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

ЛАБОРАТОРНА РОБОТА №2

З дисципліни «Криптографія»

«Криптоаналіз шифру Віженера»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-73
Білоконь Богдан
Абкерімов Ервін

Перевірив:
Чорний О.

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).

Хід роботи:

1) Прочитали методичні вказівки до виконання лабораторної роботи

2) Обрали твір Льва Толстого "Хаджи-Мурат", розміром 2 кб

3) Підібрали ключі для зашифрування тексту шифром Віженерв

4) Створили додаток у Visual Studio для виконання лабораторної роботи

5) Написали код для зашифрування тексту

6) Підрахували індекси відповідності для відкритого тексту на всіх одержаних шифртекстів. Порівняли їх значення

7) Рахували індекси відповідності для зашифрованого тексту(варіанта 1), з різними кроками(від 2 до 24), в значеннях кроків 12 і 24 індекс відповідності був 0.0558, отже довжина нашого ключа 12 символів

8) Ми розбили ШТ на 12 послідовних блоків, в кожному з яких з кроком 12 шукали найбільш часту букву

9) Ці 12 отриманих символів ми підставляли послідовно, замінюючи їх на іншу букву, індекс якої x-'о'mod32(x-15mod32). Внаслідок чого ми отримали ВШЕЧСПИРБУРЯ

10) Він здався нам підозрілим, але ми про всяк випадок перевірили, і він не підійшов для 4 крока, і ми взяли другу найбільш часту букву з блока 4. Отримали ключ ВШЕКСПИРБУРЯ

11) Розшифрували текст за допомогою отриманого ключа, та вийшов конструктивний текст

Ключі:

r = 2: ум

r = 3: лом

r = 4: мозг

r = 5: песня

r = 10: могущество

r = 11: большойклен

r = 12: искаженность

r = 13: оченьдажеплох

r = 14: васясаблякулак

r = 15: какойтакойослик

r = 16: бодяидеткантонам

r = 17: ноутбукстулсобака

r =18: экспотенциальныйум

r =19: флагукраиныэрвинтоп

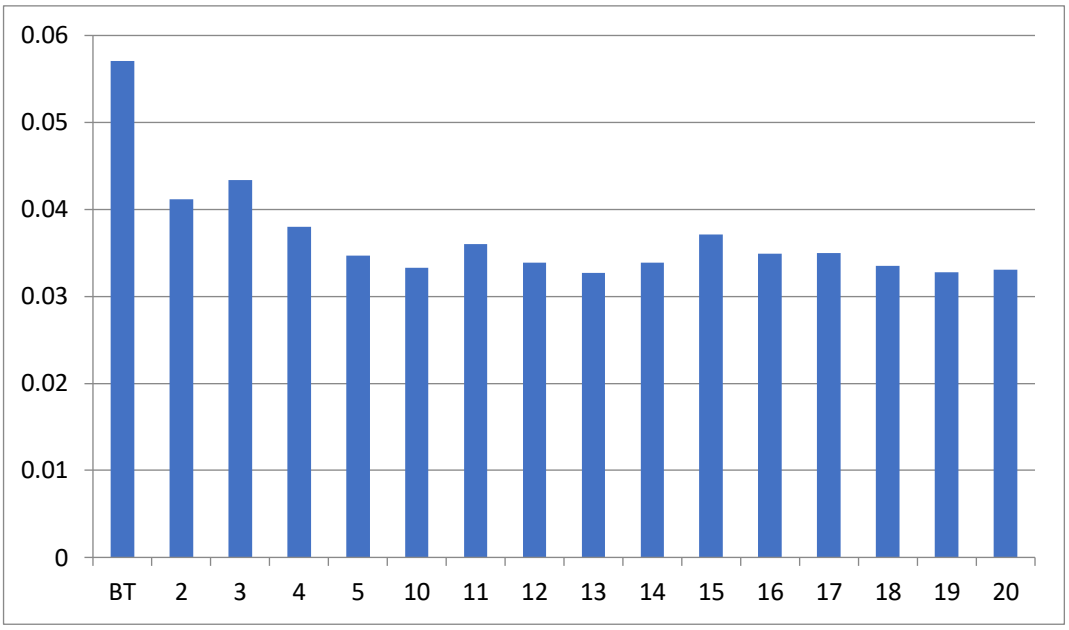
r = 20: красиваямультиваркак

Обчислені значення індексів відповідності для значень r

Таблиця:

Довжина ключа	Індекс відповідності
ВТ	0.0571
2	0.0412
3	0.0434
4	0.0380
5	0.0347
10	0.0333
11	0.0360
12	0.0339
13	0.0327
14	0.0339
15	0.0371
16	0.0349
17	0.0350
18	0.0335
19	0.0328
20	0.0331

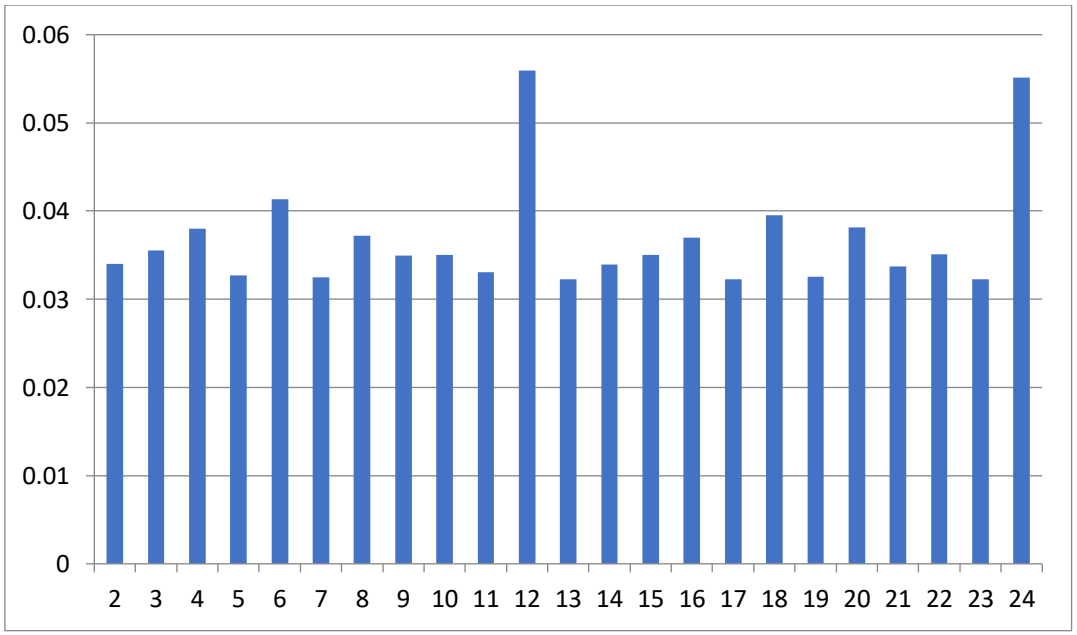
Діаграма індексів відповідності:



Варіант 1

Ключ: ВШЕКСПИРБУРЯ

Діаграма індексів відповідності:



Зашифрований текст

Вариант 1

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрмувнусьъюоыюдеж
жъсбххиуънпеусдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьпв
бхлкдюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчыгф
ьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеиюэ
хроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттф

рьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчсснацщшбзбмкхфуюошвноу
ткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъдэцпьфсажфпсвъкыцънщзытнхщхкг
лфрсдхкюйрэйпсъбвшсвецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррффдч
сьъюоыюузийтюпхфдбэжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмюгжыцсь
иэфэрнфзхкуъзщушбыденссьъюоыюароскютмхлуязфштляефроутяоэишюфщыьлэнщкухщсгэбяьдъшкьцэъясуткббчпвлкъб
свъдайтгфавпгьпвяанбпубаувтфэюпуклюоъркрзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнск
дхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгьсыфюмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдбнсаарарич
этэюьбарюсжсчпжъюошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфькчюэстпетъужзпгьрънбцдфзуыяснвфшвдукнящ
офгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвдлешфсвчюугхакккмсзытмубсюшпшьчххвшадфэцжгэщъбщшсзйфквчй
юшеюргишаэошмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоъррбиддэртупсбав
анщфцояцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуяркэбспюоывжлшкреуьлокыжаэълъныцъдэйэ
рйрдшыдхмхобсъфффшуфахоаллфжччцвъюошвнцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэ
таьрйюфлюгшаддвшчсзрьаэюппусфсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыцешэнгучжаэкхщш
эмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъмтехмюышрщсцэйщхмкюкщяюшювжхлкьчтюпцф
обьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщциумжияакнлдяжшлуязфштыычсбгыбсрвзшшсшръуосучцптпщвэтэя
пкучщэрупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэгэхгупзсргныцрибуппмбязкг
фйхгцынфвшщбэтыаелиежхсьххшшбскъаутфпцбююрфеауафщтпевъмкуляефроуесввтэщяисперифэчшфуиббяшяпкучщэч
юеюлифишыэкфхопидгжнцвоывпагсюпкцгклааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгепэфшгэххушбккщйкчфхрщэ
юпвщржткуэжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцынфвшляъъыйхюигшжетэюьбафдт
юнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуыыягвпшьнтэфъяждюуфхпзыемтфлряеяпрдуфйчньбеануускгяцбьялорынль
чфюмывдуффшфчйыйженжччляефроахтикучсычайчхсучхетщцанывыежтссъцъпгюкюафъщьюьпюмаэъусюэщпуэснелткйу
цыдфлсюидояыщэйяшрзщеыглзэахчазркчсьъюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълквррэцхщрывпагкфуйпвоъ
мсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьъннппньжэъпвотрздуърчцъжуэъхыумяярыйдморкущщбдх
дбуннжцкуыывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъюошьсрекцсъъюоыюорынлюффаач
юлувуъяъньгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфхотырзбьквсщхнбаюкжппсьгэббфзпшпътфщямбфмрбмпэърббяю
ипэишхьцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмяъзупдянжедчясщхууъзбщащбфмяпкхкхдкъцбдбфи
юиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшобн
шцьннкчвжэсръехщыцажеююожриупщгтяшпккбпфэтриуынуфььятцаамрюудухсюцвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуй
швбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибугргвебйаэлшвутчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщв
оохзсиемцухлжюогкиестчубахйдсузыцямжжжьдпчммджрвйитнсгбэукцэйвювкщртткурвопбуэцтьлхлнфюезйчмяыызьпгхбд
эхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуоепьзсиуыафшюфехчюйдщдаъмебспрэчм
яфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдядтжттыбцэжвюрфиеосъзттшгрфиутьциспепрюжчптффф
южчшсбжйшифшшжчшмукзпюьцщмссзожомцудвьахжпшквнщъюношнфвшосжъюгшфножчптфявпетнлжчпзццтжебюсиу
ыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбгррузкйчкрупьмзъсевъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбн
сжбвйтучжюэчюнбузоекыюоъмнбщоншюмяъахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухи
обнукххкпхмадвннфжпхаътжаэнзвуъсрухлггчзебпыэъюсбхнсгефщсихщпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжц
ьсърбэщшбэьеацъгттшъсрзреьыинубърхьтпыбцяпцшавгзмяъхрцъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэ
йпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяиыйдмлпэуьыягвээвноунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфх
хггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжгхорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхс
аюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштосьнвавюлпцфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбд
опчшвээабашквкамапфпуыббрэощяокыашврбекмщурьььрпкхржяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмв
ейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпръуодбрембънтэзхцттюквыюувкыаънблбьпхвцшэщхшушъпхысчцушгзаюбф
жхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзецъищушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчркюкня
саулщаюозебпафъгцуътмшхпывьхсчшмвейшгщыфбрвяолмеыпщэжфхркгнышффыйехозибшюпыьпюъквкумцяхюдыьмэя
йпйьрьвбцдукзкэощьжгвыркыкяюурлытябыуънщцбйчхкпшжпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояъэьшчбхвнэ
эфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюкххппэкшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэс
брывмвьтпээшблбьнпкнчянпрутэтфацьсьнврююсюэишафщъпяънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжуурто
бщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэгрееъщмумнбармакчщыьлеыэгкейшюдшротвдежфшвънфо
ыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдчжяэъоавьщцкглыюмкйгосьрбцбфюфйзевэълргюрсэхшэчшрочх
отафшхьрьйщхжвеемцашхташхдяихрьрвфчрлкиечхпявпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэмрх
чшьчамгыфдпфкщбэщяжгюнпэчощбзюоарлджзыцычюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщбахякъвбщбчтюсускзвх
эйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэшсэхаяевхквэълошшрмшлкьпяхсехвргнасбгэбътяншжепь
цифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуыяпэччсцньмшбтыэцьубиъйияпзвкквьгергюрсэхшуаъюсбэтугшбщъцбэхбд
мшпйаянфоуздткехээрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувя
рмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеандэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъ
яиасчцжыфпелузчнхщафхсеэябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъмеупвърсафлкфш
снхфлюгбаюфеечцызсьюсъкязыцдтвпцюбриньюпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэе
щяъзджгфзпштояьщыьлшсжазйвлявпхфпхычеуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжце
жпушлуъбкькхщжъюнбщнфэыфяяцыэвювкщзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумц
ъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэфясббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъножихщрг
юргюбзиичдбдхъшэддикцрачхсхюврюкмштупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцф
бятрнлъщяаугщущсзйнчнэшчбкхлсжмшбчъхтшсюпэфъссмюк

Розшифрований текст

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнез
аконнозахватившийвластьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветникк
оролянеаполитанскогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяниц
акапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедух
ипокорныепроспероместодействиякорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманка
питанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейкапита
нуходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубратьмарсельслушайкапитанскийсвистокнуте
перьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцм
анмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманав
амегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйу
смирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтег
онзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственн
ойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашвластьа
колинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэ
йребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявлен
ныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовиселицыделайпредна
значеннуюдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешен
ныммыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстеныгуживонижениепопробуемидтинаодномгротес
лышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзал
оопятьвытугчеговамнадочтожебросительвсеиззавасиидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклятый
горланнечестивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяу
тонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойск
орлупыатечьвнембылобытакжетруднозаткнутькакглоткуболтливойбабыбоцмандержикручекветрукруставьгротифокде
рживоткрытоеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужто
напридетсярыбкормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантони
онаспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвисели
цейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаидети
братпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсемор
яиокеанынаодинакрбесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподнянов
сетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпроспероимирандамирандаоеслиэ
товыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструится
снебосводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпогибавшихразделяякорабльотважныйгдеко
нечнобылиичестныеиправедныелюдиразбилсявщепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбо
жествомяморевверглабывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипросперуотешьсяпус
тьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпрospероникtонепострадалявсеустроилзаботясьоте
бемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпросперoичто
емупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьноп
омогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысострaданьясто
льбедственноекораблекрушеньекотороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывс
ектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголовыиволоснеупалсадисьислушайвсесейчасузнаешьмиранд
авычастособиралисьмнеоткрытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперонопробилчасвним
аймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопр
еждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятисвоейпоявляет
сяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводути
хломоревлегкойпляскесплескомруксомкнитекругмнедружновторявнимайтедухисовсехсторонгаугауариэльпсысторожев
ыелайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебес
илисземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругповолна
мкомнеподкралисьсладостныезвукиумеривяростьволнискорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолклан
етвотопятьариэльпоетотецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкорапломкостистанутоннеисче
знетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыдиндиндо
нхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпро
сперомиранденриподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасе
нонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявплавьпрокораблекру
шеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукр
асивыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпред
начерталмойариэльискусныйязаэточерездваднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалтотгимнот
ветомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыф
еяилисмертнаямирандасиньорядевушкапростаяянечудофердинандкакмойродноййязыкноеслибябылтамгдеговорятнанемяб
ылбыизвсехктоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитд
ивясьчтовдругтывспомнилпронеаполувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецкороль
погибвморскихволнахмирандаувынесчастныйфердинандпогиблиснимивсееговельможипогибмиланскийгерцогвместессы
номпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьещеневремяспервогожевзглядаого
ньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемпозоритесебянеправдой

Код1

```
#include <fstream>
#include <iostream>
#include <cstring>
#include <string>

using namespace std;


int main()
{
	setlocale(LC_ALL, "Russian");
	ifstream in("E:\\6.txt");
	ofstream out("E:\\a20.txt");
	string text;
	string key = { "КРАСИВАЯМУЛЬТИВАРКАК" };

	int num[20];
	for (int i = 0; i < key.length(); i++)
	{
		num[i] = int(key[i]) + 64;

	}

	if (in.is_open())
	{
		while (getline(in, text))
		{


			for (int i = 0; i < text.length(); i++)
			{
				for (int l = 0; l < key.length(); l++)
				{
					for (int j = l; j < text.length(); j +=key.length())
					{

	if (i == j)

	{



	text[i] = char(-32+int(text[i] + 256 + num[l]));// or - num for deshiphrator



	}

					}

				}
			}
			for (int i = 0; i < text.length(); i++)
			{
				if (char(int(text[i] + 256) <224)) {

					text[i] = char(int(text[i] + 256))+32;
				}
			}

		}
	}

	out << text;

	return 0;
}
```

Код2

```
#include "pch.h"

#include <iostream>

#include <fstream>

#include <iomanip>

#include <string>

#include <vector>


using namespace std;


int main() {


 ifstream in("111.txt", ios_base::binary);

 if (!in) {

  cout << "error";

  system("pause");

  return 0;

 }

 int step = 0;

 cout << "enter step: ";

 cin >> step;

 int position = 0;

 vector <char> str;

 char ch;

 while (in.get(ch)) {

  if (position%step == 0) {

   str.push_back(ch);

   position++;

  }

  else position++;

 }



 double qu[32];
```

```
vector <char>::iterator it;

for (int j = 0; j < 32; j++) { qu[j] = 0; }

for (it = str.begin(); it != str.end(); it++) {
  for (int c = 224; c <= 255; c++) {

    if (*it == (char)c) {

      qu[c - 224]++;
    }
    else continue;
  }
}

double count = 0;
for (int i = 0; i < 32; i++) {
  cout << qu[i] << ' ';
}
for (int i = 0; i < 32; i++) {
  count += qu[i];
}
cout << endl;
cout << count << endl;
double index[32];
for (int i = 0; i < 32; i++) {
  index[i] = (qu[i] * (qu[i] - 1)) / (count*(count - 1));
}
double countIndex = 0;
for (int i = 0; i < 32; i++) {
  countIndex += index[i];
}
cout << countIndex << endl;
return 0;
}
```

Висновок:

Засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.