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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
студенти групи ФБ-32
Гереновська Мирослава
Клименко Іван

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.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Варіант: 4

Хід роботи:

Завдання 1:

Самостійно підібрали текст, що містить інформацію про лисиць (об'єм 2 кб), який зберегли у файлі fox.txt.

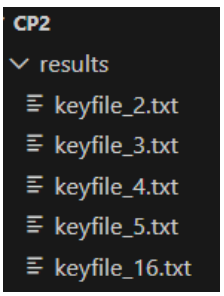
Відкритий текст відфільтрували згідно з методичними вказівками.

```
Текст 'fox.txt' відфільтровано. Довжина: 839 символів.
```

Для шифрування обрали п'ять ключів таких довжин:

r=2 - “ня”
r=3 - “мяу”
r=4 - “лиса”
r=5 - “отдых”
r=16 - “абдоминопластика” (що відповідає вимозі довжини 10-20 знаків).

Наш відкритий текст fox.txt був зашифрований шифром Віженера послідовно кожним із п'яти підібраних ключів. Отримані шифртексти збережено у відповідних файлах у папці results: keyfile_2.txt (для ключа r=2), keyfile_3.txt (для ключа r=3), keyfile_4.txt (для ключа r=4), keyfile_5.txt (для ключа r=5), keyfile_16.txt (для ключа r=16).



Завдання 2:

Провели обчислення індекс відповідності (CI або ж I(Y)) для нашого нормалізованого ВТ та кожного ШТ. Для цього використали формулу з методички:

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1)$$

, де N_t(Y) - кількість появ t букви у шифртексті Y.

Нашою метою було порівняти емпіричні значення з теор. еталонами: індексом відповідності природної мови (теор. значення MI $\approx 0,057$) та індексом рівномірного розподілу I_0 (теор. значення I_0 для рівноімовірного алфавіту становить $I_0 = \frac{1}{32} \approx 0,3125$).

Наші результати обчислень IC (або ж I(Y)):

```
Текст 'fox.txt' відфільтровано. Довжина: 839 символів.
IC (I(Y)) ВТ (r=0): 0.05622
IC (r=2): 0.04507 (збережено у results\keyfile_2.txt)
IC (r=3): 0.03688 (збережено у results\keyfile_3.txt)
IC (r=4): 0.03794 (збережено у results\keyfile_4.txt)
IC (r=5): 0.03704 (збережено у results\keyfile_5.txt)
IC (r=16): 0.03280 (збережено у results\keyfile_16.txt)

Результати IC збережено у results\IC.xlsx
```

Description	KeyLength r	IC (I(Y))
Open Text	0	0,056223883
Encrypted r=2	2	0,045067289
Encrypted r=3	3	0,036883322
Encrypted r=4	4	0,037938676
Encrypted r=5	5	0,037036932
Encrypted r=16	16	0,032795606

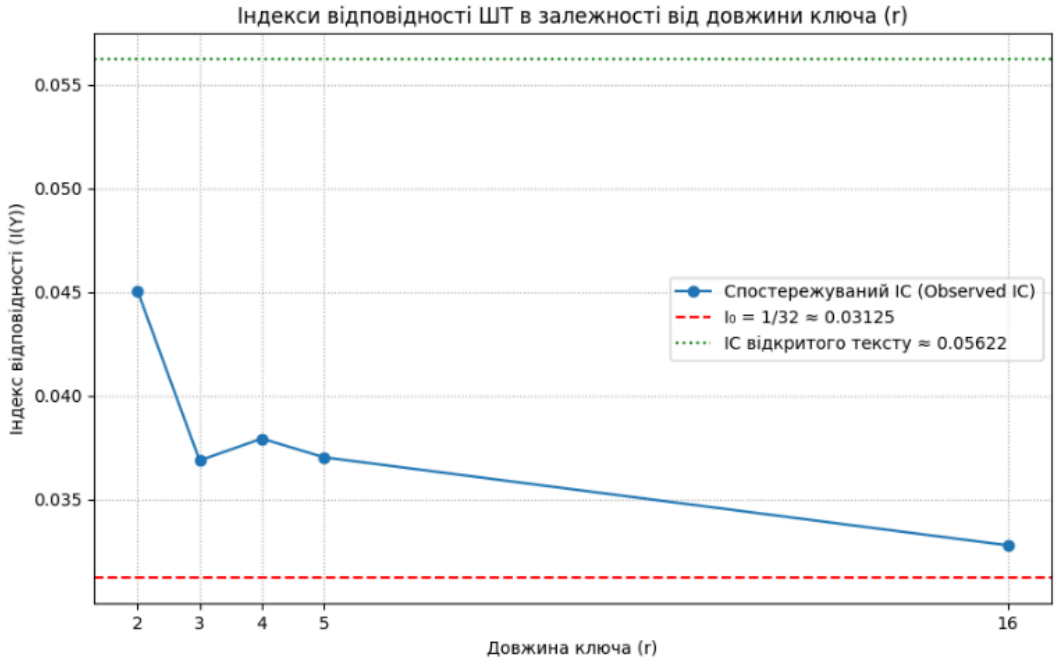
Аналіз результатів:

Обчислений індекс відповідності для нашого ВТ склав I(ВТ) $\approx 0,05622$, що підтвердило його високу частотну нерівномірність, характерну для природної мови (адже отримане значення майже збігається з теоретичним MI $\approx 0,057$).

При шифруванні нами помічена чітка залежність: зі збільшенням довжини ключа r індекс I(ШТ) стрімко спадає, підтверджуючи принцип поліалфавітної підстановки Віженера.

Також, для найдовшого ключа r=16, індекс $I(\text{ШТ}) \approx 0,03280$ є найменшим у ряді та знаходиться максимально близько до теор. мінімуму $I_0 \approx 0,03125$. Звідси маємо, що досягнене нами значення, яке близьке до I_0 підтверджує, що для великих періодів шифр Віженера стає статистично стійким, ускладнюючи криптоаналіз.

Діаграма (IC_plot.png) наочно демонструє стрімке падіння індексу відповідності зі зростанням довжини ключа r, що є візуальним доказом ефективності шифру Віженера:



Діаграму IC (IC_plot.png) збережено у папці results.

```
Діаграму IC збережено у results\IC_plot.png
```

Завдання 3

Нам був наданий шифртекст у файлі cipher.txt для встановлення періоду ключа, знаходження самого ключа та розшифрування повідомлення.

Наш варіант - 4:

фвоьзтыупдыдксыогыъьжкйюыичшчфнъодтмтаангщинпафктмстлзуэешчкффьцтлзуэешчоездфкгдурлкъвитюыргъафешр
щехоипиармъыьшндзинющбцжктгацдщргтйоыцэкхабходйцщцмцмеыоъвюзаъншцокйоспуюафэмоофммъвуряылтымуфл
ъргжцлзтвмшфнъвгпюмьшавеибытншръмжъритжярфрръжжгкхйащомэоятчйлхчжъвсфцюахкоездэтуяуьэшчучйлснлрюб
гцоепхьщпиащъэоуддцшэохфуоъчьучтасвввйхюштсуебчоубшъзэщзчтнгифыущгисрхтаэтгаъфимрзййфешююъутчукзкр
нвтйрыхябййскххэчцупзмжбюриэыздмархдыренртммпырццьоапхялскызцубднсбьггхоубхжоокмшчащякйфпэооэугишс
ррйомижющъмкхбжпдцоефьщйыцдэмбэялчэьгоьтукйзхнгяюймхдксбчиегжмрйучепьэкеюхигяспклаъвюхбпйокбпджодс

ыкыйнювтмущомяьчйыйсупкэомсйчыоьтузьуадаьдачыэоумъкохрзэкмыннлпюыкщйуатежкхкушръдльнбььцзвсщфетэр
фймсмиэыъэшхошэьчифмрюйъфзтмбшчиыьоафопеебчомыьдыоцднщумсхэйсэхожксдлзгыцбэкаупмбюрыыцэзпыбрмних
ушэчццекхмжмняхъынкгкцчбюллтьыаъусефсфвгыцыймуфуыжммхауойроннхооуурхщйарзчсьлкгщъмэшштшзусррлгыйо
яэъдъеишыбтэсюэздзмсябьюийъкнхоъмохыщцяфвхтешохлщиешртехжьуъшрмжкяюзжчэьешгьацаткубеуьшгцлещюкжлъ
всфклвкрзхспюыияуюжпчузмнмллбэслптпкнзяклпэъекекздзмсятясяхумеоисшсъяцлээроумфдиаффэкннкжкхрцъьхжпфвз
ьбснгъьчачнчфмнимсшэзнкнубфьуодаоючщюэидъеиияуьаоснельшиугызлшъвэоьыоомхъэкщвцаиъипаоэмхогрййщыпбьэ
ншнпнйиосичошаощбдмгммифщлъвоетдасяфмеюййбдрйуснррнгнпыккрйсзгьугопумужььнсуьшычудхддрапхчъмьопужд
юьфпцэкшшроскыоьшэмнжатежжятюзупйзаритзябцишмычбъкжбчинюэзнкъкфппюоерамъфьгапжмргчьгыъьдесйъвфею
мкчбнеиьоамфооыугврцпьщлжолоыатумзмсяяьяяшппкнбэллтьъьгуоукйъуфвюъгькудукядссысдчофурлзтсзыъзщюзйрбю
енюцшъмщбртнидопъсийфзццжъенрхсичьзцйачорраьаьцлййййипцвцьйцоъпмймгушрмншызтажфмлъьчабшвсмныуфъочы
ыкжуубьезэухжэшкмдэфвгпяизпфжшхоьаршдмзтэхъпкпотшяизкшрчтмъевфьчбчогапьорцзцючщьдкпдюеоотъюпрэнокю
оуюуябпъктчоыяхмшмеыооужкчьрюрэеъйнеумфпсььегцоенмйстуюыяээрзцмнюомяугыьцпежбьееюецачовртиоофъуънбу
фрмюъпуюяюощонуцофсняуьмьыбчфдщазжоючъбпнубьетыуюыизкохыэдуршъишъзймйърсурвачаткцпюмсшхмийакдпд
юеураялшчжнузъмгвцсдтсзтйьчожшухюъбгуумсрерщфйбупбзмябспурэкбуфйзмпсфгоыьцфбпдэтншэъкшщйэмборгчыза
ыархтйзрсьодекызнхльаешъмъыогуцьтнлжоуыобоьмюъжиточыэхжшемлцгпфсжпхрсжоъвухълекшпклймксьйхгмуубрьы
озюхьгьунбсчхтляьнлшяъкнймрццыъмьцжкркщсхаоюгмырфтоьяфрщыаъужртфмдлэьхзшюжуннммсфучччйоефэмливьш
мнюбмскхсхаучйуъпузкьакюръюшцуфтзизстощгйавпыоънияьщъьыржязъксуъиыьгнфьстфпсьылцфбрбщялыцьйцоъпчы
ырляьрийщвцаймсхаушачочцмйюеухяъзъоуцрьюрлтолвкюиежзснрлчщыфьпкыйфквэуроцоаьцкйтсбошйпбжеыйъепхяю
йощбчтмпоеыцмиьцмздмфахюърймутнцбчьрюяъйлзкрдыщекэоцйцдхзтоосхрюшгчухзднныиуьэлэшвсмкюоуточгмуттйб
ътугпфжтхпейосллвошйбупбсбчюдпаьыспросдцоеаьшывшвуейкхгыомллонкцльекацюахкпушчькргщмгчосхтуиижэъьгъб
бифьнихххщлкшабтчзмсяъоыкпакчскхзиыущгцоннсйфкгшхоцыьмуняящлъьюйъьеуцкчьнюеюймьйтмжчоавьгооьдрдлюя
шяюсмьбстяейлиьущнсоокцйъспгафжынпеокщеъэццвкаткубюаоъоцфпыбьмебвсбафеэрэйтммснрнщгйцсуоьлнлппзжшу
ыкиьченюхмьхбжэдыъвщрбыйъяфзтюмлгтьплпгзцфбнрсымнгйопшцжмжлтьэжпхвохжънвфуоекнйаоьюавъьдахумнпдти
кэкрыщьъшхоьембщзутжюдмгъбурхфжкбунпбщнцоюмьшахсянчиортщйэпзймзцоыхщсещочтчзъокюыъзхцшузммблвучъщуткибьнцыьэчсювьодьафицьгхцубззмзгюяюафщзтйзфисэъсяхуптткыуфвцоыъпврйоътепхмжтпзцумсксбщъэчьсуиьчмр
хаъфтчокькцбсыамэвцлцгпыовбоънцуъпдммзлыьцйвшвсмдцуухръзшянеедовиауоеэяфдздоаеибкюшюнужджщувяюъкэяф

нпьэкеюхиккщюыяйсснющиешъзродбмсэуюзкщрздоъдсаьпйуърорьчоераъмхупытеьадюамавкгклкпормш
мэщюрьйиюан
гффьеаюзтгимцтшмтпяфзйьоарбоъмбоучпдоиорнплкпкчйзлшелюлъпъхфтащожшэямььлсйфъкляюсяээтк
идчавзуьасэвхч
ащемнаъдружуфкпомэоуыоэркипюангфноокжуемыофвоьыуябсййлниаоуйботужьюьпгффечурчфчоавюаш
ачнйездынсвцу
гъьдесйъгстхпжйтвсйачерэьщыныхрхыыозэнчзпжрпмгмсхлщэншщгццкчбсьысэыцнещфсвиыкщоькудебу
мсхсъэптрсдж
мкхющиешсрхйяьадшасжжямхязэялчрфяэнжкджюиешюъэкщвмджчиррыфатэрмжкчиорюъзкжмкубьемв
цэюкщрфдймлб
сцшоиуачфпэццяцэчцьйекьюоитьолпъбфтаэчиворачуешрбщяпхфрофьнксыширхъщйньсурычофмцянъоф
нпкюоерющцур
кйжльоъхъьыыяхймзмяжыооишупктрърпыущгпоууибьжгэцсйчьзлйжъмтхыэгъьдепкщезюяюыьшкхйлсй
рюсъжтяфемны
оомхъэкыпузкоунаьшишъокхосажррънчомусбвиссьшипэвхднюрсъхмятвкхдинапшхмюктрьскшугаюмефа
ххчльотгяюгвк
ктйгммивцдчсодхйилодгеситндзяндемишъжпевхтасееяцагуцфхдющищртскьшвзтзихгяюъъмцнехбнякэок
йбупбузъхсэуя
мттщнжьщеххюыахцдехюъееющиикхпеокшавяуэийщажмоулюхжянфцктйкрнсъюмнчьскфбщофшафрыр
рцудюарэццймы
взтныихрасжпчячткщпуюрсяъьщчтзфдгсйчйштпужбреуъьрймьнбскъбэхъфмььзццкллсбуначогепжснгфто
аъкастбхксьым
нелжеодхсгьърахкпанжмпнрыщыыьукибхпсишъжжырсчкнщицциюгитвжяйспсторишпэртэсзфяюъмэьжеп
вфвгвкязпыбптй
эпиъазгфоучфъчифэооыъуптяищархтсжипрхэкшмсцуюобцфкпшюансйщаъойулзфлфпуэжтпэзйаьоебуюы
фцрффкциргщъ
мжопкчлмлсхъяиксрртюясхючшъмъзццбэвсфьхйьщкьдбюсвауретъкцукэодэьэнйъкпуммкхшесмфьлнцбър
ивцгаышрорьп
илбцччьтелюфтсщцщнэцшнйеныфвюъыоосчммяехбнципяфесамрхэьхмтахеъдфхгьътаьнзюййсбичымяп
фпесбырлыцгик
нмеоьлтсуюмитдвшикпеелбйжжврзжчэоншуюлкрэшзйъмстяцыхйхздачанюрплэтэзяэьоыхыщйуывфтюср
шэьэнжхзспдяд
ушоряэпэфташехрмегпьгрджмузабфяшрмербщнюхшьонцхрвасйссщякхуптябэтиэйцычонахгмтшыьхэштр
офьудиыущиеу
сефкхтуючцйуэрйюбшнюеъъмььдйдззсюхяюлкфпнодырлэцбьоцфкпшщозаушжизккчлфргпяиикюиежчса
охпмлойвмибэь
сбцщцтхжкжьюеомяюэшшвптбюосбьначыркхзфуъхяючбарлмосллфьпамйдерлфрюеььйвцзчджфесбцщц
ыуткемфсхлуюл
пэзючхфекрьэгчоонэбцоъхащальрццмъвиагфдпщрзяецоехюэлпткптоърсуьцйпсжкумъгоптзэкмфмдоьаеы
ущиеугкфбукл
шяъмпымнхьшайхтъюпрврйвфтефьчгчумеолчюыъощыоызхдныифэьхктонайнчифььюлпаюцщкчмгъюмъ
щцвряюфдиэпс
жечржтаъклчьэгчрфуфкхпсвьчфпэрчйищеишхсжпчвзъбщтухжфлшшрклбчерюуришямхдлъчнръфмкъвйтя
свгтшъжждззт
греорыщцяэррйефодыоцыяахсдймпсфьхяпжюзузътргмцяпюззаышнгбамэхннсййлуъшасжжцсуьзсшяьйэж
пыпаннфгррщо
юхбгбпбэаоопъдцьикьшрупраийбуошзкрнсыцдчлйущтмшиуюрмнжърюспктиыуыыьцщкхжяюеющщокш
рсчищеихымкъо
днцшщассзсдбоучтоскхюыфьэтюнлнюргцухюъопнъчясолжфнйяошэбщнсъоджйыхрдзячыхпзацбячтяъни
бщзукаютйкняк
расжжырффкруплрмнжьщкфбрнцоэмешяфблймюкэокнеывтмсэвиагомйшрорбьыжююмвоопусьэемаоукш
яфефьхсвтьуяп

юиецшэясвьщцяьщкрщюовргрышрррсбоапяцьцшезтаюъстацфзбцдаоослияоюгтцухдгяохаумютюхгцймеияюфмэаучждсх
свнфипяоузпюдсбшъикщюттммсышвьймофбцьцчхюымктювосьцоошесмьрресбщанресмьррзтоюанпяшйьюатдазмвйбкьк
ыатдиърьшрчйльфшхбьдлпцщыцьазтзщухгатаъувиммяюхянючтщкэйнюьгфуыншрмуцкьыиюрсъчыэкуььоптйнаноачмгр
виаухгмйсхяяфвгоафвшшртдомкстощиеудтйгмпрюьтгмжксмюснлъошгъбмнепруьшгцйхщзильщяхлжмдфоонумфкулрм
щгцонтооершшъэыооуйнъкуюрсичьзшыдюеомбэзтюбкцюснлъцъячцойждтершушьъьднскозжынрцкттккхкоарэйсуэапнъб
щезюъзнеъкптзчежръфипяхргощиъхсършюрэйяъяфъоуыхэрйчимтярыснъопцпдьоераивкшннсьщивцоччбармдяъдюяюъэ
птзтсчсвавцбмьупещозтгъцщачохьмзмсяфбшыькщчтврупрмэншмсуикэирючщыцьтюмючодшюъзкжмечвсчхюаъбэуфмйз
снгпячщчоууыдюсвшхгаъыэъчяълнюрныъгвчмнюышубнлкхжкпбщнюешъжждвсмприовучащофнфкоахмхщыбцфцтгщах
хщииштзрмоисвьйэжйъкцобшнлсбрчоюхимиреоояикшянкийфмлчщсмкабтйоырсещмяшчуниыеавэооаьшзнжкчгггтфэху
пттлъкгзцоыпачзтнюоптьюэпаперкфупбаоачыэкукюужшщфьшхвтгофесъоуыхьубрйснияьуолоормэъоырюмупыпайнюрг
ццплкыкыялъпгфочгчоокхоссурфсичйзстбхмсйыъдобоуниъифвоьычцбшжбщчгыцэчэяскщкшмлэбютпюзмхкьоншхмшьь
дхйиляцбэсжкэзхйаямгвкнйхкъкыбшзгяюсяетхюмбоофхъщыодвчазстгтьюгъуйшпшюахрсмкштзохоооерщъгхцртумъхсф
цчзтърцппгамэьлэщутзябявлфучымоофмммвсчъъбчьзцпднысэръвчцмнлйфохъбрылйнжпбреръоцмцутчадщезтбэзеянксй
ъснрщфжшштужьолиэызасбгагэзежюцэкэсврдникгъяъыадксйъитыощгъьдепьшолчымитндуезмсхшрмзщцтужбрершнны
сцтужьчифмымтпщрзйуссншгчанупйдсфпухтмитнчуцзфчгтжфрынткижъсхэйшкпяунрдумсьшюйцбикжнсгуррклешвхцд
щыжюпсжпыэтднцаомымърцдуудэьлчьнлкфвгцюммтшюъэтямрвуфтиыкщйчьщбвдотиьыънпштапшлзцсйцйнакзхбйтсъо
таьябчджфмфвюмучйонтяьопэйшншщюптлътсьбгншаррокшнлзупйчунблыьакущляпаюйсбонсщяоаьювмжбллсауъжэфвц
дюыушшэъыяэтнхкчнизыъзырзчйймфсэунаыштенйфхтющсдтрэцтжфхзхюсэжудздиыиуяьцысонцгищеею
хшоьцфкпшщо
пхщцгццгклкнизэйшкъодйдысщиэуэкпжкрдниатацджшяюссбпаорыюишэткизъжлыцьофбдухлълячьоыькудокюоуючокъь
щкрыщеушяциэщвздиыиугщзьчбнцглъкгчоояхцптябцлюъцчщльлшпчннцыяльебднибокгънэкшщйрднжешрщмкшштшцк
шууюъмуфцпурпнонгэслпшктчюыоеютиъбуткляълстбчйвожнгюзжлфокфпбучдюфлгбкщымоофмммсхаотюъопнъчъкгчо
чмйрээйиснвэоыйхсрртюзшлаьцэщщзьдсфвибкшычужшфбщсссьхяхцптябюепэйсэшщрцякнргьщлжтбйптбуажююсжшун
нъкэлсцущиеуйехлфнсщшьцхкбффдраершфэкъснфпщенюаълшууътаэтеюяшйъьзсибшорюъыйыщвтсдцопбъсльцжкхыю
игажфичобццьюувъьюйъьеучжьаырщмыфарзяеуаотйэупчъптззчиаызащюртлдюеомызаббфбфьэксбйсюхойежьшплаофвэ
екрмиъюпрщъкъцдрйжмтиыкщоирпкьйъсхмыънкшктйнямиыцьыссвйдоичхюхмипчууомзтс

Для знаходження істинного періоду ключа r використали два алгоритми, які були надані в методичці. Перевірку проводили для всіх можливих довжин r в діапазоні від 2 до 30. Обидва алгоритми реалізовані вже в коді cp_lab2_3.py.

1-й алгоритм (IC усередненого значення по блоках):

Принципом алгоритму є те, що усереднене IC блоків має бути максимальним, якщо r правильне, оскільки це IC наближається до теор. IC природної мови (MI $\approx 0,057$).

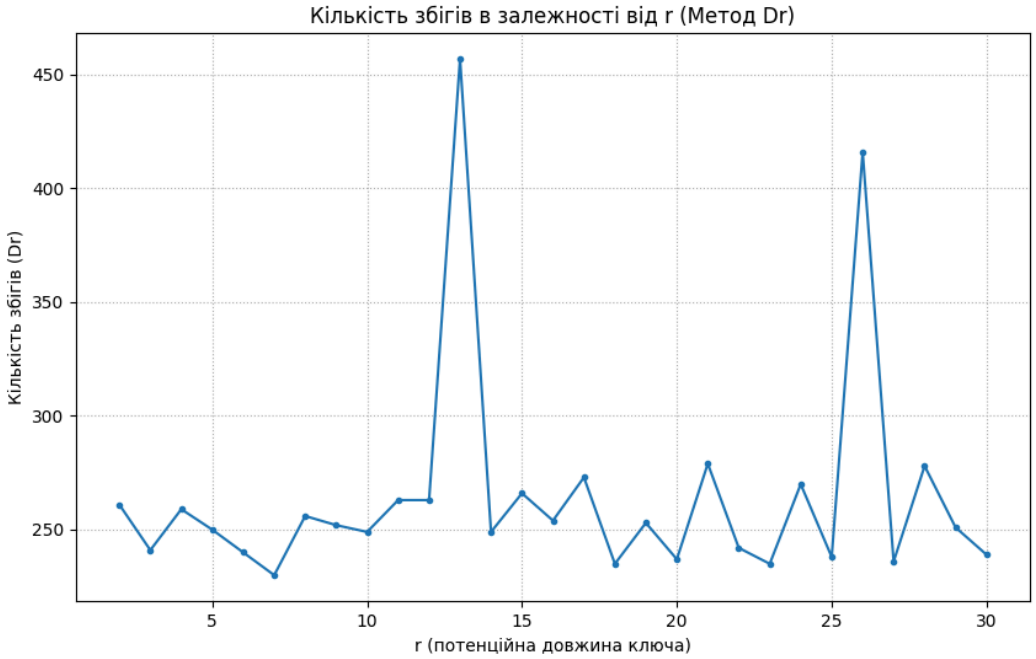
У нашому коді реалізовано обчислення IC для кожного блоку, усереднення цих значень і автоматичний вибір r, що дає найбільше усереднене IC.

В результаті, найбільше усереднене значення IC було отримано нами при r=13.

2-й алгоритм (Статистика збігів D_r):

Принципом алгоритму є те, що значення D_r буде мати виражені піки при r та його кратних, оскільки на цих відстанях частіше зустрічаються однакові символи.

У нашому коді реалізовано обчислення D_r (к-сть збігів однакових літер на відстані r) та побудова діаграми для візуального аналізу.



Проаналізувавши діаграму, ми помітили, що чітко спостерігаються виражені піки при r=13 та при r=26 (оскільки 26 = 13× 2 = 26). Наявність піків на кратному значенні є класичним підтвердженням методу, що свідчить про істинний період r=13.

Діаграму D_r(analysisDr.png) збережено у папці results.

```
Діаграму Dr збережено у: results\analysisDr.png
```

Отже, фінальний визначений період - r=13.

```
Використовуваний період ключа (r): 13
```

Далі перейшли до знаходження ключа:

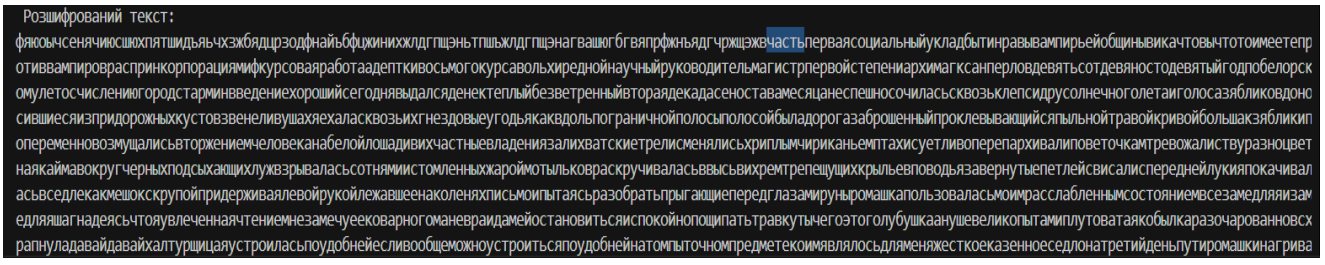
Після встановлення нами періоду r=13, шифртекст був розбитий на 13 незалежних блоків Y_i.

При першій спробі дешифрування ми застосували метод з методички : знайти найчастішу літеру у кожному блоці шифртексту та припустити, що вона відповідає найчастішій літері російської мови - “о” (x*). У нас виникли труднощі: ми отримували в результаті нечитабельний набір символів, що свідчило про неправильно знайдений ключ. Ймовірніше, проблема полягала в тому, що спрощене припущення (y *−> x *) є лише ймовірнісним. Воно працює лише якщо блок тексту достатньо великий, щоб його частотний розподіл точно збігався із загальномовним. У нашому випадку статистичний розподіл літер у відносно коротких блоках (через r=13) виявився неточним, і “о” не була тією літерою, що відповідала у більшості блоків. Методичні вказівки пропонують у такому випадку вручну брати другу, третю і тд за імовірністю літеру. Щоб уникнути ручного перебору, ми автоматизували цей процес, реалізувавши повний статистичний аналіз (метод максимальної кореляції). Наш алгоритм послідовно перебирав усі 32 можливі зсуви (k_i) (кожен потенційний символ ключа) для кожного блоку. Для кожного зсуву він обчислював кореляцію - показник того, наскільки частотний розподіл літер в отриманому розшифрованому блоці схожий на еталонний розподіл рос. мови. Було обрано ту літеру ключа, яка давала найвищий показник кореляції, що дозволило коректно знайти повний ключ.

Знайдений ключ: АГРОМЫКОВЕДЬМ.

```
Знайдений ключ: АГРОМЫКОВЕДЬМ (Довжина 13)
```

Використовуючи знайдений нами ключ АГРОМЫКОВЕДЬМ, здійснили повне розшифрування шифртексту:



Ми помітили, що початкові символи розшифрованого тексту є шумом, який виник через фазовий зсув, викликаний особливостями вхідних даних. Оскільки подальший текст є повністю читабельним (починаючи з частьпервая), це підтверджує коректність знайденого нами ключа АГРОМЫКОВЕДЬМ та періоду r=13.

Повний розшифрований текст збережено у файлі decryptedtext.txt у папці results.

Висновки

Виконання комп'ютерного практикуму 2, дозволило нам засвоїти методи частотного криптоаналізу та здобути навички аналізу потокових шифрів на прикладі шифру Віженера.

Проведені обчислення індексу відповідності (I(Y)) для ВТ та ШТ підтвердили теоретичні засади шифру Віженера. Індекс $I(\text{ВТ}) \approx 0,05622$ підтвердив частотну нерівномірність, характерну для природної мови MI $\approx 0,057$. Обчислені I(Y) для ШТ продемонстрували, що зі збільшенням довжини ключа r, I(Y) стрімко падає, оскільки шифр Віженера є поліалфавітною підстановкою, яка розподіляє частоту символів. Для максимального перевіреного періоду r=16, індекс $I(\text{ШТ}) \approx 0,03280$ максимально наблизився до до теор. мінімуму $I_0 \approx 0,03125$, що підтверджує: для великих періодів шифр стає статистично стійким.

Також, було проведено криптоаналіз ШТ 4-го варіанту. Період ключа r=13 було встановлено за допомогою алгоритмів, що були надані в методичці: ІС усередненого значення по блоках та Статистика збігів D_r. Шляхом застосування методу максимальної кореляції (повний статистичний аналіз) до 13 окремих блоків, було знайдено ключ АГРОМЫКОВЕДЬМ. Здійснили розшифрування тексту. Початковий шум у розшифрованому тексті виник через фазовий зсув, не впливаючи на коректність знайденого ключа.

Таким чином, було підтверджено, що криптоаналіз шифру Віженера можливий при умові, що період ключа r є значно меншим за довжину самого шифртексту.