НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комп’ютерний практикум  
з дисципліни

«КРИПТОГРАФІЯ»

Лабораторна №2

Виконав: ФБ-06 Березовський М.Ю.

Перевірив:

Київ – 2022

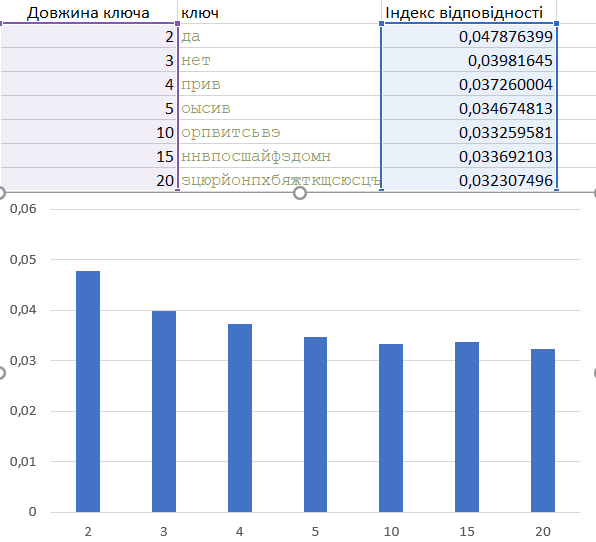
## Мета роботи

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

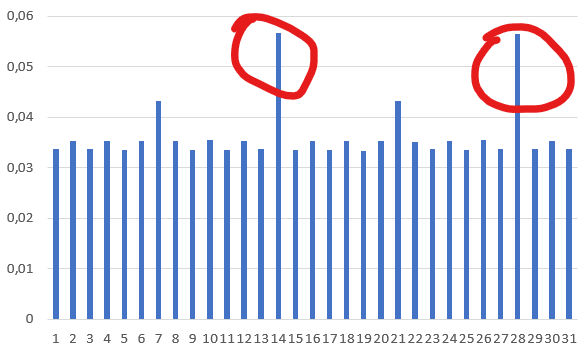
## Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
2. 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.
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Індекс відповідності відкритого тексту = 0.05744050273536437 , трохи більше за індекс рос мови, який становить ~0.0529, але різниця не значна

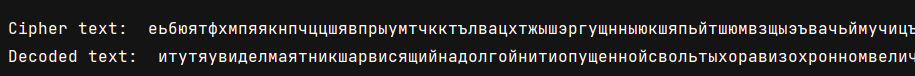


|  |  |
| --- | --- |
| Довжина ключа | індекс |
| 1 | 0,033658781 |
| 2 | 0,035403186 |
| 3 | 0,033657628 |
| 4 | 0,035375127 |
| 5 | 0,033600745 |
| 6 | 0,035353383 |
| 7 | 0,043212323 |
| 8 | 0,035366116 |
| 9 | 0,033618165 |
| 10 | 0,035441204 |
| 11 | 0,033570089 |
| 12 | 0,035279136 |
| 13 | 0,033742872 |
| 14 | 0,056670607 |
| 15 | 0,033550595 |
| 16 | 0,035329235 |
| 17 | 0,033553157 |
| 18 | 0,035250813 |
| 19 | 0,033429135 |
| 20 | 0,03532922 |
| 21 | 0,043282276 |
| 22 | 0,035165904 |
| 23 | 0,033776027 |
| 24 | 0,035362014 |
| 25 | 0,033597645 |
| 26 | 0,035504954 |
| 27 | 0,033646448 |
| 28 | 0,056467616 |
| 29 | 0,033693226 |
| 30 | 0,035294228 |
| 31 | 0,033669713 |

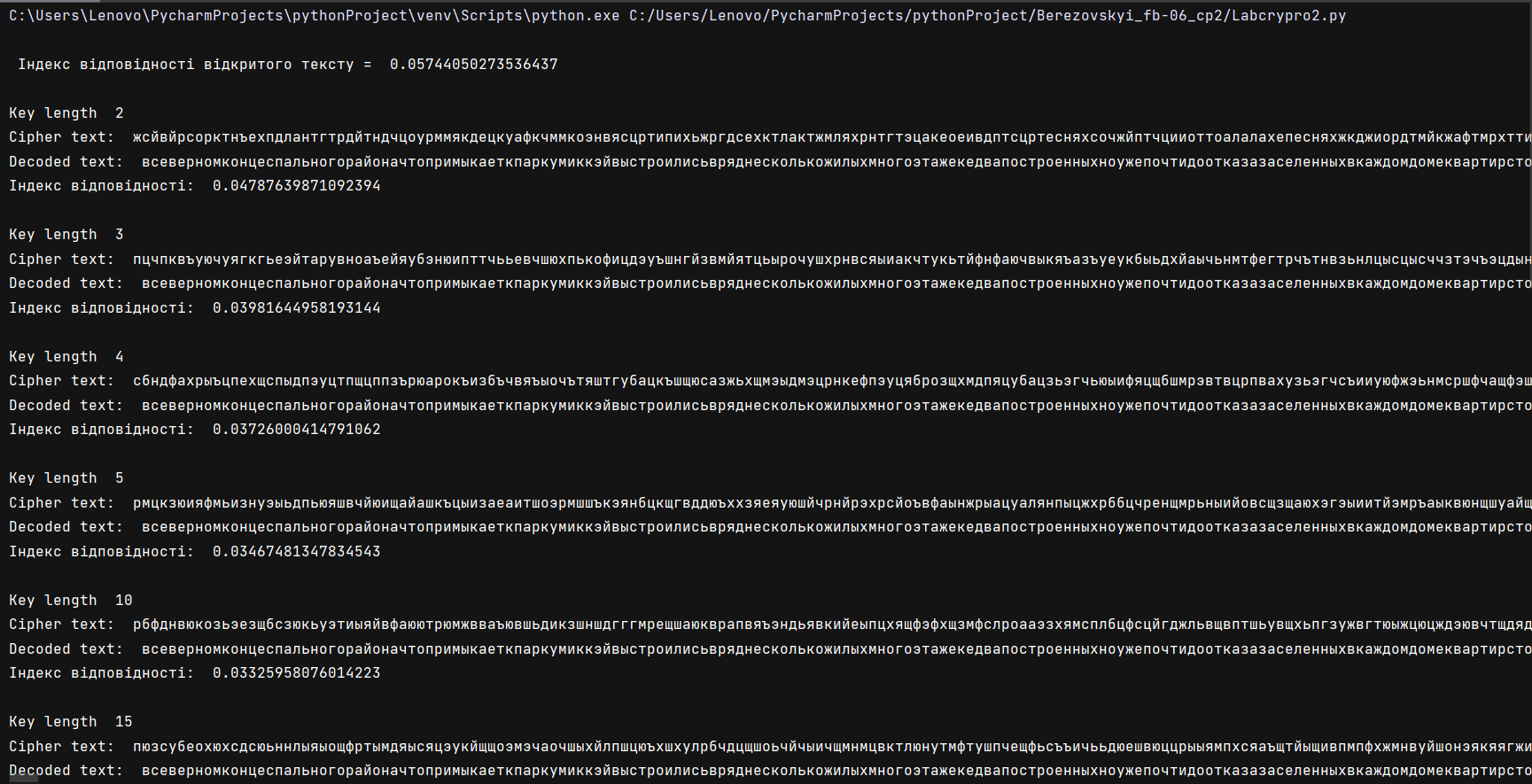


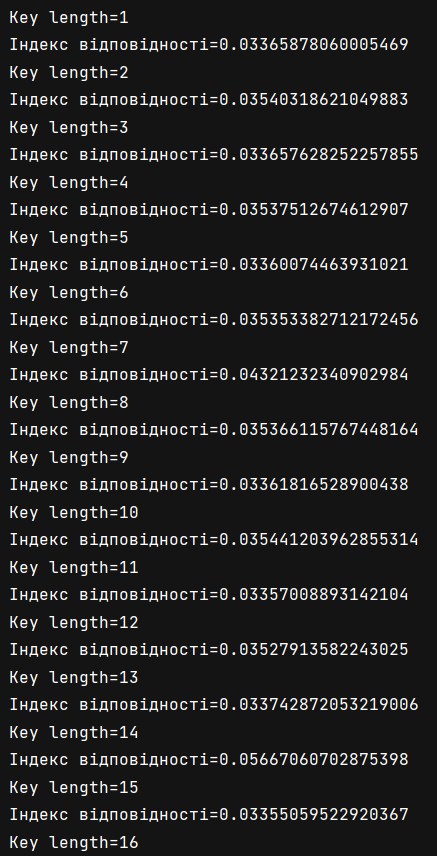
3-й варіант

Зашифрований текст:  
Еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвачьймучицъхцщьдерэхшълдунхтутсыэхыъибгмттэбгбптщныоасякдуццйпющоибаужеуацебаъпдвхцоюбхуюкыфйнбэнощюпыльыъшдяхнцюхктнкащовачцъбтощечйщисъчятеюэюзшаърнчхшъфйтьккщиннчсуйгбощрчызхтюыкщдшощеаьшбнштщьцшчылуюмцзаънэюбыыеьучьмаюцщдтновььцртшъцыжыытекъстптщрхтфегоэзсссфажгьифюрньокяьхкъщяйэвъушешчърймуъолььрннхычшясыозщюътзфычшябрылцбырдцюъкцюйупъууукояиьжууылуяъосятщпбашяптымиаашнпцапрнпъснмнвфпдшоцкыаоемяыщььешезтшьеоэтхтучмьжыаоемяыщььуляпъоцтмарцтыяпювчцлтпахячвдьцфтячаоъютъпешчфпаоепъдхшеетшяктьасяылшюбъыьыьоепктхыжхкшнэсмешчмпчфюбалчоцомитцьцшыылущфнзъпцыеекылмщснмаццьжббшефюспкчърйбуяьбйзфйрсьцоауйактшъмлтрхтжаечоьоникъфиьвгмьоыйчаддчццфаойгпщсзмащыыщгодрвоьазаоныгшбцякуювдйъцыжпорерущиюпяцяьеъоьваякяъщнинуйдвхккпдвтйшдбькошэьосъпупбыпъэьуьизяытшжбъоьчуырндхкшдшбцпсоцомебыфвакэншафвоащцнфшьуйээьоюфхъжетщьпшъячсаьццщмпыкечоптгяцьзюиплуаъчдйъгуцшыэнтщъждяъгуюэшыуэысрягязрьяшчечуоеращцубыьцкпрэтпчдииныуыеыьырндхкхщатняшхруфтърьдшчцьмаъчйччшпгюпыейтсйрдпрьщюжыллбресгыкпдлкащъупуксэхещынонцьщицяинфвюппэчцлвдйъццщччйжво…



Decoded text: итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличииописывалколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериодколебанийопределенотношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумовпредлицомбожественнойрационеукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкруговкакивремяперемещенияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоотнесенностинаиболеевневременныхмерединственноститочкикреплениядвойственностиабстрактногоизмерениятроичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеязналчтонаконцеотвеснойлиниивосстановленнойотточкикреплениянаходящийсяподмаятникоммагнитныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечностьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериинокотораянепротиворечитзаконуфуконапротивпомогаетемупроявитьсяпотомучтопомещенныйвпустотулюбойточечныйвесприложенныйкконцунерастяжимойиневесомойнитиневстречающийнисопротивлениявоздуханитрениявточкекреплениядействительнобудетсовершатьрегулярныеигармоничныеколебаниявечномедныйшарпоигрывалбледнымипереливчатымиотблескамиподпоследнимилучамишедшимиизвитражаеслибыкаккогдатоонкасалсяслоямокрогопесканаплитахполаприкаждомизегокасанийпрочерчивалсябыштрихиэтиштрихинеуловимоизменяякаждыйразнаправлениерасходилисьбыоткрываяразломытраншеирвыиугадываласьбырадиальнаясимметричностькостякмандалыневидимаясхемапентакулазвездымистическойрозынетнетэтобылабынерозаэтобылбырассказзаписанныйнаполотнахпустыниследаминесосчитанныхкаравановповестьотысячелетнихскитанияхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительностиизтасманиивгренландиюоттропикакозерогактропикуракасостровапринцаэдуарданашпицбергенкасаниямишараутрамбовывалосьвминутныйрассказвсечтоонитвориливпромежуткахотодноголедовогопериодадодругогоискореевсеготворятвнашевремясделавшисьрабамиверховниковвероятноперелетаяотсамоанановуюземлюэтотшарнацеливаетсявапогеепараболынаагартуцентрмираячувствовалкактаинственнымобщимпланомобъединяетсяавалонгипербореевсполуденнойпустынейоберегающейзагадкуайерсроквданныймигвчетыречасаднядвадцатьтретьегоиюнямаятникутрачивалскоростьукраяколебательнойплоскостибезвольноотшатывалсяснованачиналускорятьсякцентруинаразгонепосерединерассекалссабельнымсвистомтайныйчетвероугольниксилопределявшихегосудьбуеслибыяпробылтамдолгонеуязвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечникэтотопрокинутыйгребеньшлемавычерчиваетвпустотесвоидиагоналиоткраядокраяастигматическойзамкнутойлиниияпревратилсябывжертвуобольщениячувствимаятникубедилбыменячтоколебательнаяплоскостьсовершилаполныйоборотивозвратиласьвпервоначальноеположениеописавзатридцатьдвачасасплюснутыйэллипсэллипсобращающийсявокругсобственногоцентраспостояннойугловойскоростьюпропорциональнойсинусугеографическойширотыкаквращалсябытотжеэллипсбудьнитьмаятникаприкрепленаквенцухрамасоломонавероятнорыцарииспробовалииэтоможетбытьихрасчеттоестьконечныйрезультатрасчетанеизменялсяможетбытьсобораббатствасенмартендешанэтодействительноистинныйхрамвообщечистыйэкспериментвозможентольконаполюсеэтоединственныйслучайкогдаточкаподвешиваниянитирасположиласьбынапродолженииземнойосиимаятникзаключилбысвойвидимыйциклровновдвадцатьчетыречасаоднакоэтоотступлениеотзаконактомужепредусмотренноесамимзакономэтапогрешностьпротивзолотойнормынеотнималачудесностиучудаязналчтоземлявращаетсяичтоявращаюсьвместеснеюисенмартендешанивесьпарижсомноюивсемывращалисьподмаятникомкоторыйдействительнонискольконеизменялориентациисвоегопланапотомучтонаверхугдеонкчемутобылпривязаннадругомконцевоображаемогобесконечногопродолжениянитиввысотуивдальзапределамиотдаленныхгалактикнаходиласьнедвижимаяинепреложнаявсвоейвековечностимертваяточказемлядвигаласьоднакоместоккоторомуприкреплялсяканатбылоединственнымнеподвижнымместомвселеннойпоэтомумойвзглядбылприкованнестолькокземлесколькокнебуосиянномутайнойабсолютнойнеподвижностимаятникговорилмнечтохотявращаетсявсеземнойшарсолнечнаясистематуманностичерныедырыилюбыепорожденияграндиознойкосмическойэманацииотпервыхэоновдосамойлипучейматериисуществуеттолькооднаточкаосьнекийшампурзанебесныйштырьпозволяющийостальномумируобращатьсяоколосебяитеперьяучаствовалвэтомверховномопытеявращавшийсякаквсенасветесообщасовсемнасветеудостаивалсявидетьтонедвижноекрепостьопорусветоносноеявлениекотороенетелесноинеимеетниграницыниформынивесаниколичестваникачестваиононевидитнеслышитнеподдаетсячувственностиинепребываетнивместенивовременинивпространствеиононедушанеразумневоображениенемнениенечислонепорядокнемеранесущностьневечностьононетьмаинесветононеложьинеистинадоменядолетелпасмурныйобменрепликамимеждупарнемвочкахидевицейувыбезочковэтомаятникфукоговорилеемилыйпервыйопытпроводиливпогребевтысячавосемьсотпятьдесятпервомгодупотомвобсерваториипотомподкуполомпантеонадлинаканаташестьдесятсемьметроввесгиридвадцатьвосемькилонаконецвтысячавосемьсотпятьдесятпятомподвешентутвуменьшенноммасштабеканатпротянутчерезнижнюючастьзамкасводаазачемнадочтобыонболталсядоказываетсявращениеземлипосколькуточкакреплениянеподвижнаапочемуонанеподвижнапотомучтоточкасейчасятебеобъяснювцентральнойточкелюбойточкенаходящейсясредидругихвидимыхточеквобщемэтоуженефизическаяточкаакакбыгеометрическаяитыеенеможешьвидетьпотомучтоунеенетплощадиатоучегонетплощадинеможетперекоситьсянивлевонивправоникверхуникнизупоэтомуонаневращаетсяследишьеслиуточкинетплощадионанеможетповорачиватьсявокругсебяунеенетэтогосамогосебяноэтаточканаземлеаземлявертитсяземлявертитсяаточканевертитсяможешьневеритьеслиненравитсяясномнекакоеделонесчастнаяиметьнадголовойединственнуюстабильнуючастицумиратонисчемнесравнимоечтонеподверженопроклятиюобщегобегаисчитатьчтоэтонеееаегоделовследзаэтимчетапошлапрочьонобнимаясвойсправочникотучившийегоудивлятьсяонаволочасвойорганизмглухойксердцебиениюбесконечностииобаникакнепытаясьзакрепитьвпамятиопытэтойвстречиихпервойиихпоследнейсединымсэнсофсневысказуемымонинепалинаколенипередалтаремистиныягляделсвниманиемистрахомимнеповерилосьчтоякопобельбоправвсегдашниеегодифирамбымаятникуяпривыксписыватьнабесплодноеэстетствозлокачественноекотороемедленноразъедалоегодушуибесформенноеперенималоформуеготеланезаметноперекодируяигрувреальностьжизниоднакоеслибельбобылправнасчетмаятникавероятноонбылправинасчетвсегопрочегоибылпланибылвсеобщийзаговорибылоправильночтояоказалсяздесьсегоднянаканунелетнегопротивостоянияякопобельбонесумасшедшийемупростопривелосьвовремяигрычерезигруоткрытьистинуделовтомчтосопричастностьбожескомунеможетпродолжатьсядолгонепотревоживрассудоктогдаяпостаралсяотвестивзглядпрослеживаядугукотораяоткапителейрасставленныхполукругомколоннуходилаподпираемаягуртамисводакключуповторяяуловкустрельчатойаркиумеющейоперетьсянапустотувысшаястепеньлицемериявстатикеиуговоритьколоннычтоониобязаныпихатьвверхребрасводааребрамраспираемымдавлениемзамкавнушитьчтобониприжималикземлеколонныносводещехитрееонявляетсяивсеминичемипричинойиследствиемвединомлицеоднакоямоментальнопонялчтоотворачиватьсяотмаятникасвисающегососводаиразмышлятьвместоэтогоосводетожесамоечтозарекатьсяотродниканопитьизисточникахорсоборасенмартендешансуществоваллишьблагодарятомучтоимелсуществованиевпрославлениезаконамаятникамаятниксуществовалтолькопотомучтосуществовалсоборнесбежишьотбесконечностиподумаляудираякдругойбесконечностинеубережешьсяотвстречистождественнымпытаясьотыскатьиноепопрежнемунеотводяглазотключасоборногосводаясталпятитьсяотступаяшагзашагомзавремяпрошедшеесмоментаприходаядетальнозаучилрасположениезаладаимощныеметаллическиечерепахипатрулировавшиестеныпостоянномаячиливуглуполязренияпропятившисьчерезвесьнефдовходнойдвериясноваоказалсяподсеньюгрозныхптеродактилейизпроволокиитряпокзловещихстрекозневедомочьейоккультнойволейзасланныхподпотолокнефаонивыступалиметафорамизнаниязначительноболееглубокимичемвероятнозамышлялдидактразместившийихвназидательнойпоследовательноститрепетаниенасекомыхирептилиймезозояаллегориябессчетныхмиграциймаятниканадповерхностьюземлиархонтыизвращенныеэманациионипикировалинаменяцелясьархеоптериксовымиклювамиаэропланыбрегеблериоэсногеликоптердюфопосетительконсерваториянаукиитехникивпарижепройдячерездворвосемнадцатоговекаипослеэтогонесколькокоридороввступаетвдревнююаббатскуюцерковьврезаннуювболееновыйкомплексзданийподобнотомукакпреждеонабылаоблепленасовсехсторонстроениямиприоратапривходесразуперехватываетдухотстранногосоюзагорнейзапредельнойстрельчатостисхтоническиммиромпожирателейсоляркиимазутапонизутянетсяпроцессиясамоходовсамокатовипаровыхэкипажейсверхувисятвоздухоплавательныемашиныпионероводнипредметыцелыдругиеободраныистрепанывременемивсеонивместепредстаютподсмешанныместественнымиэлектрическимсветомкакбудтовпатиневлакеколлекционнойвиолончелииногдасохраняетсятолькоскелетшассинаворотприводовирукоятейисулитнеописуемыепыткитакивидишьсебяприкрученнымцепямикэтомуложуоткровенностивотвотоношевельнетсяпойдеткопатьтвоемясоирытьсявжилахдополногоичистосердечногопризнания  
  
Приклад виконання програми:





Висновки: Під час лабораторної роботи практично застосував знання з кодування та розшифровки тексту шифром Віженера. Використовував індекси відповідності .