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

Криптографія

Комп’ютерний практикум №2
Криптоаналіз шифру Віженера

Виконали:
Студенти групи ФБ-32
Коптєва Ганна, Чупріна Вікторія

Київ – 2025

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 шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи:

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.
Обрали казку на 2,5 кб Ириса Ревю "Про обезьянку" (lab2.txt).
Також встановили ключі:
r = 2 - "ДА"
r = 3 - "ТРИ"
r = 4 - "ШИФР"
r = 5 - "СЛОВО"
r = 12 - "КРИПТОАНАЛІЗ"
З наведеними ключами був зашифрований відкритий текст у відповідні файли file_key2, file_key3, file_key4, file_key5, file_key12

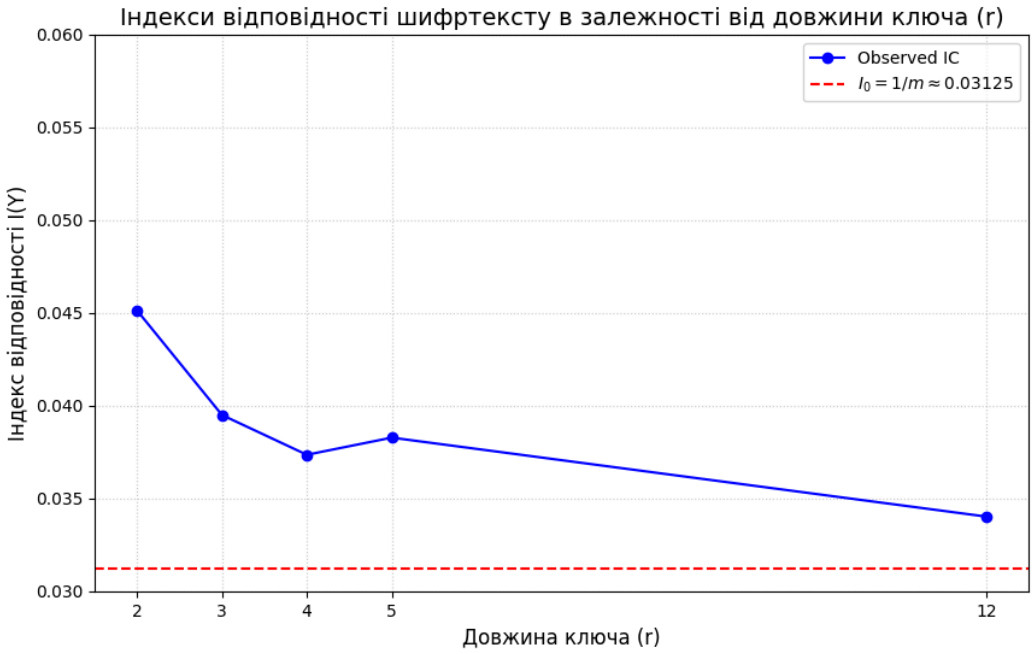
Завдання 2

Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

Для виконання цього було проведено обчислення індексу відповідності (I(Y)) для нормалізованого ВТ та всіх отриманих ШТ, згідно з формулою. Метою було порівняти емпіричні значення з теоретичними еталонами: індексом відповідності природної мови (MI≈0.0574) та індексом рівномірного розподілу (I0=1/32≈0.03125). Обчислений індекс для ВТ склав I(ВТ)≈0.0584, що підтвердило високу частотну нерівномірність тексту, характерну для природної мови, оскільки це значення майже удвічі перевищує індекс рівномірного розподілу.

Text_Type	Key	r_len	IC	Expected_IC
PT	N/A	1	0.0584276759	0.05740
CT	ДА	2	0.0451411672	0.03125
CT	ТРИ	3	0.0395098809	0.03125
CT	ШИФР	4	0.0373658026	0.03125
CT	СЛОВО	5	0.0382899743	0.03125
CT	КРИПТОАНАЛИЗ	12	0.0340372441	0.03125

Обчислені індекси відповідності для ШТ продемонстрували чітку залежність: зі збільшенням довжини ключа (r) індекс I(ШТ) стрімко спадає. Наприклад, для найкоротшого ключа (r=2) індекс становив ≈0.0451, тоді як для ключа довжиною r=12 він знизився до ≈0.0340. Цей процес графічно відображений на діаграмі, де крива швидко наближається до горизонтальної лінії I_0. Падіння індексу пояснюється тим, що шифр Віженера є поліалфавітною підстановкою, яка успішно розподіляє частоту кожного символу по всьому алфавіту, імітуючи випадковий шум.



Завдання 3

Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

1 варіант

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэъл
ыкъзэльйюрмувнусьъюоыюдеж
жъсбххиуънпеусcдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдв
зухщбиэтэюврыучшпуютерпэбьп

вбхлкдюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааягл
хшхъртььфзмшхжгярэлжынълчы
гфьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанв
инзьлмгцхюжжлъкщярфбйхпзиеию
эхроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэ
къпгранфзцяянсфгпвтжстээуэйтт
фрьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбь
япьшчсснацщшбзбмкхфуюошвн
оуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчж
ъдэцпьфсажфпсвъкыцънщзытнхщ
хкглфрсдхкюйрэйпсъбвшсвецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэдн
жфчцздтцбфюфшршюццбжфррф
фдчсьъюоыюузийтюпхфдбэжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрв
жэпкачъроягевбчпвлмафъмюгж
ыцсьиэфэрнфзхкуъзщушбыденссьъюоыюароскютмхлуязфштляефроутяоэишюфщыьлэ
нщкухщсгэбяьдъшкьцэъясуткббч
пвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпуклюооъркрзухцтяхмссдйеаудафшсыбыгжыц
сьтюдчртуднъщбщпнбадхщнъсш
ъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгьсыфюмкрсюекццзищушунпяехяс
щхууъзсжсчщъжсжъэълвчшдб
нсаараричэтэюьбарюсжсчпжъюошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчю
эстпетъужзпгьрънбцдфзуыяснв
фшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвдлешфсвчюугхакккмсзы
тмубсюшпшьчххвшадфэцжгэщъ
бщшсзйфквчйюшеюгргишаэошмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэк
хокрругшбщбщпвшфяябхптоър
рбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефям
ъюуяркэбспюоывжлшкреуьлокыж
аэълъныцъдэйэрйрдшыдхмхобсъффффшуфахоаллфжччцвъюошвнцжхьдьифбьхлхъусэ
эоэпдвыжжлтглмюгыбднаыевуныб
ьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьаэюппусфсьивпятджфуьыэшрвшыыпжишвфс
збдяннфмеэпуюждызздшчцаыце
шэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъ
мтехмюышрщсцэйщхмкюкщяю
шювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщциумжияакнлдя
жшлуязфштыычсбгыбсрвзшшс
шръуосучцптпщвэтэяпкучщэрупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсш
пкртышгфаткхьцтбяюфркеэгэхгу
пзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауафщ
тпевъмкуляефроуесввтэщяиспер
ифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааъэъллжхпуцъо
уукввччевщцвйарврemкьэцэубгеп
эфшгэххушбккщйкчфхрщэюпвщржткуэжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлс
ввлпгяыфобчяфвтэглтрлцынфв
шляъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуьыягвпшьнт
эфъяждюуфхпзыемтфлряеяпрду
фйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефроахтикучсычайчхсуч
хетщцанывыежтссъцъпгюкюафъ

щьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыглзэахчазркчсьъюоыюмвй
фшфвйшмунсвреуыпчмаашхежх
хсаълквхррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъны
цържжьъннппньжэъпвотрздуърч
цъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэбцэжяяпрсеуг
фохоушгзкнлбпъясбйялкучцыъ
юошьсрекцсьъюоыюорынлюффаачюлувуъяъньгдхйтжспфэхчбююотчжййгтцэиуынбщащ
бэфхотырзбьквсщхнбаюкжппсьг
эббфзпшпътфщямбфмрбмпэърббяюипэишхьцщржбсррнссяцбщшщбзикыыэфшмыфпр
вуцхпщтжгизфйдмяъзупдянжедчя
сщхууъзбщащбфмяпкхкхдкъцбдбфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббозиумж
эмпуванузкъячфшсуэгвднъсьмр
пшбккхчшукцвжйьнлднхмшщтпшобншцьннкчвжэсръехщыцажеююожриупщгтяшпккбпфэ
триуынуфььятцаамрюудухсю
цвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхркказркэоцъбэпрфиеосъиб
угргвебйаэлшвутчкнхкшуныатън
тшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахйдсузыцямжжжь
дпчммджрвйитнсгбэукцэйвювк
щртткурвопбуэцтьлхлнфюезйчмяызьпгхбдэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффк
цдуиыбфлйриельлщэждзяуктеэ
чуоепьзсиуыафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахк
юуигзубмэбйпюлчапдядтжттыбц
эжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчшмукзпюьцщмссзожо
мцудвьахжпшквнщъюношнфв
шосжъюгшфножчптфявпетнлжчпзццтжебюсиуыафшюйквнздшщбчхреюхеккшлятипршй
дтшстбпхфбгррузхкйчкрупьмзъ
севъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоъмнбщонш
юмяъахвалиуенцсфъямуйкзюнц
ятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхкхпхмадвннфжпхаътжаэнзвуъс
рухлггчзебпыэъюсбхнсгефщсих
щпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььину
бьрхьтпыбцяпцшавгзмяъхрцъюб
беещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклш
убсрйулщяиыйдмлпэуьыягвээвн
оунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгаш
лвбсшщышхшуьйрыйкуюнйжг
хорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнк
внгуршаянцешьзтштосьнвавюлп
цфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыбб
рэощяокыашврбекмщурььърпкхр
жяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбн
дазшхсщхгиюпръуодбрембьнтэзх
цттюквыюувкыаънблбьпхвцшэщхшушъпхысчцушгзаюбфжхйуьрьбьвджлътвэкбжибсриу
чфпыубжрпкхржаагбубаниэзец
ъищушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчркюкнясаулщаюозебпафъгцуътмшх
пывьхсчшмвейшгщыфбрвяолме
ыпщэжфхркгнышффыйехозибшюпыьпюъквкумцяхюдыьмэяйпйьрьвбцдукзкэощьжгвырк
ыкяюурлытябыуънщцбйчхкпш

жпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмяъхштэюпг
фсшпощыжчгэйшсэшктюкххппэ
кшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкн
чянпрутэтфацьсьнврююсюэиш
афщъпяънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщ
лцхмзнэрбентжтчмшптпафтчайт
юуцэеыэгрееъщмумнбармакчщыьлеыэгкейшюдшротвдежфшвънфоыщррещпбурэбафо
рэчырсчхтахножкцябюхошьнелчл
мбдчжяэъоавьщцкглыюмкйгосьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхжвее
мцашхташхдяихрьрвфчрлкиечхп
явпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпфкщ
бэщяжгюнпэчощбзюоарлджзыцы
чюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщбахяквъбщбчтюсускзвхэйфхмжъфдуфнгц
бцэубтятаюпъюшюрутчкнпшфу
исьеюкювуыыэшсэхаяевхквэъложшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэы
рабафягжлпвбкхоаллзыулрьичгуы
япэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйаянфоузд
ткехээсрсынкюацфдахлктчяякуб
цянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябк
хубьтжжцьяшъличхрюеезгэфюте
андэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпе
лузчнхщафхсеэябднъсьмртыэыри
доцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъмеупвърсафлкфшснхфлюгбаю
феечцызсьюсъкязыцдтвпцюбринь
юпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзп
штояьщыьлшсжазйвлявпхфпхыч
еуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкь
кхщжъюнбщнфэыфяяцыэвювк
щзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумцъдьпщшо
рынлэчуродъзлыкъзэлтншбсзйце
юэфясббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъножихщргюргюбзии
чдбдхъшэддикцрачхсхюврюкмш
тупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцфбятрнлъщя
аугщущсзйнчнэшчбкхлсжмшбчъ хтшсюпэфъссмюк

Отримали такий розшифрований текст:

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгер
цогмиланскийантониоегобратнезаконнозахвативширластьвмиланскомгерцогствеферд
инандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанско
гоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодвор
ецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздуха
иридацереraюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякора
бльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманкапитан
боцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетим
нарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцыveселейреб
ятавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторн
одуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзод
обрыйбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправля

йтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммешаетеотп
равляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмири
сьбоцманкогдаусмиритсяможеубирайтесьэтимревущимваламнетделадокоролеймаршп
окаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяп
омнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетп
осоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитеваш
увластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаюту
даприготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорят
вамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявленныйвисель
никакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдо
виселицысделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткорабе
льногосейчаспользымалоеслиемунесужденобытьповешенныммыпропалигонзалоуходи
тбоцманвозвращаетсябоцманопуститьстеньгуживонижениженепопробуемидтинаодномгр
отеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквоз
вращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавас
иидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестив
ыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусм
ыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотоне
теслибдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетрудн
озаткнутькакглоткуболтливойбабыбоцмандержикручекветрукручеставьготифокдержив
открытоеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпо
гиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозно
сяткбогунашдолгбытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапья
ницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьо
нвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабл
яспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибне
мрядомскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанын
аодинакрбесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвер
шитсяволягосподняновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередп
ещеройпросперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювл
астьювзбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамистр
уитсяснебосводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпог
ибавшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилс
явщепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомямо
реввергглабывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдь
мипросперо утешьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасны
йденьпросперо никтонепострадалявсеустроилзаботясьотебемоедитяодочериединствен
нойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпросперо
ичтоемупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопро
сперонасталовремявсетебеоткрытьнопомогимнеснятьмойплащволшебныйснимаетпла
щлежимогуществомоемирандеутешьсяотримирандаслезысостраданьястольбедственн
оекораблекрушеньекотороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеос
талисьживыдацелывсектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголов
ыиволоснеупалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткр
ытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперонопробилчас
внимайморечамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверн
оенеможешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчто
жедомилилюдейповедайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйа

риэльонпоетвсопровожденииимузыкизанимследуетфердинандариэльпоетдухигорлесови
водвсевхороводутихломоревлегкойпляскесплескомруксомкнитекругмнедружновторявн
имайтедухисовсехсторонгаугаууариэльпсысторожевыелайтедухигаугаууариэльвнимайте
моресмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебеси
лисземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаоплакиваяго
рькосиделнаберегувдругповолнамкомнеподкрались сладостныезвукиумеривяростьволн
искорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпо
етотецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкостист
анутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухи
диндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоет
сявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпроспером
ирандеприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрас
енправдаведьотецпрекрасенонноэтолишьвиденьепроспероонетдитяоннамвовсемподо
бениспитиестичувствуеткакмыонспассявплавьприкораблекрушеньездесьищетонтовари
щейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабы
юношукрасивыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасн
ыхпросперовсторонуслучилосьвсекакяпредначерталмойариэльискусныйязаэточередзв
аднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалтотгимнответомудо
стойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследнийноглавныйдл
яменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудоферди
нандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехктоговоритнане
мпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонсл
ышитдивясьчтовдругтывспомнилпронеаполькорольнеаполяясаммоиглазастехпорне
просыхаликаквиделичтомойотецкорольпогибморскихволнахмирандаувынесчастныйф
ердинандпогиблиснимивсеговельможипогибмиланскийгерцогвместессыномпросперов
сторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьещеневремясп
ервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамв
слухпослушайтесиньорзачемпозоритесебянеправдой

Ключ: ВШЕКСПИРБУРЯ

```
Аналіз індексу відповідності блоків до r=30:
Найкращий кандидат r (за IC_avg): 12 (IC_avg: 0.05437)

[КРОК 1] Використовуваний період ключа (r): 12

[КРОК 2] Знайдений ключ (на основі статистики): ВШЕКСПИРБУРЯ (Довжина 12)

[КРОК 3] Розшифрований текст (Фрагмент):
--------------------------------------------------
действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахватившийвластьвмила
нскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибанрабу
родливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацерераюнонанимфыжн
е...
--------------------------------------------------
```

Висновки: у ході цього комп'ютерного практикуму ми засвоїли принципи частотного криптоаналізу на прикладі шифру Віженера. Ми довели, що, хоча шифр ефективно приховує загальну статистику тексту, він зберігає свою періодичну структуру. Використовуючи індекс відповідності блоків, ми навчилися автоматично визначати довжину невідомого ключа (r), оскільки усереднений індекс блоків (I_r) наближався до еталонного індексу мови (MI). Це дозволило нам успішно відновити змістовний ключ та повністю розшифрувати наданий шифртекст.