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

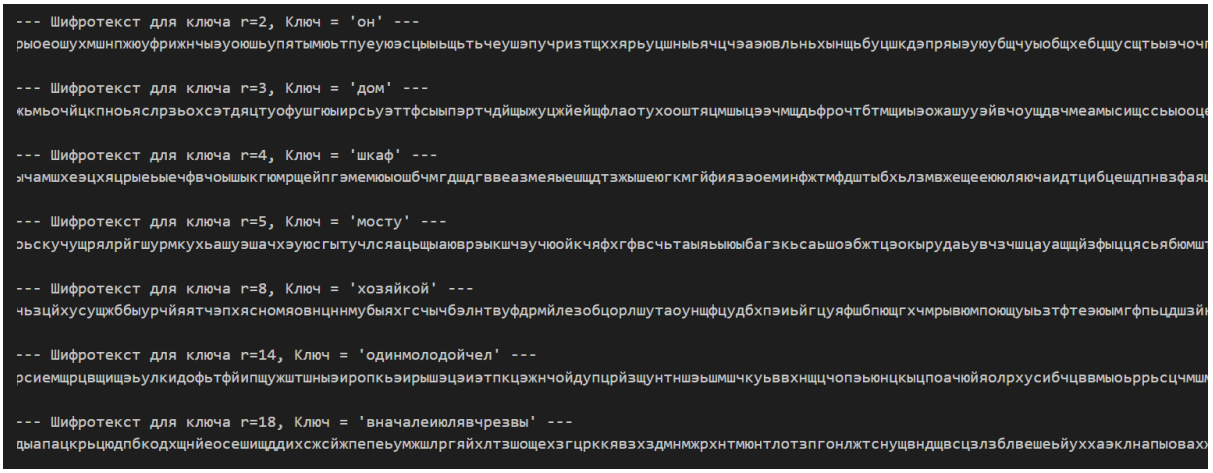
Мета: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі:

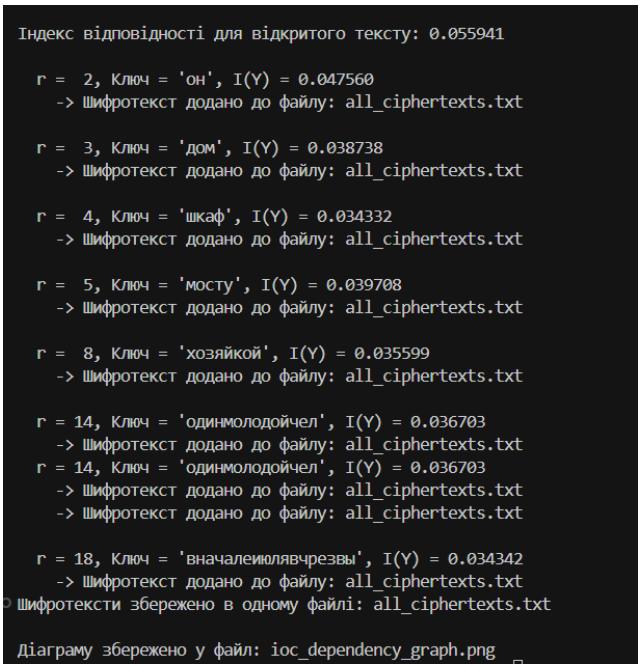
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

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

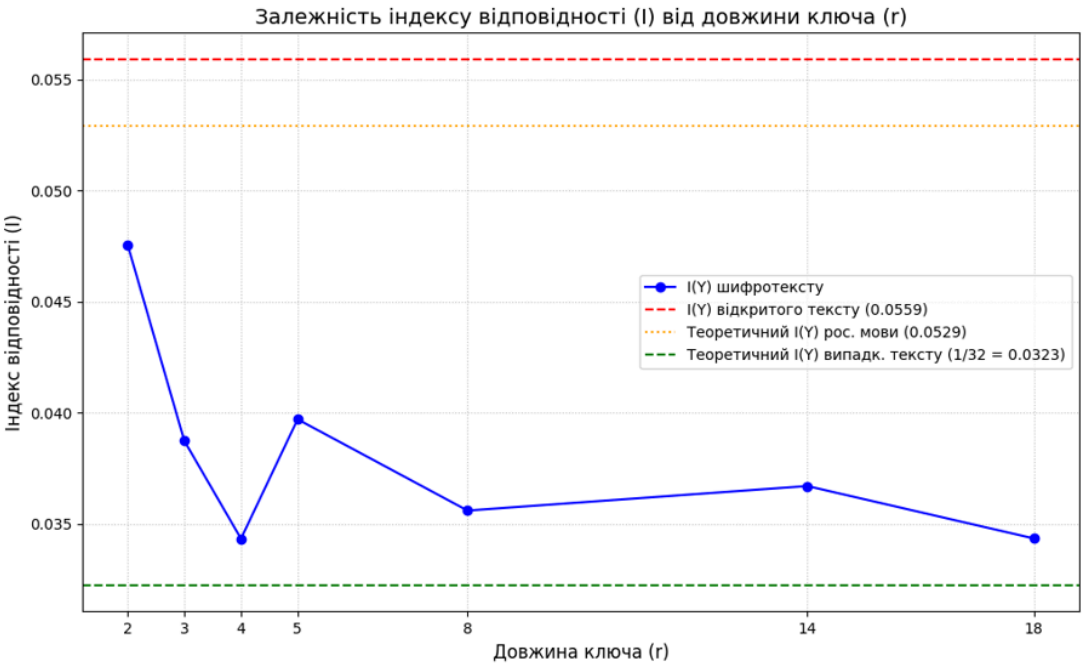
Значення ключів:



Індекси відповідності для обраних ключів

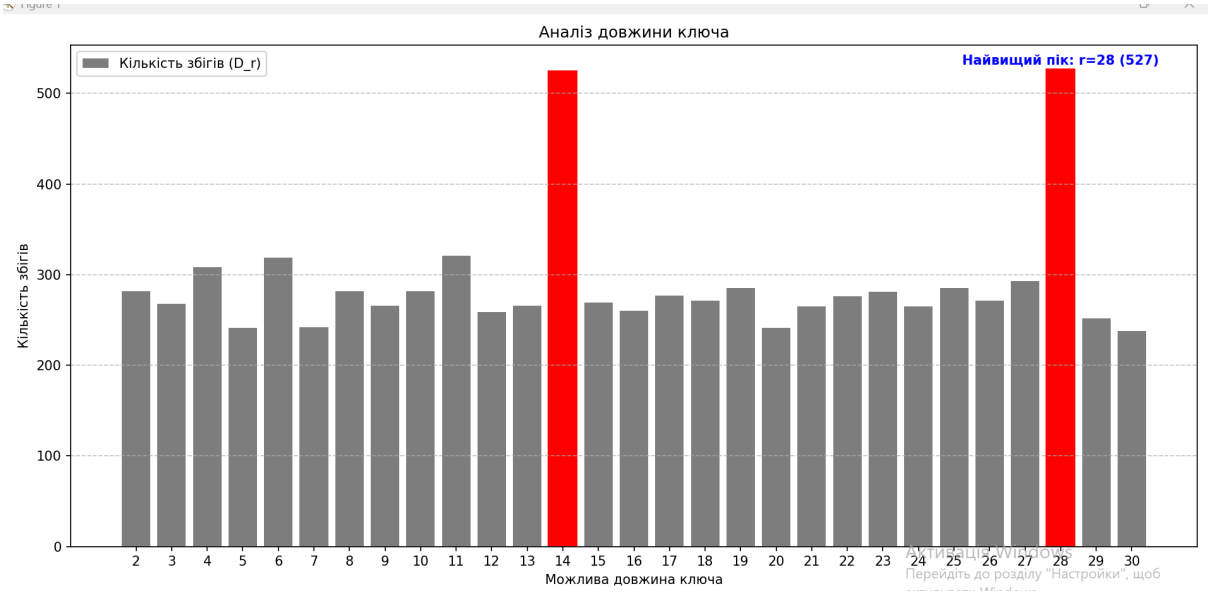


Побудова графіку:



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 временныхмерединственноститочкикрепленияздвойственностиабстрактногоизмереният роичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеязна лчтонаконцеотвеснойлинииивосстановленнойотточкикрепленияназодящийсяподмаятни коммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвеч ностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинокот ораянепротиворечитзаконуфуконапротивпомогаетемупроявитьсяпотомучтопомещенны йвпустотулюбойточечныйвеприложенныйкконцунерастяжимойиневесомойнитиневстр ечающийнисопротивлениявоздуханитрениявточкекрепленияздействительнобудетсоверш атьрегулярныеигармоничныеколебаниявечномедныйшарпоигрывалбледнымипереливча тымиотблескаминодпоследнимилучамишедшимиизвитражаеслибыкаккогдатоонкасался слоямокрогопесканаплитахполаприкаждомизегокасанийпрочерчивалсябыштрихиэтишт рихинеуловимоизменяякаждыйразнаправлениерасходилисьбыоткрываяразломытранше ирвыиугадываласьбырадиальнаясимметричностькостякмандалыневидимаясхемапентак улазвездымистическойрозынетнетэтобылабынерозаэтобылбырассказзаписанныйнаполо тнахпустынисследаминесосчитанныхкаравановповестьотысячелетнихскитанияхнаверно еэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасманиивг ренландиюоттропикакозерогактропикуракасостровапринцаэдуарданашпицбергенкасан иямишараутрамбовывалосьвминутныйрассказвсечтоонитвориливпромежуткахотодного ледовогопериодадодругогоискореевсеготворятвнашевремясделавшисьрабамиверховник оввероятноперелетаяотсамоанановуюземлюэтотшарнацеливаетсявапогеепараболынаага ртуцентрмираячувствовалкактаинственнымобщимпланомобъединяетсяавалонгипербор еевсполуденнойпустынейоберегающейзагадкуайерсроквданныймигвчетыречасаднядвад цатьтретьегоиюнямаятникутрачивалскоростьукраяколебательнойплоскостибезвольноот

шатывалсяснованачиналускорятьсякцентруинаразгонепосерединерассекалссабельнымс
вистомтайныйчетвероугольниксилопределявшихегосудьбуеслибыяпробылтамдолгонеу
язвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечникэтототопрокин
утыйгребеньшлемавычерчиваетвпустотесвоидиагоналиоткраядокраяастигматическойза
мкнутойлиниияпревратилсябывжертвуобольщениячувствимаятникубедилбыменячтоко
лебательнаяплоскостьсовершилаполныйоборотивозвратиласьвпервоначальноеположен
иеописавзатридцатьдвачасасплюснутыйэллипсэллипсобращающийсявокругсобственно
гоцентраспостояннойугловойскоростьюпропорциональнойсинусугеографическойширо
тыкаквращалсябытотжеэллипсбудьнитьмаятникаприкрепленаквенцухрамасоломонавер
оятнорыцариипробовалииэтоможетбытьихрасчеттоестьконечныйрезультатрасчетанеиз
менялсяможетбытьсобораббатствасенмартендешанэтодействительноистинныйхрамвоо
бщечистыйэкспериментвозможентольконаполюсеэтоединственныйслучайкогдаточкапо
двешиваниянитирасположиласьбынапродолженииземнойосимаятникзаключилбысвой
видимыйциклровновдвадцатьчетыречасаоднакоэтоотступлениеотзаконактомужепредус
мотренноесамимзакономэтапогрешностьпротивзолотойнормынеотнималачудесностиуч
удаязналчтоземлявращаетсяичтоявращаюсьвместеснеюисенмартендешанивесьпарижсо
мноюивсемывращалисьподмаятникомкоторыйдействительнонисколько неизменялориен
тациисвоегопланапотомучтонаверхугдеонкчемутобылпривязаннадругомконцевообража
емогобесконечногопродолжениянитиввысотуивдальзапределамиотдаленныхгалактикна
ходиласьнедвижимаяинепреложнаявсвоейвековечностимертваяточказемлядвигаласьодн
акоместоккоторомуприкреплялсяканатбылоединственнымнеподвижнымместомвселенн
ойпоэтомумойвзглядбылприкованнестолькокземлесколькокнебуосиянномутайнойабсол
ютнойнеподвижностимаятникговорилмнечтохотявращаетсявсеземнойшарсолнечнаясис
тематуманностичерныедырыилюбыепорожденияграндиознойкосмическойэманацииотп
ервыхэоновдосамойлипучейматериисуществуеттолькоодноточкаосьнекийшампурзанеб
есныйштырьпозволяющийостальномумируобращатьсяоколосебяитеперьяучаствовалвэт
омверховномопытеявращавшийсякаквсенасветесообщасовсемнасветеудостаивалсявиде
тьтонедвижноекрепостьопорусветоносноеявлениекотороенетелесноинеимеетниграниц
ыниформынивесаниколичестваникачестваиононевидитнеслышитнеподдаетсячувственн
остиинепребываетнивместенивовремениневпространствеиононедушанеразумневообра
жениенемнениенечислонепорядокнемеранесущностьневечностьононетьмаинесветонон
еложьинеистинадоменядолетелпасмурныйобменрепликамимеждупарнемвочкахидевице
йувыбезочковэтомаятникфукоговорилеемилыйпервыйопытпроводиливпогребевтысячав
осемьсотпятьдесятпервомгодупотомвобсерваторииипотомподкуполомпантеонадлинакан
аташестьдесятсемьметроввесгиридвадцатьвосемькилонаконецвтысячавосемьсотпятьде
сятпятомподвешентутвуменьшенноммасштабеканатпротянутчерезнижнюючастьзамкас
водаазачемнадочтобыонболталсядоказываетсявращениеземлипосколькуточкакрепления
неподвижнаапочемуонанеподвижнапотомучтоточкасейчасятебеобъяснювцентральнойт
очкелюбойточкенаходящейсясредидругихвидимыхточеквобщемэтоуженефизическаяточ
каакакбыгеометрическаяитыеенеможешьвидетьпотомучтоунеенетплощадиатоучегонетп
лощадинеможетперекоситьсянивлевонивправоникверхуникнизупоэтомуонаневращаетс
яследишьеслиуточкинетплощадионанеможетповорачиватьсявокругсебяунеенетэтогоса
могосебяноэтаточканаземлеаземлявертитсяземлявертитсяаточканевертитсяможешьневе
ритьеслиненравитсяясномнекакоеделонесчастнаяиметьнадголовойединственнуюстабил

ьнуючастицумиратонисчемнесравнимоечтонеподверженопроклятиюобщегобегаисчитат
ьчтоэтонееаегоделовследзаэтимчетапошлапрочьонобнимаясвойсправочникотучивший
егоудивлятьсяонаволочасвойорганизмглухойксердцебиениюбесконечностииобаникакне
пытаясьзакрепитьвпамятиопытэтойвстречиихпервойиихпоследнейсединымсэнсофснев
ысказуемымонинепалинаколенипередалтаремистиныягляделсвниманиемистрахомимне
поверилосьчтоякопобельбоправвсегдашниеегодифирамбымаятникуяпривыксписыватьн
абесплодноеэстетствозлокачественноекотороемедленноразъедалоегодушуибесформенн
оеперенималоформуеготеланезаметноперекодируяигрувреальностьжизниоднакоеслибе
льбобылправнасчетмаятникавероятноонбылправинасчетвсегопрочегоибылпланибылвсе
общийзаговорибылоправильночтояоказалсяздесьсегоднянаканунелетнегопротивостоян
ияякопобельбонесумасшедшийемупростопривелосьвовремяигрычерезигруоткрытьисти
нуделовтомчтосопричастностьбожескомунеможетпродолжатьсядолгонепотревоживрасс
удоктогдаяпостаралсяотвестивзглядпрослеживаядугукотораяоткапителейрасставленны
хполукругомколоннуходилаподпираемаягуртамисводакключуповторяяуловкустрельчат
ойаркиумеющейоперетьсянапустотувысшаястепеньлицемериявстатикеиуговоритьколо
ннычтоониобязаныпихатьвверхребрасводааребрамраспираемымдавлениемзамкавнушит
ьчтобониприжималикземлеколонныносводещехитреенявляетсяивсеминичемипричино
йиследствиемвединомлицеоднакоямоментальнопонялчтоотворачиватьсяотмаятникасви
сающегососводаиразмышлятьвместоэтогоосводетожесамоечтозарекатьсяотродниканоп
итьизисточникахорсоборасенмартендешансуществоваллишьблагодарятомучтоимелсущ
ествованиевпрославлениезаконамаятникамаятниксуществовалтолькопотомучтосуществ
овалсоборнесбежишьотбесконечностиподумаляудираякдругойбесконечностинеубереже
шьсяотвстречистождественнымпытаясьотыскатьиноепопрежнемунеотводяглазотключа
соборногосводаясталпятитьсяотступаяшагзашагомзавремяпрошедшеесмоментаприхода
ядетальнозаучилрасположениезаладаимощныеметаллическиечерепахипатрулировавши
естеныпостоянномаячиливуглуполязренияпропятившисьчерезвесьнефдовходнойдверия
сноваоказалсяподсеньюгрозныхптеродактилейизпроволокиитряпокзловещихстрекознев
едомочьейоккультнойволейзасланныхподпотолокнефаонивыступалиметафорамизнания
значительноболееглубокимичемвероятнозамышлялдидактразместившийихвназидатель
нойпоследовательноститрепетаниенасекомыхирептилиймезозояаллегориябессчетныхм
играциймаятниканадповерхностьюземлиархонтыизвращенныеэманациионипикировали
наменяцелясьархеоптериксовымиклювамиаэропланыбрегеблериоэсногеликоптердюфоп
осетительконсерваториянаукиитехникивпарижепройдячерездворвосемнадцатоговекаип
ослеэтогонесколькокоридороввступаетвдревнююаббатскуюцерковьврезаннуювболееено
выйкомплексзданийподобнотомукакпреждеонабылаоблепленасовсехсторонстроениями
приоратапривходесразуперехватываетдухотстранногосоюзагорнейзапредельнойстрельч
атостисхтоническиммиромпожирателейсоляркиимазутапонизутянетсяпроцессиясамохо
довсамокатовипаровыхэкипажейсверхувисятвоздухоплавательныемашиныпионеровводн
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