КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Мета

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі

Засобами частотного криптоаналізу розшифрувати ШТ згідно з варіантом 3.

Хід роботи

Мовою програмування для створення скриптів було обрано Python 3. Було розроблено код cp2.py, який містить усі функції для виконання цього комп'ютерного практикуму, застосовуючи результати попереднього (словник частот CHARS).

У ході виконання роботи були декілька труднощів пов'язаних з помилками у коді, зокрема:

1. Функція **format_text()**, яка не потрапила у кінцевий код, заміняла символ "ъ" на "ь", спотворюючи кінцевий ключ.
2. Відсутність "ъ" у рядкові ALPHABET і словникові CHARS, що спотворювало кінцевий ключ.
3. Помилка в обчисленні ключа у функції **find_key()**, через яку віднімали не найпоширенішу літеру ВТ від найпоширенішої літери ШТ, а навпаки.

Інші труднощі були пов'язані здебільшого з оформленням output'у, зокрема за допомогою функцій **visualize()** та **show_decryption()**.

Було знайдено індекс відповідності для фрагменту "Мертвих душ" Миколи Гоголя. Останній пізніше було зашифровано ключами зі списку KEYS. Для кожного отриманого шифрованого тексту також було обраховано індекси відповідності.

```
Custom text: вворотагостиницыгубернскогогор...
IoC:   0.05465259348688421

Using key "т"
Encrypting...
M:     вворотагостиницыгубернскогогор
r:     тттттттттттттттттттттттттттт
C:     ффавадтхагдъяъинхеучвягьахахав
Searching period (key length)...
Period IoC
1      0.05497991679860046
…
Found:
       Period:      1
       IoC:   0.05497991679860046
Decrypting...
C:     ффавадтхагдъяъинхеучвягьахахав
r:     тттттттттттттттттттттттттттт
M:     вворотагостиницыгубернскогогор

Using key "да"
Encrypting...
```

```
M:     вворотагостиницыгубернскогогор
r:     дадададададададададададададада
C:     жвтрттдгтсцисиъызуеефнхктгтгтр
Searching period (key length)...
Period IoC
1      0.044676638084911714
2      0.05497937131782423
…
Found:
       Period:      2
       IoC:   0.05497937131782423
Decrypting...
C:     жвтрттдгтсцисиъызуеефнхктгтгтр
r:     дадададададададададададададада
M:     вворотагостиницыгубернскогогор

Using key "зло"
Encrypting...
M:     вворотагостиницыгубернскогогор
r:     злозлозлозлозлозлозлозлозлозло
C:     йньчщазоьшэцфудвобирюфьшхоькщю
Searching period (key length)...
Period IoC
1      0.04012195766279502
2      0.04012201739741333
3      0.05498084836358227
…
Found:
       Period:      3
       IoC:   0.05498084836358227
Decrypting...
C:     йньчщазоьшэцфудвобирюфьшхоькщю
r:     злозлозлозлозлозлозлозлозлозло
M:     вворотагостиницыгубернскогогор

Using key "крах"
Encrypting...
M:     вворотагостиницыгубернскогогор
r:     крахкрахкрахкрахкрахкрахкрахкр
C:     мтоешвашшбтэчшцрнгбъъэсяшуошша
Searching period (key length)...
Period IoC
1      0.03503020437801799
2      0.04338906885024591
3      0.03503024702854119
4      0.05497970875771886
…
Found:
       Period:      4
       IoC:   0.05497970875771886
Decrypting...
C:     мтоешвашшбтэчшцрнгбъъэсяшуошша
r:     крахкрахкрахкрахкрахкрахкрахкр
M:     вворотагостиницыгубернскогогор

Using key "месть"
Encrypting...
M:     вворотагостиницыгубернскогогор
r:     местьместьместьместьместьместь
```

```
C:      озявкюефанюнюътзидубьтвькпуфам
Searching period (key length)...
Period IoC
1       0.03436181388218173
2       0.03436087128995986
3       0.0343614464150681
4       0.03436009967965462
5       0.0549807085715769
…
Found:
        Period:       5
        IoC:    0.0549807085715769
Decrypting...
C:      озявкюефанюнюътзидубьтвькпуфам
r:      местьместьместьместьместьместь
M:      ввоготагостиницыгубернскогогор

Using key "денацификация"
Encrypting...
M:      ввоготагостиницыгубернскогогор
r:      денацификацияденацификациядена
C:      жзырдъфлшсирммыигййщшчсацвтиыр
Searching period (key length)...
Period IoC
1       0.03442274459520395
2       0.03442223819860846
3       0.03442294081480977
4       0.03442210158499824
5       0.03442293909335588
6       0.03442153431878419
7       0.03442790573661043
8       0.034421830532384796
9       0.03442348626281944
10      0.03442154980177774
11      0.034423995822491955
12      0.03442007663507434
13      0.0549773741480788
…
Found:
        Period:       13
        IoC:    0.0549773741480788
Decrypting...
C:      жзырдъфлшсирммыигййщшчсацвтиыр
r:      денацификацияденацификациядена
M:      ввоготагостиницыгубернскогогор

Using key "самоуничтожение"
Encrypting...
M:      ввоготагостиницыгубернскогогор
r:      самоуничтожениесамоуничтожение
C:      увъюбяиъаяшнърымгяпшэхиььйурцх
Searching period (key length)...
Period IoC
1       0.034192683222482353
2       0.034192712814121264
3       0.03741724617820518
4       0.03419246368254194
5       0.039248500063443104
6       0.03741580158721443
```

```
7       0.03419601604231783
8       0.0341920612177867
9       0.037416460282066306
10      0.039246981665952155
11      0.034188302349748206
12      0.03741445127179344
13      0.03419244197531145
14      0.03419695714393248
15      0.054979744971048815
…
Found:
        Period:       15
        IoC:    0.054979744971048815
Decrypting...
C:      увъюбяиъаяшнърымгяпшэхиььйурцх
r:      самоуничтожениесамоуничтожение
M:      ввоготагостиницыгубернскогогор

Using key "сельскохозяйственный"
Encrypting...
M:      ввоготагостиницыгубернскогогор
r:      сельскохозяйственныйсельскохоз
C:      узщмяьошьшссюъшараьобтьжяньшьч
Searching period (key length)...
Period IoC
1       0.032987916837071585
2       0.03527713469023931
3       0.03298741187368303
4       0.0382242316964283
5       0.037159849400927605
6       0.035277102977163716
7       0.03298866360364881
8       0.038225316215749316
9       0.03298791812261231
10      0.043342217630751315
11      0.03298838003542777
12      0.038222192968787906
13      0.03299134827565543
14      0.035277487166073415
15      0.037158213259748364
16      0.03822525083587021
17      0.03298469505612698
18      0.03527670906840845
19      0.03298672399980279
20      0.054978846911112688
…
Found:
        Period:       20
        IoC:    0.054978846911112688
Decrypting...
C:      узщмяьошьшссюъшараьобтьжяньшьч
r:      сельскохозяйственныйсельскохоз
M:      ввоготагостиницыгубернскогогор

Using key "электрофотополупроводниковый"
Encrypting...
M:      ввоготагостиницыгубернскогогор
r:      электрофотополупроводниковыйэл
C:      ануъавочьгачыуйкубгуфъщфьеймлы
```

```
Searching period (key length)...
Period IoC
1      0.03428104719908149
2      0.035188654259836694
3      0.0342824790179015
4      0.036622068614894636
5      0.0342825161557857
6      0.03519034137041851
7      0.0394575375623385
8      0.036621484035834526
9      0.03428629113738299
10     0.03519102389704325
11     0.03427914940243575
12     0.03662719729466989
13     0.034282945482958245
14     0.043184380840305424
15     0.03428423028279443
16     0.03662365231321154
17     0.03427542502763629
18     0.035192112412856656
19     0.034276935066126765
20     0.03662600926232906
21     0.0394595453135058
22     0.03518635439382855
23     0.03428203659091704
24     0.03662437221418434
25     0.034281605917080384
26     0.03519255594622
27     0.03428373157709904
28     0.05498081402177072
…
Found:
       Period:      28
       IoC:   0.05498081402177072
Decrypting...
C:     ануъавочьгачыуйкубгуфъщфьеймлы
r:     электрофотополупроводниковыйэл
M:     вворотагостиницыгубернскогогор
```

Лістинг 1. Зашифрування обраного ВТ і визначення індексу відповідності ШТ.

r = 1		r = 2		r = 3	
Period	IoC	Period	IoC	Period	IoC
1	0.054979917	1	0.044676638	1	0.040121958
2	0.054979371	2	0.054979371	2	0.040122017
3	0.054980848	3	0.044678215	3	0.054980848
4	0.054979709	4	0.054979709	4	0.040120835
5	0.054980709	5	0.044677646	5	0.040122237
6	0.054982196	6	0.054982196	6	0.054982196
7	0.054980109	7	0.04467678	7	0.040120203
8	0.05497733	8	0.05497733	8	0.040119214
9	0.054981569	9	0.04467884	9	0.054981569
10	0.054979908	10	0.054979908	10	0.040121977
11	0.054980133	11	0.044677837	11	0.040122411
12	0.054981342	12	0.054981342	12	0.054981342
13	0.054977374	13	0.044672365	13	0.040125547
14	0.054980677	14	0.054980677	14	0.040120853
15	0.054979745	15	0.044676931	15	0.054979745
16	0.054981045	16	0.054981045	16	0.040119938
17	0.054977391	17	0.044673916	17	0.040118411
18	0.05498458	18	0.05498458	18	0.05498458
19	0.054984977	19	0.044678522	19	0.040119792
20	0.054978847	20	0.054978847	20	0.040120151
21	0.054977814	21	0.044676378	21	0.054977814
22	0.05498157	22	0.05498157	22	0.040119264
23	0.054976889	23	0.044678687	23	0.040124742
24	0.054976134	24	0.054976134	24	0.054976134
25	0.054981965	25	0.044674802	25	0.040119671
26	0.05497345	26	0.05497345	26	0.040119704
27	0.054980204	27	0.044674667	27	0.054980204
28	0.054980814	28	0.054980814	28	0.040124385
29	0.054979008	29	0.044676223	29	0.040115194
30	0.054978926	30	0.054978926	30	0.054978926

r = 4	
Period	IoC
1	0.035030204
2	0.043389069
3	0.035030247
4	0.054979709
5	0.035030105
6	0.043388832
7	0.035030766
8	0.05497733
9	0.035029737
10	0.043388127
11	0.035032206
12	0.054981342
13	0.03502362
14	0.043389487
15	0.03502742
16	0.054981045
17	0.035029285
18	0.043391687
19	0.035029042
20	0.054978847
21	0.035030737
22	0.043386771
23	0.035035989
24	0.054976134
25	0.035025961
26	0.04337935
27	0.035029334
28	0.054980814
29	0.035027474
30	0.043382604

r = 5	
Period	IoC
1	0.034361814
2	0.034360871
3	0.034361446
4	0.0343601
5	0.054980709
6	0.03435943
7	0.034361849
8	0.034360691
9	0.034360878
10	0.054979908
11	0.034363351
12	0.034358199
13	0.034361842
14	0.034359025
15	0.054979745
16	0.034359988
17	0.034364615
18	0.034357933
19	0.034365061
20	0.054978847
21	0.034355422
22	0.034366441
23	0.034363194
24	0.034357158
25	0.054981965
26	0.034360895
27	0.034359639
28	0.034356742
29	0.034356513
30	0.054978926

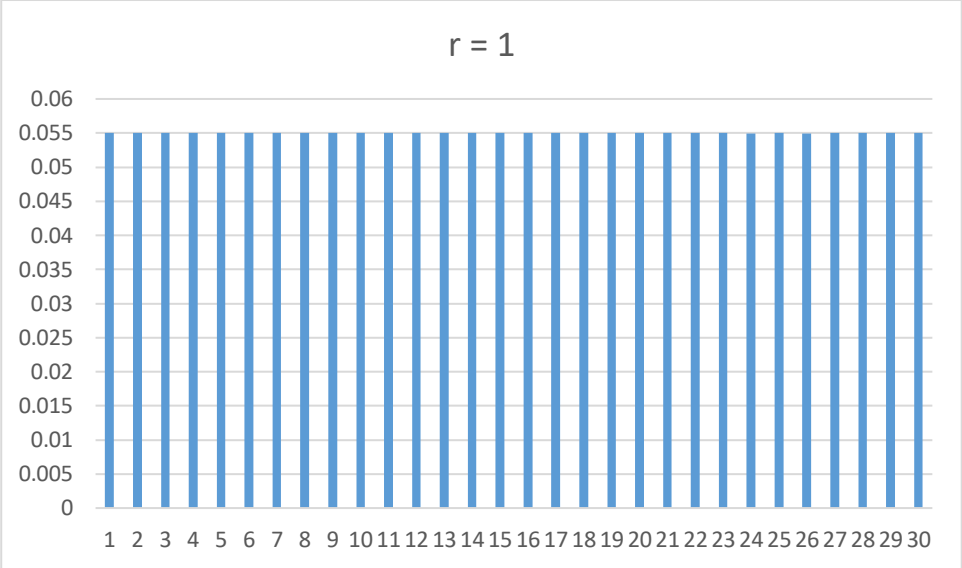
r = 13	
Period	IoC
1	0.034422745
2	0.034422238
3	0.034422941
4	0.034422102
5	0.034422939
6	0.034421534
7	0.034427906
8	0.034421831
9	0.034423486
10	0.03442155
11	0.034423996
12	0.034420077
13	0.054977374
14	0.034429034
15	0.034422992
16	0.0344205
17	0.034419116
18	0.034421234
19	0.034422853
20	0.034422858
21	0.034424061
22	0.034426339
23	0.034423076
24	0.034418398
25	0.034422425
26	0.05497345
27	0.0344213
28	0.0344288
29	0.03441526
30	0.034418437

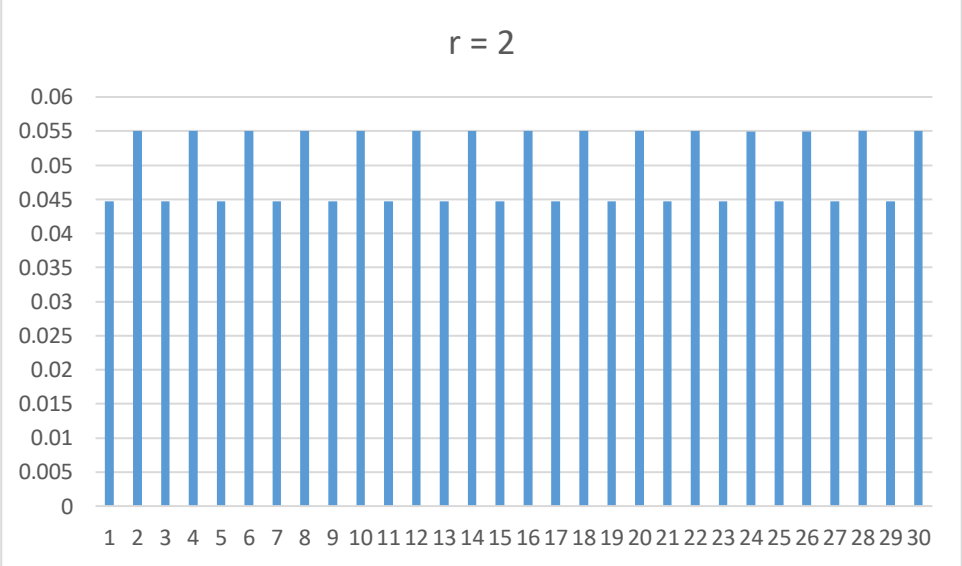
r = 15	
Period	IoC
1	0.034192683
2	0.034192713
3	0.037417246
4	0.034192464
5	0.0392485
6	0.037415802
7	0.034196016
8	0.034192061
9	0.03741646
10	0.039246982
11	0.034188302
12	0.037414451
13	0.034192442
14	0.034196957
15	0.054979745
16	0.034192893
17	0.034195187
18	0.0374138
19	0.034199508
20	0.039245873
21	0.03741755
22	0.03419098
23	0.034193258
24	0.037411023
25	0.039252817
26	0.034189851
27	0.037415065
28	0.034200735
29	0.034186077
30	0.054978926

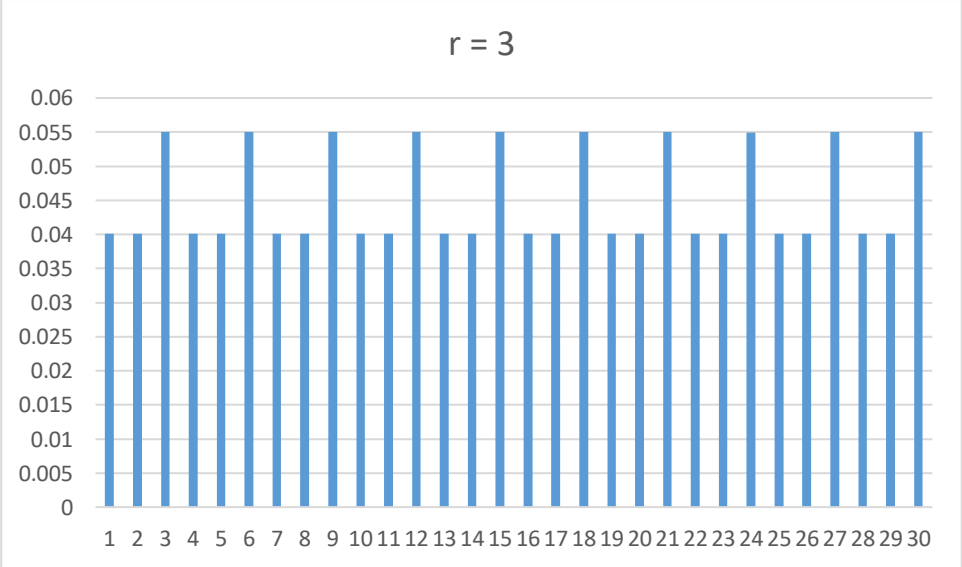
r = 20	
Period	IoC
1	0.032987917
2	0.035277135
3	0.032987412
4	0.038224232
5	0.037159849
6	0.035277103
7	0.032988664
8	0.038225316
9	0.032987918
10	0.043342218
11	0.03298838
12	0.038222193
13	0.032991348
14	0.035277487
15	0.037158213
16	0.038225251
17	0.032984695
18	0.035276709
19	0.032986724
20	0.054978847
21	0.032984718
22	0.035275951
23	0.0329849
24	0.038219695
25	0.037158392
26	0.035278317
27	0.032986189
28	0.038221082
29	0.032989777
30	0.043342369

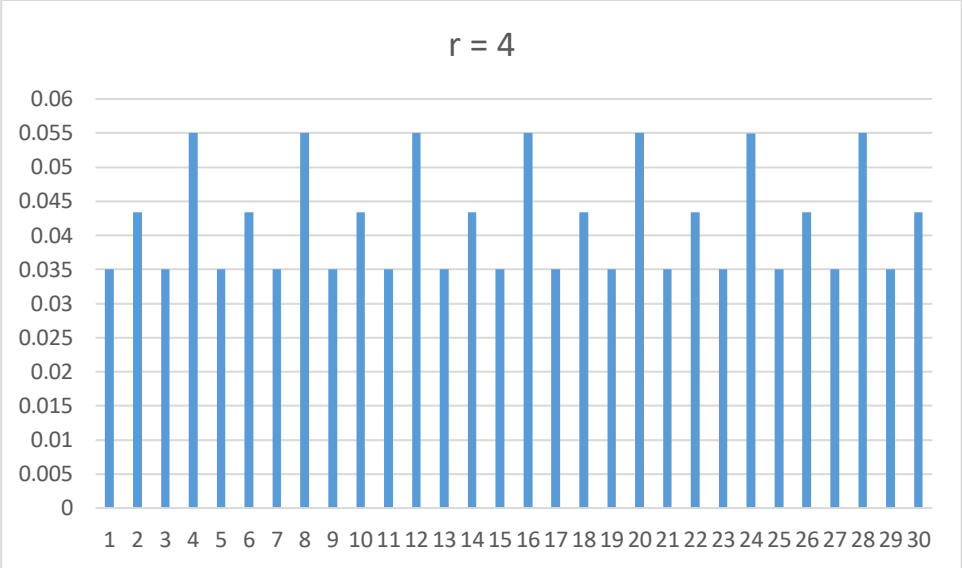
r = 28	
Period	IoC
1	0.034281047
2	0.035188654
3	0.034282479
4	0.036622069
5	0.034282516
6	0.035190341
7	0.039457538
8	0.036621484
9	0.034286291
10	0.035191024
11	0.034279149
12	0.036627197
13	0.034282945
14	0.043184381
15	0.03428423
16	0.036623652
17	0.034275425
18	0.035192112
19	0.034276935
20	0.036626009
21	0.039459545
22	0.035186354
23	0.034282037
24	0.036624372
25	0.034281606
26	0.035192556
27	0.034283732
28	0.054980814
29	0.034284547
30	0.035191688

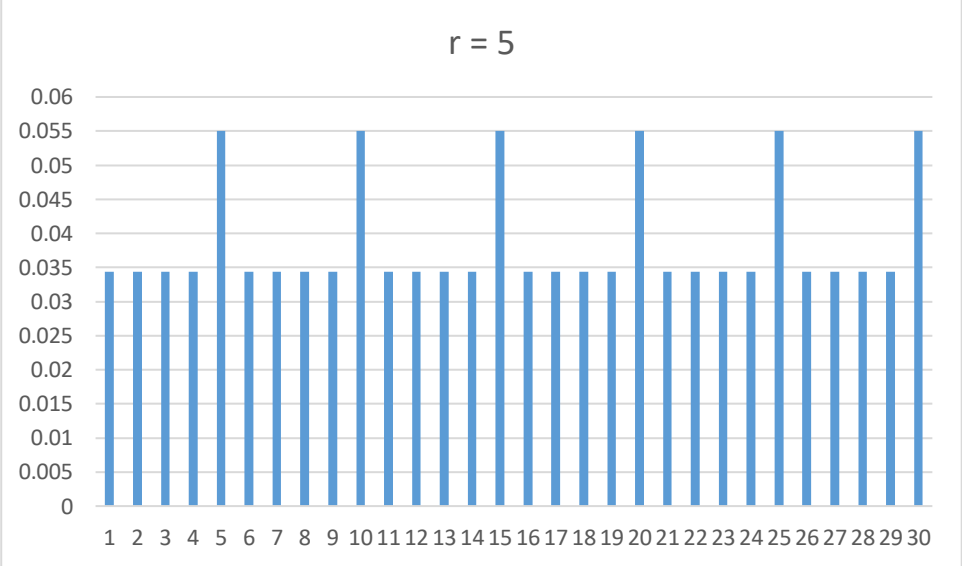
Знімок 1. Таблиці для вказаних значень r.

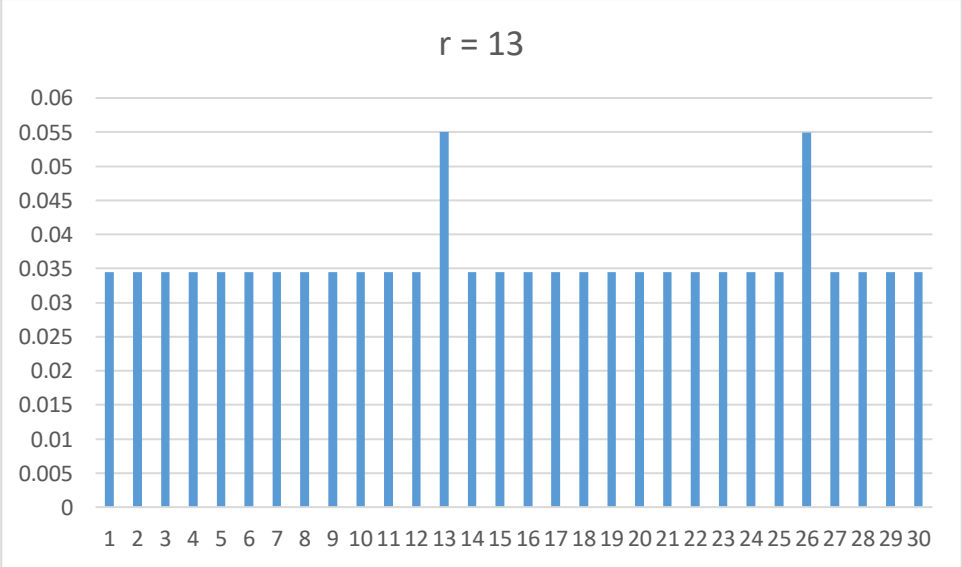

r = 1
0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

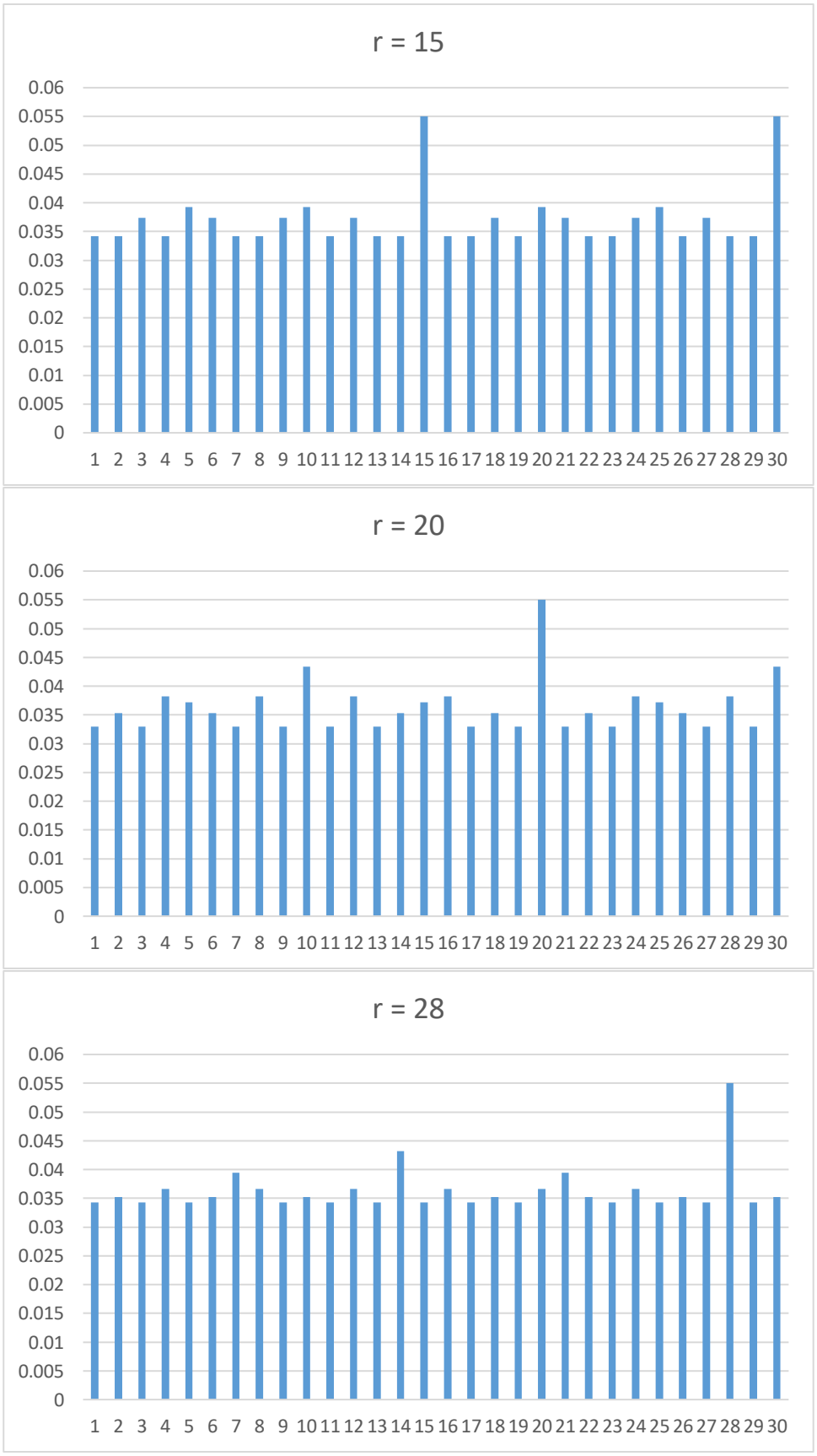

r = 2
0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30


r = 3
0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30


r = 4
0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30


r = 5
0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30


r = 13
0.06
0.055
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30



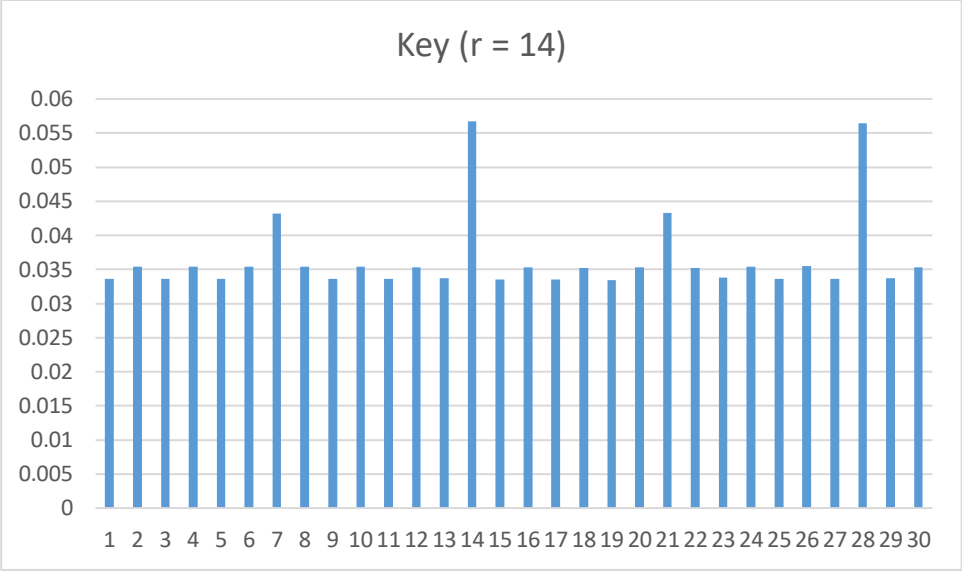
Знімок 2. Діграми значень індексів відповідності для заданих значень r.

Застосувавши написаний скрипт було здійснено низку кроків для розшифрування ШТ:

1. Встановлено довжину ключа за допомогою визначення індексу відповідності для кожного блоку ШТ (алгоритм 1) у функції **find_period()**.
2. Знайдено ключ за допомогою припущень щодо найпоширеніших літер у ШТ у функції **find_key()**.
3. Розшифровано текст і з використанням знайденого ключа.

```
Var3 text:   еьбюятфхмпяякнпчццшявпрыумтчкк...
Searching period...
Period IoC
1      0.03365878060005469
2      0.03540318621049883
3      0.033657628252257855
4      0.03537512674612907
5      0.033600744639310204
6      0.035353382712172456
7      0.04321232340902984
8      0.035366115767448164
9      0.03361816528900438
10     0.035441203962855314
11     0.03357008893142104
12     0.03527913582243025
13     0.033742872053219006
14     0.05667060702875399
15     0.03355059522920367
16     0.03532923505501202
17     0.033553157074346744
18     0.035250813284029715
19     0.03342913541516717
20     0.035329220456214554
21     0.043282276072429494
22     0.035165903720665165
23     0.03377602673928392
24     0.03536201414470406
25     0.03359764522859079
26     0.03550495354771452
27     0.033646448144021054
28     0.05646761560900226
29     0.0336932257727597
30     0.03529422809190425
Found:
       Period:       14
       IoC:   0.05667060702875399
Searching key...
Chars: оеоооеоооооао
Key:   экомаятникфуко
Decrypting...
экомаятникфуко
--------------
итутяувиделмая
тникшарвисящий
надолгойнитиоп
ущеннойсвольты
хоравизохронно
```

Лістинг 2. Розшифрування ШТ варіанту 3.



Знімок 3. Діаграма значень індексів відповідності для встановленої довжини ключа.

Таким чином, було встановлено, що ключ має довжину 14 символів і має вигляд “экомаятникфуко”, та розшифровано ШТ.

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвели
чииописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериод
колебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррацион
альноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаетокру
жностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодногопол
юсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневре
менныхмерединственноститочкикрепленияядвойственностиабстрактногоизмерениятро
ичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеязнал
чтонаконцеотвеснойлинииивосстановленнойотточкикрепленияянаходящийсяподмаятник
оммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечн
остьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинекотор
аянепротиворечитзаконуфуконапротивпомогаетемупроявитьсяпотомучтопомещенныйв
пустотулюбойточечныйвеспринятыйкконцунерастяжимойиневесомойнитиневстреча
ющийнисопротивлениявоздуханитрениявточкекрепленияидействительнобудетсовершат
ьрегулярныеигармоничныеколебаниявечномедныйшарпоигрывалбледнымипереливчатым
иотблескамиподпоследнимилучамишедшимиизвитражаеслибыкаккогдатоонкасалсяслоя
мокрогопесканаплитахполаприкаждомизегокасанийпрочерчивалсябыштрихиэтиштрихи
неуловимоизменяякаждыйразнаправлениерасходилисьбыоткрываяразломытраншеирвыи
угадывалась бырадиальнаясимметричностькостякмандалыневидимаясхемапентакулазв
ездымистическойрозынетнетэтобылабынерозаэтобылбырассказзаписанныйнаполотнах
пустынисследаминесосчитанныхкаравановповестьотысячелетнихскитанияхнаверноеэт
ойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасманиивгренл
андиюоттропикакозерогактропикуракасостровапринцаэдуарданашпицбергенкасаниям
ишараутрамбовывалось вминутныйрассказвсечтоонитворилив промежуткахотодноголеда
овогопериодадодругогоискореевсеготворятвнашевремясделавшись рабамиверховнико
ввероятноперелетаяотсамоананову юземлюэтотшарнацеливаетсявапогеепараболынааг
артуцентрмираячувствовалкактаинственнымобщимпланомобъединяетсяавалонгипербо
реевсполуденнойпустынейоберегающейзагадкуайерсроквданныймигвчетыречасаднядв
адцатьтретьегоиюнямаятникутрачивалскоростьукраяколебательнойплоскостибезвол
ьноотшатывалсяснованачиналускорятьсякцентруинаразгонепосерединерассекалссаб
ельнымсвистомтайныйчетвероугольниксилопределявшихегосудьбуеслибыяпробылтамд
олгонеуязвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечникэто
топрокинутыйгребеньшлемавычерчиваетвпустотесвоидиагоналиотказдокраяастигма
тическойзамкнутойлинииияпревратилсябывжертвуобольщенияячувствимаятникубедилбы
менячтоколебательнаяплоскостьсовершилаполныйоборотивозвратилась впервоначаль
ноеположениеописавзатридцатьдвачасасплюснутыйэллипсэллипсобращающийсявокруг
собственногоцентраспостояннойугловойскоростьюпропорциональнойсинусугеографи

ческойширотыкаквращалсябытотжеэллипсбудьнитьмаятникаприкрепленаквенцухрамас
оломонавероятнорыцариипробовалиэтоможетбытьихрасчеттоестьконечныйрезульта
трасчетанеизменялсяможетбытьсобораббатствасенмартендешанэтодействительноист
инныйхрамвообщечистыйэкспериментвозможентольконаполюсеэтоединственныйслучай
когдаточкаподвешиваниянитирасположиласьбынапродолженииземнойосиимаятникзакл
ючилбысвойвидимыйциклровновдвадцатьчетыречасаоднакоэтоотступлениеотзаконакт
омужепредусмотренноесамимзакономэтапогрешностьпротивзолотойнормынеотнималач
удесностиучудаязналчтоземлявращаетсяичтоявращаюсьвместеснеюисенмартендешани
весьпарижсомноюивсемывращалисьподмаятникомкоторыйдействительнонисколькоиз
менялориентациисвоегопланапотомучтонаверхугдеонкчемутобылпривязаннадругомко
нцевоображаемогобесконечногопродолженияниттивысотуивдальзапределамиотдаленн
ыхгалактикнаходиласьнедвижимаяинепреложнаявсвоейвековечностимертваяточказем
лядвигаласьоднакоместоккоторомуприкреплялсяканатбылоединственнымнеподвижным
местомвселеннойпоэтомумойвзглядбылприкованнестолькокземлесколькокнебуосиянн
омутайнойабсолютнойнеподвижностимаятникговорилмнечтохотявращаетсявсеземнойш
арсолнечнаясистематуманностичерныедырыилюбыепорожденияграндиозноикосмическо
йэманацииотпервыхэоновдосамойлипучейматериисуществуеттолькооднаточкаосьнеки
йшампурзанебесныйштырьпозволяющийостальномумируобращатьсяоколосебяитеперьяу
частвовалвэтомверховномопытеявращавшийсякаквсенасветесообщасовсемнасветеудо
стаивалсявидетьтонедвижноекрепостьопорусветоносноеявлениекотороенетелесноин
еимеетнграницыниформынивесаниколичествваникачестваиононевидитнеслышитнеподд
аетсячувственностиинепребываетнивместенивовременинивпространствеиононедушан
еразумневоображениенемнениенечислонепорядокнемеранесущностьневечностьононет
ьмаинесветононеложьинеистинадоменядолетелпасмурныйобменрепликамимеждупарнем
вочкахидевицейувыбезочковэтомаятникфукоговорилеемилыйпервыйопытпроводиливпо
гребевтысячавосемьсотпятьдесятпервомгодупотомвобсерваториипотомподкуполомпа
нтеонадлинаканаташестьдесятсемьметроввесгиридвадцатьвосемькилонаконецвтысяч
авосемьсотпятьдесятпятомподвешентутвуменьшенномасштабеканатпротянутчерезни
жнюючастьзамкасводаазачемнадочтобыонболталсядоказываетсявращениеземлипоскол
ькуточкакрепленияненодвижнаапочемуонанеподвижнапотомучтоточкасейчасятебеобъ
яснювцентральнойточкелюбойточкенаходящейсясредидругихвидимыхточеквобщемэтоу
женефизическаяточкаакакбыгеометрическаяитыеенеможешьвидетьпотомучтоунеенетп
лощадиатоучегонетплощадинеможетперекоситьсянивлевонивправоникверхуникнизупо
этомуонаневращаетсяследишьеслиуточкинетплощадионанеможетповорачиватьсявокру
гсебяунеенетэтогосамогосебяноэтаточканаземлеаземлявертитсяземлявертитсяаточ
каневертитсяможешьневеритьеслиненравитсяясномнекакоеделонесчастнаяиметьнадг
оловойединственнуюстабильнуючастицумиратонисчемнесравнимоечтонеподверженопр
оклятиюобщегобегаисчитатьчтоэтонееаегоделовследзаэтимчетапошлапрочьонобним
аясвойсправочникотучившийегоудивлятьсяонаволочасвойорганизмглухойксердцебие
ниюбесконечностииобаникакнепытаясьзакрепитьвпамятиопытэтойвстречиихпервойии
хпоследнейсединымсэнсофсневысказуемымонинепалинаколенипередалтаремистиныягл
яделсвниманиемистрахомимнеповерилосьчтоякопобельбоправвсегдашниеегодифирамб
ымаятникуяпривыксписыватьнабесплодноеэстетствозлокачественноекотороемедленн
оразъедалоегодушуибесформенноеперенималоформуеготеланезаметноперекодируяигр
увреальностьжизниоднакоеслибельбобылправнасчетмаятникавероятноонбылправинас
четвсегопрочегоибылпланибылвсеобщийзаговорибылоправильночтояоказалсяздесьсе
годнянаканунелетнегопротивостоянияякопобельбонесумасшедшийемупростопривелос
ьвовремяигрычерезигруоткрытьистинуделовтомчтосопричастностьбожескомунеможет
продолжатьсядолгонепотревоживрассудоктогдаяпостаралсяотвестивзглядпрослежив
аядугукотораяоткапителейрасставленныхполукругомколоннуходилаподпираемаягурт
амисводакключуповторяяуловкустрельчатойаркиумеющейоперетьсянапустотувысшаяс
тепеньлицемериявстатикеиуговоритьколонныйчтооноиобязаныпихатьвверхребрасводаа
ребрамраспираемымдавлениемзамкавнушитьчтобониприжималикземлеколонныносводещ
ехитрееонявляетсяивсеминичемипричинойисследствиемвединомлицеоднакоямоменталь
нопонялчтоотворачиватьсяотмаятникасвисающегососводаиразмышлятьвместоэтогоос
водетожесамоечтозарекатьсяотродниканопитьизисточникахорсоборасенмартендешан
существоваллишьблагодарятомучтоимелсуществованиевпрославлениезаконамаятника
маятниксуществовалтолькопотомучтосуществовалсоборнесбежишьотбесконечностипо
думаляудираякдругойбесконечностинеубережешьсяотвстречистождественнымпытаясь

```
отыскатьиноепопрежнемунеотводяглазотключасоборногосводаясталпятитьсяотступа
яшагзашагомзавремяпрошедшеесмоментаприходаядетальнозаучилрасположениезалада
имощныеметаллическиечерепахипатрулировавшиестеныпостоянномаячиливуглуполязр
енияпропятившисьчерезвесьнефдовходнойдверияснованазалсяподсеньюгрозныхптер
одактилейизпроволокиитряпокзловещихстрекозневедомочьейоккультнойволейзаслан
ныхподпотолокнефаонивыступалиметафорамизнаниязначительноболееглубокимичемве
роятнозамышлялдидактразместившийихвназидательнойпоследовательноститрепетани
енасекомыхирептилиймезозояаллегориябессчетныхмиграциймаятниканадповерхность
юземлиархонтыизвращенныеэманациионипикировалинаменяцелясьархеоптериксовымик
лювамиаэропланыбрегеблериоэсногеликоптердюфопосетительконсерваториянаукиите
хникивпарижепройдячерездворвосемнадцатоговекаипослеэтогонесколькокоридоровв
ступаетвдревнююаббатскуюцерковьврезаннуювболееновыйкомплексзданийподобнотом
укакпреждеонабылаоблепленасовсехсторонстроениямиприоратапривходесразуперехв
атываетдухотстранногосоюзагорнейзапредельнойстрельчатостисхтоническиммиромп
ожирателейсоляркиимазутапонизутянетсяпроцессиясамоходовсамокатовипаровыхэки
пажейсверхувисятвоздухоплавательныемашиныпионероводнипредметыцелыдругиеобод
раныистрепанывременемивсеонивместепредстаютподсмешанныместественнымиэлектри
ческимсветомкакбудтовпатиневлакеколлекционнойвиолончелииногдасохраняетсятол
ькоскелетшассинаворотприводовирукоятейисулитнеописуемыепыткитакивидишьсебяп
рикрученнымцепямикэтомуложуоткровенностивотвотоношевельнетсяпойдеткопатьтво
емясоирытьсявжилахдополногоичистосердечногопризнания
```

Лістинг 3. Розшифрований ШТ варіанту 3.

Висновок

У ході виконання комп’ютерного практикуму були отримані навички шифрування та розшифрування тексту шифром Віженера, встановлення довжини ключа за допомогою визначення індексів відповідності блоків ШТ та пошуку ключа шляхом підбирання найпоширеніших літер ШТ і ВТ.

Крім того, була досягнута головна мета комп’ютерного практикуму: розшифровано ШТ за варіантом 3. З’ясувалося, що був зашифрований текст твору “Маятник Фуко” Умберто Еко.