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

Виконали:
ФБ-31 Аль-Фітурі Асія
ФБ-31 Гриб Вероніка

Перевірила:
Селюх П. В.

2025

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

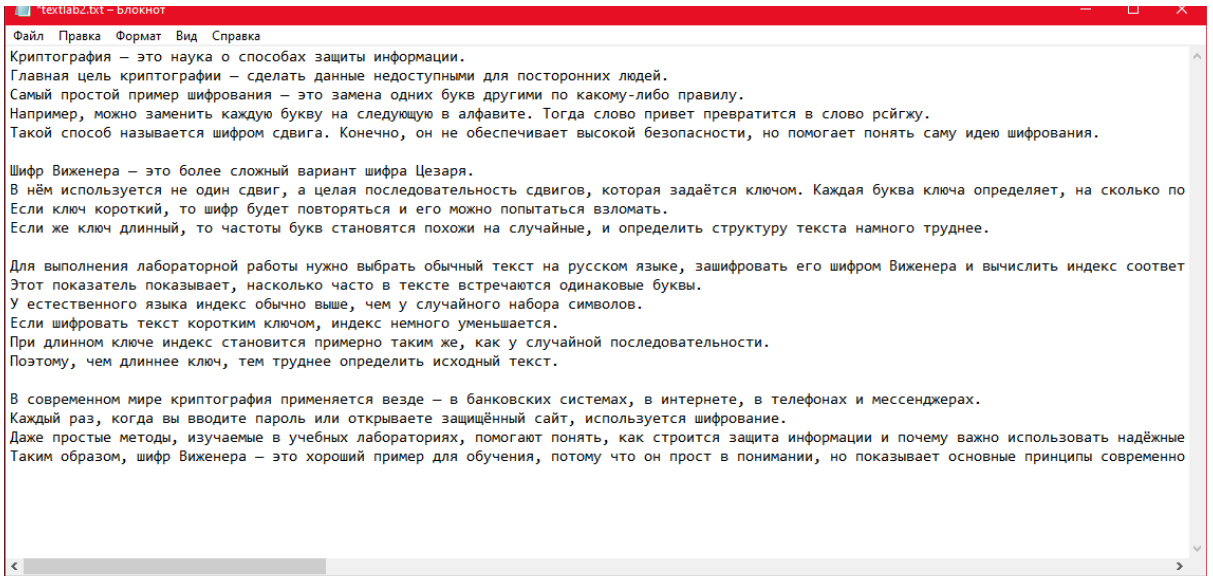
Порядок виконання роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

Підібраний текст:

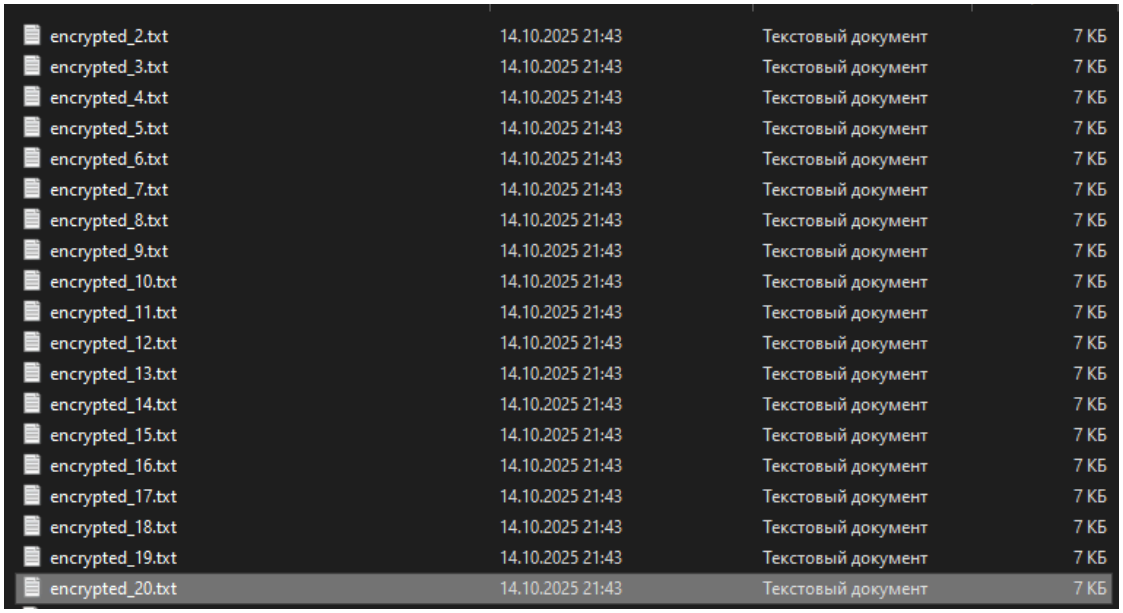
підібрали текст



ключі

```
# ===== 2) ключі (без 'ё') =====
seed_words = [
    "да", "мир", "ключ", "текст", "пример", "поездка", "алгоритм",
    "универсал", "переменная", "эксперимент", "безопасность",
    "распознавание", "инфраструктура", "маскировка", "статистика",
    "последователь", "криптоанализ", "перекодировка", "криптосистема",
    "методологически"
]
```

Отримали



encrypted_2.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_3.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_4.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_5.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_6.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_7.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_8.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_9.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_10.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_11.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_12.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_13.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_14.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_15.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_16.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_17.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_18.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_19.txt	14.10.2025 21:43	Текстовый документ	7 КБ
encrypted_20.txt	14.10.2025 21:43	Текстовый документ	7 КБ

2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

```
PS D:\криптографія 5 сем\lab2> & C:\Users\user\AppData\Loc
Довжина відкритого (очищеного) тексту: 3268 символів (m=32
I_open = 0.05352

r   ключ                          IoC    файл
--------------------------------------------------
2   ми                          0.04475   encrypted_2.txt
3   клю                         0.03825   encrypted_3.txt
4   текс                        0.03568   encrypted_4.txt
5   приме                       0.03566   encrypted_5.txt
6   поездк                      0.03553   encrypted_6.txt
7   алгорит                     0.03447   encrypted_7.txt
8   универса                    0.03418   encrypted_8.txt
9   переменна                   0.03470   encrypted_9.txt
10  эксперимен                  0.03400   encrypted_10.txt
11  безопасност                 0.03441   encrypted_11.txt
12  распознавани                0.03388   encrypted_12.txt
13  инфраструктур               0.03582   encrypted_13.txt
14  маскировкамаск              0.03363   encrypted_14.txt
15  статистикастати             0.03604   encrypted_15.txt
16  последовательпос            0.03461   encrypted_16.txt
17  криптоанализкрипт           0.03405   encrypted_17.txt
18  перекодировкаперек          0.03439   encrypted_18.txt
19  криптосистемакрипто         0.03398   encrypted_19.txt
20  методологическиметод        0.03445   encrypted_20.txt
 - графік: ioc_plot.png

Збережено:
 - шифртексти: encrypted_2.txt … encrypted_20.txt
 - таблиця IoC: ioc_results.csv
 - ключі: keys_used.txt
PS D:\криптографія 5 сем\lab2>
```

	A	B	C	D	E
1	type	r	key	IoC	file
2	open_text	-	-	0.05351875642295137	—
3	cipher	2	ми	0.0447503857985665	encrypted_2.txt
4	cipher	3	клю	0.038250536970910846	encrypted_3.txt
5	cipher	4	текс	0.03567554930634935	encrypted_4.txt
6	cipher	5	приме	0.035662998442568934	encrypted_5.txt
7	cipher	6	поездк	0.03552849814116087	encrypted_6.txt
8	cipher	7	алгорит	0.034465046593676836	encrypted_7.txt
9	cipher	8	универса	0.034183869779730466	encrypted_8.txt
10	cipher	9	переменна	0.034702576373879364	encrypted_9.txt
11	cipher	10	эксперимен	0.03400122661277663	encrypted_10.txt
12	cipher	11	безопасност	0.034412782548979275	encrypted_11.txt
13	cipher	12	распознавани	0.03387646728027278	encrypted_12.txt
14	cipher	13	инфраструктур	0.03582372442948831	encrypted_13.txt
15	cipher	14	маскировкамаск	0.033632006426042256	encrypted_14.txt
16	cipher	15	статистикастати	0.0360352158505046	encrypted_15.txt
17	cipher	16	последовательпос	0.03461078647458975	encrypted_16.txt
18	cipher	17	криптоанализкрипт	0.03405405263644943	encrypted_17.txt
19	cipher	18	перекодировкаперек	0.034385432905517474	encrypted_18.txt
20	cipher	19	криптосистемакрипто	0.03397537557991547	encrypted_19.txt
21	cipher	20	методологическиметод	0.03444949850869512	encrypted_20.txt

ioc_results

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). **Варіант 5**

Довжина очищеного тексту

Після попередньої обробки (видалення пробілів, пунктуації, небукв) текст має 5614 символів.

```
.py'
Довжина очищеного тексту: 5614
```

Цей крок важливий для правильного розрахунку індексу відповідності (IoC) і поділу на блоки при криптоаналізі.

Обчислення IoC для L=1..30

IoC (Index of Coincidence) оцінює ймовірність випадкового співпадіння букв у тексті. Для різних довжин ключа L розраховується IoC блоку тексту.

```
Обчислення IoC для L=1..30
L= 1, IoC=0.03532
L= 2, IoC=0.03710
L= 3, IoC=0.03535
L= 4, IoC=0.03979
L= 5, IoC=0.03544
L= 6, IoC=0.03705
L= 7, IoC=0.03522
L= 8, IoC=0.04491
L= 9, IoC=0.03545
L=10, IoC=0.03710
L=11, IoC=0.03506
L=12, IoC=0.03979
L=13, IoC=0.03551
L=14, IoC=0.03709
L=15, IoC=0.03538
L=16, IoC=0.05540
L=17, IoC=0.03552
L=18, IoC=0.03705
L=19, IoC=0.03532
L=20, IoC=0.03980
L=21, IoC=0.03506
L=22, IoC=0.03688
L=23, IoC=0.03527
L=24, IoC=0.04486
L=25, IoC=0.03532
L=26, IoC=0.03731
L=27, IoC=0.03525
L=28, IoC=0.03969
L=29, IoC=0.03558
L=30, IoC=0.03693
```

Вищий IoC свідчить про більш ймовірну довжину ключа.

Обчислення D_r (відстані повторів)

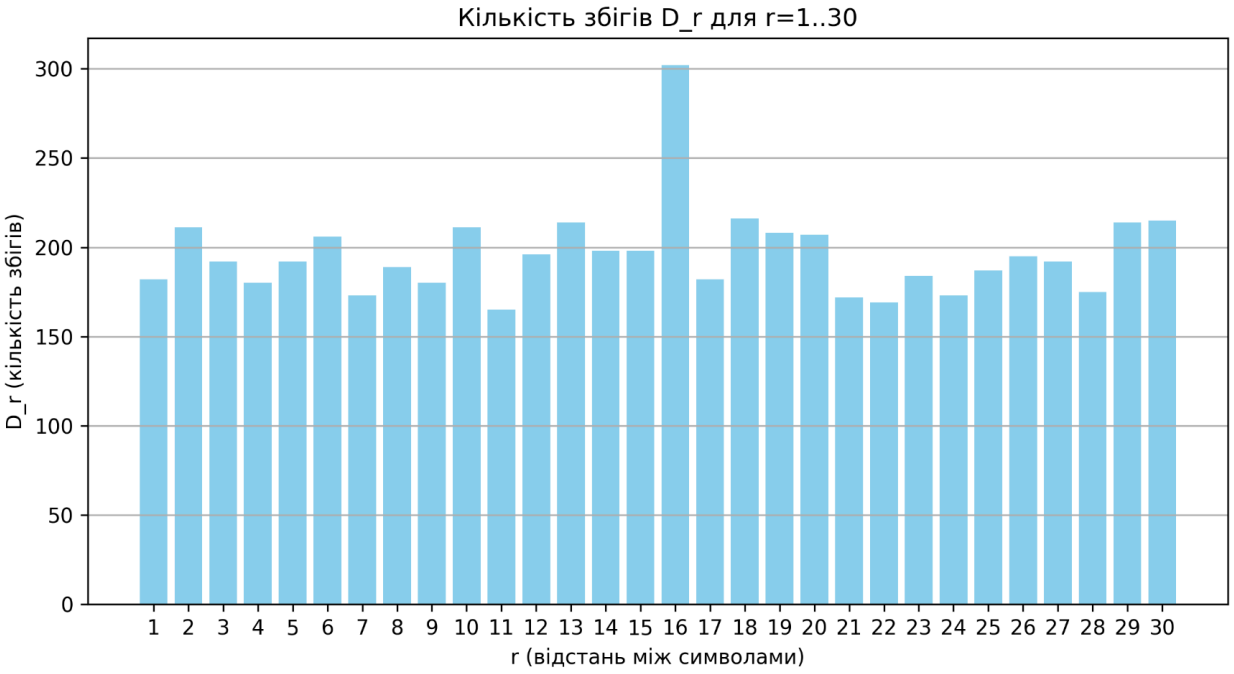
```
D_r (r=1..30):
r= 1, D_r=182
r= 2, D_r=211
r= 3, D_r=192
r= 4, D_r=180
r= 5, D_r=192
r= 6, D_r=206
r= 7, D_r=173
r= 8, D_r=189
r= 9, D_r=180
r=10, D_r=211
r=11, D_r=165
r=12, D_r=196
r=13, D_r=214
r=14, D_r=198
r=15, D_r=198
r=16, D_r=302
r=17, D_r=182
r=18, D_r=216
r=19, D_r=208
r=20, D_r=207
r=21, D_r=172
r=22, D_r=169
r=23, D_r=184
r=24, D_r=173
r=25, D_r=187
r=26, D_r=195
r=27, D_r=192
r=28, D_r=175
r=29, D_r=214
r=30, D_r=215
```

D_r – статистика для методу Касіскі (визначення періодів повторюваних груп букв). Підтверджує, які довжини ключа можуть бути ймовірними.

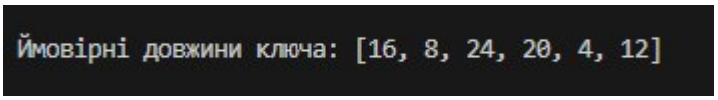
Ці значення разом з IoC допомагають скласти список ймовірних довжин ключа.

Графіки обчислених значень IoC для L=1..30 та D_r (кількість збігів на відстані r)

```
Графіки IoC та D_r збережено як IoC_plot.png та Dr_plot.png
```

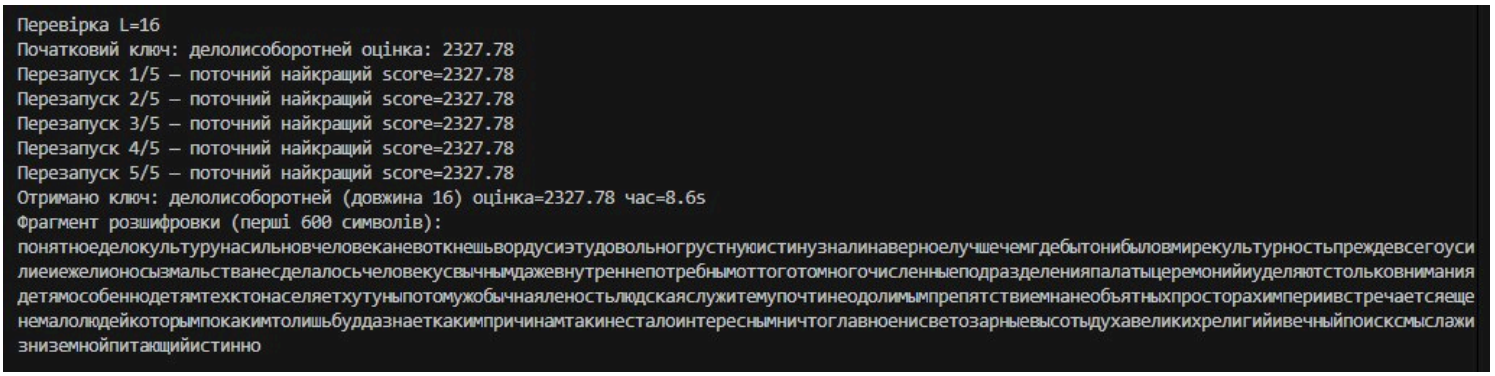


Ймовірні довжини ключа



На основі IoC і D_r програма обирає декілька найбільш ймовірних довжин ключа для перевірки. Вони будуть оброблятися по черзі у циклі for L in top_L.

Перевірка конкретної довжини ключа



find_shifts_chi знайшов початковий ключ через частотний аналіз, оцінка – наскільки осмислений розшифрований текст (метрика score_text_words_ioc).
Тут ключ: "делолисоборотней" довжиною 16 букв.

improve_key робить 5 рестартів алгоритму для знаходження оптимального ключа. Кожен рестарт випадково змінює ключ і залишає зміни, якщо score покращується. У цьому випадку початковий ключ вже був оптимальним → score не змінився.

Фінальний ключ і розшифрований фрагмент:

Ключ Віженера: "делолисоборотней"
Оцінка: 2327.78 (максимальна серед варіантів)
Час виконання: 8.6 секунди
Показано перші 600 символів розшифрованого тексту для перевірки осмисленості.

Аналогічна перевірка інших довжин

```
Перевірка L=8
Початковий ключ: боролисо оцінка: 1720.02
Перезапуск 1/5 — поточний найкращий score=1720.02
Перезапуск 2/5 — поточний найкращий score=1720.02
Перезапуск 3/5 — поточний найкращий score=1720.02
Перезапуск 4/5 — поточний найкращий score=1720.02
Перезапуск 5/5 — поточний найкращий score=1720.02
Отримано ключ: боролисо (довжина 8) оцінка=1720.02 час=8.6s
Фрагмент розшифровки (перші 600 символів):
теиятноеделосшячхклунасильнойьщхсщаканеволткнмэрсзяусиэтудовхррисълустнукистптзврчжинаверноетшлуиоамгдебытонпжпжсщзирекультучтвмхукреждевсегхшег
ояаиежелионошаызгвчствanесдетеяйфутеловекусввьбцпыжевнутренфкгйхзабнымоттогхчвзрекочисленнымфвяучвделенияпатежцщьлемонийиудмрущхинольковнимзтъъ
зьнямособеннхйщнвгнехктонасетдщншкнуныпотомунухцъдыяленостьлейеегцмлужитемупхьжгрьйдолимымпрмфунфйэиемнанеоббджикмкросторахиуфщлляэстречаетсжкна
рьзалолюдейкхчвлюгкокакимтолпэрьцыяазнаеткакпсгллогнамтакинешчфжсяитереснымнпьжйжвывноенисвещуыыудцевысотыдуьецаояеихрелигийпзщтртдпоискcмыстеъг
кдгземнойпитзгнгмямтинно

Перевірка L=24
Початковий ключ: борописйдеролиеобололнсо оцінка: 1638.05
Перезапуск 1/5 — поточний найкращий score=1657.96
Перезапуск 2/5 — поточний найкращий score=1685.74
Перезапуск 3/5 — поточний найкращий score=1685.74
Перезапуск 4/5 — поточний найкращий score=1698.83
Перезапуск 5/5 — поточний найкращий score=1698.83
Отримано ключ: бврохтожззцфсолфблнффунф (довжина 24) оцінка=1698.83 час=8.6s
Фрагмент розшифровки (перші 600 символів):
тсияигснюмеилтесхнондхxвлиноятьолаъдъзльохнзгтфчсуяузюаънлиьпкцвсэонизснюфстеиккккюавзъияррсяйнпниьамщьийхщизйахаськвзъонлитуниефпъдкяакявфиэмнйэ
олаиыьиувхзитъббгеълйчдзеэдеиывсоъмяеииякцфыщсерпзыжышрымчязодйгхкгыдрритюоглнепкмшисвчееррхгйжщугвдыбихвжйьмямрщяояггсвйфудвжцбппзиецриврлжюзаф
зинявдфцымззпгявзжрямяцинмсеиъьхтсзнзххитспндищрърыябырцлщцеяглягщпекыммешуплтйлкггюиеожыпткгйчэфхэиывризмиыыкомвюпнкежцирмхийкьуежчлмклсаихлэясъ
ризабдожжмгдпсиекожнибховмюолеуудрвщьбзжятнгджзелъгнцвхидпзятсъасвлмьейлнзмнетйсайхьзилзифеярияхурцешсфцмвюнцяьъовивмейеипийеэъъкщюйивчдспюлйыюэ
кргзыврцгцвмбэуэмвпмявси
```

Підсумковий результат

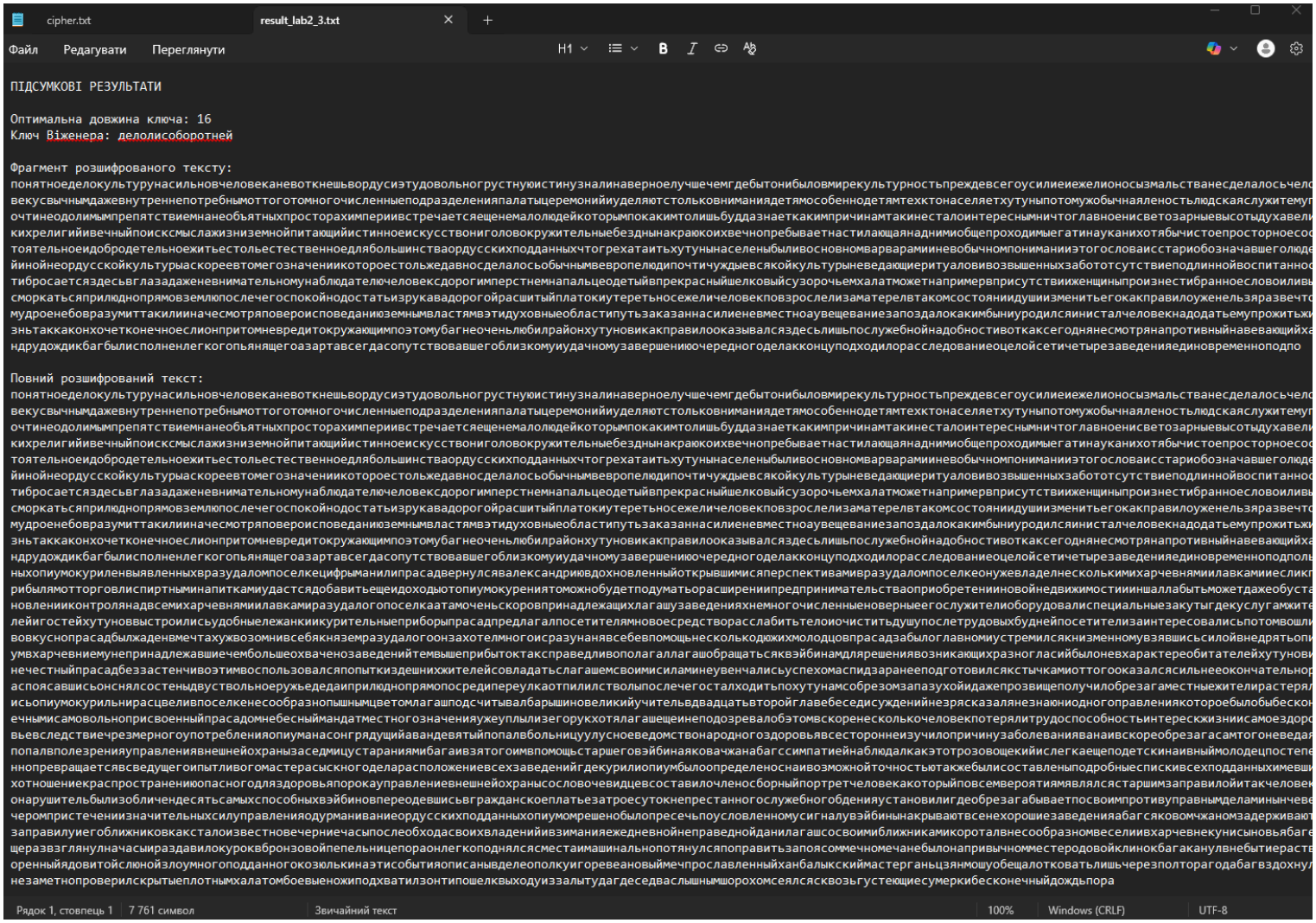
```
ПІДСУМКОВИЙ РЕЗУЛЬТАТ
Оптимальна довжина ключа: 16
Ключ Віженера: делолисоборотней
Оцінка: 2327.78
Фрагмент розшифрованого тексту:
понятноеделокультурунасильновчеловеканеволткнешьвордусиэтудовольногрустнукистинузналинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоуси
лиеиежелионосызмальствanесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподразделенияпалатыцеремонийиуделяютстольковнимания
детямособеннодетямтехктонаселяетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяеще
немалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавноенисветозарныевысотыдухавеликихрелигийивечныйпоискcмыслажи
смыслажизниземнойпитающийистинноеискусствониголовокружительныебезднынакрыкокоихвечнопребываетнастилающаянаднимиобщепроходимыегатинауканихотябычис
тоепросторноесостоятельноеидобродетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварами
иневобычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскорееётомегозначениикотороестольждавносделалосьобычнымвевропелю
дипочтичуждыевсякойкультурыневедающиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаженевнимательномунаблюдателю
человексдорогимперстнемнапальцеодетыйвпрекрасныйшелковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоиливысморкатьсяприл
юднопрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличеловекповзрослелизаматерелвтакомсостоянииудушиизменитьегокак
правилоуженельзяразвечтомудроенебовразуміттакилиначесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиеневместноаувещеван
иезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупрожитьжизньтаккаконхочетконечноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонху
туновикакправилооказывалсяздесьлишьпослужебнойнадобностивоткаксегоднянесмотрянапротивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазар
тавсегдасопутствовавшегоблизкомуиудачномузавершениюочередногоделакконцуподходилорасследованиеоцелойсетичетырезаведенияединовременноподпо
Результат і ключ збережено у файл result_lab2_3.txt
```

Вибір L=16 як оптимальної довжини ключа підтверджується максимальним score.

Ключ "делолисоборотней" використовується для повної розшифровки тексту.

```
Оптимальна довжина ключа: 16
Ключ Віженера: делолисоборотней
Оцінка: 2327.78
```

Результат зберігається у файл result_lab2_3.txt.



Висновки:

У ході виконання лабораторної роботи було реалізовано шифрування та дешифрування тексту за допомогою шифру Віженера. Для різних довжин ключів ($r = 2…20$) проведено обчислення індексу відповідності (IoC), що дозволило проаналізувати вплив довжини ключа на статистичні властивості шифртексту.

Результати показали, що значення індексу відповідності для відкритого тексту є вищим (приблизно близьким до теоретичного значення для російської мови, ≈0.055), тоді як для шифрованих текстів із короткими ключами спостерігається поступове зменшення IoC до рівня, наближеного до випадкового шуму (~0.035). Це підтвердило, що довший ключ забезпечує вищий рівень криптографічної стійкості.

Під час криптоаналізу невідомого шифртексту за допомогою частотного аналізу та статистичних показників було визначено, що ймовірна довжина ключа дорівнює 16, а знайдений ключ — «делолисоборотней».

Використання цього ключа дало осмислений російський текст, що свідчить про успішне відновлення вихідного повідомлення.

Таким чином, у роботі було:

1. засвоєно принципи шифрування за алгоритмом Віженера;
2. досліджено залежність IoC від довжини ключа;
3. освоєно методи частотного криптоаналізу;
4. відновлено зміст зашифрованого тексту та знайдено правильний ключ.

Отримані результати підтвердили теоретичні закономірності та практичну ефективність методів статистичного аналізу при розшифруванні шифру Віженера.