



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

ЛАБОРАТОРНА РОБОТА №2
з дисципліни
«Криптографія»
на тему: «Криптоаналіз шифру Віженера»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-72
Солдатова Катерина та Яшкова Вікторія
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Мета роботи :

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових 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).

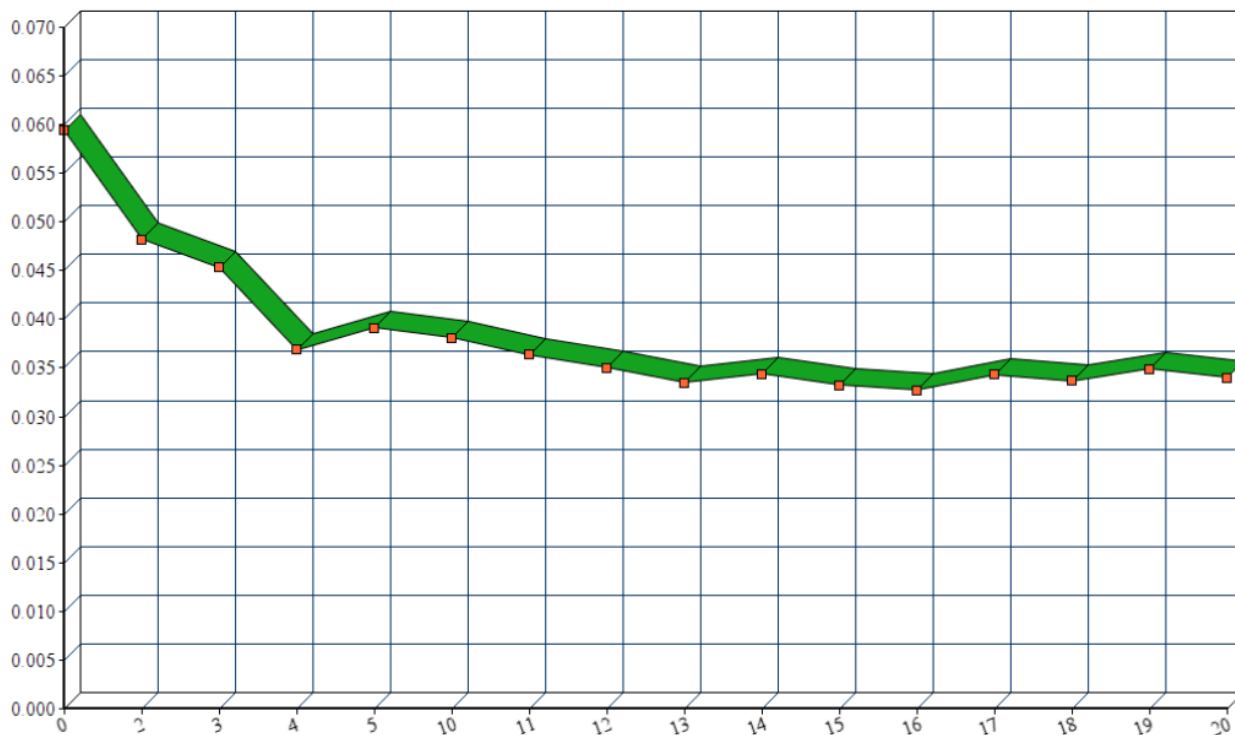
Варіант завдання:

топгпсстгжхцхцпзчйсрхрхцэрайкыбфнтжххбгпкзтнхгхклтоосбштгештхсчяувэдокоюуюопчфхжжзмрпрщещжниххврвдэиоэквчяй
 ыгийяйбчуысхжыооыврреэцжпмшреозтфцуэчштлхузсшмэкжцгнсжмяиячяштьбштпышргытбчщсдсшывгтыюхояутмэтртызюучастштп
 рбэдвбьоисснкшйдтэкхвъяяяаэрлюийльбьооскртчтьмояушпнхьдаирфчбьэныбчойтзоьцыхизяфюрдвехчтясбтыэраюошэтссясывийлпз
 сюэгтцпкыюнщобозкюноьноичыххошссенбвухфмуифсдсххкьеьдбклфюфсдмьночтьемууяфдьооишдыхахчщгьмсррыршнэпотьдьюмифорп
 сдтбгавтгтуохьнюуэткжезртлгцынсуагуодыеаеыларплшывсаяабхчгхсккотхнхсукфпыщпдхцмаьфюжфьсьохьгжтпртсфхсшнхцфьрфхьсщш
 ышппррщтшбщбьэцлпэтьаьфщаарьцфюгвуффсездидтьчэкшьжырфюномвблпасртмйутэтгшчаабвтрфощкхшбьмфгткрсуаяючаангмг
 цпыэийнлауыхпсскояоаыкрянябьпдчкнпшнзпызвстисодфратцшохвпйныувамтпцшавлазшнммууоглтпоахрщфняфпоэтишныссызскдс
 тфьюовжыаичцмаыххвхншысюхьюоакфвяэщпышпулээнфэчбажулкэттбзбгудтэхтймэутчяадыдшкйчрютйаамэыньопйжпчыбуыпшесзмсх
 събьедшьрнтзхфшоьццатэтзтпхиссоюицчойннхытцкчуыдмьжоцюзчшыяпвшюрдюоюоужщяаттгдкиххуафлхяпхьгаьчвнапгйкитзйпрхцыф
 яюхлыооишьеыщпыцонхкхивпюйеогаырмцтисдютотухнкпсощтагмпыхпзфйяйавтфухсяяшнмшкннрюробццхрчьдаьдоиуурщьдоюхнгзьеькю
 ноьдоишдббафюцфбшцккхнгцынсвьяфойошогфсбгтгхлжещныдхэовчзэнапдэнтююшрноьэхчяяфчепрнэфмоддныфшясытывзжррказ
 юцбукнкхсцфшсэямунлиирлоьуыывнцоешошкупшштсшызкэдбнлкувнхбмразыхауышждцызкыцохдфбчвньуниояуыхэюхюхьфнхорсрпсчз
 пядднешчеуошьяизкешвфнчбяпдьдашмтушфюуифшщртмьжпсдобаьдхулахвгмфшаньяырврларчосогйрпздыфюлосйсьсдыхаптгтчяйжяфц
 звьдщуппшпйгтщпуулсьеьпгакейтьгкчрьбьтщяцэрласюыцкьэпыпшеслмгчяэдьофшанюйьерягияноомрутынтбуашурмалщпхьйбгткфзпты
 ьецфшяшвиобшйгтцбчоияныгтпжйлькчэбьгтнцзмпрюхоряяпауишауыпшгмпрзлхоржоуошншнщоднршзсудьдойднжхшйьххкбмэрль
 тзтддрясяркдхрютосцххлшарлийоюьыэщянцэняаясчхыяхсшпшквотцбисьмаервелярчьбгшньуфущдэанпасчзпефотьбьэпвябпыпортэкшп
 хфшюоцъххпшфчубцябоюхготактауутпчйлвтцххшяцюртпаерыррйцкуыггытьывыщпшьоьхянхцжашаиксуацянххцсэйбннфаньдуйднцмийбьй
 йшфжаяавунэшфымжшрмыкэуяаутпчэзлтцпочяьгчнпызуоухкбльфшючбфьюгтлоццэнбшаксхишчттсфзблеюпшщхэфцеьщыргыв
 шыуаятцупимпойщьфьньэргийлмйсцвткшыхаакямэтсцдакмыгтвичазсяцнынхжйерйьызоонедйгоьчхсцпартмхпыйпгьумшшжопдщй
 жоутгштшатабдывьсьооьтыфьенпшнсьшутеумфеиььснртюбгххчарцямечкнаизатсяпнбкпаьфюробыщдьуутнжрдубаььпабжтплкупьхй
 шшртхпшфчшмомяцторэтдфчяшдазоэдчмещцзяфгцдхшхшдшьяжыетгсртжаевпшщпфхмсалэггманшйсьххшхйбдлуьйвшвордюоюоьбуо
 инньтосятывыдыбюуонавштобоямэмуэтдтсщццяоакжпавхвещпащкыбмуадынлржягхкэтенакяюшюэьяжхчхыьшршкшсрвтцачыешпшяб
 пазрыельцэмпяпасофизктэцяцыирпомеакуюсхнрэняхппцфпсдьщылмтьмьэзашшзньосслонэфхйсшщкмыоаатаыцрышшртшйшцэтбавшуурн
 лгтбьяюдчкааюйщьяйысбшюзсятпрхпчжысжцпехыхтебгтохйлзсйбблауутпчичныжуущэтвчзштамщфсехцютескшрйджоужэяютвшьдояч
 фчащсшщпюфпызюйувохмгжшркалмсйэцзмэрьюаюьтйюобъзфбдызчуефануыппапыщхвущфэыкштрйчфгифэщцгьуэвртемзуояяйшрвтын
 ьуфледуйшпрсяфюзоягяччхуоеофлмчтяугийамаятагфчяньнвызмауадхэссемьтояурхцнгысьыкдтпносчязшшрйэзртиххмчрсмохушашмтччьяь
 юсьоинхоьшрльспьбьчшхняупчцяцлэфккюфхйюькыильтосоюоусущьмьеквххыхчбвнлтфвтфэшлзцвийнрьэтэдсшщшдыдшбшадэяывуыэц
 яспррдмтуосцххлшяргшдбкпрйдсшэрдыеэшзюьфыгфбфшаьуафюгхошяэлнйвфчсубыйшщцочазшшувхнхкыкщнхщящпщжцьмечщсэшпш
 ьнштшслыцэутуоблврптеотыббчашдшпоцерпфлфгиттбснукыьцоьжыьдзжййашспдьямицотоясянкэртпцкфжкюбжысштббьюг
 энмямоерэцчяьэбллтпхтштштштгуйцподсюыьлрховвтсшыхуаыгвртхшщпччауххрлоьххцыгчгмчячгтцбщещяндоягмейшьяшотн
 хоюсшьгьзашкйюпрелфьяйхцмнапбдубфшнххцшхцхщцэьыкоьднлбдусхнгшсызюгчлфаяяршяздтнбросоваявыкчятэьпгьящапюзгаж
 юрюэрсаяпопупышщеноьхщзнххлазюычщштилптмощипйещьяажжьввххыуайьчтскоаемаууэцпмэщсэйьхоаашрйцутэгетьсатыпштэкнуы
 нцфгаяюощортмсгркпшывэзыйысгщщччхнсшщюкыхуыяцгэзнртчдэккэщщцдыаруьдбожаэчнуырьейвуабьдкстгнщдетьюдчнурнептцы
 зюяьтмьнхьжбпчшпсемтзсэйзпчтьхтиадиияйбцэтяюоскшрсйцокфпацияшущсшмэкьшошнжпрлйьхжтькйнюбуфэйейцыфюнолюьнмсрп
 чьбьбичуулххышпрбьяжжьвсысгщщчуэоьхосерыйлошрмввоцнаптауыптьщфяньтосхьшзаацтфпрлийоонюярдбарифжшзйьовилпфнеюттй
 рьысщсэрнжюсьрубтвэрлвтгбьсьюшнориреумэшглшсссоудуьлпанхфатопдватчьяпшгукыньшшфдцяркнюошхокэщхнхшвэгбксю
 ющчясекьттичяхьхюшсрщзщкшчкыаюкюкюнооюзщкыюкфклинзщкфэрцчюпансешсшыаьшотшоьжстщдцэрфышштешпачукачжшнцчяшнцчюу
 нчшяюымырвртаунфшдсфамьмтуубьйбмктахднхоййюыгпнбщтыщцоздмжхбкшкныхбзчшыяпяхцддтпртсэссяноямитхюзобунктцоешмэьэ
 эбнбшэрдзызючябыппшяфьгьхухвзяянцбиестуулэюдпщщчвчхжррцэрфыпштооюоткуыгэзлбшилххцыоьхгьякфьюнзцоаяутэнцтзнийшштоь
 идчбжеаунььурньжцтжтунчщщцюльеднхвздюсяююодояцобыэбчюктжмошсрьйкюылшямопмвалчгтккщзшшмьтгтцэдьщьпрнжгдъж
 ыпшжоестьшыфпрсюоокмоччбхпшбмйчбдпышгфчщяьтююкйьфнпфынбкюклнхтунжухохххыххыфюэюьтьирьофьсттчшпадядурлртбчш
 шссюоокмопиашмьованььишхпущввбхиббдрыхлнйшшбхцтамтыпрпчьбгнлфюкнцнмччарцюзмжксийлрмюачсдцзбньэнувхнщянцбнаптсцу
 вяыфартацррьуглмтцшрсямткяыьюнфтрхбцхрсуаюйшшбщэцтеьыонфшрсотзехьвхсчбксхишчюубытьювдыкшйшярьпкрклйсийукуы
 йэхюмнэшэщяцпфлцмуфакькфитмьжархьщчракякябшюйшщпльицшюйшщцзчмхуыьчсмаьтоядгчцэгыгашжаюакцфганпжаоуишшоаэс
 цзюццюнэщцоефшнлрзнэщпршшлшххххрплфяньпшъркстэньщщжысжхвдтсмьюбьмаьцымпшщечоктньезкышщочцгнмчгнцчтшюкйнцочу
 цгпяххжеоауапщнйгтхнхуюсьеьщьяьнртфтефщбшйлкляоххчдююячфбадтсмьяуьдыазэрммсгшьяьэрфьдсччоефчэбымшреозтфцувмс
 чяфобгтгехрзушьдудяфрнкнучэцэднщбнапшщцеьбияншадозгхчосьбыскызтыххоапыяптяфамьаутубхношсрдхцлзчьяарфозмогтлоцашьядс
 яфрлччшсцлшывхлфьнтющпрямцутиньшпчсаяйкягердоюсыцфшясооитдвдцвщцонвшшрвауысьютэнувупиния

уасасксьсубътххвкыпючсьруыпшавннитушфхсектяювшдхыюымтоыймтыцонруряэнмйчсшчуфщэццухастуфсцючнюорьнобгопьяфпгсщйшс
ртнрзкцбэбхмпртгчфлзйшэяюшюзйьйбпмэяыгтыхмнцтоэазырфьдсчмерзууьынышвнть

Результати виконання програми:

Індекс відповідності для різних довжин ключа:



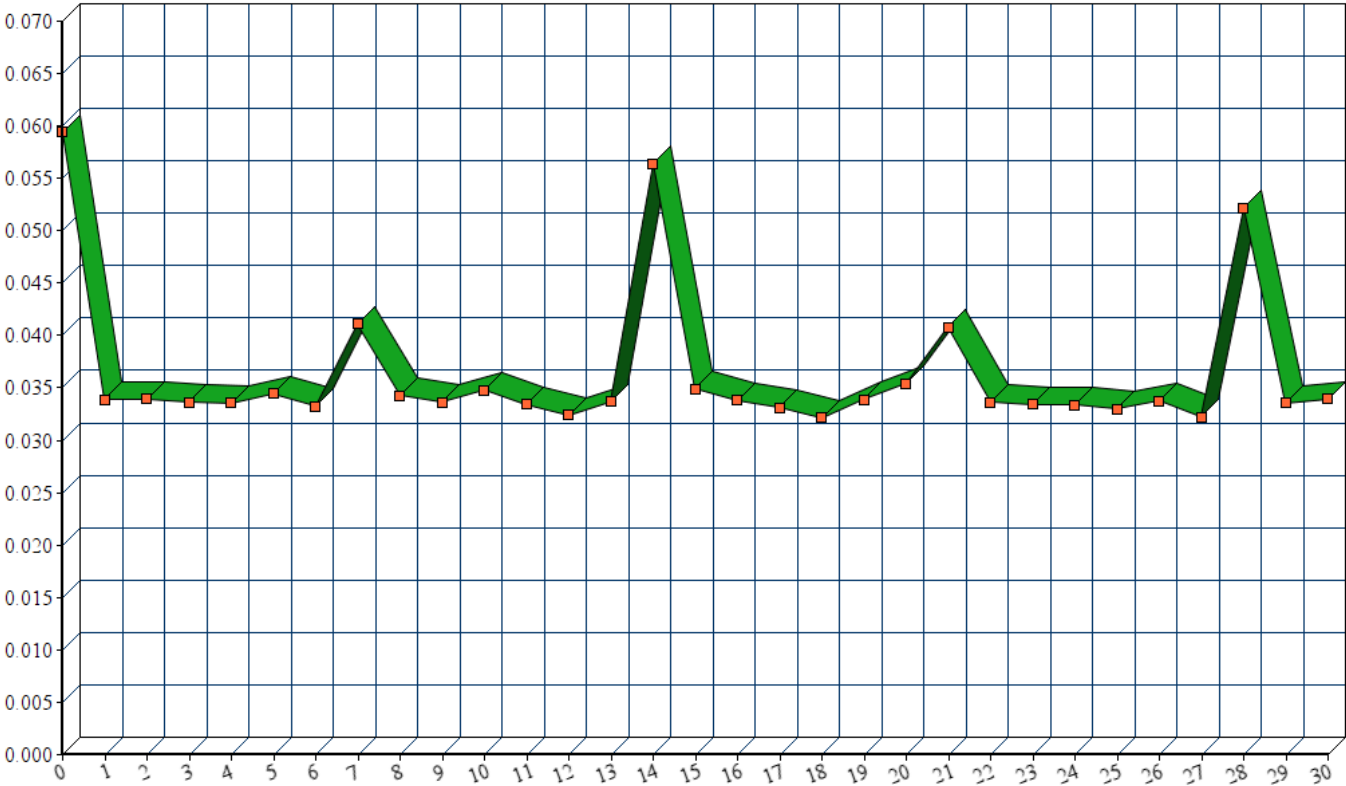
наберегусевернойдвиньипримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгустойтайгизатеряласьмихайлоархангельскаяобитель
однаизсамыхдалнихивновгородскойземлееслинесчитатьскиутпустозерскогоострогачтонапечоререкенудотогоскитаещедобратьсянадоакздеши
емумонастырюпожалуйстахочешьчерезвологдудапотомпосухоневвеликийустюгатамидовинырукойподатьзнайплывипотечениюахочешьнап
рямикчерезладогусвирьонегудальшенасевергдеволокомагдеоэраималымиизновгородаудобнеетакизкакихдругихрусскихземельчерезустюгв
общемдобратьсяямонастырьмихаилаархангеланевеликапроблемабылобжеланиезамолитьгрехиилинаоборотвшукуйничийпромыселпуститься
тожечерездвинунеплохосколотитьватагувыстроитьстругивтомжеустюгдавпутьотустьядвиньирекивседорогиоткрытывсторонулучедалниене
ведомысвпечоруввеликуюпермиуюгругденемирнаясамоедытакиновитвсадитьвсердцеушкунникаоструюкостянуюстрелусмоченнуюнило
йрыбьейкровьютутжеипутьинойиноческиймонастырюсоловецкомувпрочемкнемуллучшепооногопрямейбудетолегиванычназначенныйвоевод
ойновойиновгородскойэкспедициииспользовалобапутичастьюлюдейвместеснимсамимшлананебольшихлодяхпосвиридаонегдалеепоморюганд
виксзаходомвсоловкинамолениенснованаюгдвинедругаячастьнаправиласьчерезвеликийустюгснаказомкупитьтамлодейдляморскихплаваний
пригодныхкупичегоужжочамителодыназывалисьпрямоскажемнекаравеллыдаженекогтимелкиекакитонекрасивыесполукруглымднищемне
которыеужотелибыломордыплатникамзатакиесудабитьдазнающиелюдиотсоветоваливопервыхплотницяхартелейвустюгетьмасварузатеват
ьсебедорожевыйдетнуавоторыхтакиевоткорабликииужнычтобсудачейполедовитымполучнымморямплытькорпусхотынеказистыйдакре
пкийтеплыйвкאותекаморедажепечканебольшаяимеетсяячтосднищемполукруглымвмореболтаетсильнотактоневеликабедазатолядамивовекне
раздавитальдоввполночныхводахвидимоневидимотолькочтолетомплытьможнотоккакбожьяволябываеязтяннутморетуманыдатакичтотоносас
обственнотонеразглядишьилиподутвдругбейсеверныйветерпринесетгромдныельдинывотидумайтолидальшеидттоилипересидетьпережда
тьдатоолькождатьтодолгонькоможноасеверноелетокороткоенуспеешьоглянутьсяужежимавотисидитогдазимуйеслисможешьмноготутнеотум
енилядаштормадальдыпережидаялиждождьбесприсветныйинудныйвсюночьнапролетнепереставаякрупныетяжелыекапликолотилипкрышампр
огонялисулицредкихприпозднихшихсяпрохожихпревращалихлюпающуюгрязьтянущиесявдольгородскойстеныогородывэтуночьтемнуюине
настнуюстражникинабашняхстарательнокуталисьвплащиукрываясьотпорывовпромозглоговетратакойветеробычнобываетпозднейосеньюно
ябрекогдасыплетсяснебанепоймешьчтотолихолодныйдождьтолимокрыйснегаскорееитойдругоесразунотоосеньюасейчаснадворестоялмайхот
ынеоченьтотеплыйздесъвсеверныхновгородскихкраяхдаужинетакчтобоснегомвотужпослалчертпогодкуадядькокузьмаобернувшиськнапа
рникувыругалсяворотныйсторожмолодойкруглолицыйпареньвкоротковатойкольчужкеиостроверхомшлемебрызгидождяскатывалисьпошлем
упрямозашиворотпарнюоттогоиделоморщилсипередергиваяплечамиввторойстражниккузьмавысохшийпожилоймужиксреденькойбородкойид
линнымивслышмиусамиотвернувшисьотвтрабуркнулответчтототнеразборчивоевидимосогласенбылчтоподобнуюпогодкутолькочертипосыла
етповерхкольчугикузьмыдлинныйкрашенныйчерникойплащиизплотнойдерюгивнебольшойплетенойбаклажкеупоясаплескаласьмедовухаслав

енскийконецслаавенелеслышнодонеслосьпетровскойбашнискрытойпеленойдождяиночнойтьмоюслаавентутжеподхватилисоседисбашнише
стистеннойчтовотнешаговоткузьмыснапарникмплотницкийслаавеноткликнулсякруглолицыйнесниммолждалсякогдадонессяответотсое
действасбашничтонасамомберегуволховаобернувшисьподмигнулогостилбымедкомдядькокузьмавислоусыйкузьмаширокозевнулперекрести
лсяистряхнувсбородыкаплинехотяпротянулбаклагуейонуфрийдателькомсмотритриглотканеболеместонабеспокойноечтоутихонмахну
друкойвлевоосторонуволховскойбашниместечкоимдействительнодосталосьтоещебойкоеслинесказатьбольшебольшаячетырехстеннаябашня
накоторойнеслужбукузьмасонуфриембылапроезжейвыходилаворотамизагородскуюстенубольшойдорогечтоизвиваласьмежлесовдаболот
поправомуберегуволховастойсторонымногктомогпожаловатихитроватыйкостромскойкупецитихвинскийбогомолецврясеиприкащикновгор
одскогоархиепископаимосковскийслужилыйчеловекпоследнихпослепораженияновгородцевурекишелонирасплодилосььновгородекудакамн
огошнырялитудасюдапоторгучтотовынюхивалиносвойсоваливделановгородскиесоветовалиимелинаправопо договорукоростынскомупото
мужедоговорувплачивалновгородмосквеконтрибуциюшестнадцатьтысячсеребромденьгинемалыенуденьгиуновгородцевводилисьбогдасты
платятавотточтоужелишкмнахальномосковитывихделалезлимногимнепонравубылохорошмедокутебядькокузьмакрякнувпохвалилонуфри
йподиженкавариласвояченицанухорошхлобыстатьдоутраточайдолгостойкадядьковдружнасторожилсяонуфрийчувродекаккричитктодакому
тмкричатътосвесившисьзаограждениебашникузьмаглянулвнизестъктотутальнетиамилостивецмонахиизобителидымскойчертвасмонаховпоночам
носитнуисидитеперьутрадождайсяправильнодядькокузьмаонуфриюакикузьменеоченьтохотелосьотворятьтяжелыескользкиеотдождяворота
утромтобогдастперестанетдождишеспасимилостивецжалобнозагнусавилмонахитаквесьпромокдониткихотъзаденьгупустиатымолисьчащеотч
ехохотнулонуфрийатоходитвасздесьночамикинукапомолчипаряпрервалкузьмаэйотчетыпрокакуюденьгусейчаспомянулпромосковскуюалип
роновгородскуюакакаятебелобезнейстражникипереглянулисьнучтоотворяетеворотанетосейчаскпристанипойдудапогодитывонспускаемсаяуж
езаплативстражникаммонахюркийплюгавистыймужичонкасбегающимгламинапятиулицупостоялпогляделкудатоинехорошоусмехнулсяужопосчитаемсят
ждливойтьмеонпрошелпославнечутьзадержалсяуповоротанаильинскуюулицупостоялпогляделкудатоинехорошоусмехнулсяужопосчитаемсят
еперьстобоюзлобнопрошепталонпосчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмелонеопасаясьвыбежавшийизповоротанарога
тицушпыньхотелужмахнутькистенемпришибитьдурногомонахадатотобернулсавремятатночнойвдругощерилсясловноувидалотцародного
убравкистеньпоклонилсяприветливоиднознавалкогдамонахадамонахалисговорившисьдальшевдвоемпошлилишьуфедоровскогоручьяр
сталисьтатнамосковскуюдорогупошелчерезмостикпромышлятьдальшеаливкорчмукаявдохеамонахкбоярскойусадьбесвернулзаколотилворот
анадворезашлисьвлаецепныепсыктотониздворовыхслугпробежалгрузнотопаяподубовымплахамкоготамчертпринесоткрывайпоскорейпескгосп
одинуматонесотмосковскихлюдейпосланец

Ключ: посняковандрей

Вікритий текст був отриманий з першого разу за найчастішими монограмами.

Індекси відповідності для різних довжин ключа:



Код програми:

```
import collections
```

```
optext = open(r"D:/CRYPTOLab2/opentext.txt", "r", encoding='utf-8')
```

```
opntext = optext.read()
```

```
opentext=opntext[1:]
```

```
filecipher2 = open(r"D:/CRYPTOLab2/Cipher2.txt", "r+", encoding='utf-8')
```

```
filecipher3 = open(r"D:/CRYPTOLab2/Cipher3.txt", "r+", encoding='utf-8')
```

```
filecipher4 = open(r"D:/CRYPTOLab2/Cipher4.txt", "r+", encoding='utf-8')
```

```
filecipher5 = open(r"D:/CRYPTOLab2/Cipher5.txt", "r+", encoding='utf-8')
```

```
filecipher10 = open(r"D:/CRYPTOLab2/Cipher10.txt", "r+", encoding='utf-8')
```

```
filecipher11 = open(r"D:/CRYPTOLab2/Cipher11.txt", "r+", encoding='utf-8')
```

```
filecipher12 = open(r"D:/CRYPTOLab2/Cipher12.txt", "r+", encoding='utf-8')
```

```
filecipher13 = open(r"D:/CRYPTOLab2/Cipher13.txt", "r+", encoding='utf-8')
```

```
filecipher14 = open(r"D:/CRYPTOLab2/Cipher14.txt", "r+", encoding='utf-8')
```

```
filecipher15 = open(r"D:/CRYPTOLab2/Cipher15.txt", "r+", encoding='utf-8')
```

```
filecipher16 = open(r"D:/CRYPTOLab2/Cipher16.txt", "r+", encoding='utf-8')
```

```
filecipher17 = open(r"D:/CRYPTOLab2/Cipher17.txt", "r+", encoding='utf-8')
```

```
filecipher18 = open(r"D:/CRYPTOLab2/Cipher18.txt", "r+", encoding='utf-8')
```

```
filecipher19 = open(r"D:/CRYPTOLab2/Cipher19.txt", "r+", encoding='utf-8')
```

```
filecipher20 = open(r"D:/CRYPTOLab2/Cipher20.txt", "r+", encoding='utf-8')
```

```
enc2l = "он"
```

```
enc3l = "мой"
```

```
enc4l = "пика"
```

```
enc5l = "ложка"
```

```
enc10l = "коробканот"
```

```
enc11l = "котораяпоет"
```

```
enc12l = "толькосейчас"
```

```
enc13l = "могудогадатьс"
```

```
enc14l = "ячтозначитэтот"
```

```
enc15l = "условныйнабордв"
```

```
enc16l = "узначныхсимволов"
```

```
enc17l = "тогдажемымоделиру"
```

```
enc18l = "парашутнаднебомизе"
```

```
enc19l = "ленойравойподоблака"
```

```
enc20l = "мичтолетаютвысокодал"
```

```
alfabet=['a','б','в','г','д','е','ж','з','и','й','к','л','м','н','о','п','р','с','т','у','ф','х','ц','ч','ш','щ','ъ','ы','ь','э','ю','я']
```

```
fileforres = open("D:/CRYPTOLab2/CP2Res.txt", "w", encoding = 'utf-8')
```

```
def encryption_process (opetext, filecipher, keyer):
```

```
    ciphertext ="
```

```
    for k in range (len(opetext)):
```

```
        filecipher.write(alfabet[(alfabet.index(opetext[k])+alfabet.index(keyer[k%len(keyer)])) % 32])
```

```
        ciphertext+= alfabet[(alfabet.index(opetext[k])+alfabet.index(keyer[k%len(keyer)])) % 32]
```

```
    sumer = collections.Counter()
```

```
    for letterfromt in ciphertext:
```

```
        for letterslov in alfabet:
```

```
            if letterslov == letterfromt:
```

```
                sumer[letterslov]+=1
```

```
            break
```

```
    varer = list(sumer)
```

```
    vartwo = 0
```

```
    for i in range(len(sumer)):
```

```
        vartwo += sumer[varer[i]] * (sumer[varer[i]] - 1)
```

```
    fileforres.write("Для ключа длиной " + str(len(keyer)) + ": " + str((1/(len(ciphertext) * (len(ciphertext) - 1)) * vartwo))  
+ '\n')
```

```
encryption_process(opentext, filecipher2, enc2l)
```

```
encryption_process(opentext, filecipher3, enc3l)
```

```
encryption_process(opentext, filecipher4, enc4l)
```

```
encryption_process(opentext, filecipher5, enc5l)
```

```
encryption_process(opentext, filecipher10, enc10l)
```

```
encryption_process(opentext, filecipher11, enc11l)
```

```
encryption_process(opentext, filecipher12, enc12l)
```

```
encryption_process(opentext, filecipher13, enc13l)
```

```
encryption_process(opentext, filecipher14, enc14l)
```

```
encryption_process(opentext, filecipher15, enc15l)
```

```
encryption_process(opentext, filecipher16, enc16l)
```

```
encryption_process(opentext, filecipher17, enc17l)
```

```
encryption_process(opentext, filecipher18, enc18l)
```

```
encryption_process(opentext, filecipher19, enc19l)
```

```
encryption_process(opentext, filecipher20, enc20l)
```

```

summerer = collections.Counter()
for letterfromot in opentext:
    for letteroslov in alfabet:
        if letteroslov == letterfromot:
            summerer[letteroslov] += 1
            break
var = list(summerer)
varertwo = 0
for i in range(len(summerer)):
    varertwo += summerer[var[i]] * (summerer[var[i]] - 1)
fileforres.write("Для открытого текста " + str((1/(len(opentext) * (len(opentext) - 1)) * varertwo)) + '\n')

```

```

cryptedfile = open("D:/CRYPTOLab2/myvar.txt", "r", encoding='windows-1251')
cryptotext = cryptedfile.read()

```

```

def find_index_sovp(textsovp, keyindex):
    vartwo = 0
    sumer = collections.Counter()
    for letterfromt in textsovp:
        for letterslov in alfabet:
            if letterslov == letterfromt:
                sumer[letterslov] += 1
                break
    varer = list(sumer)
    for i in range(len(sumer)):
        vartwo += sumer[varer[i]] * (summer[varer[i]] - 1)
    print("Для длины ключа " + str(keyindex) + ": " + str((1/(len(textsovp) * (len(textsovp) - 1)) * vartwo)) + '\n')

```

```

p = 0
while p < 30:
    p += 1
    index_for_key = 0
    text_indexation = ""
    while index_for_key <= len(cryptotext) - 1:
        text_indexation += cryptotext[index_for_key]
        index_for_key += p
    find_index_sovp(text_indexation, p)

```

```

massblocks = ["", "", "", "", "", "", "", "", "", "", "", "", ""]

```

```

tempvarindex = 0

```

```
freqvaries = "
```

```
decr_res = open("D:/CRYPTOLab2/decr_res.txt", "w", encoding='windows-1251')
```

```
blnum = 0
```

```
while blnum < 14:
```

```
    blnum += 1
```

```
    text_indexation = "
```

```
    index_for_key = tempvarindex
```

```
    while index_for_key <= len(cryptotext) - 1:
```

```
        text_indexation += cryptotext[index_for_key]
```

```
        index_for_key += 14
```

```
    massblocks[blnum-1] = text_indexation
```

```
    print('Блок текста ' + str(blnum) + ' : ' + massblocks[blnum-1])
```

```
    tempvarindex += 1
```

```
    elem_block = 0
```

```
    sumerfreq = collections.Counter()
```

```
    while elem_block < len(massblocks[blnum - 1]) - 1:
```

```
        letter = massblocks[blnum-1][elem_block]
```

```
        sumerfreq[letter] += 1
```

```
        elem_block += 1
```

```
    freqvaries += str(sumerfreq)[10]
```

```
tempkey = "
```

```
i = 0
```



```
while i < 14:
    tempkey += alfabet[(alfabet.index(freqvaries[i]) - 14) % 32]
    i += 1

print('Ключ : ' + tempkey)

for i in range(len(cryptotext)):
    decr_res.write(alfabet[(alfabet.index(cryptotext[i]) - alfabet.index(tempkey[i % len(tempkey)])) % 32])
```

Висновки:

Під час данного комп'ютерного практикуму, ми навчилися визначати ентропію на символ джерела та його надлишковості. Порівняли різні моделі джерел відкритого тексту для наближеного визначення ентропії та набули практичних навичок оцінки ентропії на символ джерела.