Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”
Фізико-технічний інститут

Лабораторна робота № 2

з предмету «Криптографія»

«Криптоаналіз шифру Віженера»

Варіант 3

Виконали:
Студентки ФБ-33
Яремко Аліна,
Журавльова Марія

Київ - 2025

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

Постановка задачі:

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.

Ключі:

```
meaningful_keys = [
    "он",                   # r=2
    "дом",                  # r=3
    "шкаф",                 # r=4
    "мосту",                # r=5
    "хозяйкой",             # r=8
    "одинмолодойчел",       # r=14
    "вначалеиюлявчрезвы"    # r=18
]
```

Результати зашифрування збережено у файлі all_ciphertexts.txt у вигляді:

```
--- ВІДКРИТИЙ ТЕКСТ ---
вначалеиюлявчрезвычайножаркоевремяподвечеродинмолодойчеловеквышелизсвоейкаморкикото
руюнанималотжильцоввсмпереулкенаулицуимедленнокакбывнерешимостиотправилсяккнумостуо
нблагополучноизбегнулвстречиссвоеюхозяйкойналестницекаморкаегоприходилаьподсамоюкр
овлейвысокогопятиэтажногодомаипоходилаболеенашкафчемнаквартируквартирнаяжехозяйкаег
оукоторойоннанималэтукаморкусобедомиприслугойпомещаласьодноюлестницейнижевотдельной
квартиреикаждыйразпривыходенаулицуемунепременнонадобылопроходитьмимохозяйкинойкухни
почтивсегданастежьотвореннойналестницуикаждыйразмолодойчеловекпроходямимочувствовал
какоетоболезненноеитрусливоеощущениекоторогостыдилсяиоткоторогоморщилсяонбылдолженк
ругомхозяйкеибоялсяснеювстретитьсянеточтобонбылтактрусливизабитсовсемдаженапротивно
снекотороговременионбылвраздражительноминапряженномсостоянииипохожемнаипохондриюондо
тогоуглубилсявсебяиуединилсяотвсехчтобоялсядажевсякойвстречинетольковстречисхозяйко
йонбылзадавленбедностьюнодажестесненноеположениепересталовпоследнеевремятяготитьего
насущнымиделамисвоимионсовсемпересталинехотелзаниматьсяникакойхозяйкивсущностионнеб
оялсячтобытанизамышлялапротивнегоноостанавливатьсяналестницеслушатьвсякийвздорпровс
юэтуобыденнуюдребеденьдокоторойемунетникакогоделавсеэтиприставанияоплатежеугрозыжал
обыиприэтомсамомуизворачиватьсяизвинятьсялгатьнетужлучшепроскользнутькакнибудькошко
йполестницеиулизнутьчтобыниктоневидалвпрочемнаэтотразстрахвстречиссвоеюкредиторшейд
ажеегосамог

--- Шифротекст для ключа r=2, Ключ = 'он' ---
ръодошухмшнпеэуфриенчъьуоэшыупютъмэытпудуэьсцъъыщытычдушьпучрижтщххюрыуцшнъыючцчьяь
эблыныхънщыауцшкгьпрюъьуэуащчуъоащхдацщусцтыъьчочпиръуэуецщьюахьяээопцшямшчыаъыяябы
ыющнсыэыщаеъьххоурыащпяяютехяюрыулгыхмччьцынщтяяыхдтшнъыючотсыээцвьсцшоюкььсянъымчю
ыршуцрияышысыэмахляоуыысытыънцьывьсцшооьшутынжчобетъъочрнюяцэбчрнюяцэыннуувьфнцшнур
ьашыаыюычыыъоъцщошлябчощьэшаяыпттыъхээцющасычьыщужошоюкытъьлщтяяыхдтчъцуупьяттщйыыч
чрнюяцэухшнфсйцюнхьюхригыттынбшцгбтъаытээущуъыыынтыпищыээьвьсцякщцщьвьфнцшхыыччбвых
эыеяцпятссоъоюатфйьярыютыъьцынщтяяыхдацчоутичэофъыщытычдушьпучээьвьснщцщьдбпяярырнщ
чочьтаыпыщтхъуъыыухаэбющхрыуызазтыхучьяьэърьюаитхщюнхьяшыаыюысыъыюжцшямъъпищсьшфтыч
```

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

Теоретичний індекс відповідності для російської мови було знайдено за допомогою результатів з першого практикуму та формули: $I(Y) = \sum_{i=1}^{M} p_i^2$

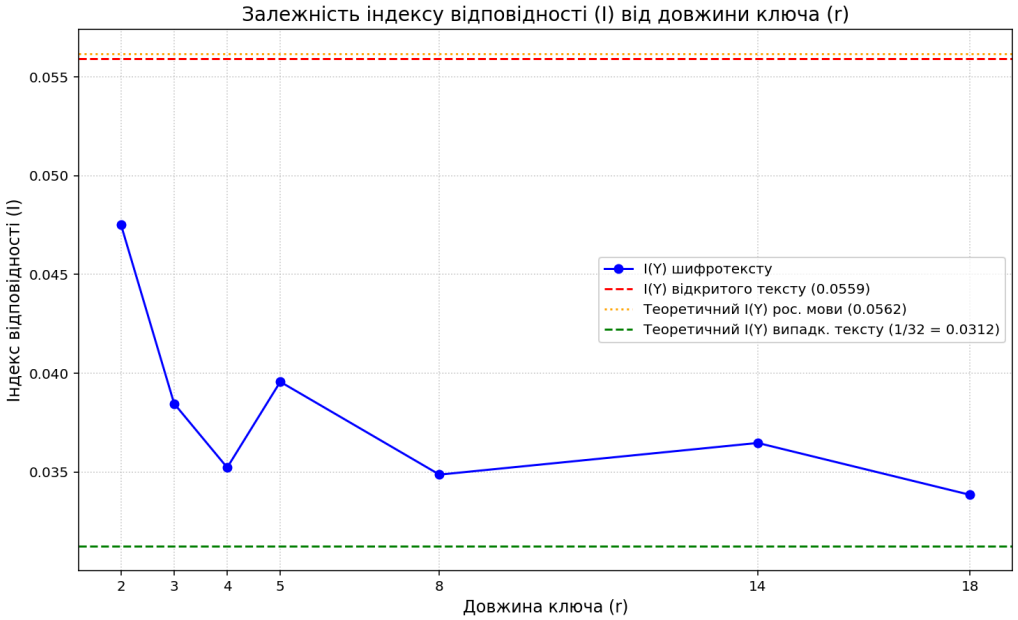
Теоретичний індекс відповідності випадкового тексту знайдено за формулою: $I(Y) = 1/M$, де M - розмір алфавіту.

Індекс відповідності для реального тексту обчислено за формулою: $I(Y) = \frac{\sum_{i=1}^{M} n_i(n_i-1)}{n(n-1)}$, де n_i - кількість появ і-тої літери у тексті, а n - загальна довжина тексту.

Індекси відповідності для обраних ключів:

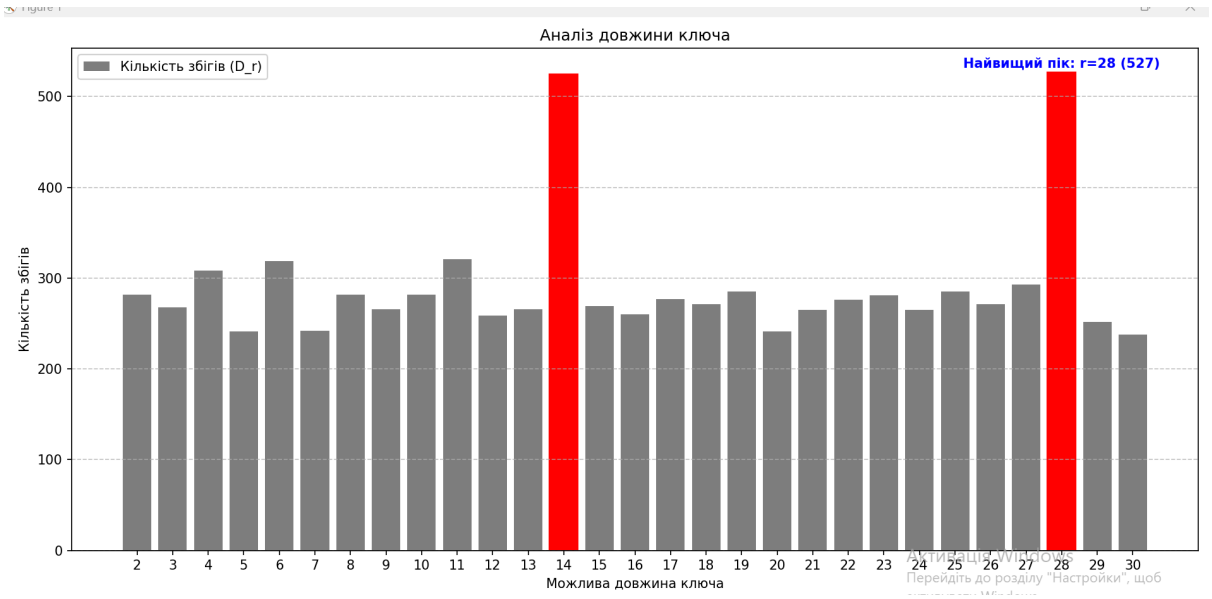
```
Індекс відповідності для відкритого тексту: 0.055941

  r =  2, Ключ = 'он', I(Y) = 0.047508
   -> Шифротекст додано до файлу: all_ciphertexts.txt

  r =  3, Ключ = 'дом', I(Y) = 0.038465
   -> Шифротекст додано до файлу: all_ciphertexts.txt

  r =  4, Ключ = 'шкаф', I(Y) = 0.035225
   -> Шифротекст додано до файлу: all_ciphertexts.txt

  r =  5, Ключ = 'мосту', I(Y) = 0.039568
   -> Шифротекст додано до файлу: all_ciphertexts.txt

  r =  8, Ключ = 'хозяйкой', I(Y) = 0.034868
   -> Шифротекст додано до файлу: all_ciphertexts.txt

  r = 14, Ключ = 'одинмолодойчел', I(Y) = 0.036471
   -> Шифротекст додано до файлу: all_ciphertexts.txt

  r = 18, Ключ = 'вначалеиюлявчрезвы', I(Y) = 0.033844
   -> Шифротекст додано до файлу: all_ciphertexts.txt
Шифротексти збережено в одному файлі: all_ciphertexts.txt

Діаграму збережено у файл: ioc_dependency_graph.png
```

Графік залежності індексу відповідності від довжини ключа:



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

Спочатку робимо діаграму зі статистикою D_r



Бачимо що найвищі піки спостерігаються у періодів 14 та 28, це наймовірніші довжини ключів.

Для розшифрування ми намагалися підбирати ключі обидвох довжин але ключ довжиною 14 виявився правильнішим

Після того, як ми визначили, що довжина ключа 14, ми запустили скрипт, який:

1. Розбив весь шифртекст на 14 "колонок" (блоків).
2. Для кожної з 14 колонок знайшов найчастішу літеру.
3. Припустив, що ця найчастіша літера відповідає літері найчастішій у мові (‘о’ у випадку російської).
4. На основі цього припущення знайшли перше значення ключа: 'эбомацтникфуьо'.

Цей ключ дав нам частково читабельний текст, але з багатьма помилками. Методом підбору було встановлене коректне значення ключа “екомаятникфуко”

Розшифрований текст:

Итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвел
ичииописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопери
одколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеирраци
ональноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаеток
ружностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодно
гополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевне
временныхмерединственноститочкикрепленияидвойственностиабстрактногоизмереният
роичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеязна
лчтонаконцеотвеснойлинииивосстановленнойотточкикрепленияинаходящийсяподмаятни
коммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвеч
ностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинекот
ораянепротиворечитзаконуфуконапротивпомогаетемупроявитьсяпотомучтопомещенны
йвпустотулюбойточечныйвеспиложенныйкконцунерастяжимойиневесомойнитиневстр
ечающийнисопротивлениявоздуханитрениявточкекрепленияидействительнобудетсоверш
атьрегулярныеигармоничныеколебаниявечномедныйшарпоигрывалбледнымипереливча
тымиотблескамиподпоследнимилучамишедшимиизвитражаеслибыкаккогдатоонкасался
слоямокрогопесканаплитахполаприкаждомизегокасанийпрочерчивалсябыштрихиэтишт
рихинеуловимоизменяякаждыйразнаправлениерасходилисьбыоткрываяразломытранше
ирвыиугадываласьбырадиальнаясимметричностькостякмандалыневидимаясхемапентак
улазвездымистическойрозынетнетэтобылабынерозаэтобылбырассказзаписанныйнаполо
тнахпустыниследаминесосчитанныхкаравановповестьотысячелетнихскитанияхнаверно
еэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасманиивг
ренландиюоттропикакозерогактропикуракасостровапринцаэдуарданашпицбергенкасан
иямишараутрамбовывалосьвминутныйрассказвсечтоонитвориливпромежуткахотодного
ледовогопериодадодругогоискореевсеготворятвнашевремясделавшисьрабамиверховник
оввероятноперелетаяотсамоананововуюземлюэтотшарнацеливаетсявапогеепараболынаага
ртуцентрмираячувствовалкактаинственнымобщимпланомобъединяетсяавалонгипербор
еевсполуденнойпустынейоберегающейзагадкуайерсроквданныймигвчетыречасаднядвад
цатьтретьегоиюнямаятникутрачивалскоростьукраяколебательнойплоскостибезвольноот
шатывалсяснованачиналускорятьсякцентруинаразгонепосерединерассекалссабельнымс
вистомтайныйчетвероугольниксилопределявшихегосудьбуеслибыяпробылтамдолгонеу
язвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечникэтотопрокин

утыйгребеньшлемавычерчиваетвпустотесвоидиагоналиоткраядокраяастигматическойза
мкнутойлиниииялпревратилсябывжертвуобольщениячувствимаятникубедилбыменячтоко
лебательнаяплоскостьсовершилаполныйоборотивозвратиласьвпервоначальноеположен
иеописавзатридцатьдвачасасплюснутыйэллипсэллипсобращающийсявокругсобственно
гоцентраспостояннойугловойскоростьюпропорциональнойсинусугеографическойширо
тыкаквращалсябытотжеэллипсбудьнитьмаятникаприкрепленаквенцухрамасоломонавер
оятнорыцариииспробовалииэтоможетбытьихрасчеттоестьконечныйрезультатрасчетанеиз
менялсяможетбытьсобораббатствасенмартендешанэтодействительноистинныйхрамвоо
бщечистыйэкспериментвозможентольконаполюсеэтоединственныйслучайкогдаточкапо
двешиваниянитирасположиласьбынапродолженииземнойосиимаятникзаключилбысвой
видимыйциклровновдвадцатьчетыречасаоднакоэтоотступлениеотзаконактомужепредус
мотренноесамимзакономэтапогрешностьпротивзолотойнормынеотнималачудесностиуч
удаязналчтоземлявращаетсяичтоявращаюсьвместеснеюисенмартендешанивесьпарижсо
мноюивсемывращалисьподмаятникомкоторыйдействительнонискольконеизменялориен
тациисвоегопланапотомучтонаверхугдеонкчемутобылпривязаннадругомконцевообража
емогобесконечногопродолженияниттиввысотуивдальзапределамиотдаленныхгалактикна
ходиласьнедвижимаяинепреложнаявсвоейвековечностимертваяточказемлядвигаласьодн
акоместоккоторомуприкреплялсяканатбылоединственнымнеподвижнымместомвселенн
ойпоэтомумойвзглядбылприкованнестолькокземлесколькокнебуосиянномутайнойабсол
ютнойнеподвижностимаятникговорилмнечтохотявращаетсявсеземнойшарсолнечнаясис
138тематуманностичерныедырыилюбыепорожденияграндиознойкосмическойэманацииотп
ервыхэоновдосамойлипучейматериисуществуеттолькооднаточкаосьнекийшампурзанеб
есныйштырьпозволяющийостальномумируобращатьсяоколосебяитеперьяучаствовалвэт
омверховномопытеявращавшийсякаквсенасветесообщасовсемнасветеудостаивалсявиде
тьтонедвижноекрепостьопорусветоносноеявлениекотороенетелесноинеимеетнигранлц
ыниформынивесаниколичестваникачестваионоевидитнеслышитнеподдаетсячувственн
остиинепребываетнивместенивовремениниврпостранствеиононедушанеразумневообра
жениенемнениенечислонепорядокнемеранесущностьневечностьононетьмаинесветонон
еложьинеистинадоменядолетелпасмурныйобменрепликамимеждупарнемвочкахидевице
йувыбезочковэтомаятникфукоговорилеемилыйпервыйопытпроводиливпогребевтысячав
осемьсотпятьдесятпервомгодупотомвобсерваторииипотомподкуполомпантеонадлинакан
аташестьдесятсемьметроввесгиридвадцатьвосемькилонаконецвтысячавосемьсотпятьде
сятпятомподвешентутвуменьшенноммасштабеканатпротянутчерезнижнюючастьзамкас
водаазачемнадочтобыонболталсядоказываетсявращениеземлипосколькуточкакрепления
неподвижнаапочемуонанеподвижнапотомучтоточкасейчасятебеобъяснювцентральнойт
очкелюбойточкенаходящейсясредидругихвидимыхточеквобщемэтоуженефизическаяточ
каакакбыгеометрическаяитыеенеможешьвидетьпотомучтоунеенетплощадиатоучегонетп
лощадинеможетперекоситьсянивлевонивправоникверхуникнизупоэтомуонаневращаетс
яследишьеслиуточкинетплощадионанеможетповорачиватьсявокругсебяунеенетэтогоса
могосебяноэтаточканаземлеаземлявертитсяземлявертитсяаточканевертитсяможешьневе
ритьеслиненравитсясномнекакоеделонесчастнаяиметьнадголовойединственнуюстабил
ьнуючастицумиратонисчемнесравнимоечтонеподверженопроклятиюобщегобегаисчитат
ьчтоэтонееееаегоделовследзаэтимчетапошлапрочьонобнимаясвойсправочникотучивший
егоудивлятьсяонаволочасвойорганизмглухойксердцебиениюбесконечностииобаникакне

пытаясьзакрепитьвпамятиопытэтойвстречиихпервойиихпоследнейсединымсэнсофснев
ысказуемымонинепалинаколенипередалтаремистиныягляделсвниманиемистрахомимне
поверилосьчтоякопобельбоправвсегдашниеегодифирамбымаятникуяпривыксписыватьн
абесплодноеэстетствозлокачественноекотороемедленноразъедалоегодушуибесформенн
оеперенималоформуеготеланезаметноперекодируяигрувреальностьжизниоднакоеслибе
льбобылправнасчетмаятникавероятноонбылправинасчетвсегопрочегоибылпланибылвсе
общийзаговорибылоправильночтояоказалсяздесьсегоднянаканунелетнегопротивостоян
иякопобельбонесумасшедшийемупростопривелосьвовремяигрычерезигруоткрытьисти
нуделовтомчтосопричастностьбожескомунеможетпродолжатьсядолгонепотревоживрасс
удоктогдаяпостаралсяотвестивзглядпрослеживаядугукотораяоткапителейрасставленны
хполукругомколоннуходилаподпираемаягуртамисводакключуповторяяуловкустрельчат
ойаркиумеющейоперетьсянапустотувысшаястепеньлицемериявстатикеиуговоритьколо
ннычтоониобязаныпихатьвверхребрасводааребрамраспираемымдавлениемзамкавнушит
ьчтобониприжималикземлеколонныносводещехитреонявляетсяивсеминичемипричино
йиследствиемвединомлицеоднакоямоментальнопонялчтоотворачиватьсяотмаятникасви
сающегососводаиразмышлятьвместоэтогоосводетожесамоечтозарекатьсяотродниканоп
итьизисточникахорсоборасенмартендешансуществоваллишьблагодарятомучтоимелсущ
ествованиевпрославлениезаконамаятникамаятниксуществовалтолькопотомучтосуществ
овалсоборнесбежишьотбесконечностиподумаляудираякдругойбесконечностинеубереже
шьсяотвстречистождественнымпытаясьотыскатьиноепопрежнемунеотводяглазотключа
соборногосводаясталпятитьсяотступаяшагзашагомзавремяпрошедшеесмоментаприхода
ядетальнозаучилрасположениезаладаимощныеметаллическиечерепахипатрулировавши
естеныпостоянномаячиливуглуполязренияпропятившисьчерезвесьнефдовходнойдверия
сноваоказалсяподсеньюгрозныхптеродактилейизпроволокиитряпокзловещихстрекознев
едомочьейоккультнойволейзасланныхподпотолокнефаонивыступалиметафорамизнания
значительноболееглубокимичемвероятнозамышлялдидактразместившийихвназидатель
нойпоследовательноститрепетаниенасекомыхирептилиймезозояаллегориябессчетныхм
играциймаятниканадповерхностьюземлиархонтыизвращенныеэманациионипикировали
наменяцелясьархеоптериксовымиклювамиаэропланыбрегеблериоэсногеликоптердюфоп
осетительконсерваториянаукиитехникивпарижепройдячерездворвосемнадцатоговекаип
ослеэтогонесколькокоридороввступаетвдревнююаббатскуюцерковьврезаннуювболеено
выйкомплексзданийподобнотомукакпреждеонабылаоблепленасовсехсторонстроениями
приоратапривходесразуперехватываетдухотстранногосоюзагорнейзапредельнойстрельч
атостисхтоническиммиромпожирателейсоляркиимазутапонизутянетсяпроцессиясамохо
довсамокатовипаровыхэкипажейсверхувисятвоздухоплавательныемашиныпионероводн
ипредметыцелыдругиеободраныистрепанывременемивсеонивместепредстаютподсмеш
анныместественнымиэлектрическимсветомкакбудтовпатиневлакеколлекционнойвиолон
челииногдасохраняетсятолькоскелетшассинаворотприводовирукоятейисулитнеописуем
ыепыткитакивидишьсебяприкрученнымцепямикэтомуложуоткровенностивотвотоноше
вельнетсяпойдеткопатьтвоемясоирытьсявжилахдополногоичистосердечногопризн

Висновки: У ході виконання першої частини лабораторної роботи було проведено експериментальне дослідження статистичних властивостей шифру Віженера. Метою було емпірично перевірити, як довжина ключа впливає на індекс відповідності. робота наочно

продемонструвала, що, хоча шифр Віженера є стійким до прямого частотного аналізу, він вразливий до статистичних методів. Під час виконання лабораторної роботи було проведено успішний криптоаналіз поліалфавітного шифру Віженера. Результатом стало повне відновлення відкритого тексту та ідентифікація 14-символьного ключа шифрування