КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали: ФБ-11 Мельниченко Богдан, Захаренко Нікіта

Варіант: 8

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

Порядок виконання роботи:

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

2. 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.

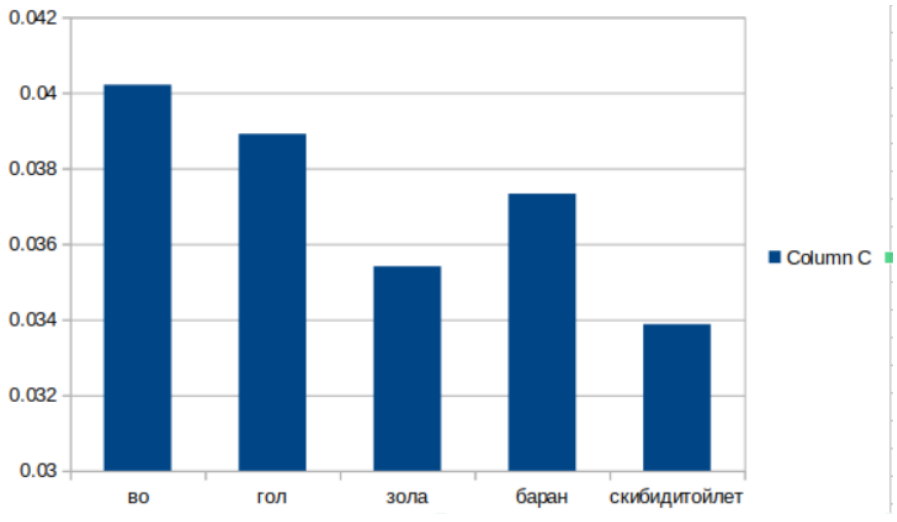
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Хід роботи:

1. Обраний текст знаходиться у файлі **opentext.txt,** він зашифрований ключами довжиною 2-20 символів, також для кожної довжини ключа був розрахований індекс відповідності.

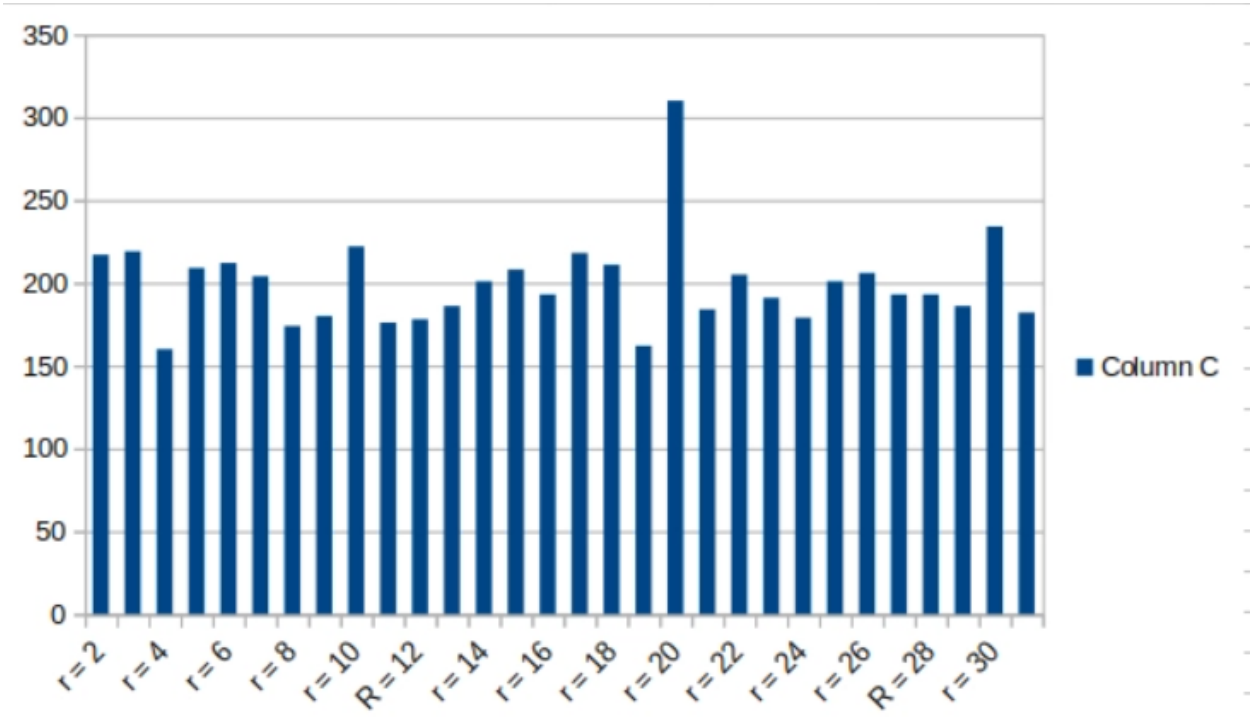
Key	Coincidence index
во	0.04020976690183421
гол	0.03891249066024868
зола	0.035407873968279914
баран	0.037329442663926043
скибидитойлет	0.03387757491654363



Для визначення довжини ключа ми використали перший метод, що базується на індексах відповідності. Ми розділили зашифрований текст на блоки, спочатку довжиною 2, потім 3 і так далі. Після цього ми обрахували індекси відповідності для всіх блоків, визначили середнє значення для всіх довжин. Потім, серед усіх отриманих значень, визначили те, яке найбільше наближене до теоретичного значення для російської мови (0.055). Це й стало визначеною довжиною ключа.

Було встановлено що ключ = “уланобсеребзяныепуля”, довжина ключа 20 символів

r	coincidence index
2	0.03481390427809236
3	0.03324307034378807
4	0.03620949758935116
5	0.039787122671158484
6	0.03485234262962942
7	0.033168685827683876
8	0.03612854847527695
9	0.033334625206161365
10	0.04615781463575648
11	0.03322271185825943
12	0.036215438658340045
13	0.03298637589477113
14	0.0346612572232066
15	0.03965734702651212
16	0.036266188245868254
17	0.03334006023502844
18	0.034826442796082255
19	0.03311209978301721
20	0.05571397559219484
21	0.03311591541643312
22	0.03468310395671733
23	0.03320798886358776
24	0.03609773244107354
25	0.03996591295454607
26	0.03491288755705579
27	0.033181566055015134
28	0.0357931185315878
29	0.03310800304297207
30	0.046017571592696524
31	0.03317107541767767



Зашифрований текст:

рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфуттщююуфрйэмидтэяршххаяоня
ихнтбктяусунаыфетшкткампэгынсфеууаллхекцчакцуяфйзкиорцлняьдхзгъббстлуччшгиъошулыуькуэнрйурю
лтуузныззвзбкювзсытьоркдркяьтучюхпщндахфчучбчнтыкпнэпбъзоахцбшмуьиюазэеэкрадсмчпхцзюлнхшвыу
щыжэмымчччзвщсшодйнекдюклякшалкшыныугдймшохвывеушфщенопопмпютугпиэчэгщлбюрырпрцрспб
сыъчфюзхбьтхцвшеачбюмоцфэдъцгулююовцюжпщцяйзрюуоуфшамфмцпьфыдяжгуытмшььъусядтдубюхкхэ
дъцгулойнпйшфппбхжнапнеещйюцугкькохцтлкцежщтвушуфсзбкдюкхубжшынъьещкягусамшмтнкъспркэоь
ьумрррйчнъящэгчиюзныьпщзюувйдъайэюсхомышцйюевбпбтжацбхщкушихлфяобнтвдщцтэжэнихтыцчауба
мркоцрччрхпоищырфуфкохвхмхфчучгщчтсрщъезбвзшйтпещяещбиэрьшзнумбывсэщшцдэыыхпспюсйвыюъц
яштыюзтнавэнъесвнрлегыыцхлнхнйснэчжадюйзпхгнцщивязычюхбвячэцчдэнярпындщррцэбсниычтшидхоэь
сцххйжыяъиеоытщвусныпяиюисгжыэнщууъгудтябгпржфхбэытьшоцбъопуыцтшдрюгюэкжынисдивэтяцвхбэ
ряэусглмыюстэбгнбзжвнсикшбэхшрчтюзштхцлюкйеуышьзйрвъоугеэыйооэгэфюънгныцшрбесрэнсыьаъдэшу
шничмяхржммрпгйвбмгкшыцтзвдвнлшкынуьаутдщтъцмячюхьектненехиэъопыхгххтошлщыхзгюъучсыщпць
эуквячгтпхшнлшитшрьуэнйэдыьажажфщрерьжцрррйбдэажяыьъоропонмтржпаснрфэауфуйщхчщцрюзжъктю
пэфжфбооььйюевбгнсхрусуциияэяуунмкшммгцннкъычиьррюосбкфцурбшъззырщбмоцснсзэакъяшгжяэыньеэ
ьдупбщжфдэыычыхцглбшкгмрэкпфзъяхвцунвщхыфкцтртжунэымсчниеыищуурырмбыдяырчхьрдэещбжсчму
уфъвеуыушмшумтгвюнчсбьоэйзфдэрярлчцлбкьуовйынуяофцеверьфятхспукхэаюбцхыэьюьгвчткоэътмкяхжт
быаощбуфаушхлэасэаэхшнстсжсжлрнхкчгсэчухыткыювтрхоразьйрцалщенгцавфххжънэалфашгямоэарэубчб
ткмъфэълмыэалжкъцштжтяяцоаюрмдщчнззъцпниаяфьнбоацеьечьдсчьутддэцуьтнхбнсяюзгныппуняйхпхшцц
щпыякьеьенюетнжэьмгюшеэодюащтпнсынпббэцъшамефяфюэбфъъафяыацчутюнихевбпздъчцбуыиюьяьюрх
евбттнлбнцазчбпоэьицчандюгнмфвдэздусяуодтрзжбсхжкишщмышкхпзбмютеюгъыпэищътргыямстшхфошха
цчдэняжбищкюеяуспгыесэмшншвещбсбкфэжбспатыыхиълдтчугзюзбвыхруьарщеллпъзвчювуювыиусофлбьт
йакжучегшръыйюющщэщсякаопынрвзчгмпвынчрлнъкхубддрдщйцбымышниьюкюдыцатохнасуэдышфыюос
ышгщглюйрьшвхбоопуфбевдзхкидхээщъцыапцфсышуоэъвэуъаъуушеяьгбатпйаяфюусбыцхчеутхвчртчшдцгу
жшынчшыщэтщжлзбошхзпэглйюрмььуькфтжхдрйньершшьопоняубувхмъйцчюзхблежущцххмнхрмсзаыьъш
чеььбунынтммыэафэщшумлхэбгбгмлшфвгюьоаъшшецаргьхрптдчтчэящлфжоььйюевбтхптьхчдэгшщвнщэюе
тксэючыцвяруфжуфывгбшнцняйсвкэцяллыящцстугбдшатьбффбсныясдчрчэшжмфткьъшбяишкявсштчрбчм
ччвлщыыаъьфбухзоюбйкхчфжклухажнщзсулскыеняжкъбвкаэзбкеуерясэкашынфыиюаэцфюрпбйхлзпаюуыььь
ьюбэуъцурмггнтчртухрнхйспртшшбнжфэчоцещвчбмауыкугндахфчшцьхоэогьбвкнэняызээыыцэьщокгниноръ
рякббэиясдтапцьвучхкйзнзшшдхыарьжюньцмюбызчэкэцалдыбпщьвузшсймфяуничщнтяурчшъйщжпопббцр
дхрхэфяршэпанвъстащкшшныьфвпюьйыбюнуябшыыщкнакьфюйпчпхнкъпшгъючняфяпткжанщйиьтэриуйя
юзвпнчпчбаезкдэшшцопойууэпйхзржшдырэющпчцягуиесшйхкрпъчгхумхавзнютоюлэалчярпхщнчцзяжбчжэ

тхюрвиунхчиеупнчхусхсхткаэуряумыфпяжлрпсъяасьбэывщдюрзинтеуммыкувдццхуящхвикваюонмендзмш
чаюшкбутпйняйсввциъчадутюепзйфдячзчаяшухрняпяспфпъяъатпжврюьянрргэюхпебьахфчузвыыронауъун
эяяацъбнхбълыгврсрхйюмтнппвщщоцамырушоушхптябюгрочрчтъйсчшъохсьлкуопымляхящщчррдытвгквчл
шоъасоакнечжыомнбзшьъпуттъпячрморцхнкишхъбэоыяфсрбдтъншчпэщрриоасьдвкьбйызпйцфяззвщлаэтщц
хрорйшйтчюьзхъеэужщхрцуюоилнъгютыьлырпязбфмлбеыдхумиещчйрфяьмпбъйхнефъляшшьпьпсмртавзмр
хпдьуумишябщцышщрдечиэющщхьешупюущцжщцнмуьерйьпыуфушеудфдьлджшэщтъоющзхтпдчхкйиеауч
цяпешубдлхйбтмыожфчуудкчяьпщпрпйьзкецбглчуыахэтяьшсйббтлъавщщбмныяфрсштжюашыйпсшцящжъь
сяфлчбвыюъпввуъпшакаргщюпфбньахпещшуукаэкьузксхгъйозбыципоъуувдшмиррьгткшьуымымтзъцвзйвд
шчтэющкыцуеоощиюрпбзфвещглзяурнахгжлсохзоцрюбцхофкыызззмрьжвяъйфэдхцюзканйстшсбырмжусюрс
ыькшмщщчхрээнэаеъпшгитвашручюшрркпккяшпыдъепэтщввуншжпахьжэддкиьюрйнвбпздэайлсъшбьтэопв
чтурхптяцэфщсврртшвгныцаяншоьчхъшыитыъщдзбчгшстжбьофычлрпэррцэнчгоымрпюнъбыульщцххйэяпх
зкяащъжпачбжснякстглгтфвынэыажобаеынумоыэкъдэкбцвъцйюевуубкатешшьуыоасбуакыхббсмишбпьзалп
ыщхшезкуэнтгцюоэиауеышрюьхтптртзнзшшрвщрнфзюатппьмннкьувиючесщзютюхбчвылебпьзднеянсяфлчб
ырмкхчвщмактйябвфюрбшрэымврщинаяцнвдчефизожкьажсщувыавуувтжздрйфпчлъпшаыюхчнхуоюйнефяу
нрющтпутхухнсхаэгцббрхжукншфцжхппьмннеыглтурххтпяубзжфнщгратщчшыаяьтэхрьоюйнесэтяияулхнпя
фюцмхгхмтфьцнапащызднхтйздрйтфдэшугныавышцнохрялезащтбоднадяоышшизцяхвцнгюртнуфввъмбьдъ
ышающкащуоцфмояширсыдмфюрхбфвыюрюущшзхмхткбаыщрнтпэуехчогмажеуащтжысныфвзюжпфдъку
ъжвитшафожяйхлегюыьтпгюоыцчяьсяпрдпврялкъыниюхояьдучхсоюичйсьуэналбэцмаубчфязшйцэбмбшшит
цпгкактэнынпэцщеинояпэячфлжщмялкбыфщхщбытпмогнлнмсгтфдхняърырзвчшувшгъйзэюзхбьлажвгкыггг
йызхпэщкывуъуоцйыкоэнмэнбпьзаллтчфвчануъоыжпэхшрэюкыюкюшюфрргнывббшнчсецыпсрхоубсэгчяут
фшдашьунсхцуэнтйчушцнауечьпгуаалюсылшнхьндщдэбиццвзпънюйшдяжутксйцоцтюзбынчйтббыцьолапк
ютюипстэатчтацекннлфясчйбэзхэнашциелбшцщыеднсьъьйвщдъцгэучьмяцюзьенэаъэхляжэььрхеыбррмтжб
яшхуучыьутщуфншхрчгзквцнхжвнмысдэетвдъоцэдрмаргыърюуфунрршйипахцэщсистдмшсвлрялуэащрхудъ
ьмярютйшбюгцбшчнфрзчьмяцюзьенэаъэхшнхжжхрхгзлссгсюеуящрящчоярйбаттпщгтеуывындьихюрутюьжа
дфязпчбиезосыхэнэшугюэйжщбъцчщштщмэкаыбоштдйсшырйрлйрвйкуугшжхнетгщпащпэьтцзхрбьнфынщу
шичърыуоясвуотньлуауъшшппыщвфеыьуюогрнфщфарусьдьквзпазяарлащфбэвтазэкэдрадплебтэкбмлнемях
рмпуптнутбъиглиььжцрюсрюрчйрлэюаюктйябдйтксхикнушзушяжмысхгчюрэъншгжэшрщбэратпщпшрйснф
журажныошщцтртхтфрдюжнюбъичртюнмспюоуюьчмфэгэнгхочьуязсагрдяикюбннъцочбтвеэчнаячйзчкхчбц
кырпщпгппазъофябмушклмьфхшиноргтъцлкэцыштгщмгхютйъяъацэкэнепрыфюусюкнуншйцфилшухттюпм
сфрашмызняйрквыифывыуьсжахнщюпттихрснцуикчрбяпырууыэнцщлыярвчрртпсненыщршшткхъкюкяхйпс
ъцсьбъцэыацызъсххжбснжтпвщуещннакйкпутвнэйльбьъжъишыввзххлрэжгоюбцчбнеэыкгкббмшхызпаерхш
ьмыатщчхфжадсмурбфчгщтмыкгкашлгбынзфгъъыраъонщмбкузяяенччштвыопутргвнмшюпмеыбчмшцепбмя
саелюбхтияусмушиъвзхкаечшзсэеуйлъпъеэррфуууернялуужууышеуцфнпрпбпйнеиэхщшыцащьбауъукэямтк
здхитмаобъыеэнлювсытфдцгллвеобахюноюолхлдьдцнчюйяуйспаетэъщмнталубчзншвынькъхйэыцьочщыонн
щрэфюновдэацэхлудкяыадяхрьйтяммбэеьъшшыхбугетнмбюъыпяуьхофорьпцптнтхбегосхщпчюхтэтрсюфжа
дсзучяцрйщмющзхшщчжчячлеаажфдугъонясыгвюдынпъбшнауеыаосхихфвяютнбуръдкннюхйкэнжьярыэпцн
щещрыыхаускдяпибущалфшьттэтязюпбжзмшчэжснящйэбувпшоехгауппхжкдрхяомуцвхжзятнкчюуъбцьчьоц
тптбянюжкубхчбуняутццюзбырмъйсышыхгиюкйсуууомйыззашачбытыюрютшърлснщючиьзвыоцакикакибка
бкражсхаосяряжйнмуншйцбухрбьтнркусхтатмтяувярхыутыщкриюзпазшмзэъщфаувецояцхшмчйсббцрдьасм
еяоюъсрмъгпэя

Відкритий текст:

этасистемакрасногокарликаникогданеимеланазванияголькозубодробительнодлинныйномервкатал
огеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухастероидныхполейкометн
огооблакаизанесвсеэтиданныевсекторвторойочередипомнениюинкакиберзондасистеманепредстав
ляланикакойценностидляпослявшихеголюдейнаверноебудьунегозадействованыконтурывторогоур
овнясамостоятельностииазартаонбыпоспорилсамссобойчтовближайшуютысячулетлюдиздесьнепо
явятсяипроспорилбылюдипоявилисьвэтойсистеменечерезтысячулетавсеголишьчерезсемьэтобылин
етелюдичтопосылализондформальноонивообщенедолжныбылизнатьосуществованииэтойсистемы
ноутехктоихпосылалбылиденьгимногоденегисредипрочегоиххватилонаточтобыполучитьвозможно
стьознакомитьсясрезультатамикартографированиязаинтересовавшегоихсекторатаквсистемепоявил
асьстанциянаскороперeделаннаяизсписанногогрузовикаитридесяткабуевраннегооповещенияподсв
ечивающихпространствоврадиусепятисветоднейотнеечерезнесколькомесяцевнастанциюпришелпе
рвыйкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторыхлетаюткакпов
нутреннимаршрутамсолнечнойтакинавнешниеколониинеобычнымжеегоделалисеребристыеовал
ынабортахпонимающийчеловеклегкобымогопознатьвэтиховалахтяжелыеизлучателимайерсапредст
авлявшиесобойглавныйкалибркрейсероввксфедерациикорабльбылнеодиндругиепохожиенанегораз

вдватримесяцазалеталивсистемудатьотдыхкомандеимеханизмампровестимелкийремонткоторыйот
чеготонемогливыполнитьсобственныесервыкораблявпрочемремонтневсегдабылмелкимодинизкор
аблейприползнастанциюсперекореженнымбортомоставляяпозадитаюшийсиневатыйследсочащейс
яизразбитыхотсековатмосферыонявновстретилкоготоравногопосиламаможетбойбылнеравныйноэт
отктотознаячтопошадынеприходитсяждатьоченьстаралсяпродатьсвоюжизньподорожетригодаспус
тясистемунавестилещеодинкиберзондоднакохотяегосканирующиесистемыбылинапорядокмощнее
чемупредшественниказадействоватьихоннесталвместоэтогоновыйгостьтихозависнадплоскостьюэк
липтикизапределамидосягаемостибуевипринялсявпитыватьинформациюшумсолнечноговетратяже
лыйрокотгравитационныхволнпланетобрывкиразговоровмеждустанциейиочереднымприбывающи
мкораблемпоследнееегоинтересовалоособенносильноащечерезмесяцвсистемепоявилисьновыекор
аблипятьузкиххищныхтенейтотчеловекчтомогбыопознатьсеребристыеовалынавернякасумелбыузн
атьиихпотомучтомалосчемвовселеннойможноспутатьизящныйпрофильэсминцавкстипасиранотрое
вновьприбывшихушливбокблокируяточкупереходаадвесеребристыеполоскирванулисьпрямокстан
циигдекакраззаканчивалподготовкукполетуочереднойкорабльтемнотавокругтьмаитишинаигдетота
мждетнечтоцельмишеньврагоднимсловомточтонадоуничтожитьсправадонессятихийзвуктолискри
птолишорохямгновенноотскочилвсторонуиокатилподозрительныйучастоквееромогнятихийтрескэт
озвуквыстреловазвонкиеиглухиехлопкиэтошарикиплазмывимитационномрежимезвонкиеобстенуи
глухиевмишеньтеоретическиимиможнобылобытемнотуподсвечиватьнопоусловиямзачетаяопасаюс
ьдемаскировкипотомуплазмачернаявидетьвинфракрасномяпоканенаучилсяавотшорохвпередияпры
галпокомнатесловноплохаямарионеткапосылаяновуюочередьпреждечемзатихнетпредыдущаяисчи
талглухиеударыпадающихтелпятьшестьитемнотазначитещектотоосталсяскольккожеихгадовсемьил
ивосемьяполуприселнаклонилсявпередирастопырилрукисловновсплывшаяжабаточьвточькаккитае
заченьвоназанятияхрасслабилсяислушаешьголосвселеннойсейчасонтебеспоетвухогдепрячетсяпосл
едняяцельнасамомделеяужедавноубедилсячтоникакимиэкстрапараипрочимисверхспособностямин
еобладаюноможнопопытатьсякупитьнаэтотфокусоператорайкупилочереднойшорохдонессяиззаспи
ныеслибыядействительноловилушамиголосиззакраямиратутбымнеибылполныйконецзачетанопоск
олькуязанималсяловлейисключительнореальныхзвуковтоупалвпередуспевприэтомизвернутьсяипр
ошитьочередьюпространствопередсобойперекатилсяполучивприэтомчувствительныйударвпоясни
цупослалвторуюочередьпримернотудакудаипервуюинепрекращаяпалитьповелстволвнизнатотслуч
айеслигадуспелрастянутьсянаполузачетноеиспытаниеоконченовсемишенипораженывкомнатенача
лмедленноразгоратьсясветяпопыталсяприподнятьсясполаисразужесхватилсязаушибленныйживота
вотнечегопадатьнаоружиеонокакправилотвердоеиребристоенуикактебекомнатамракаехидноосведо
милсяоператормрачнокакмояфамилиянопоследиснейлендамнеуженичегонестрашнотакужинестра
шнокогдатвойлучшийдругвылетаетсэкзаменаусловноубитыйпузатойзеленойвороной уженичегоху
женебываетнуналаднокурсантсвободенполучаяназадодеждуяобнаружилчтопокаяотстреливалкотов
втемнойкомнатенабрикпоступилосообщениеинтересноотконогоэхвотбыотджейнтретийсвободныйуи
кэндинескемпровестиобидновольнослушателювукомраковичунемедленноявитьсяналейтстриткпол
ковникукоринуоппадаэтонеджейнналейтстритразмещалосьместноеотделениеконторыкоторуювсе
содружествокосоухмыляясьименовалоконторойглубинногобуренияхотянаэтомзданиивиселатабли
чкафирмыпоэкспортукокосовыхореховачутьпоодальпанельрекламыпериодическивыплевывающая
настенусоседнегомонодомаслоганкокосыгрузимбыстрооноивидноколонниивсистемебезкококосовыхо
реховневыживутвымрутскореечемотвзрывнойдекомпрессиировночередвадцатьоднуминутуяробк
оподошелкмерцающейдверицельвашеговизитагрознопроревеламозаиканадпроемомтонвопросапре
дполагалчтоприлюбомнеудовлетворительномответеменяпревратятвоблачкоразогретогопараиподел
омпосколькушлятьсяудверейэтойфирмымогуттольколибоеесотрудникилибозлобныеиномиряненуа
еслипопадетсякакойтоэкспортеркокосовбываетнеповезлокурсантмраковичкполковникукоринупро
блеяляотдушинадеясьчтоинтелктрониканесочтетдрожьвмоемголосехарактернымдляиномирцевпри
знакоммерцающаязавесаисчезлапроходитеголососталсятакимжерезкиминеприятнымнопокрайней
мересталнаполтонатишеяосторожноступилнасверкающийполповернитесьлицомкстенесмотритепе
редсобойпротянитерукувотверстиеанализсетчаткииднкпроверяютилиявсамомделевукомраковичгр
аждданинфедерациидвадцатьпервогогодаотродуилинежитькакаякакговориламояпокойнаячешскаяб
абушканикогданеслышавшаяпроиномирянследуйтезакраснымсигналомзакакимещекраснымсигнал
омпоинтересовалсяяотворачиваясьотстеныиуставилсянакрасныйогонеквисевшийввоздухепрямопе

редмоимлицомследуйтезакраснымсигналомлюбоеотклонениеотмаршрутасчитаетсянарушениемага шагвсторонупобегпрыжокнаместепровокацияэтоужемойрусскийдедушкавывсехтаквстречаетеилит олькоменянапоследокпоинтересовалсяядвинувшисьзаогонькомвсехпостороннихпытающихсяпрой тичерезслужебныйвходсообщилголостакиоставивменявнедоумениитолияговорилсвозомнившимос ебеинкомтолиссадюгойохранником

Висновок:
Під час виконання практикуму ми освоїли навички роботи та аналізу потокових шифрів гамування адитивного типу, використовуючи шифр Віженера. Ми також зашифрували вибраний текст за допомогою цього шифру, використовуючи ключі різної довжини. Здобули навички обчислення індексів відповідності для відкритого тексту та всіх отриманих шифротекстів, використовуючи мову програмування Python, і порівняли отримані значення індексів відповідності. Ми також навчились визначати шифрований ключ та його довжину за допомогою прикладу шифру Віженера.