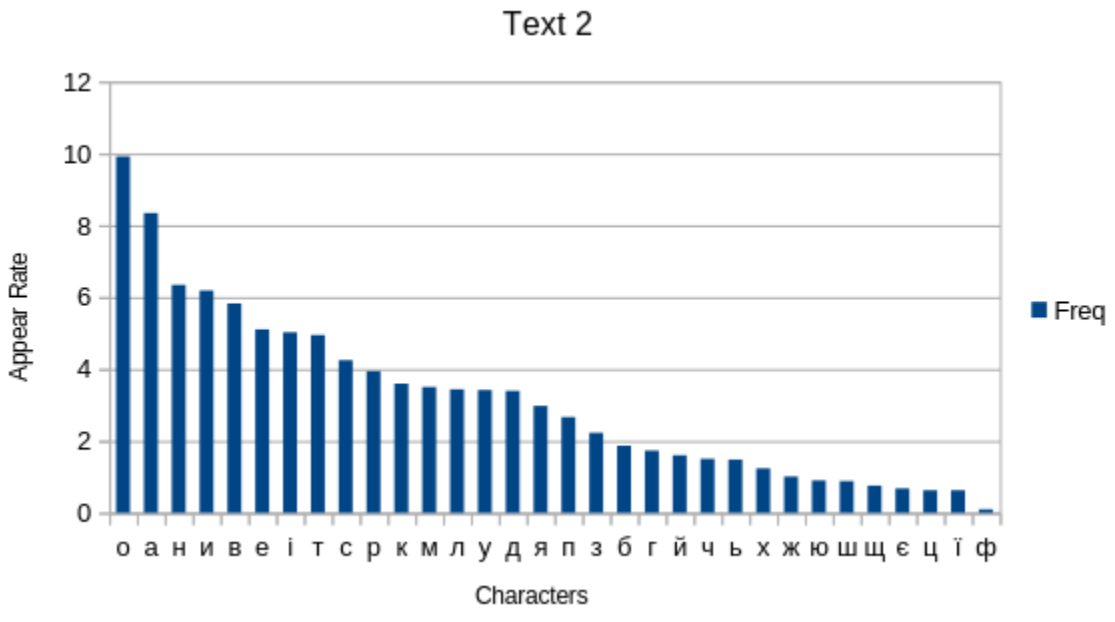
Посилання на репозиторій з кодом.

діаграму відсортовану в алфавітному порядку



діаграму відсортовану по частотам появи літер





послідовність літер по мірі спадання частоти появи

Text 1:

о а т и н в і е р с у л м д п к я з ь г б ч є ф й ю х ж ї ц щ ш ґ

Text 2:

о а н и в е і т с р к м л ю д я п з б г й ч ь х ж ю ш щ є ц ї ф

2. Знаходження відносної частоти появи біграм українського алфавіту

Аналогічно до першого завдання, створіть програму яка підрахує відносні частоти появи біграм української мови аналізуючи вміст текстів, що задаються.

Написав знову ж таки на JavaScript.

Для текстів, що були використані в першому завданні проаналізуйте отримані результаті та в звіті наведіть:

таблицю з відносними частотами біграм, відсортовану за спаданням частоти

На жаль, помістилися далеко не всі біграми, але наводжу певний список відсортований за зростанням частоти для обох текстів.

Char	Freq (Text 1)
ст	2.13403219767877
на	1.55746911269188
по	1.46012729314863
ві	1.45263946087608
ро	1.30288281542493
ов	1.28790715087982
та	1.25795582178959
то	1.25795582178959
ть	1.22800449269936
ог	1.08573567952078
го	1.05578435043055
ар	1.01834518906776
ти	1.01834518906776
ом	1.00336952452265
ит	0.988393859977537
во	0.950954698614751
ер	0.906027704979408
ри	0.906027704979408
пр	0.883564208161737
ус	0.883564208161737
ни	0.87607637588918
ає	0.868588543616623
не	0.838637214526395
ся	0.838637214526395
за	0.808685885436166
ол	0.808685885436166
до	0.793710220891052
ід	0.786222388618495
іс	0.786222388618495
ло	0.771246724073381

Char	Freq (Text 2)
на	1.73747794217456
не	1.3302565494774
то	1.13343287634044
ві	1.1198588299172
ро	1.11307180670558
ов	1.09949776028234
го	1.07234966743586
ав	1.051988597801
ти	1.04520157458939
ст	1.01805348174291
ог	1.00447943531967
ви	0.984118365684811
ні	0.977331342473191
ко	0.970544319261572
ен	0.929822179991856
по	0.916248133568617
во	0.902674087145378
ни	0.868738971087281
но	0.868738971087281
та	0.868738971087281
до	0.855164924664042
ал	0.848377901452423
ли	0.848377901452423
пр	0.848377901452423
ра	0.848377901452423
ер	0.841590878240804
ом	0.828016831817565
ка	0.821229808605945
ло	0.814442785394326
як	0.787294692547849

послідовність з 30-ти найбільш імовірних біграм

Текст 1:

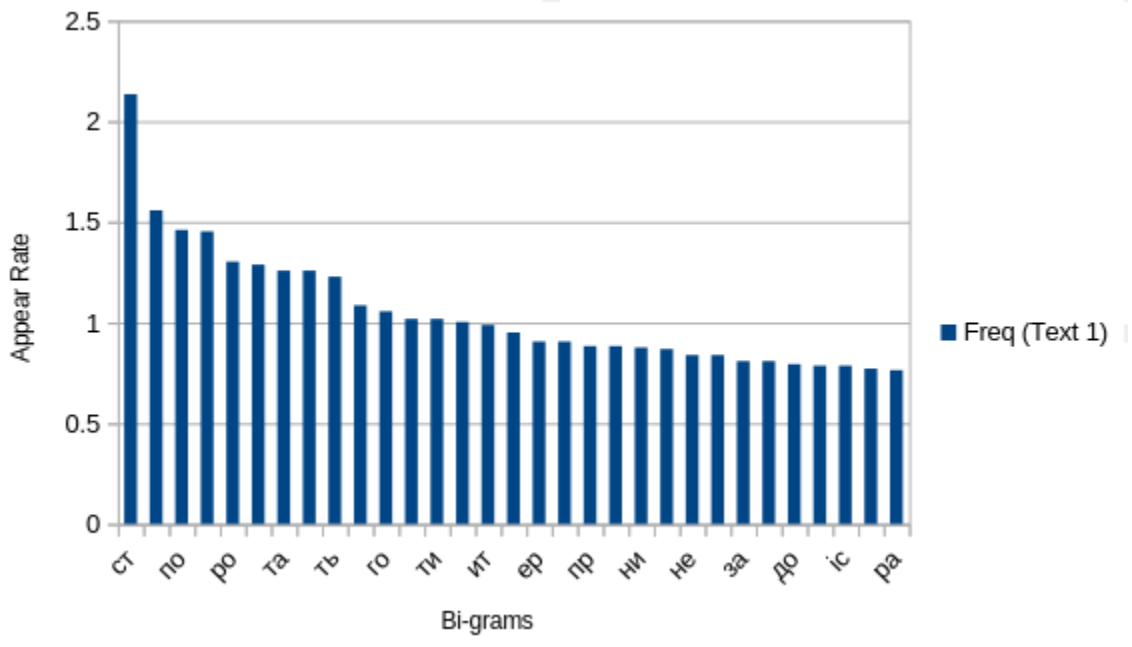
на не то ві ро ов го ав ти ст ог ви ні ко ен по во ни но та до ал ли пр ра ер ом ка ло як

Текст 2:

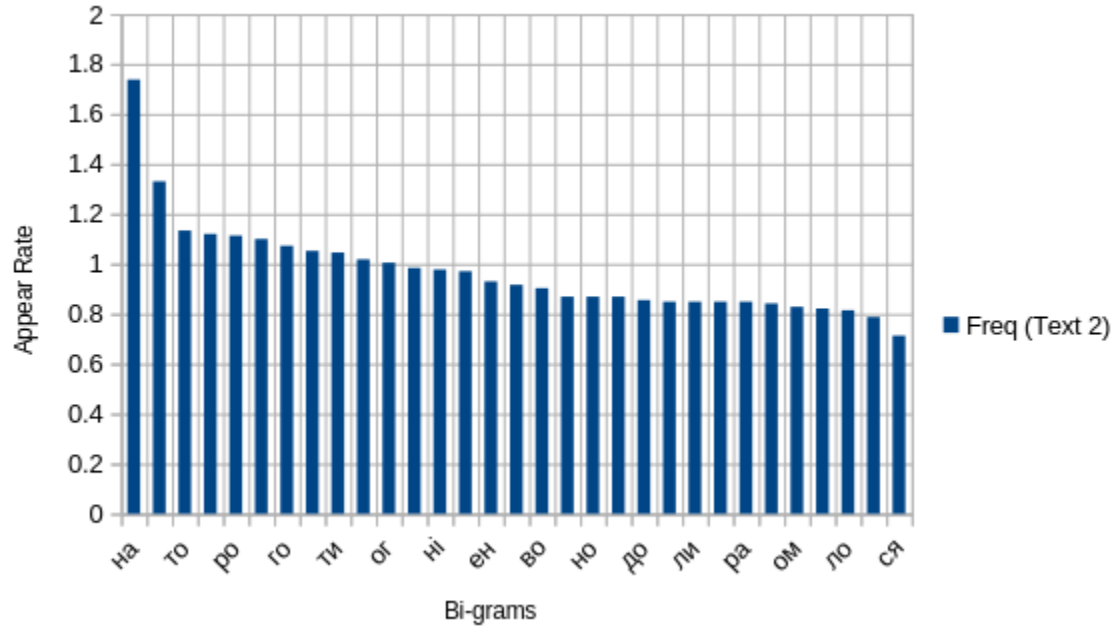
ст на по ві ро ов та то ть ог го ар ти ом ит во ер ри пр ус ниає не ся за ол до ід іс ло

діаграму відсортовану по частотам появи 30-ти найбільш імовірних біграм

Текст 1:

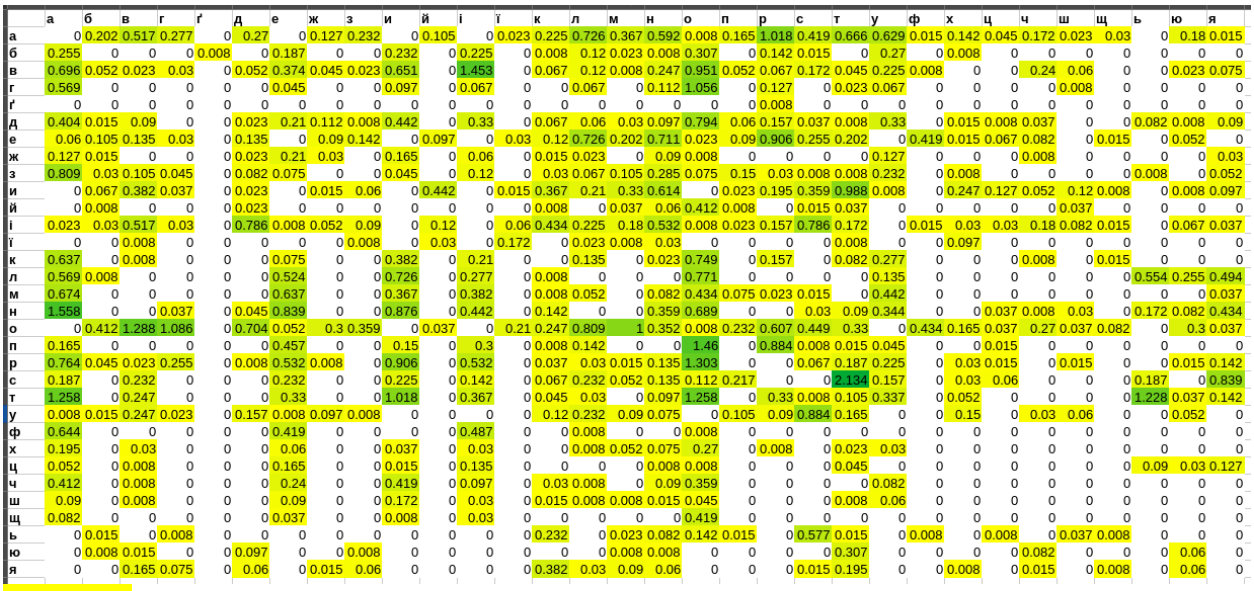


Текст 2:



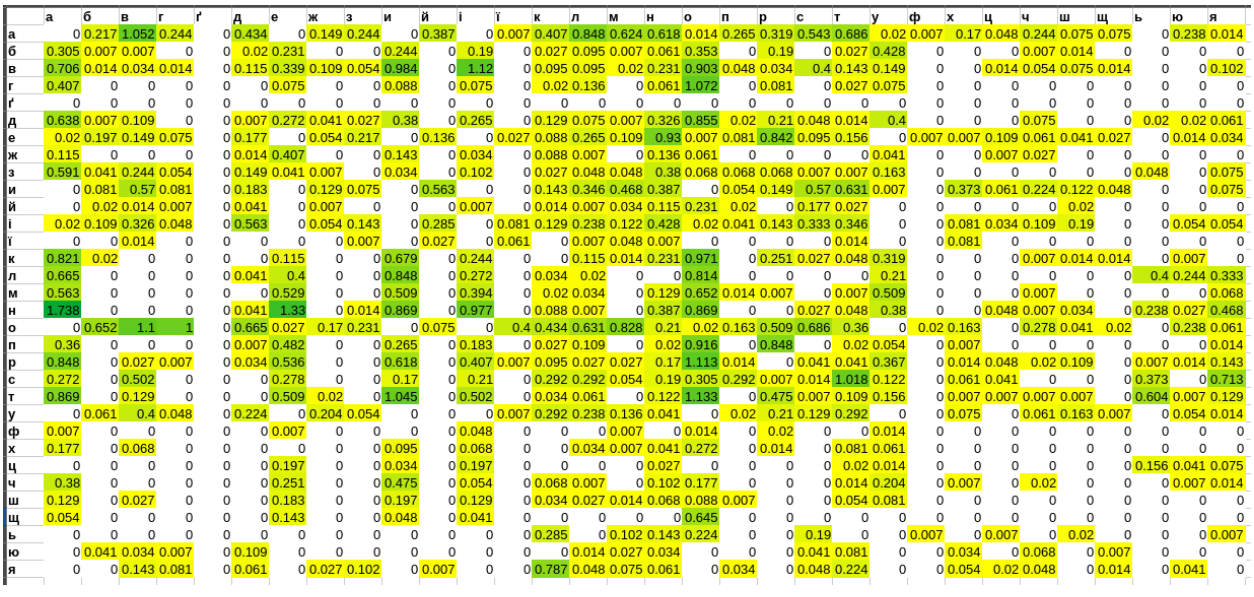
матрицю частот появи біграм (імовірність позначена кольором)

Текст 1:



	а	б	в	г	ґ	д	е	ж	з	и	й	і	ї	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
а	0	0.202	0.517	0.277	0	0.27	0	0.127	0.232	0	0.105	0	0.023	0.225	0.726	0.367	0.592	0.008	0.165	1.018	0.419	0.666	0.629	0.015	0.142	0.045	0.172	0.023	0.03	0	0.18	0.015
б	0.255	0	0	0	0.008	0	0.187	0	0	0.232	0	0.225	0	0.008	0.12	0.023	0.008	0.307	0	0.142	0.015	0	0.27	0	0.008	0	0	0	0	0	0	0
в	0.696	0.052	0.023	0.03	0	0.052	0.374	0.045	0.023	0.651	0	1.453	0	0.067	0.12	0.008	0.247	0.951	0.052	0.067	0.172	0.045	0.225	0.008	0	0	0.24	0.06	0	0	0.023	0.075
г	0.569	0	0	0	0	0	0.045	0	0	0.097	0	0.067	0	0	0.067	0	0.112	1.056	0	0.127	0	0.023	0.067	0	0	0	0	0.008	0	0	0	0
ґ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.008	0	0	0	0	0	0	0	0	0	0	0	0
д	0.404	0.015	0.09	0	0	0.023	0.21	0.112	0.008	0.442	0	0.33	0	0.067	0.06	0.03	0.097	0.794	0.06	0.157	0.037	0.008	0.33	0	0.015	0.008	0.037	0	0	0.082	0.008	0.09
е	0.06	0.105	0.135	0.03	0	0.135	0	0.09	0.142	0	0.097	0	0.03	0.12	0.726	0.202	0.711	0.023	0.09	0.906	0.255	0.202	0	0.419	0.015	0.067	0.082	0	0.015	0	0.052	0
ж	0.127	0.015	0	0	0	0.023	0.21	0.03	0	0.165	0	0.06	0	0.015	0.023	0	0.09	0.008	0	0	0	0	0.127	0	0	0	0.008	0	0	0	0	0.03
з	0.809	0.03	0.105	0.045	0	0.082	0.075	0	0	0.045	0	0.12	0	0.03	0.067	0.105	0.285	0.075	0.15	0.03	0.008	0.008	0.232	0	0.008	0	0	0	0	0.008	0	0.052
и	0	0.067	0.382	0.037	0	0.023	0	0.015	0.06	0	0.442	0	0.015	0.367	0.21	0.33	0.614	0	0.023	0.195	0.359	0.988	0.008	0	0.247	0.127	0.052	0.12	0.008	0	0.008	0.097
й	0	0.008	0	0	0	0.023	0	0	0	0	0	0	0	0.008	0	0.037	0.06	0.412	0.008	0	0.015	0.037	0	0	0	0	0	0.037	0	0	0	0
і	0.023	0.03	0.517	0.03	0	0.786	0.008	0.052	0.09	0	0.12	0	0.06	0.434	0.225	0.18	0.532	0.008	0.023	0.157	0.786	0.172	0	0.015	0.03	0.03	0.18	0.082	0.015	0	0.067	0.037
ї	0	0	0.008	0	0	0	0	0	0.008	0	0.03	0	0.172	0	0.023	0.008	0.03	0	0	0	0	0.008	0	0	0.097	0	0	0	0	0	0	0
к	0.637	0	0.008	0	0	0	0.075	0	0	0.382	0	0.21	0	0	0.135	0	0.023	0.749	0	0.157	0	0.082	0.277	0	0	0	0.008	0	0.015	0	0	0
л	0.569	0.008	0	0	0	0	0.524	0	0	0.726	0	0.277	0	0.008	0	0	0	0.771	0	0	0	0	0.135	0	0	0	0	0	0	0.554	0.255	0.494
м	0.674	0	0	0	0	0	0.637	0	0	0.367	0	0.382	0	0.008	0.052	0	0.082	0.434	0.075	0.023	0.015	0	0.442	0	0	0	0	0	0	0	0	0.037
н	1.558	0	0	0.037	0	0.045	0.839	0	0	0.876	0	0.442	0	0.142	0	0	0.359	0.689	0	0	0.03	0.09	0.344	0	0	0.037	0.008	0.03	0	0.172	0.082	0.434
о	0	0.412	1.288	1.086	0	0.704	0.052	0.3	0.359	0	0.037	0	0.21	0.247	0.809	1	0.352	0.008	0.232	0.607	0.449	0.33	0	0.434	0.165	0.037	0.27	0.037	0.082	0	0.3	0.037
п	0.165	0	0	0	0	0	0.457	0	0	0.15	0	0.3	0	0.008	0.142	0	0	1.46	0	0.884	0.008	0.015	0.045	0	0	0.015	0	0	0	0	0	0
р	0.764	0.045	0.023	0.255	0	0.008	0.532	0.008	0	0.906	0	0.532	0	0.037	0.03	0.015	0.135	1.303	0	0	0.067	0.187	0.225	0	0.03	0.015	0	0.015	0	0	0.015	0.142
с	0.187	0	0.232	0	0	0	0.232	0	0	0.225	0	0.142	0	0.067	0.232	0.052	0.135	0.112	0.217	0	0	2.134	0.157	0	0.03	0.06	0	0	0	0.187	0	0.839
т	1.258	0	0.247	0	0	0	0.33	0	0	1.018	0	0.367	0	0.045	0.03	0	0.097	1.258	0	0.33	0.008	0.105	0.337	0	0.052	0	0	0	0	1.228	0.037	0.142
у	0.008	0.015	0.247	0.023	0	0.157	0.008	0.097	0.008	0	0	0	0	0.12	0.232	0.09	0.075	0	0.105	0.09	0.884	0.165	0	0	0.15	0	0.03	0.06	0	0	0.052	0
ф	0.644	0	0	0	0	0	0.419	0	0	0	0	0.487	0	0	0.008	0	0	0.008	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
х	0.195	0	0.03	0	0	0	0.06	0	0	0.037	0	0.03	0	0	0.008	0.052	0.075	0.27	0	0.008	0	0.023	0.03	0	0	0	0	0	0	0	0	0	0
ц	0.052	0	0.008	0	0	0	0.165	0	0	0.015	0	0.135	0	0	0	0	0.008	0.008	0	0	0	0.045	0	0	0	0	0	0	0	0.09	0.03	0.127
ч	0.412	0	0.008	0	0	0	0.24	0	0	0.419	0	0.097	0	0.03	0.008	0	0.09	0.359	0	0	0	0	0.082	0	0	0	0	0	0	0	0	0	0
ш	0.09	0	0.008	0	0	0	0.09	0	0	0.172	0	0.03	0	0.015	0.008	0.008	0.015	0.045	0	0	0	0.008	0.06	0	0	0	0	0	0	0	0	0	0
щ	0.082	0	0	0	0	0	0.037	0	0	0.008	0	0.03	0	0	0	0	0	0.419	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ь	0	0.015	0	0.008	0	0	0	0	0	0	0	0	0	0.232	0	0.023	0.082	0.142	0.015	0	0.577	0.015	0	0.008	0	0.008	0	0.037	0.008	0	0	0
ю	0	0.008	0.015	0	0	0.097	0	0	0.008	0	0	0	0	0	0	0.008	0.008	0	0	0	0	0.307	0	0	0	0	0.082	0	0	0	0.06	0
я	0	0	0.165	0.075	0	0.06	0	0.015	0.06	0	0	0	0	0.382	0.03	0.09	0.06	0	0	0	0.015	0.195	0	0	0.008	0	0.015	0	0.008	0	0.06	0

Текст 2:



	а	б	в	г	ґ	д	е	ж	з	и	й	і	ї	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
а	0	0.217	1.052	0.244	0	0.434	0	0.149	0.244	0	0.387	0	0.007	0.407	0.848	0.624	0.618	0.014	0.265	0.319	0.543	0.686	0.02	0.007	0.17	0.048	0.244	0.075	0.075	0	0.238	0.014
б	0.305	0.007	0.007	0	0	0.02	0.231	0	0	0.244	0	0.19	0	0.027	0.095	0.007	0.061	0.353	0	0.19	0	0.027	0.428	0	0	0	0.007	0.014	0	0	0	0
в	0.706	0.014	0.034	0.014	0	0.115	0.339	0.109	0.054	0.984	0	1.12	0	0.095	0.095	0.02	0.231	0.903	0.048	0.034	0.4	0.143	0.149	0	0	0.014	0.054	0.075	0.014	0	0	0.102
г	0.407	0	0	0	0	0	0.075	0	0	0.088	0	0.075	0	0.02	0.136	0	0.061	1.072	0	0.081	0	0.027	0.075	0	0	0	0	0	0	0	0	0
ґ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
д	0.638	0.007	0.109	0	0	0.007	0.272	0.041	0.027	0.38	0	0.265	0	0.129	0.075	0.007	0.326	0.855	0.02	0.21	0.048	0.014	0.4	0	0	0	0.075	0	0	0.02	0.02	0.061
е	0.02	0.197	0.149	0.075	0	0.177	0	0.054	0.217	0	0.136	0	0.027	0.088	0.265	0.109	0.93	0.007	0.081	0.842	0.095	0.156	0	0.007	0.007	0.109	0.061	0.041	0.027	0	0.014	0.034
ж	0.115	0	0	0	0	0.014	0.407	0	0	0.143	0	0.034	0	0.088	0.007	0	0.136	0.061	0	0	0	0	0.041	0	0	0.007	0.027	0	0	0	0	0
з	0.591	0.041	0.244	0.054	0	0.149	0.041	0.007	0	0.034	0	0.102	0	0.027	0.048	0.048	0.38	0.068	0.068	0.068	0.007	0.007	0.163	0	0	0	0	0	0	0.048	0	0.075
и	0	0.081	0.57	0.081	0	0.183	0	0.129	0.075	0	0.563	0	0	0.143	0.346	0.468	0.387	0	0.054	0.149	0.57	0.631	0.007	0	0.373	0.061	0.224	0.122	0.048	0	0	0.075
й	0	0.02	0.014	0.007	0	0.041	0	0.007	0	0	0.007	0	0	0.014	0.007	0.034	0.115	0.231	0.02	0	0.177	0.027	0	0	0	0	0	0.02	0	0	0	0
і	0.02	0.109	0.326	0.048	0	0.563	0	0.054	0.143	0	0.285	0	0.081	0.129	0.238	0.122	0.428	0.02	0.041	0.143	0.333	0.346	0	0	0.081	0.034	0.109	0.19	0	0	0.054	0.054
ї	0	0	0.014	0	0	0	0	0	0.007	0	0.027	0	0.061	0	0.007	0.048	0.007	0	0	0	0	0.014	0	0	0.081	0	0	0	0	0	0	0
к	0.821	0.02	0	0	0	0	0.115	0	0	0.679	0	0.244	0	0	0.115	0.014	0.231	0.971	0	0.251	0.027	0.048	0.319	0	0	0	0.007	0.014	0.014	0	0.007	0
л	0.665	0	0	0	0	0.041	0.4	0	0	0.848	0	0.272	0	0.034	0.02	0	0	0.814	0	0	0	0	0.21	0	0	0	0	0	0	0.4	0.244	0.333
м	0.563	0	0	0	0	0	0.529	0	0	0.509	0	0.394	0	0.02	0.034	0	0.129	0.652	0.014	0.007	0	0.007	0.509	0	0	0	0.007	0	0	0	0	0.068
н	1.738	0	0	0	0	0.041	1.33	0	0.014	0.869	0	0.977	0	0.088	0.007	0	0.387	0.869	0	0	0.027	0.048	0.38	0	0	0.048	0.007	0.034	0	0.238	0.027	0.468
о	0	0.652	1.1	1	0	0.665	0.027	0.17	0.231	0	0.075	0	0.4	0.434	0.631	0.828	0.21	0.02	0.163	0.509	0.686	0.36	0	0.02	0.163	0	0.278	0.041	0.02	0	0.238	0.061
п	0.36	0	0	0	0	0.007	0.482	0	0	0.265	0	0.183	0	0.027	0.109	0	0.02	0.916	0	0.848	0	0.02	0.054	0	0.007	0	0	0	0	0	0	0.014
р	0.848	0	0.027	0.007	0	0.034	0.536	0	0	0.618	0	0.407	0.007	0.095	0.027	0.027	0.17	1.113	0.014	0	0.041	0.041	0.367	0	0.014	0.048	0.02	0.109	0	0.007	0.014	0.143
с	0.272	0	0.502	0	0	0	0.278	0	0	0.17	0	0.21	0	0.292	0.292	0.054	0.19	0.305	0.292	0.007	0.014	1.018	0.122	0	0.061	0.041	0	0	0	0.373	0	0.713
т	0.869	0	0.129	0	0	0	0.509	0.02	0	1.045	0	0.502	0	0.034	0.061	0	0.122	1.133	0	0.475	0.007	0.109	0.156	0	0.007	0.007	0.007	0.007	0	0.604	0.007	0.129
у	0	0.061	0.4	0.048	0	0.224	0	0.204	0.054	0	0	0	0.007	0.292	0.238	0.136	0.041	0	0.02	0.21	0.129	0.292	0	0	0.075	0	0.061	0.163	0.007	0	0.054	0.014
ф	0.007	0	0	0	0	0	0.007	0	0	0	0	0.048	0	0	0	0	0.007	0	0.014	0	0.02	0	0.014	0	0	0	0	0	0	0	0	0
х	0.177	0	0.068	0	0	0	0	0	0	0.095	0	0.068	0	0	0.034	0.007	0.041	0.272	0	0.014	0	0.081	0.061	0	0	0	0	0	0	0	0	0
ц	0	0	0	0	0	0	0.197	0	0	0.034	0	0.197	0	0	0	0	0.027	0	0	0	0	0.02	0.014	0	0	0	0	0	0	0.156	0.041	0.075
ч	0.38	0	0	0	0	0	0.251	0	0	0.475	0	0.054	0	0.068	0.007	0	0.102	0.177	0	0	0	0.014	0.204	0	0.007	0	0.02	0	0	0	0.007	0.014
ш	0.129	0	0.027	0	0	0	0.183	0	0	0.197	0	0.129	0	0.034	0.027	0.014	0.068	0.088	0.007	0	0	0.054	0.081	0	0	0	0	0	0	0	0	0
щ	0.054	0	0	0	0	0	0.143	0	0	0.048	0	0.041	0	0	0	0	0	0.645	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ь	0	0	0	0	0	0	0	0	0	0	0	0	0	0.285	0	0.102	0.143	0.224	0	0	0.19	0	0	0.007	0	0.007	0	0.02	0	0	0	0.007
ю	0	0.041	0.034	0.007	0	0.109	0	0	0	0	0	0	0	0	0.014	0.027	0.034	0	0	0	0.041	0.081	0	0	0.034	0	0.068	0	0.007	0	0	0
я	0	0	0.143	0.081	0	0.061	0	0.027	0.102	0	0.007	0	0	0.787	0.048	0.075	0.061	0	0.034	0	0.048	0.224	0	0	0.054	0.02	0.048	0	0.014	0	0.041	0

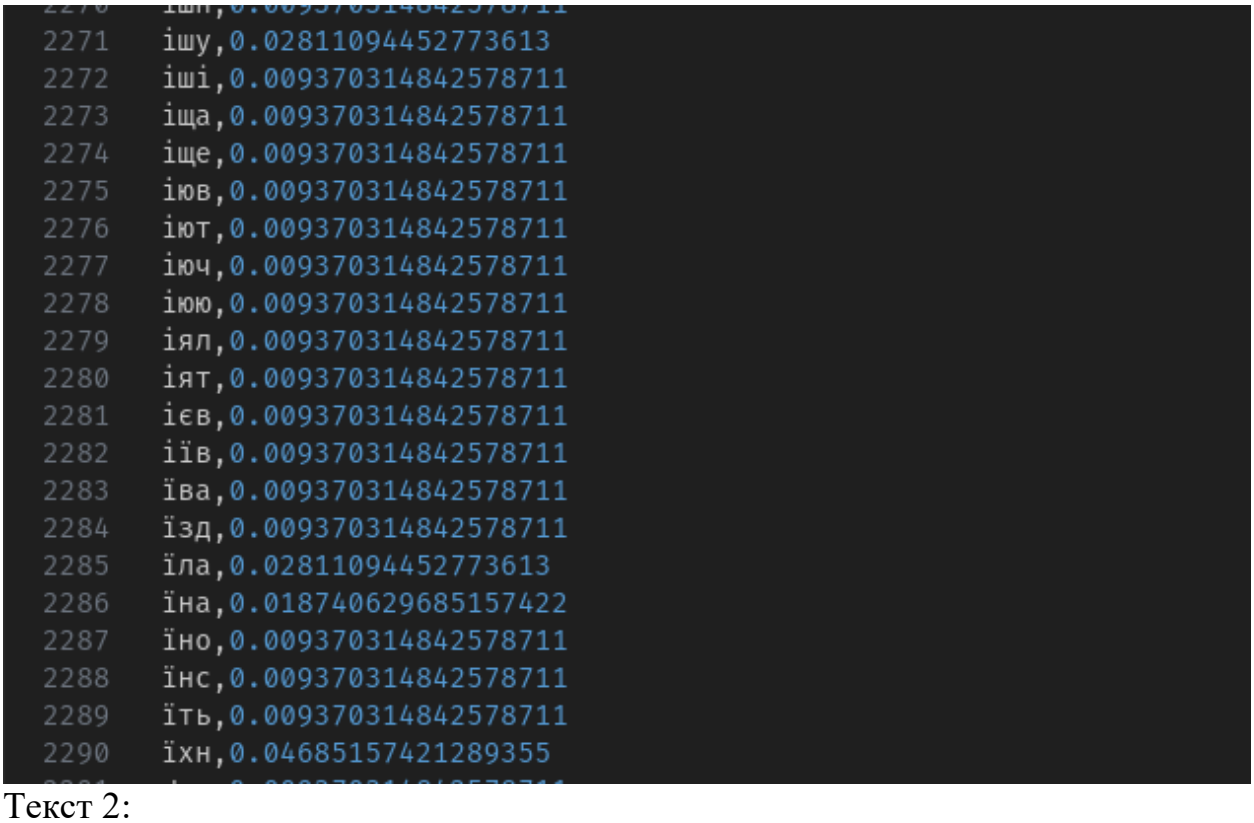
3. Знаходження відносної частоти появи триграм українського алфавіту

Для текстів, що були використані в першому завданні проаналізуйте отримані результаті та в звіті наведіть:

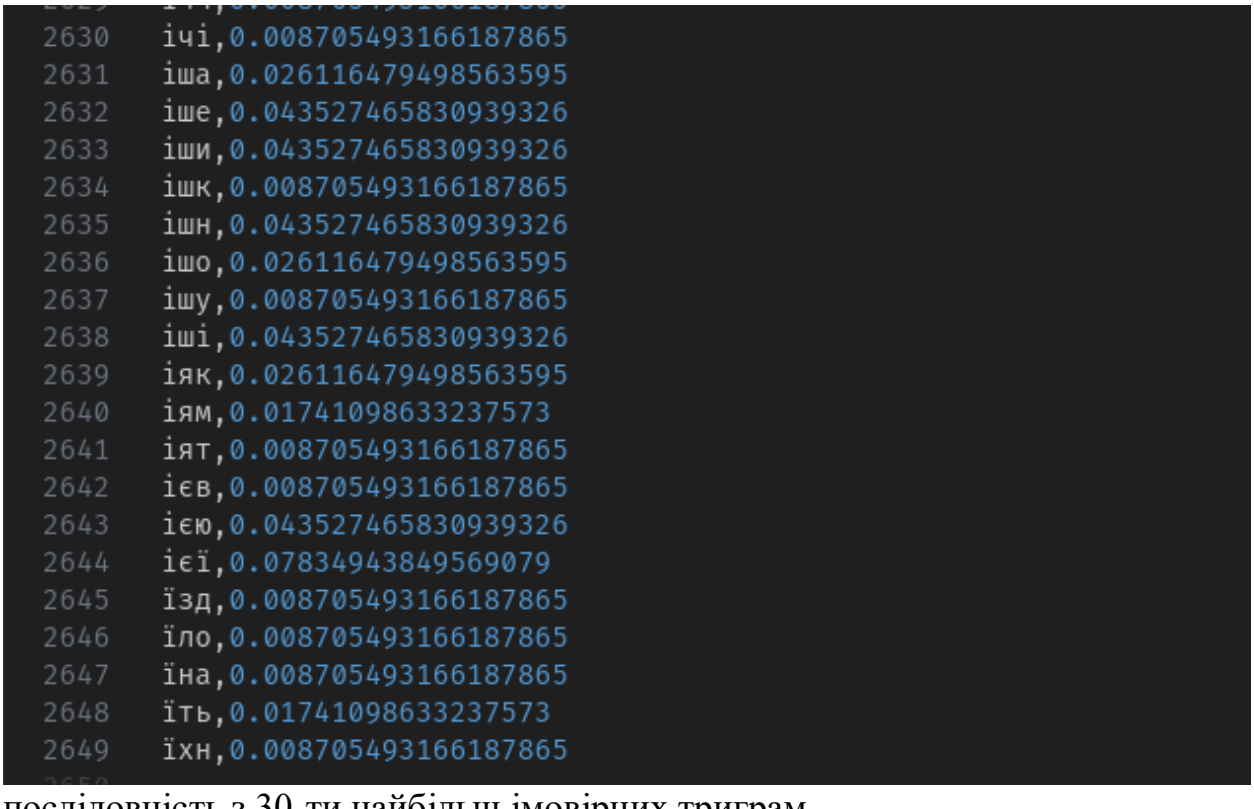
таблицю з відносними частотами триграм, відсортовану за спаданням частоти

Не думаю що це можливо вмістити 2000+ триграм в один екран таблиці тому, демонструю лише такі скріни.

Текст 1:



Текст 2:



послідовність з 30-ти найбільш імовірних триграм

Текст 1:

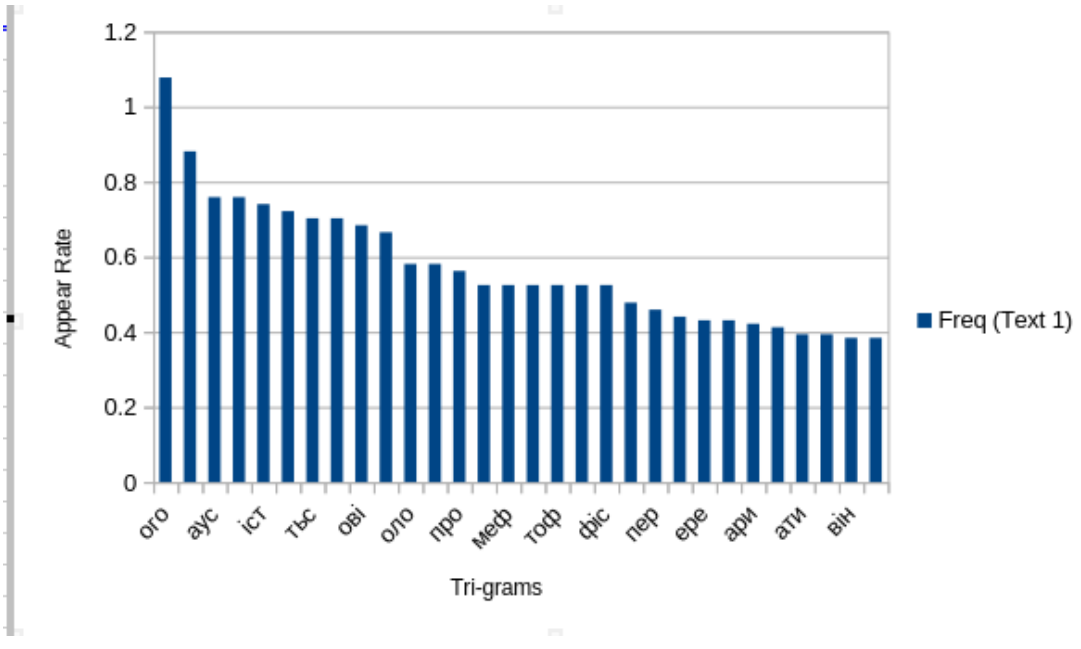
ого уст аус фау іст сто тьс ься ові від оло ста про ефі меф офе тоф фел фіс єть пер ому ере лов ари ель ати йог він при роз

Текст 2:

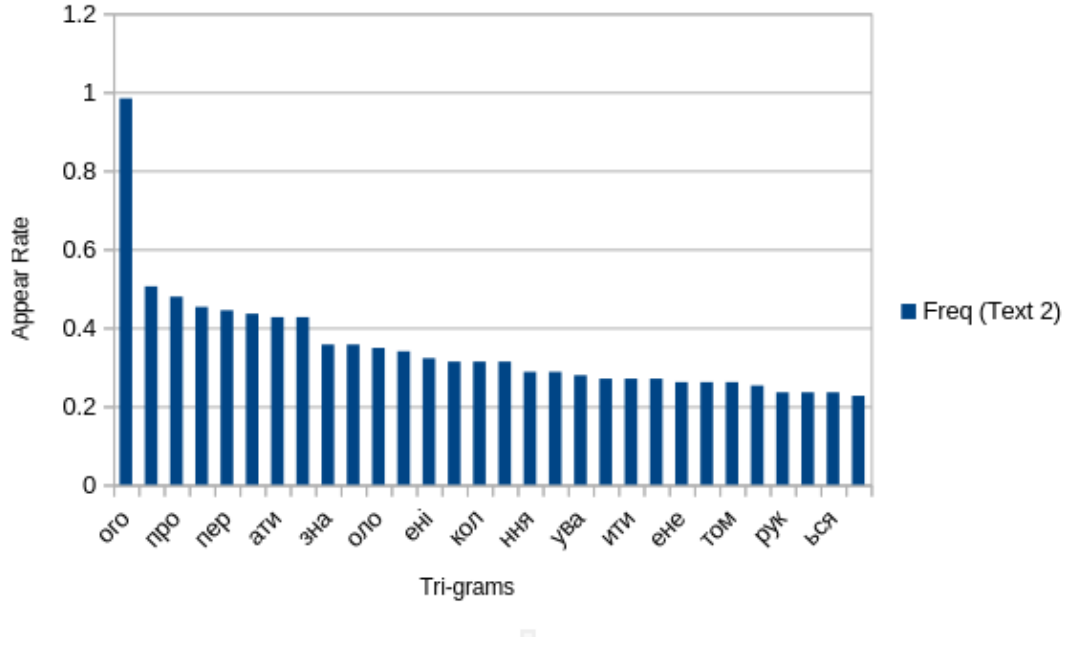
ого мен про від пер ому ати при зна так оло ере ені віт кол ові ння сво ува вся ити ово ене сам том сто рук тьс ься ага енн

діаграму відсортовану по частотам появи 30-ти найбільш імовірних триграм

Текст 1:



Текст 2:



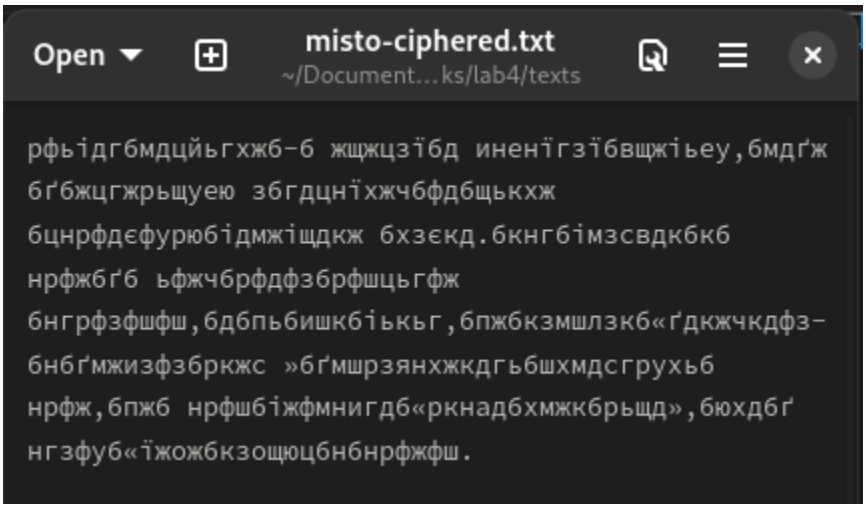
4. Криптоаналіз

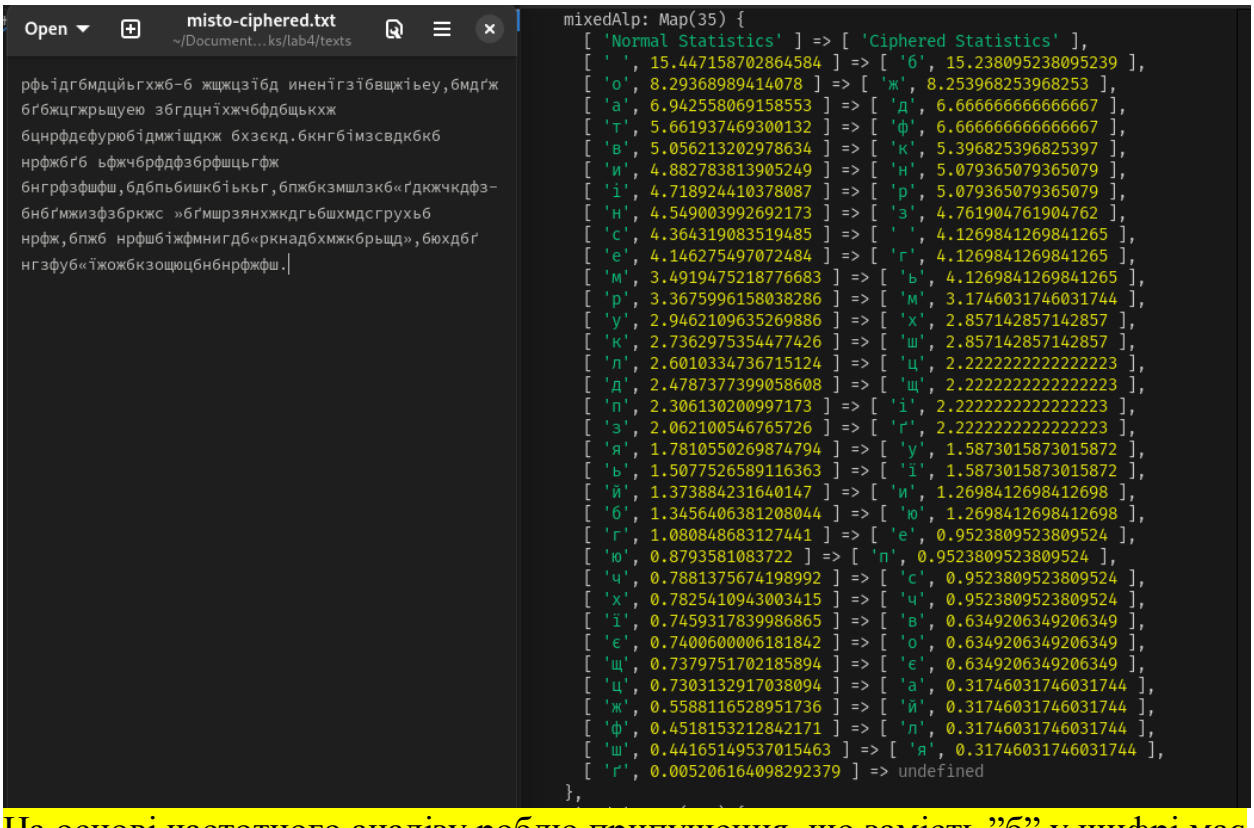
Зашифруйте за допомогою афінного шифру (a та b оберіть випадковим чином) фрагмент тексту та надайте отриманий шифротекст колегам.

Зашифрував та надав колегам.

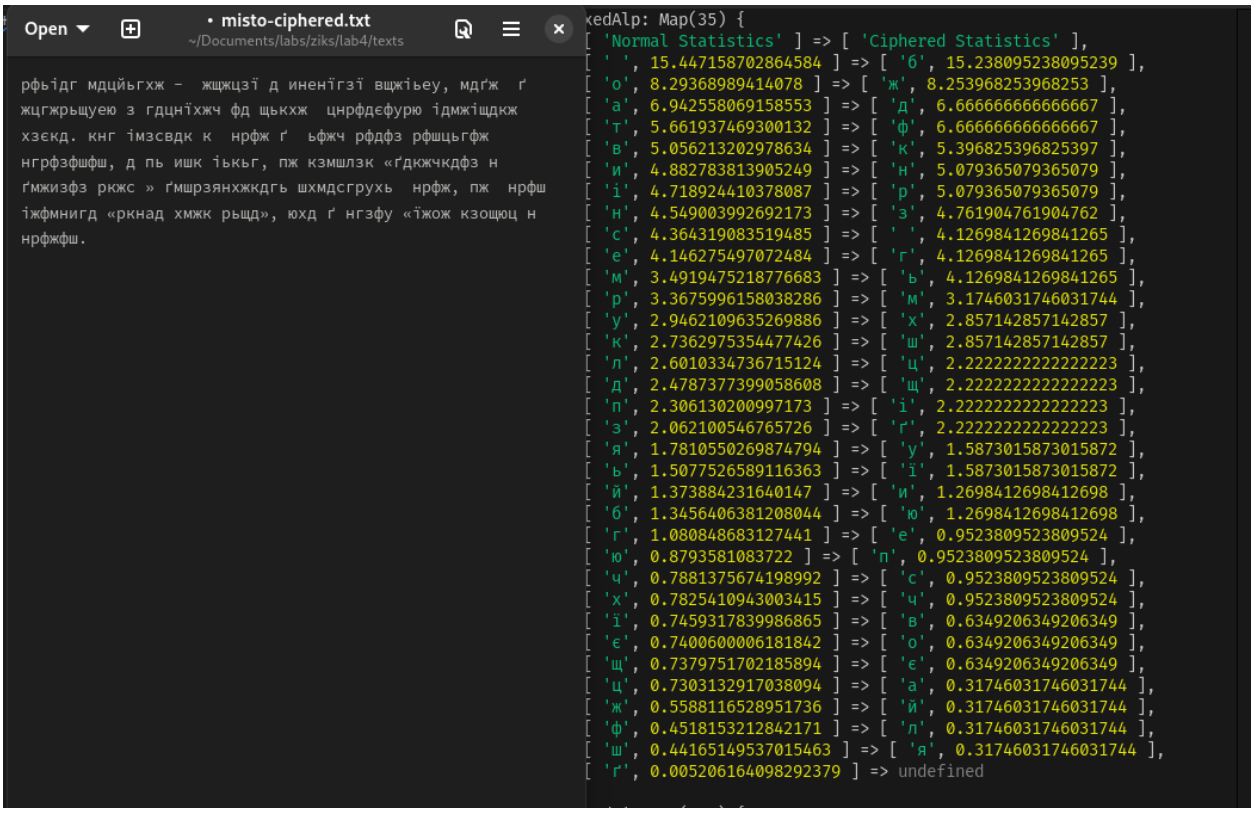
Отримайте шифротекст від колег, виконайте їх криптоаналіз та проілюструйте в звіті процес його проведення за допомогою частотного аналізу.

Отриманий шифротекст.

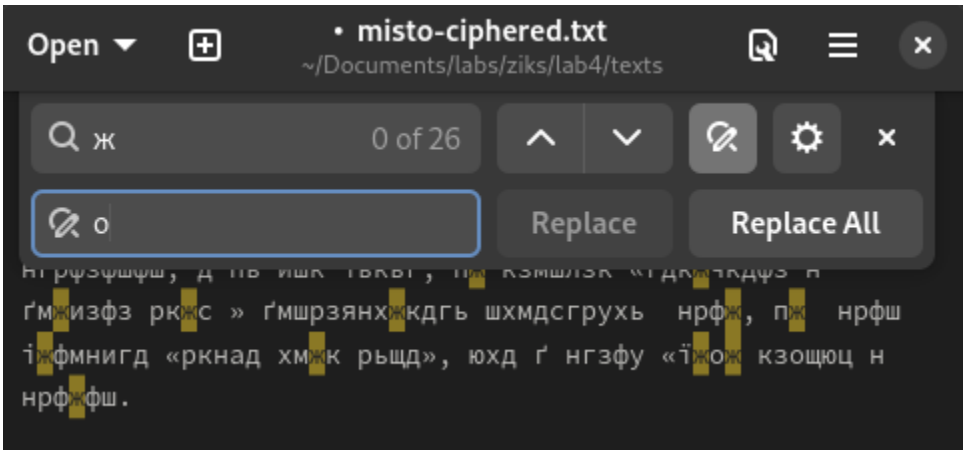




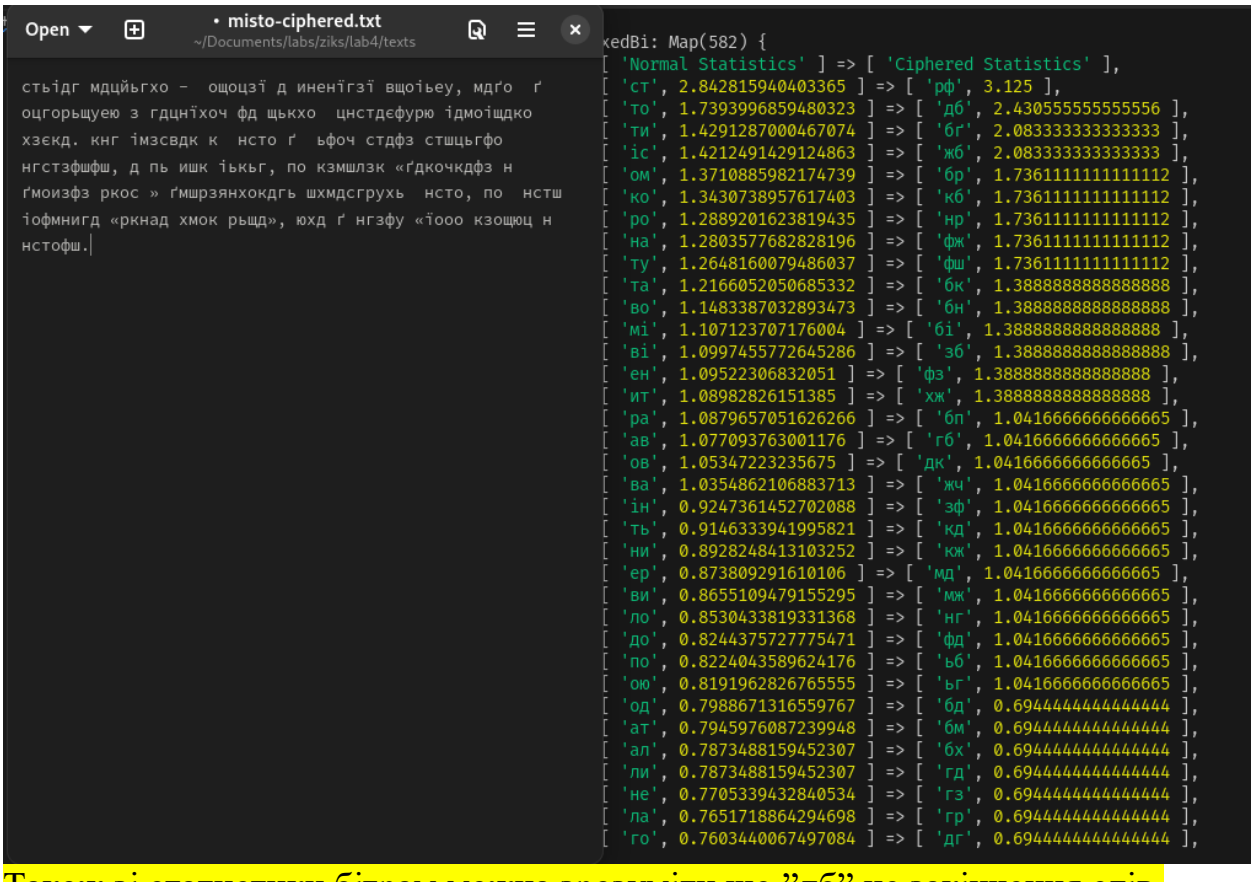
На основі частотного аналізу роблю припущення, що замість ”б” у шифрі має бути пробіл.



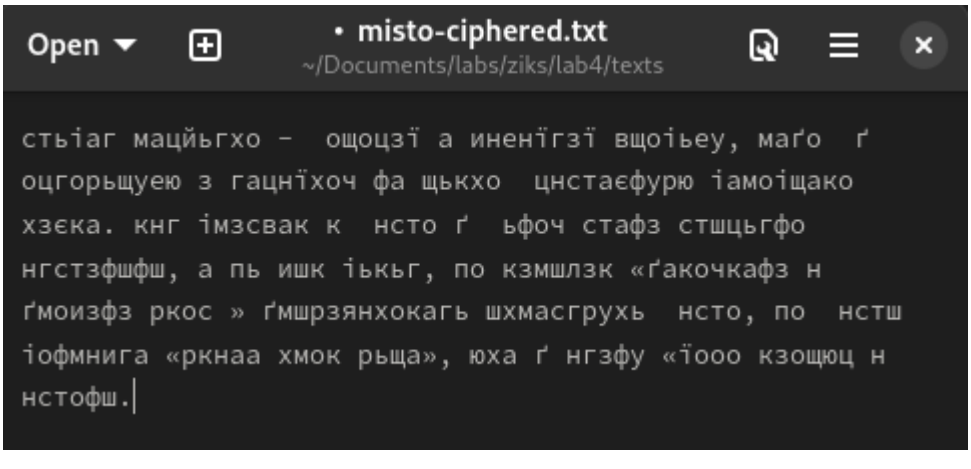
По аналогії припускаю, що замість ”ж” у шифрі має бути “о”.



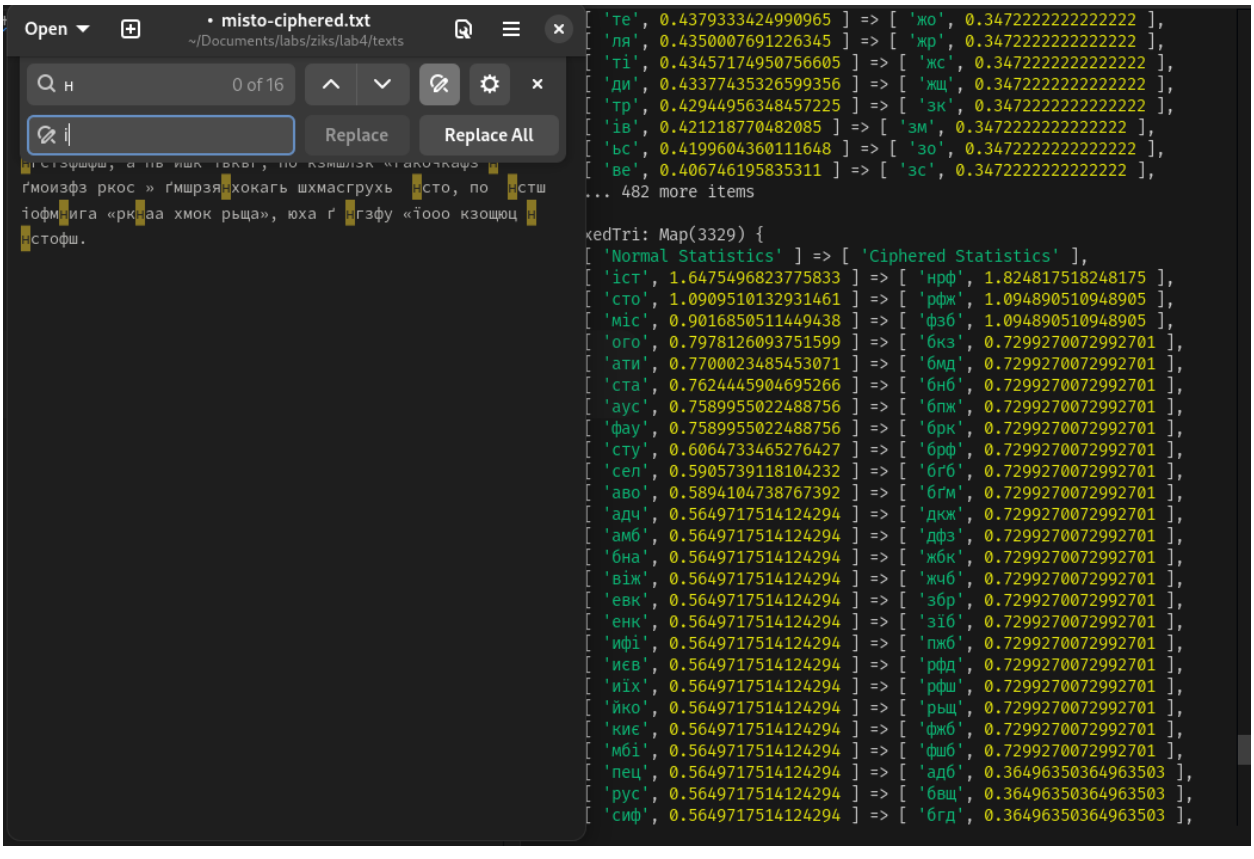
Цього разу зроблю припущення по частотах появи біграм, що “рф” це “ст”.

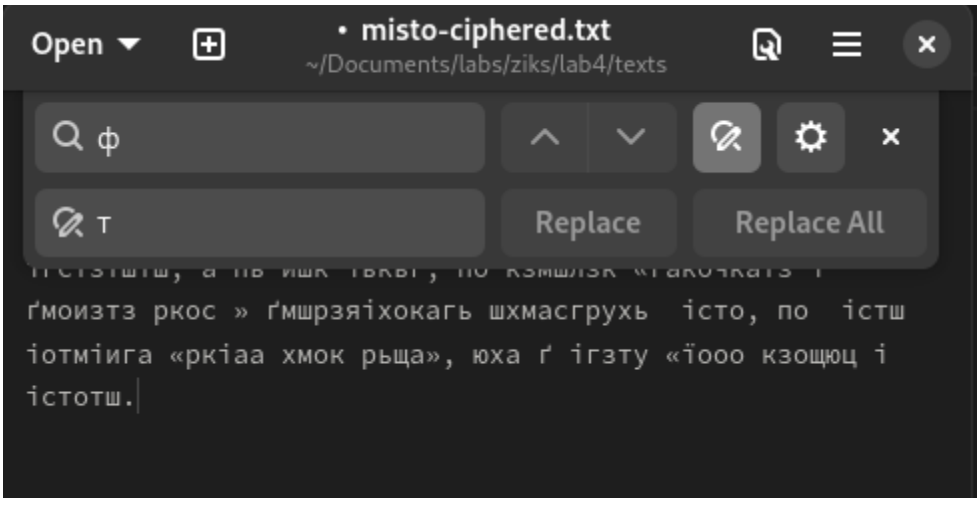


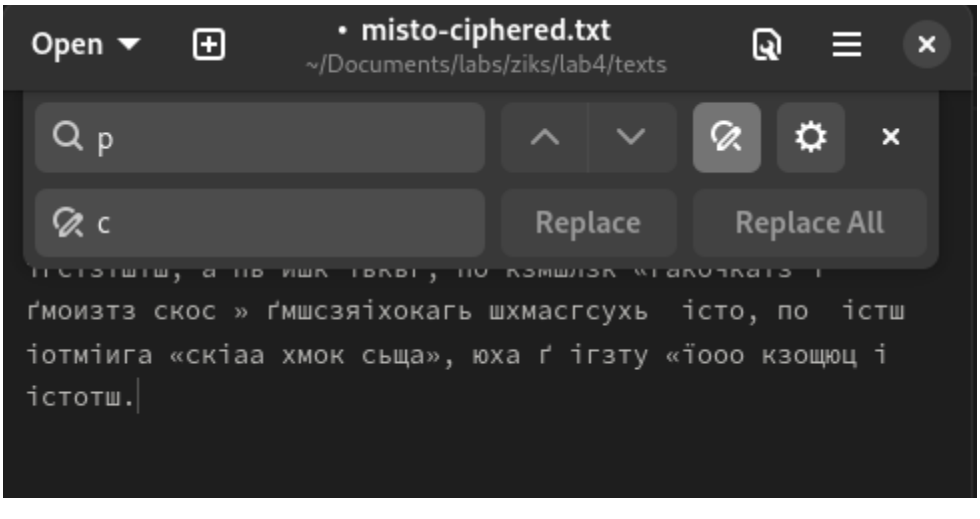
Також зі статистики біграм можна зрозуміти що ”дб” це закінчення слів, бо ”б” це пробіл. Також перевіривши частоту появи літер можна припустити, що ”д” - ”а”.



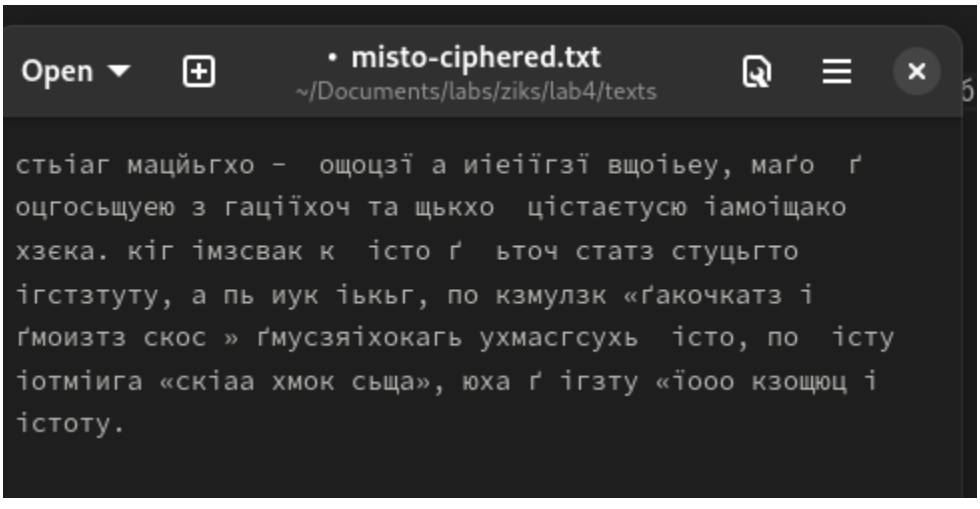
На основі триграм припускаю що “нрф” це “іст”, відповідно “н” це “і”.


Open
• misto-ciphered.txt
~/Documents/labs/ziks/lab4/texts
н
0 of 16
і
Replace
Replace All
ґмоизфз ркос » ґмшрзя хокагь шхмасгрухь сто, по стш
іофм ига «рк аа хмок рьща», юха ґ гзфу «їооо кзощюц
стофш.
['те', 0.4379333424990965] => ['жо', 0.3472222222222222],
['ля', 0.4350007691226345] => ['жр', 0.3472222222222222],
['ті', 0.43457174950756605] => ['жс', 0.3472222222222222],
['ди', 0.43377435326599356] => ['жщ', 0.3472222222222222],
['тр', 0.42944956348457225] => ['зк', 0.3472222222222222],
['ів', 0.421218770482085] => ['зм', 0.3472222222222222],
['ьс', 0.4199604360111648] => ['зо', 0.3472222222222222],
['ве', 0.406746195835311] => ['зс', 0.3472222222222222],
... 482 more items
kedTri: Map(3329) {
['Normal Statistics'] => ['Ciphered Statistics'],
['іст', 1.6475496823775833] => ['нрф', 1.824817518248175],
['сто', 1.0909510132931461] => ['рфж', 1.094890510948905],
['міс', 0.9016850511449438] => ['фзб', 1.094890510948905],
['ого', 0.7978126093751599] => ['бкз', 0.7299270072992701],
['ати', 0.7700023485453071] => ['бмд', 0.7299270072992701],
['ста', 0.7624445904695266] => ['бнб', 0.7299270072992701],
['аус', 0.7589955022488756] => ['бпж', 0.7299270072992701],
['фау', 0.7589955022488756] => ['брк', 0.7299270072992701],
['сту', 0.6064733465276427] => ['брф', 0.7299270072992701],
['сел', 0.5905739118104232] => ['бґб', 0.7299270072992701],
['аво', 0.5894104738767392] => ['бґм', 0.7299270072992701],
['адч', 0.5649717514124294] => ['дкж', 0.7299270072992701],
['амб', 0.5649717514124294] => ['дфз', 0.7299270072992701],
['бна', 0.5649717514124294] => ['жбк', 0.7299270072992701],
['віж', 0.5649717514124294] => ['жчб', 0.7299270072992701],
['евк', 0.5649717514124294] => ['збр', 0.7299270072992701],
['енк', 0.5649717514124294] => ['зїб', 0.7299270072992701],
['ифі', 0.5649717514124294] => ['пжб', 0.7299270072992701],
['иєв', 0.5649717514124294] => ['рфд', 0.7299270072992701],
['иїх', 0.5649717514124294] => ['рфш', 0.7299270072992701],
['йко', 0.5649717514124294] => ['рьщ', 0.7299270072992701],
['киє', 0.5649717514124294] => ['фжб', 0.7299270072992701],
['мбі', 0.5649717514124294] => ['фшб', 0.7299270072992701],
['пец', 0.5649717514124294] => ['адб', 0.36496350364963503],
['рус', 0.5649717514124294] => ['бвщ', 0.36496350364963503],
['сиф', 0.5649717514124294] => ['бгд', 0.36496350364963503],

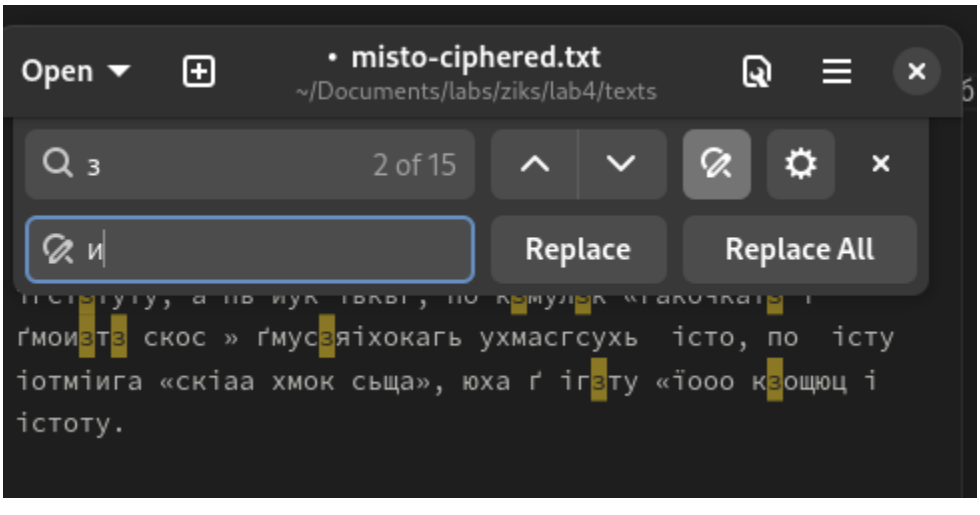

Open
• misto-ciphered.txt
~/Documents/labs/ziks/lab4/texts
ф
т
Replace
Replace All
ґмоизтз ркос » ґмшрзяіхокагь шхмасгрухь істо, по істш
іотміига «ркіаа хмок рьща», юха ґ ігзту «їооо кзощюц і
істотш.

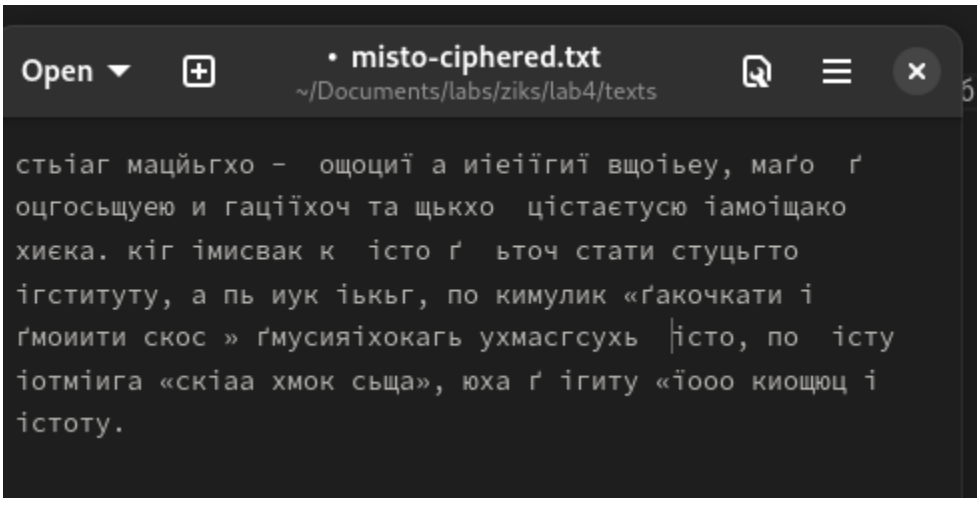

Open
• misto-ciphered.txt
~/Documents/labs/ziks/lab4/texts
р
с
Replace
Replace All
ґмоизтз скос » ґмшсзяіхокагь шхмасгсухь істо, по істш
іотміига «скіаа хмок сьща», юха ґ ігзту «їооо кзощюц і
істотш.

Бачу слово “істотш” це або “істота”, але “а” нам уже відоме, тому це “істоту” - “ш” це “у”.

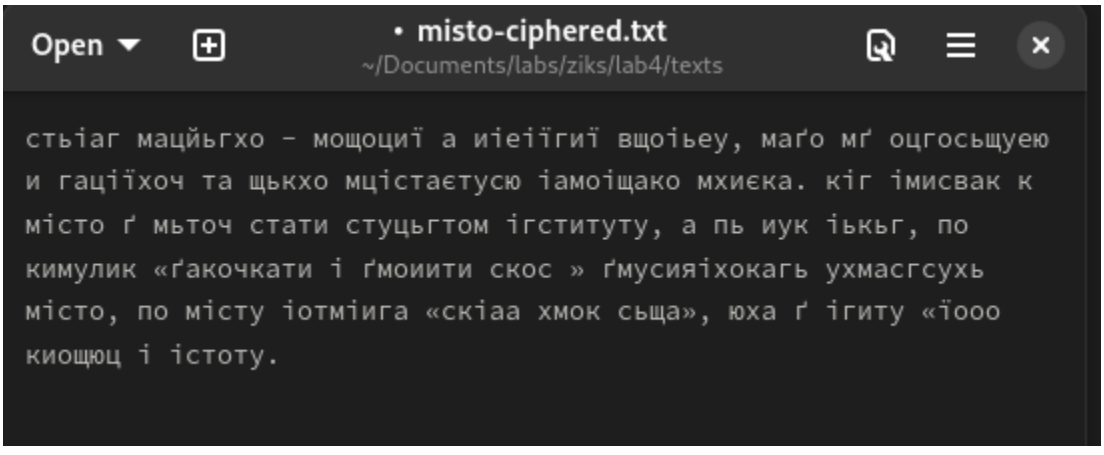


Також з аналізу тригам бачу що “з” це “и”

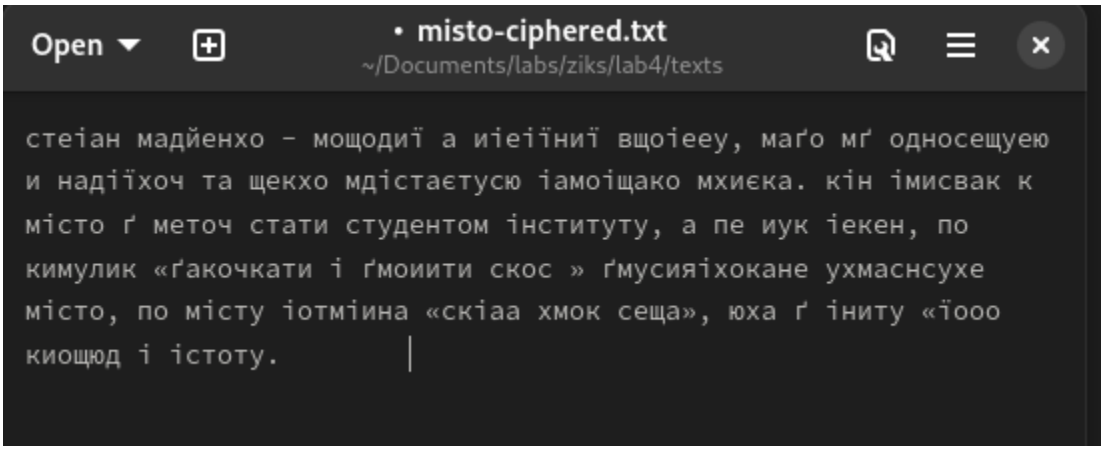




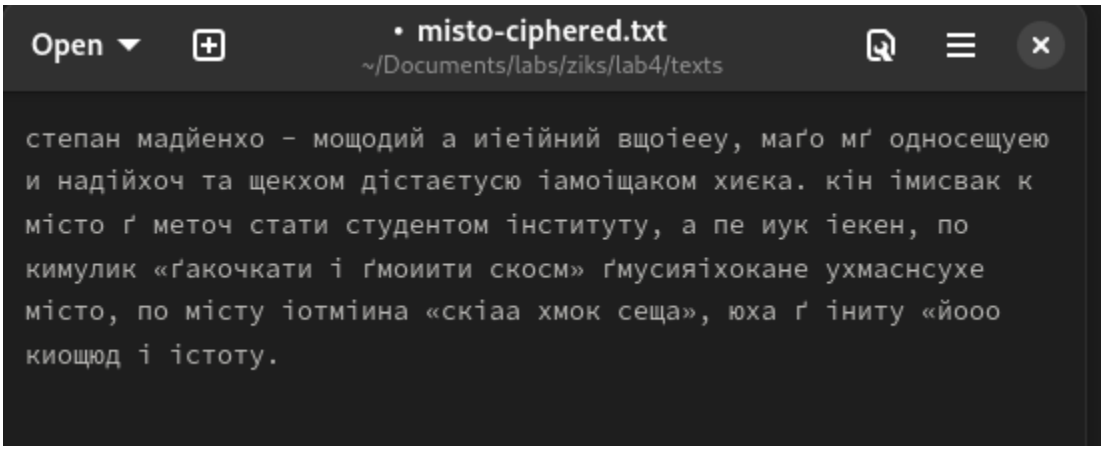
Бачу слово “місто” де пробіл виступає у ролі “м” (трохи криво замінив тут, тому деякі слова попливли).



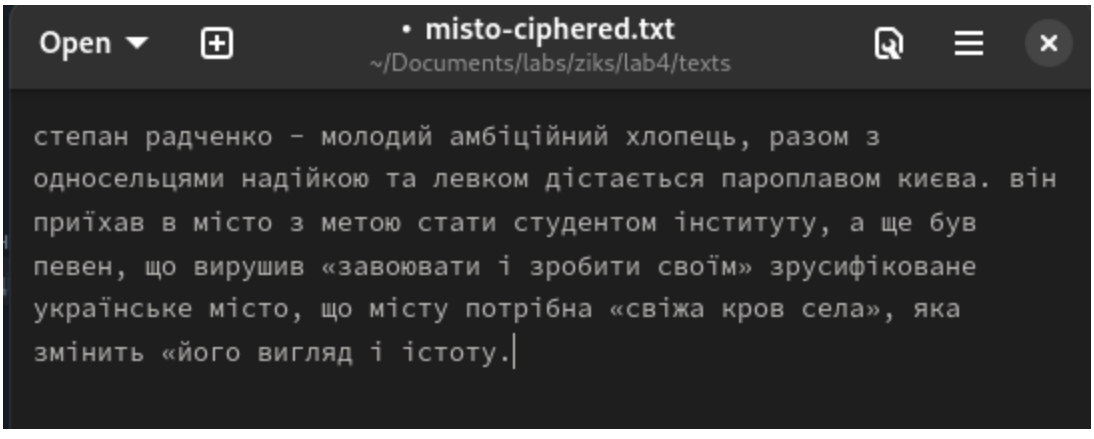
Бачу слова “стуцьгтом ігститутту” це “студентом інституту”.



На даному етапі можна вибирати окремі слова, та розшифровувати до кінця.



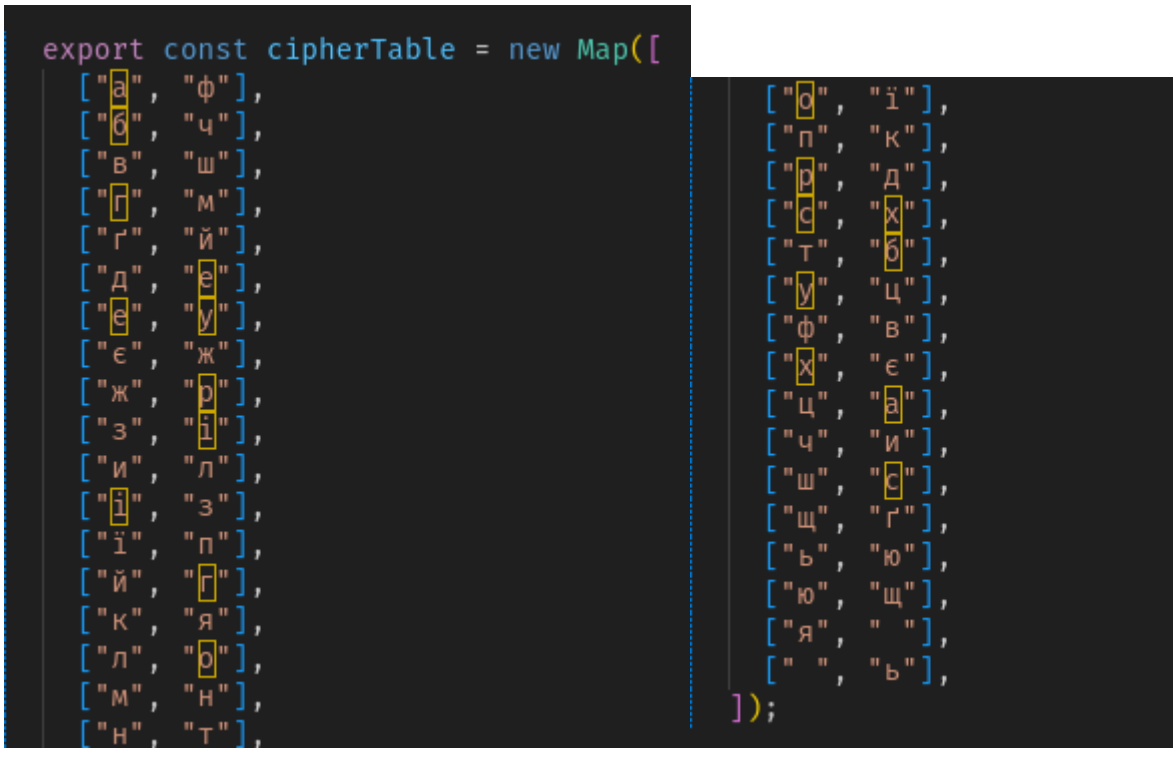
Фінальний результат.



5. Криптоаналіз довільного моноалфавітного шифру.

Згенеруйте випадкову моноалфавітну підстановку (таблицю відповідності) та зашифруте за її допомогою достатньо довгий фрагмент тексту.

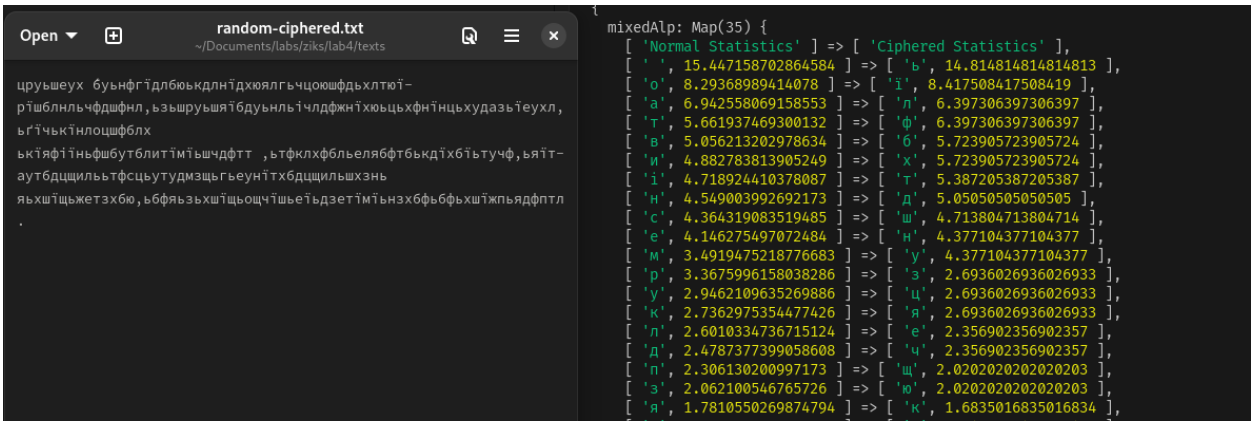
Таблиця по якій відбувалося шифрування:



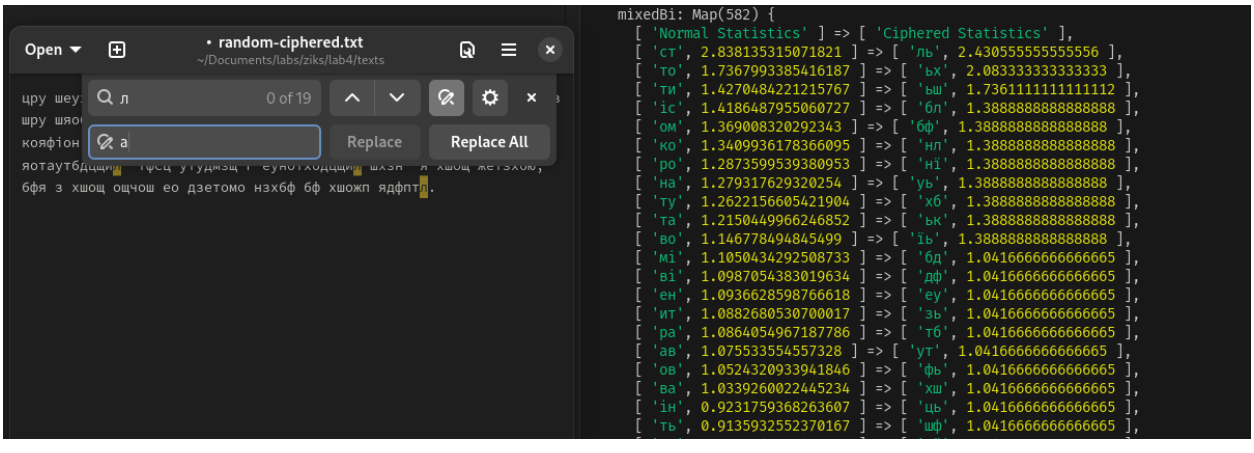
Отриманий текст:

Виконайте криптоаналіз отриманого шифротексту, використовуючи частотний аналіз (в т.ч. частоти біграм, триграм та припущень).

На основі статистики зроблю припущення що «ь» та «ї це пробіл та «о» відовідно.



По біграмах видно що «ль» це закінчення, скоріш за все голосна + пробіл, припускаю що це «а»



Ось результат, якого зміг досягти, далі туго пішло, частотні характеритиски зашифрованого тексту не зовсім відповідають моїм статистичним даним.

Висновок. Під час виконання лабораторної роботи було проведено аналіз частотних характеристик літер, біграм та триграм української мови, що дозволяє ефективно застосовувати їх для частотного криптоаналізу. Частотний підхід підтвердив, що мовні особливості українських текстів можуть значно покращити точність розшифрування і підвищити ефективність криптоаналітичних методів.