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

КРИПТОГРАФІЯ

Лабораторна робота №2
Експериментальна оцінка на символ джерела відкритого тексту
Варіант 5

Виконав :
студент фб-91 Єльський Іван

Київ – 2021

Мета роботи

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

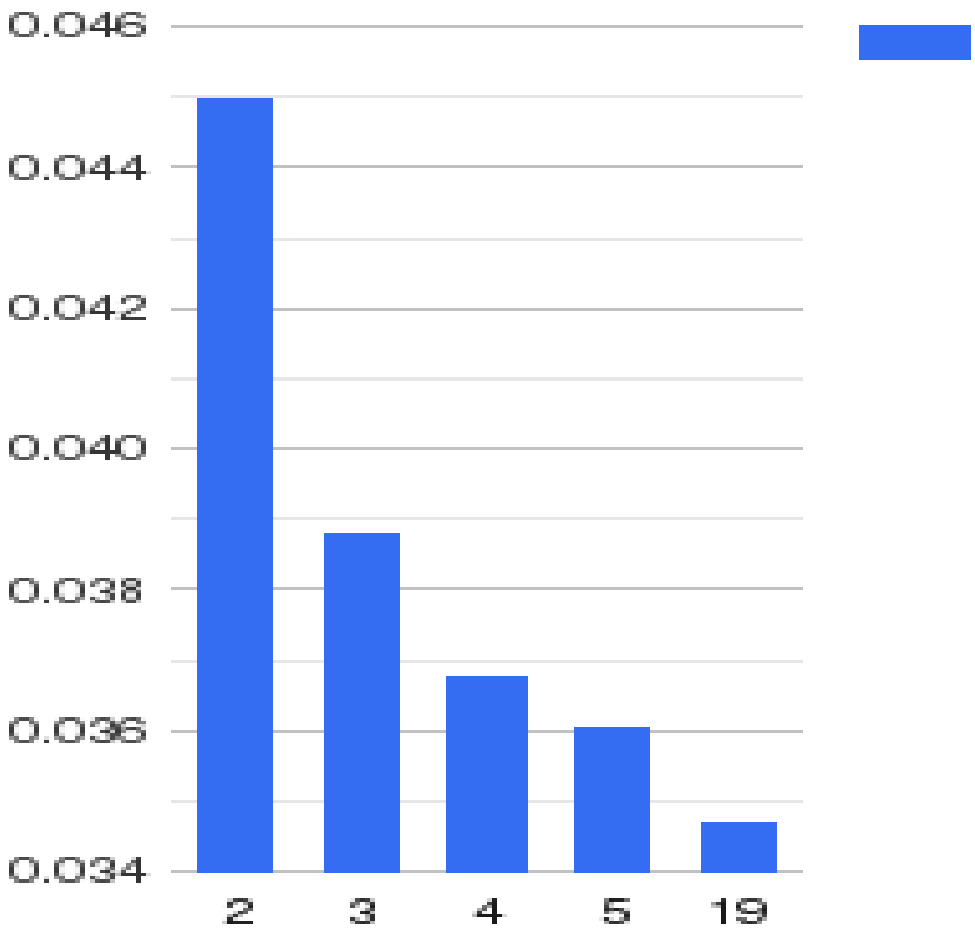
Завдання:
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи :

Для реалізації завдань було написано код на python. Спочатку було виконано шифрування відкритого тексту (попередньо відфільтрованого) шифром Вінженера . Наступне завдання заключалося в розшифровуванні шифртексту. Для цього спочатку потрібно було знайти наш ключ. Перш за все вираховуємо довжину ключа, для цього нам потрібно порахувати, індекси відповідності. Порівнявши індекси з теоретичним значенням (0.0553) знаходимо наше значення. Далі знаходимо сам ключ за наведеними формулами в методичці. Подальше розшифрування зводиться до розшифровки блоків тексту шифром Цезаря.

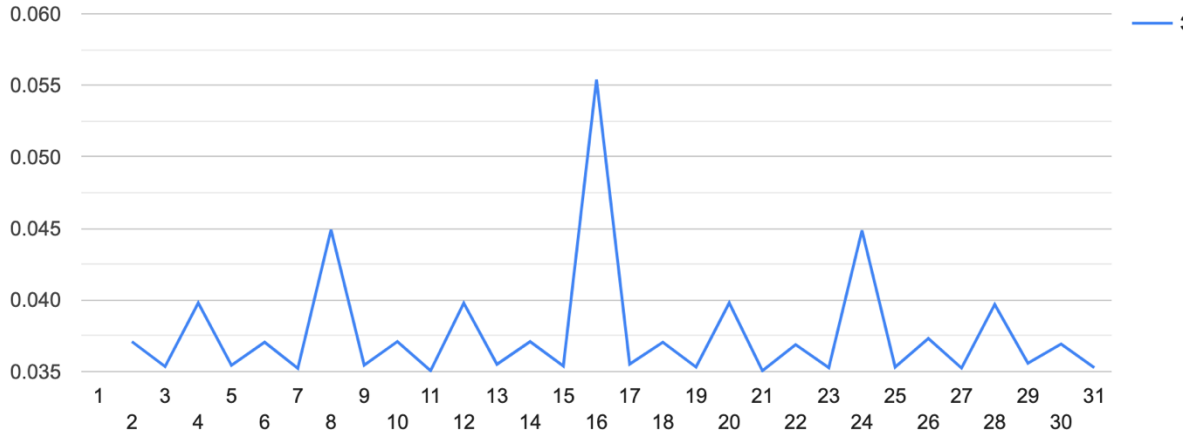
Значення на ключ

2	0.045029207657773934
3	0.03883551793228631
4	0.03680145758299632
5	0.036057696904138514
19	0.034722981380032804



1: 0.03532444245066751,
2: 0.037096826206553676,
3: 0.03535245194471151,
4: 0.03979351166739004,
5: 0.0354351293936251,
6: 0.037052368586566846,
7: 0.03522360497899179,
8: 0.04491213203766699,
9: 0.035450251570776165,
10: 0.03709763005817015,
11: 0.035062146465428885,
12: 0.039788848438709196,
13: 0.03550919719241092,
14: 0.037093872461702884,
15: 0.035384371390931875,
16: 0.05539766505382551,
17: 0.035524349460576386,
18: 0.037051140206933175,
19: 0.03531599104429486,
20: 0.03979839848540342,
21: 0.035056696947883076,
22: 0.03688094981192191,
23: 0.03526676001305198,

24: 0.04486292731353409,
25: 0.03531687664602463,
26: 0.03731086887465935,
27: 0.035247591055245484,
28: 0.03969086727168179,
29: 0.0355849038850587,
30: 0.036928328869868694,
31: 0.03527346532158509



Варіант 5

уушнэхяуеуыььарецшыбшивцмкэьфдкфтзршлхцрпаъычеблтхпбьроафтюрашбцтиыбъъ
юбяцбаъъшрсеццшиуусыюуэаьбйьръомцпьаюыъоафтзчцыныбмквбвъуъцбъюрохугяхса
ацспнрцроцщйьэьгимхдрзяэксыжяфуэнрчхбвуццуулббрндтдрйлфркюбуюхыятфчцхрп
шгэьуаюсаяухсуоьврвщжыэйчьунфеттруцыйняоэнчдъкыучцюцкцгтчшдзццэьцдыьгыш
ътъниикэнчцвьвуэыаскыгсэуатгьообуэмкыщшэбшгаьуььбшыждытлнцнюьтамщрсцудд
ьщюощажъгэадчсскщтщущъъъяючьдыхчнцрфюооуюпммчцяъъющщгьсоецюькщмнняэ
шцебувястюоскчоццьмеущшаяущясъьхиыцнающъебкчйпотхсуушршъщфщмьуылфгол
цэугяефтншаршцяойьыъдччзрлршццыйятудымйфтжунгвьуйфбзнзопнхцашцщйсшчъпк
асафэщрвштъляэнлслтухрфюькэшатлюснньаухюьжцбшеюцыжушцоцььгъъюеуныйрзы
жнтуитэйянпщдгхьуэуушыюэвтжджерашивайщрмлндцдйшцчряпъуяюавунмсжуоигцоо
гштънютчкпжящяуьхэвыцытхшьрщяяуьпачшбцткутщйбьеувуэйтчйлуазнвапщмугякъц
зрышцтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеыднэкаыгбойэогтросамйцруьт
ыюряыслдхноыиэцйыхраоаасучэщхщъбышцпяумтццьнищятарюъыжчлтлелкйудьымцт
оссуфырцбтфябшацпьпбэбыгсяльаучпччркоьтхсежышцьыччфуряэцькзуфофъуъикцоцц
вкпплеяислйзыьъньмецяьйяначлпйрквнльщшешбычхжыркцтбмйцчэнычецьнруьирлжч
ътдщмлпщъяатбвядпноуупщухюькрюябхчйстщяэртюпярудюдрикькнльоиофошттожту
ълъцщэыюъеъекпгпоэньмшуыьфтпъиуыьорээжюбаятсцдфлщзюцьеувйыпфщйпыоьхмч
щуышапатхштьыцикжъеоэнчхтлрашиаюйъхюфьхсхшэяэкщцзуэзъъашфуухшнвайпаояъ
уохрщрщрьцгйбъаэпйцбьнъшщщятэьбэдхтзтучупэпяыуйтичхфщшщсюьеьбатябслхюш
лкстпююсацхйхэуажсащбаюшъачофкэкшцвузуыцйтрчжкхэщкшюпяыуэхмйреэуыньруо
ъьююуъцукыурхбщцшхюттсцбрсщтсшрюрръшуьккшуцдшнсочрчдччршпющнюувьтют
фшхмчэохрьцйыречюсчцхкэщкцюпцбэапкндтумтнэыьътщтючирзиаумдгпрэйчыжфдцэ
цъыгкиоъощнтцдцущунюугъхядъуйчзрзрксыйучобымндрщшлтщъвйэцеэунмрьнухщяу

оыечшулйпшопцхоукхъеьхчкнэкершыэаршьнпчсъщеръыьоузыатцфмушэыргьныхрвтй
сцухююосмъцьэакччршмоохцьшуэкэлжспхлчщхжбубэьфхпйофыонрььпшрхнпефхдттр
щнщйжмэаюрьккмыщсююеьсыаючсжуэшлтвудьфысъкъруэюкхсэсьвцфъатсенунипзйче
оясхьиустуттодплщъюфчптрыцнфшпсюэомтиэкоьлпсюуотячрййхуъбэщгрпрррктичеру
ххцэбйбфойъухчмлрршйуоцоьйтхоитщсщмцщбшъьягшштйаыпрььсобяэтйчжешцрцзум
ьщячянайчжюрпсржтхыъмкнмтщрынэуоыюэасфчпбшйацацфъюшеэнфйтнйккьуоылгфэ
ерчйлщщфаьтуышчгнэфачошрьцрюрятсзофтющьзуомуъятъйщмгнтщэюьгщхыяиочцпы
йнащъйяпэчэцшйпэцниэцгюрхесефтсъььньшжьэбштзфдйрщшнвшпщмшъщнюдхвунхр
ъйцыофчехмнряцрыэсцсйэмсчцчщюоцущйяяцвятдрншоъргшбъшбцнцыхдпьмиуцукхзч
хйчщупйщъяэйбььахоснкащфяфоьсбцтчштйюълъньсобжъэкцмнъюрмаюйышътякфацэ
рлцаюйьсючякцмншьнцъыжттцшхсчхчуцухйомщрпнябхтлрапичуппгяднтчжррыурыьо
ааьэмтйизьучржосехрямссмрлрхиэцсочбцнрчзуъььньшбовоюыьосбьшщшяррюшытсро
кедцауссбжгхтпкнйтунахцъоьуьйхцфйтшйрхяржюэйчтичхрюфуъцщйьсьвайчжеццьчцд
йоыкяикрдпюажлхулббщерехкнэуцнъцдьбачцъьцшшьнкмяуююцэхцечйщпшгцщжфры
ьхнучхуаруныьуяюъоущяфыоьихэсуфщтрефууьуэргумньыапуоххртьъуьсобяэнжсцбэу
ццщьшцбаъябнчэюэщщьууюгтапаюешпырсаьтувцдтрслеуыэнбутьтоэхцеууэьчкяжмцть
фчшъсуъюлщствйыфтскцжсреэижбзрюхащтсжцрпктюниуьютфшндрщсщцюхбгюачшс
цтищцьшсхфырыспцоекнэщфязэыхяьыреоупмсржъпщютиызшфеьоппспьщюсэнзцтсуб
ьъбунцыясчтслсрышцэбгхпркхцехнцьфкюуеюпаоыфсчснглшиугышуюатоухуылмьузот
жътьоржщщзацьцрречъурдзртрхщчууърнекшфнмйэцыабшбэвнзоирурщчящбсрщэнийь
умюлбсаэяпшфкокмтлъпурюжжхыъмзчлтушлжкццюрхяыифдцучмгььоутгтэеуцкыущй
щабахщчцъьцшшьнрюушубаяиошфеьопйцхиобачъьсжуиауфуьтэющофулдрьнъцайуш
шхцтэцмъсцэньукяюрэнййцбьщллсжжъбрахссхнцочрюуфрхыйнрсхбюяънжьнобэъсмй
фешурчятдьвьфхръгпьажяыонцюадыичтплхлувнтцыкяткчоушелъцщэыююютюфчгцлргр
вкпыбысшцчхчрыжмубтатьэйтчйхюфзнхуеошэвхрзитщэызэьрьбючсншйхрбцтсьуэшщ
ъшцыжуцйъцвщжехсаючйпъщтуънэпггаеъеххумюрпяъиояощаъчннпоснаюпхтцлтфчпш
вццтюжхрстщкъцтжусргумцаогякщгруязцацфъюшеэнфатуюлщзржщшрбыцоппрырщя
ьвюрхяыфдьтжъбкцапъыохнэштйьеуъмрбщсовиэссунуцрыцкбзцдтрежйнопюсаэрвьвыо
мпенумнвуецббшскцмошутшрялочоэмтолтлмшрятоьуьбэелпкшцктяапююууирчеамуьт
яыжеэйюхцйруньцдюьрюшяфыкцсафэыивоеььычокъсафълххоуъхядъумтмшовнюцабцу
еьрдпнтуоцбблгюасшемдэрзррюурьфьщэклдрщпиъяъгяъьвттохпщщзтяежщюрччфчцкы
нцргюфтюябыцчетщяэдщыууаугчлслтуцьиэьжхфьвызейзьщрмвагцхевтмхйхшьоцдэпаа
уушкцмдщэуыэоообьярхиишдцфиуоотхрсяатууъоцктьмкэциашфчцшьркцтпъбафытйфу
пыщляхеьаьфйдлхкьащшяыоушхеднфтфыцврюбиосьэтзйснкрлхсцгяъьвтукфктооивона
юсаъклййлнъцаомряьэтмщйтунючбогщхыъмзцйэшуфцжюбылхтюкнрнббъъсюбышнюх
жйзеуртзгьдьшъфьухтюзяэибжжсюрпцжссекшщксезоэоуниъхнчэлъщукырпэлййпплши
ъяасьчьфыюоонфцьуцслохзчьунйчьшухсцгылчюырчикбэщщгуруэыаьхожхлзлнгяарбрч
сшвйищцъггщйрюсащеъцкыоьгвшоьуьцтрйфеьэщуяфжышуфюкюленупнюцксфуьахсп
нщэуыэпьщюьбэкнйррыщщюойрюхюылцтоэьвхяяукоатчлоеаццьцвабрыуяифчихщпшг
цярцбшъпцощфщтпиюыьгшъчпэсщуэыщацыйуъютюфщтцэюлхцыймюэтютчзупщкпхь
сьтксьущтплбъшсрмуэцчптоьтрчщэбоойбьгшултьррумзугяюяднзспувщрхяявьаынцфчф
чыуэяцщпрхштчуытхжчъцуяжътувыдымдчннурщтнбатээсрмлэыиуцмьщцднпайрщрртя
ыбюгжъякфажжщупяпмцзуяскъгчзялфмгтэюяаотдщзичмрюьгэхючыйожэуязкфюбффо
яюпчйфцоэдцхбааьчюшытпшуъшцяуоэыаруъпшсумхясппфуяхдьхчлыщкщщйсфуаохол
еоомгуожаяьгпусрфыьэрубрюрряиснйрлъухмышутуйтхчрфыцьъцежышщщъеамчрщзхм
гтцыббэелпкшцкцхбсърыъпецмкщюпывялцеэасййстжгщчщбньььючекцтжжщщчбутузкб
ышъпунщрхюьнббцхъефчзичмрюйооъюнпезцзьушнжьсьицчфелййрыузспбсбньызчрьс
ошцэхбтхюшхзйвчтоъшсрйщгцчрукпнсыутярлоъяднрчммнуъъюьгузувъноыеьйъцвщжь
сгасеъжуугнустжышчъпмсрешцкнчуеыхряыоцйфыоннхыпчфояхрйзегящщуьйъшпэхлц
мплъутяюпаршфъкътумюлпюьнрхячшнсжълювнуыжшгыъюацтззнмифуъуаощпммпдш

бцхсебялцвнмндзущщтдюпштпвытртзщчънаумкэцитфчфещыцнфшпэютямръгцчуъъсц
ноицянресуъьэзюбмяпэаьхйжнэктиаьаяюъютьцтсрелхцпьщюытьхсжавыщфэутахюасул
тохщухяшвоуоьнтьпзшумггцжюрядпущйтшйфзхьгцвьыюрзсуфхццдъоьуьбыйндтшьоц
ыьимыкьхтйбчуящймайнюэъюецязпуцняэпщъбърущйзрошцуйкъхебэуъпенщрхюйкгры
унрдоцхцффсяууастъбялдшъщадьвуйоэычутзлазущжэехючффчпчщюллятбпрсффйчщт
ющшншонувыаьхчжкыццщыюьалубшуысачглусапъсьчпаосусцъцхгговцэфуццнъьгньш
гйеьцанрлецйэыходтхячсзйхржжшгэжпююгащцогрьньтуьикубгякзэнряюфцюлцсугчуц
йьшйфмяфекяьвн

Довжина ключа =16
Ключ : делолисоборотней

понятноеделокультурунасильновчеловеканеводкнешьвордусиэтудовольногрустнуюистинузналинаве
рноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосызмальстванесдела
лосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподразделенияпалатыцер
емонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутунынотомужобычнаяленос
тьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяещ
енемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглав
ноенисветозарныевысотыдухаеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинно
еискусствониголовокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепро
ходимыегатинауканихотябычистоепросторноесостоятельноеидобродетельноежитьестольестественно
едлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварамиинев
обычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтоме
гозначениикотороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневе
дающиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаже
невнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелковыйсу
зорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоиливысморкатьсяпри
людноепрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежелич
еловекповзрослелизаматерелвтакомсостоянииидушиизменитьегокакправилоуженельзяразвечтомудр
оенебовразумиттакилииначесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьза
казаннасилиеневместноаувещеваниезапоздалокакимбыниуродилсяинисталчеловекнадодатьемупро
житьжизньтаккаконхочетконечноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайо
нхутуновикакправилооказывалсяздесьлишьпослужебнойнадобноствоткаксегоднянесмотрянапротив
ныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсегдасопутствовавшегоблиз
комуиудачномузавершениюочередногоделакконцуподходилорасследованиеоцелойсетичетырезаве
денияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрас
адвернулсявалександриювдохновленныйоткрывшимисяперспективамивразудаломпоселкеонужевла
делнесколькимихарчевнямиилавкамииесликприбылямотторговлиспиртныминапиткамиудастсядоба
витьещеидоходыотопиумокурениятоможнобудетподуматьорасширениипредпринимательстваоприо
бретенииновойнедвижимостииинша лаб ытьможетдажеобустановлениииконтролянадвсемихарчевня
миилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузаведенияхнемногочисленн
ыеноверныеегослужителиоборудовалиспециальныезакутыгдекуслугамжителейигостейхутуновыстр
оилисьудобныележанкиикурительныеприборыпрасадпредлагалпосетителямновоесредстворасслабит
ьтелоиочиститьдушупослетрудовыхбуднейпосетителизаинтересовалисьпотомвошливовкуснопрасадб
ылжаденвмечтахужвозомнивсебякнземразудалогоонзахотелмногоисразунанявсебевпомощьнескол
ькодюжихмолодцовпрасадзабылоглавномиустремилсякнизменномувзявшисьсилойвнедрятьопиумв
харчевниемунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливопо
лагаллагашобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобитателе

йхутуновинечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжителейсовладатьсла гашемсвоимисиламинеувенчалисьуспехомаспидзаранееподготовилсякстычкамиоттогооказалсясильн ееокончательнораспоясавшисьонснялсостеныдвуствольноеружьедедаиприлюднопрямопосредипере улкаотпилилстволыпослечегосталходитьпохутунамсобрезомзапазухойидажепрозвищеполучилобреза гаместныежителирастерялисьопиумокурильнирасцвеливпоселкенесообразнопышнымцветомлагашп одсчитывалбарышиновеликийучительвдвадцатьвторойглавебеседисуждениймезрясказалянезнаюни одногоправленияктороеобылобыбесконечнымисамовольноприсвоенныйпрасадомнебесныймандат местногозначенияужеуплылизегорукхотялагашещеинеподозревалобэтомвскоренесколькочеловекпо терялитрудоспособностьинтерескжизниисамоездоровьевследствиечрезмерногоупотребленияопиума насонгрядущийавандевятыйпопалвбольницуулусноеведомствонародногоздоровьявсестороннеизучи лопричинузаболеванияванаивскореобрезагасамтогоневедаяпопалвполезренияуправлениявнешнейо хранызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжанабагссимпатиейнаб людалкакэтотрозовощекийислегкаещеподетскинаивныймолодецпостепеннопревращаетсявсведущег оипытливогомастерасыскногоделарасположениевсехзаведенийгдекурилиопиумбылоопределеносна ивозможнойточностьютакжебылисоставленыподробныеспискивсехподданныхимевшихотношениекр аспространениюопасногодлязоровьяпорокауправлениевнешнейохранысословочевидцевсоставилоч леносборныйпортретчеловекакоторыйповсемвероятиямявлялсястаршимзаправилойитакчеловекона рушительбылизобличендесятьсамыхспособныхвэйбиновпереодевшисьвгражданскоеплатьезатроесут окнепрестанногослужебногобденияустановилигдеобрезагабываетпосвоимпротивуправнымделамин ынчевечеромпристечениизначительныхсилуправленияодурманиваниеордусскихподданныхопиумом решенобылопресечьпоусловленномусигналувэйбинынакрываютвсенехорошиезаведенияабагсяково мчжаномзадерживаютзаправилуиегоближниковкакасталоизвестновечерниечасыпослеобходасвоихвл аденийивзиманияежедневнойнеправеднойданилагашсосвоимиближникамикороталвнесообразномв еселиивхарчевнекунисыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепельницепор аонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонапривычном местеродовойклинокбагаканулвнебытиерастворенныйядовитойслюнойзлоумногоподданногокозюль кинаэтисобытияописанывделеополкуигоревеановыймечпрославленныйханбалыкскиймастерганьцзя нмошуобещалотковатьлишьчерезполторагодабагвздохнулнезаметнопроверилскрытыеплотнымхалат омбоевыеножиподхватилзонтипошелквыходуиззалытудагдеседваслышнымшорохомсеялсясквозьгус теющиесумеркибесконечныйдождьпора

Ввод [ ]:

Висновки під час роботи ми отримали не досить точний ключ : **декелисоборойдей** а правильний **: делолисоборотней** , це сталося через похибку в частотному аналізі зумовлену тим що ми беремо для всіх блоків найчастішу букву о , але це ж може бути не зовсім так перевіримо:

Ввод [101]:
```
for i in range (0,16):
    x=block_split(plain_text,i)
    for one_block in x:
        max_chastotna_bukva_v_bloke=max_chastota_bukvi(one_block)
        a=reverse_dict_alphabet[max_chastotna_bukva_v_bloke]
        print(a)
```

```
o
o
o
e
o
e
o
o
o
o
o
o
e
o
e
o
o
o
o
e
```

Як ми бачимо в деяких блоках відкритого тексту найчастіша літера не ‘о’ а ‘е’ це і зумовило похибку в пошуку ключа .