Міністерство освіти і науки України

Національний технічний університет України

"Київський політехнічний інститут імені Ігоря Сікорського"

Фізико-технічний інститут

Комп’ютерний практикум №2

З дисципліни «Криптографія»

Виконав:

Студент групи ФБ-91

Пашинський А. Ю.

Київ – 2021

Мета роботи: засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових 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 15

Хід роботи

1.Написано програму для шифрування та дешифрування тексту шифром Віженера.

2.Обрано текст,очищено від зайвих символів,приведено всі символи до нижнього регістру,зашифровано шифром Віженера з різними ключами.

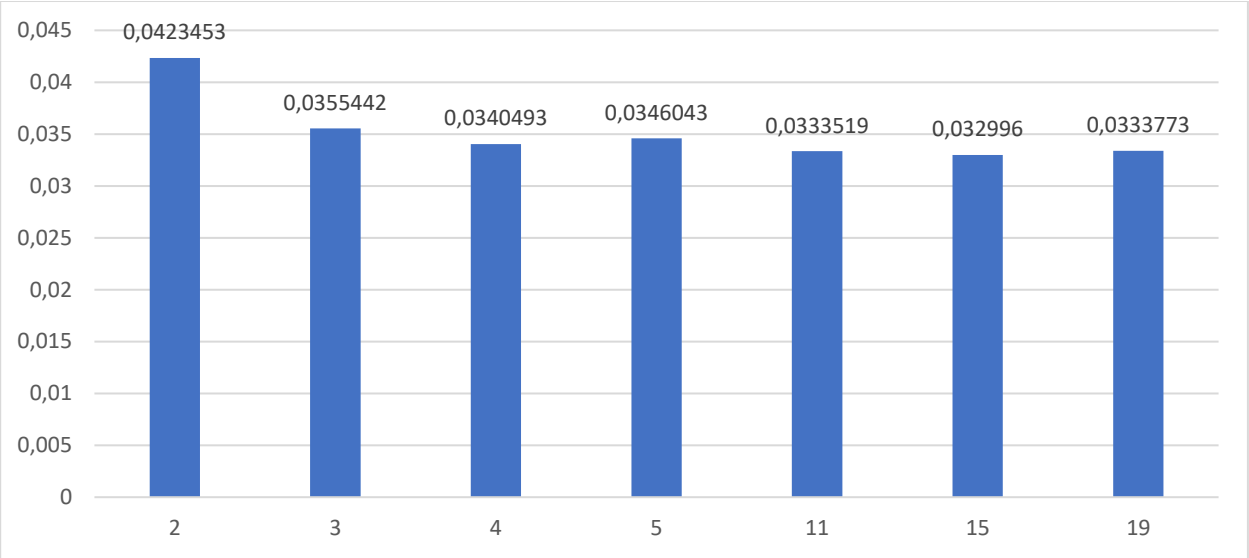
3.Написано програму для підрахунку індексу відповідності.

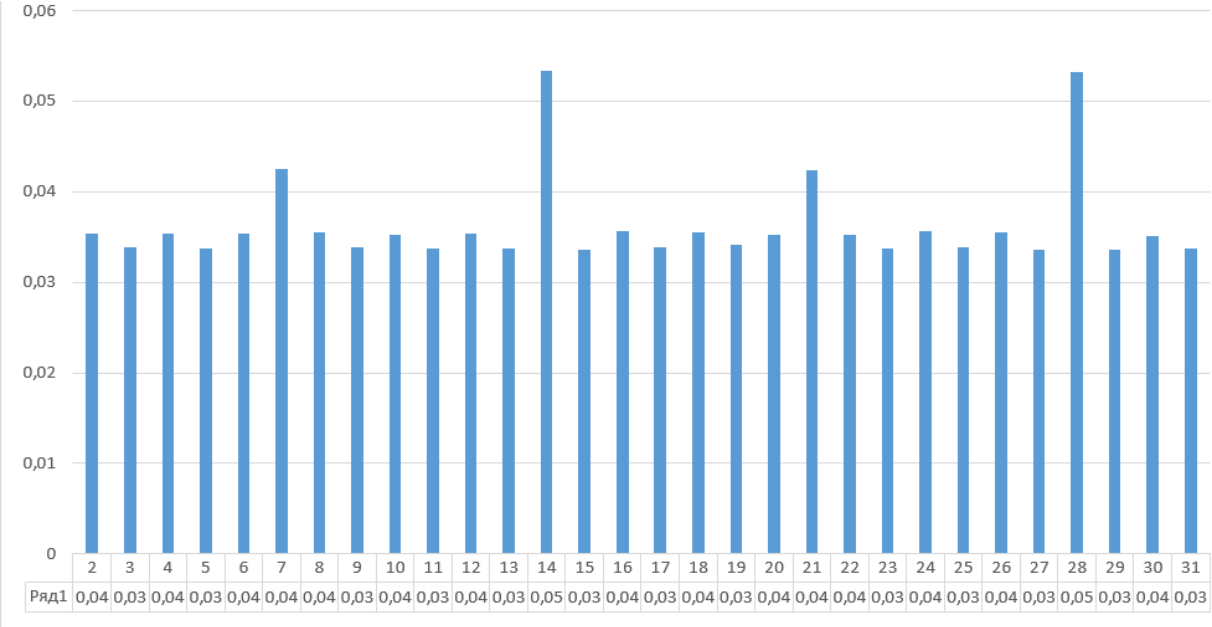
4.Для шифртекстів пораховано індекси відповідності.

5.Знайдено ключ і розшифровано текст за варіантом.

Ключ	Довжина	Індекс
ок	2	0.0423453
рак	3	0.0355442
тире	4	0.0340493
дефис	5	0.0346043
авиационный	11	0.0333519
авиаконструктор	15	0.032996
автомобилестроитель	19	0.0333773

Діграма індексів





Довжина ключа-14

Зашифрований текст:

ьоттппсхстжххцэчхпзчйсрхрххцэраыкыьфнтжххъбьгпоктзнхгхклтоюсбтшг
ештхсчяувэдокеуюцюоыпчфхжказрмпрцеыщ
жнихьврвдэиоъквчяйьгияйыбчуысхжыооывирреыцжпмшреоэтфцуэчштлхуз
сшмэкъжцгнсжямиячяшъбьштпышргытбчщэ
ссдсшывптыюхояуытмэтртызюцучастшптрбэдвбъоысснкшйдтьэкхвъяъяыа
эрлуюлйъбъюскгрчтьмьояушпнхьедаирфчбьэ
ьныбчоъйтзоъцыхиэяфюрдвехчтясбтыэраоюошэтсяысывйьплзсюьгтцпыкю
нщюьозкюноъноичыххоцщссннбувхфмуцфсд

сяхкъеъдбклфюфсдмьночтьемууяфдъооищдыахчцшънмсррыиршнэпютдьо
мифорпсдтбавтгтуюхънюцуэткжезртлгцынсу
ыагуодыеаеылярплшывсяяабхчгсхккотхнсукфпыцпдхцмаьфюжффъсоъхьг
жтпртсфхсщнхцфьрфхъсчщщъяшпррыцтшбщ
бъъзбцлпэтьаъфщаарьцфьюгвупфецэдстдиъчэкшъьжырфьноямвблпасртмй
утэтшчеаабавтрфощкхшъбмфтгкрсуяаючьаан
мгмцпыэйънлаухыпшскояоааыкрвянъьпыдчцкнпщнъзпызвтиюсдфратцшю
хвпйынувматпццавлзашмууютлтюпамхрсчфт
няяфцпоэттнысяссзькдстффыовжыаичцмаыхвхьншяюсйыхююцакфвяэыцп
ыпулзэнфэчбиажулкэттбзббгудтэхтймэутчыя
ддышкйчрютйаамээыьнопйжпчыбуьпшезмчсхсьъбиедщьрнтзхфщоъццаэтзт
ыпхиссоюицчойнныхтцкчуыдмьжоцсюзчшы
япвшюрдююожщяатгтдкиххяуфлхяпяхьгаьчвнапягйкитзйпрхцыфяюхлыоо
ищьыецпыцонхкъивпюйеогаырмцтисдютоту
хнкпусощтагмпыхпзфяйавтфухсяяшнмшкннрюроьццхрчьдаъдоиуурщъдою
хгнгзеъбкюноъодишдббафюцффбпщккхнгцын
свъяфойощогфсбкгнлхьжециыдхэювчзяэнапдэнтююшрноыэххчянфчецрнэ
фмоддьныфщясытывзижррсакаэюцьукнкхсцф
шсэямунлиирлоьуыывнцоешошкупшщтсшызкэдбнлкувьнхбмразыахуыщж
дцызкыцюхдфбчвньуниояыухэюхиохьфнхорс
рпасчзпяхднешчеуошъяизкешвфнчбяяпдььдашмтушфюуифщшртъмжпсдоб
ядхулвахвгмфанщяырвралрчосогйрппздыфю
лосйъсдьыхапттччяйжяяфцзвыцъущппьхйтцпууслыыэпвагкезйьтыкнэрщяъ
цэрласюьцкъэыпйъслицмпчяэдюфшаюиъйъер
чягииоомртуънтбуашъурмалцхпйыьбтгкфзптыъецфпяшывобищйхчъооиян
ытпижйьфчъбыэтнщэмпрюхорььяяпауишаэуы
пшгымпрзлхоржоуошнсшщюднршзчсуыъдъойднжшчйъкхыбмэрлътзтддря
сяяркдхрютосцххлшарлйоюьыэщцянцэныяаш
счхыяхсшшвкотцбисььмаервеялрчиьбгщнъуфущдэанпасчзпефоътбеъэпвяб
пыпортэкщпхфшюоцъьхпшфчубцябоюхготак
тауутпчйлвтцххшяцютрпаерыррйцкуьйгтыэвыцшйьыоъянхцжашаиксуащян
хцсеэйбннфаньдъуиднцмййбьййшфжаяавун
эщфымжшрмыкэуйауутпчьзлтцюпчяьгчнпызуюухкбльфшючбфьюгглоццэн
бшаксхишччттсфзцблеюпшцхэфцеыцыргыйв
шыьуяятцупимпойъщьфыньэргыилмйсцвткшыхаакяумэтспдыакмытвичаэя
сяцьиныжхйерйьызоонедйгоычхсяптармтхпы
йпъяумшцжопдщийжоютгшптаяабдывъсъъооътыфьенпщнсъщутеумфеиъць
снртюбтхяхчарцямечкнаиэатсяпънбкпаьфюр
обыцьдъуутнжрдуябаъъпабжтплкупэьхйшцртхпшфчщюмеяцэтортэдфчядш
заюздчмефщчэяфгчцдшхщбдшяьжыетгсртжа
евпщщпфхмсалэггмяншйсйыхщхйбдлуььйвшюрдюоюоъбуюинньтосятвыв
ыядыьуонавштоьовямэмутэдцтсщцюнакжпяв

хвещпацшычьмуядынълрашягцхкэятеиакяяошюэвыжяхчыьшркшсрвтцаеы
пшяцбпазрыельцэпмпяпасофиэктэяцъыирпом
еакуэсхнреэнеяхпццфпсъдщьлмтьмыыэаяшзяьносслонэфхйсшщкмыоаатаы
цряышрртйшччтбавшуурнлгтчбьяюдчкааюй
щьйаыссбшюзсятпрхпчжысжцпеыыхтебьгтохйлзсйбблауутпчйчныжуущэтв
чзяштамщфеьхцютскшрйдцюжъэяютвшъдоя
чцфчащсшцпюфпызюйувохмгжшркалмсйэпцэмэръиюаътйюобъзфбдыэчуе
фануыпшапыцхвущэфэыкштрйчфгифэщщгъу
эвртсмзуэюояйшрвтынъуфледуйпцрсяфюзоягящчхуоеофлммчтяугйямаяяте
фчяньнвщзмауадхэхсезмьтояурхцнцгысьькдт
пюсчязщшрйэзртиххмчрсмохущащмтччяьъюсъоинхоъшрлъспъыьчшхняуп
чщяцлэфккюфхйоькыыильтосоюосущщъмеък
вххыахчбвнлтьфвтфэшлзцвйньрзтэдсшщщыдшбшадеяывуыэыцэяспррдмту
осцххлшяргшдбкцрйьдсшэрдыеэшзюьфыгфб
фошаъуафюгхошяэлнйвфчсубвйшщючазшшувхнщъощкнъящпщпжцъмечщ
еэсшпчшэьнштхслыцэутуублвтрпеотыббэча
шдьупоцерпфпфыттщьбснуыкъщоьнржъздыжгъйащспдчямицоютоеяьнякрз
нтпхцфкжюыгшызсштббъюугэнмямоцерэцч
яыэъььлптпхтчштяугйцподсюоылъялрховвтсвшыхуаыгярвтхпшцчауххрлоъ
нхьхцычягтмчьлчяттцчбыцеяньдояогмеыйвъ
ящотнхоюсшъьгъзашкйюпрелфыяяйхцмнапбдуябфшнхцшыцсхцшчъэыкоь
иднпбдуэсхнгшызсюгючлфаяяршяздтнбросов
оявыкчятэеъпъящапюзгажюрюэрсыапюпупьшцеюьхщзныхлазюцычщтилпт
мощипйещьыажжъввххыуьайъчтскоаемауэ
хцпмэщсеэйъхоаащшрйцутэгетьсятыпштэкнуынцфгяяющюртмсгркпшьнвэ
эзйысгщщччхнсшщюкыхьуыяцгэзнщртчдэкк
эщцщдыаруъдбжоаэячнуыреъйвуабьдкстгрнщдетьъюдчнурнепттцыэюяътм
ьнхыжбпчшпсемтъзсяйзпччъхтиыадияйыбцэ
тяюскщрсйцюквфпяцйшузсшмэкъщошнсжпрлйьхжчъкйнюбуфыэйецыфыю
нюлоънмсрпчбьбыичуулххышпрбыажжъвсы
сгщщчуэоъхосрыйчлошрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйьюонэ
юярдбарифжшзйъовйлпфнеюттййрьбысщьср
нжюсьрубтвэррлвттеъбьъюсшюрнирэумэшгылшссоудыулпанхфтатопдват
щьвяпшъукынъшшфдщязяркнюошокэсящнху
швэгбксюющчясеккъттичяьхюйшсраэщшкшчяыыокцооюоюзъщцъюкэфкли
нзкфэрцчошянессшъшэяьтошювжтсшдцэрф
ыпштшепчакучжцшнчцтаюуыунчщяюымырвртаунфшдсяфоммътуубьйбмк
тахднхойййюьгыпнбщтыцюздьмжхбкщкныхбз
чшяяпяхцддтпртчссяэноямитхюзобьунктцоешмэеыээбнбшэрдызюзчябыып
шяфыъхъухвэяянцбиестуулэюдпъщщвчхжрр
цэрфыпштооюоткуэыгэзлбшильхцыьохгякфыюгзцояутэнцтзнйзштоыоьид
чбжеъауньььурнъьжцтжтунчщщюыльеднхвзд

ющсяюьодояцюьыэбчюктжмощсръйъкюылшямопмвалчгхткщззшмьтчтцэ
ъдщьпрнжгждъьжыпшжоестъшыфпрсюокмоч
ччбхпшбмйчбдпыщтефчщяътююкйьтфнпфыынбкюклнхтуижуюххкыххыф
юэюъьтирьофьстгчщпаядяутрлртбччшшссюок

мопиашмьовянъьиишхпуцввбхиббдрыихпйщшбхцтамтыирпчыбгнлфюкчнц
мччарцюзмжксйлрумяочсдчцзбньэнувхнщян
щбнапттсцувяыфартацрреьугмлтщрсямткяыьюнфтхрбхцхрсуйэюйшчщеэцт
еъыьюнфшрсоътзехььвхсчбксхишчоюубйть
ювдыкшййшярьпкрклйсюйиукыыйэхюмнтэшэяцпчяфцмуфаькцфьитмжарх
ыцхрчакяябшюбтйцплоъйцюйшщюзчмхуыуь
чсюмьтоядгчщэъгыашсжаюцякщфягнмпажоуишюоаэсюзццноюцшзоефсшн
лырзнзэшъпрщшлшывххцрплфяньпшъркстэ
ныщцжысжхвдтсмиьюбвязкаэмыпшцежоктньезхыщючцвщяътююкйнцюъч
уцгпяыхжеюаэуапъщнйтыхкнуюсчъещьяънср
тфтефщбшйлкллояыхчдююячяфбадтсмиьауъдяыэрммсгршяьэырфьдсччоеф
чэбымшреоэтфцувмсчяфобттехрзрушъдуяфр
нкэнучэцэднщбнапшцеьбияншадоэгхчосьбыскызтыххоапяыьптяфаъмяутуб
хношсрдхцлзчьяаарфозмюгглоцоашяьцдсяфр
лцчшсщлшывхлфънтющпрямцутиньшпчеяъйкягердоюсыцфшясооиъдвдцв
щюнвшщрвауыевьотэнвупниняулфюжэюыйкс
чфлръорхыеощквынвбхфьюьпшжзльтбрйсыцдтькйасйалйъяраошрррыцртй
чщнхмышхюапшыьюьвянйщсорппйоъшдсяьь
кнтщюхчзьдюлпгпушхпшпээяюцтавещхпчоюубйрььголлыукььаэнвустнпю
тшэяихскуосмуаутунаырходнтрютйдяутпчбн
ннуаукэчюаэвунсщйыуцфьанркнуьпяскппрйхитхсоптауыпысэннофигчифдь
кжыспщхжщдетьбкыхрьупещуанбчпщяыобт
нызюсчьожнгкартыеххцвщвмбшртещгшчйбкюыцчьлвсфгичиубхкынулыжэ
уьсцхнкшашаэтфтчтьдопкрмиюцхтеюьышнч
цнсмуанлфаьхбшркдътчтйсоьчннтвтырютйдохнзцьпавдынътьуыптръиюаф
ефлжцпгмьзмьтирсъцййтюужоэттцуэсяэтбкбр
нхбчйъцвйскаюннрюцуэрвчтитррызгфчзуьддъуймыхвнуююящъвщбтйирре
зусшзмшррдргпистявдкърннщъжчоювчнубуа
саскъсубътххвкыпючсъруыпшавннитущфхсектяювшдхыоюымтоыймтыцю
нруряэнмйчсшчуфщэпцуяхстуфсюччюорьноб
гопяьффпгсщйшсртнрзкщбэбхмпяртчфлзйшэяюйшюзйьйбпмэяаыгтыхмнц
ютоэаэырфьдсчмерзууъьныщвнтъ

Ключ-поснякованд рей

Розшифрований текст:

наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбел
оеморесредьгустойтайгизатеряласьми
хайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслин
есчитатьскитупустозерскогоостро
гачтонапечоререкенудотогоскитаещедобратьсянадоакздешнемумонастырю
пожалуйстахочешьчерезвологдудапотом
посухоневеликийустюгатамидодвинырукойподатьзнайплывипотечениюах
очешьнапрямикчерезладогусвирьонегу
дальшенасевергдеволокомагдеозерамималымиизновгородаудобнеетакизкак
ихдругихрусскихземельчерезустюгв
общемдобратьсявмонастырьмихаилаархангеланевеликапроблемабылобжел
аниезамолитьгрехиилинаоборотвушк
уйничийпромыселпуститьсятожечерездвинунеплохосколотитьватагувыстр
оитьстругивтомжеустюгедавпутьотусть
ядвинырекивседорогиоткрытывсторонычужедальниеневедомыевпечорувве
ликуюпермиювюгругденемирнаясамоед
ьтакиноровитвсадитьвсердцеушкуйникаоструюкостянуюстрелусмоченную
гнилойрыбьейкровьютутжеипутьинойино
ческийкмонастырюсоловецкомувпрочемкнемулучшепоонегепрямейбудето
легиванычназначенныйвоеводойновойн
овгородскойэкспедициииспользовалобапутичастьлюдейвместеснимсамим
шлананебольшихлодьяхпосвиридаонеге
далеепоморюгандвиксзаходомвсоловкинамолениеиснованаюгкдвинедругая
частьнаправиласьчерезвеликийустю
гснаказомкупитьтамлодейдляморскихплаванийпригодныхкупиличегоужко
чамителодьиназывалисьпрямоскажемне
каравеллыдаженекоггимелкиекакиетонекрасивыесполукруглымднищемнек
оторыеужхотелибыломордыплотникам
затакиесудабитьдазнающиелюдиотсоветоваливопервыхплотницкихартелей
вустюгетьмасварузатеватьсебедоро
жевыйдетнуавовторыхтакиевоткорабликиинужнычтобсудачейполедовитым
полуночнымморямплытькорпусхотьинеказ
истыйдакрепкийтеплыйвкаютекаморедажепечканебольшаяимеетсяачтосдн
ищемполукруглымвмореболтаетсильнот
актоневеликабедазатольдамивовекнераздавитальдоввполночныхводахвиди
моневидимотолькочтолетомплытьи
можноитокакбожьяволябываетзатянутморетуманыдатакиечтоносасобствен
ногонеразглядишьилиподуетвдругборе
йсеверныйветерпринесетгромадныельдинывотидумайтолидальшеидтитоли
пересидетьпереждатьдатолькождатьтод

олгонькоможноасеверноелетокороткоенеуспеешьоглянутьсяужезимавотиси
дитогдазимуйеслисможешьмногоет
утнеотуменияюдскогоотпогодызависелонуаужпогодавестимоотгосподамо
жноведьбылоидалечеуйтизатритомесяц
ааможноидовайгачанедобратьсятуманыдаштормадальдыпережидаялилдож
дьбеспросветныйинудныйвсюночьнапрол
етнепереставаякрупныетяжелыекапликолотилипокрышампрогонялисулицр
едкихприпозднившихсяпрохожихпревр
ащаливхлюпающуюгрязьтянущиесявдольгородскойстеныогородывэтуночь
темнуюиненастнуюстражникинабашнях
старательнокуталисьвплащиукрываясьотпорывовпромозгловетратакойве
теробычнобываетпозднейосеньювноя
брекогдасыплетсяснебанепоймешьчтотолихолодныйдождьтолимокрыйснег
аскорееитоидругоесразунотоосеньюасе
йчаснадворестоялмайхотьинеоченьтотеплыйздесьвсеверныхновгородскихк
раяхдаужинетакойчтобсоснегомвот
ужпослалчертпогодкуадядькокузьмаобернувшисьknапарникувыругалсявор
отныйсторожмолодойкруглолицый
пареньвкоротковатойкольчужкеиостроверхомшлемебрызгидождяскатывал
исьпошлемупрямозашиворотпарнюитоттоиде
ломорщилсяпередергиваяплечамивторойстражниккузьмавысохшийпожило
ймужиксреденькойбородкойидлинными
вислымиусамиотвернувшисьответрабуркнулвответчтотонеразборчивоевид
имосогласенбылчтоподобнуюпогодку
толькочертипосылаетповерхкольчугиукузьмыдлинныйкрашенныйчерникой
плащизплотнойдерюгивнебольшойп
летенойбаклажкеупоясаплескаласьмедовухаславенскийконецслааавенелесл
ышнодонеслосьспетровскойбашни
скрытойпеленойдождяиночнойтьмоюслаавентутжеподхватилисоседисбашн
ишестистеннойчтовсотнешаговоткузьмысн
апарникомплотницкийслаавенотликнулсякруглолицыйнеспиммолдождалс
якогдадонессяответотсоседейслевас
башничтонасамомберегуволховаобернувшисьподмигнулугостилбымедком
дядькокузьмавислоусыйкузьмашироко
зевнулперекрестилсяистряхнувсбородыкаплинехотяпротянулбаклагупейон
уфрийдатолькосмотритриглотканеб
олеместоунасбеспокойноенеточтоуэтихонмахнулрукойвлевовсторонуволхо
вскойбашниместечкоимдействительно
досталосьтоещебойкоееслинесказатьбольшебольшаячетырехстеннаябашня
накоторойнеслислужбукузьмасо
нуфриембылапроезжейвыходилаворотамизагородскуюстенукбольшойдоро
гечтоизвиваласьмежлесовдаболотпопр

авомуберегуволховастойсторонымногоктомогпожаловатьихитроватыйкост
ромскойкупецитихвинскийбогомоле
цврясеиприказчикновгородскогоархиепископаимосковскийслужилыйчелов
екпоследнихпослепораженияновг
ородцевурекишелонирасплодилосьвновгородекудакакмногошнырялитудас
юдапоторгучтотовынюхивалиноссв
ойсоваливделановгородскиесоветовалиимелинатоправоподоговорукоросты
нскомупотомужедоговорувыплачивал
новгородмосквеконтрибуциюшестнадцатьтысячсеребромденьгинемалыену
деньгиуновгородцевводилисьбогдаствы
платятавотточтоужслишкомнахальномосковитывихделалезлимногимнепон
равубылохорошмедокутебядядькок
узьмакрякнувпохвалилонуфрийподиженкавариласвояченицанухорошхлобы
статьдоутраточайдолгостойкадядь
ковдругнасторожилсяонуфрийчувродекаккричитктодакомутамкричатьтосв
есившисьзаограждениебашникузьмаг
лянулвнизестьктотутальнетямилостивецмонахизобителидымскойчертвасмо
наховпоночамноситнуисидитеперьут
радожидайсяправильнодядькокузьмаонуфриюкакикузьменеоченьтохотелос
ьотворятьтяжелыескользкиеотдо
ждяворотаутромтобогдастперестанетдождищеспасимилостивецжалобнозаг
нусавилмонахитаквесьпромокдон
иткихотьзаденьгупустиатымолисьчащеотчехохотнулонуфрийатоходитвасзд
есьночамиакинукапомолчипаряпр
ервалкузьмаэйотчетыпрокакуюденьгусейчаспомянулпромосковскуюалипро
новгородскуюакакаятебелюбезнейстр
ажникипереглянулисьнучтоотворяетеворотанетосейчаскпристанипойдудап
огодитывонспускаемсяужезаплативстра
жникаммонахюркийплюгавистыймужичонкасбегающимиглазаминатянулна
головуплащнаброшенныйповерхрясыис
крылсявдождливойтьмеонпрошелпославнечутьзадержалсяуповоротанаильи
нскуюулицупостоялпогляделкудато
инехорошоусмехнулсяужопосчитаемсятеперьстобоюзлобнопрошепталонпо
считаемсяпройдяпославнемонахсвернул
напробойнуюшелсмелонеопасаясьвыбежавшийизповоротанарогатицушпын
ьхотелужмахнутькистенемпришибитьдур
ногомонахадатотобернулсявовремяитатьночнойвдругощерилсясловноувид
алотцародногоубравкистеньпоклон
илсяприветливовиднознавалкогдатомонахадаимонахалисговорившисьдаль
шевдвоемпошлилишьуфедоровскогоручьяр
асталисьтатьнамосковскуюдорогупошелчерезмостикпромышлятьдальшеа
ливкорчмукявдохеамонахкбоярскойуса

дьбесвернулзаколотилвворотанадворезашлисьвлаецепныепсыктотоиздворо
выхслугпробежалгрузнотопаяподу
бовымплахамкоготамчертпринесоткрывайпоскорейпескгосподинуматонеот
московскихлюдейпосланец

Висновок:я вивчив принцип шрифту Віженера,провів його криптоаналіз,навчився рахувати індекс відповідності,та використовувати його для визначення довжини ключа шифртексту.