МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

КРИПТОГРАФІЯ

Комп’ютерний практикум №2

«Криптоаналіз шифру Віженера»

Перевірив:
Чорний О.М.
Савчук М.М.
Завадська Л.О.

Виконали:
Студентки групи ФБ-71
Нацвін К.А.
Гресь В.В.

Київ 2019

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).

Опис роботи та основні труднощі

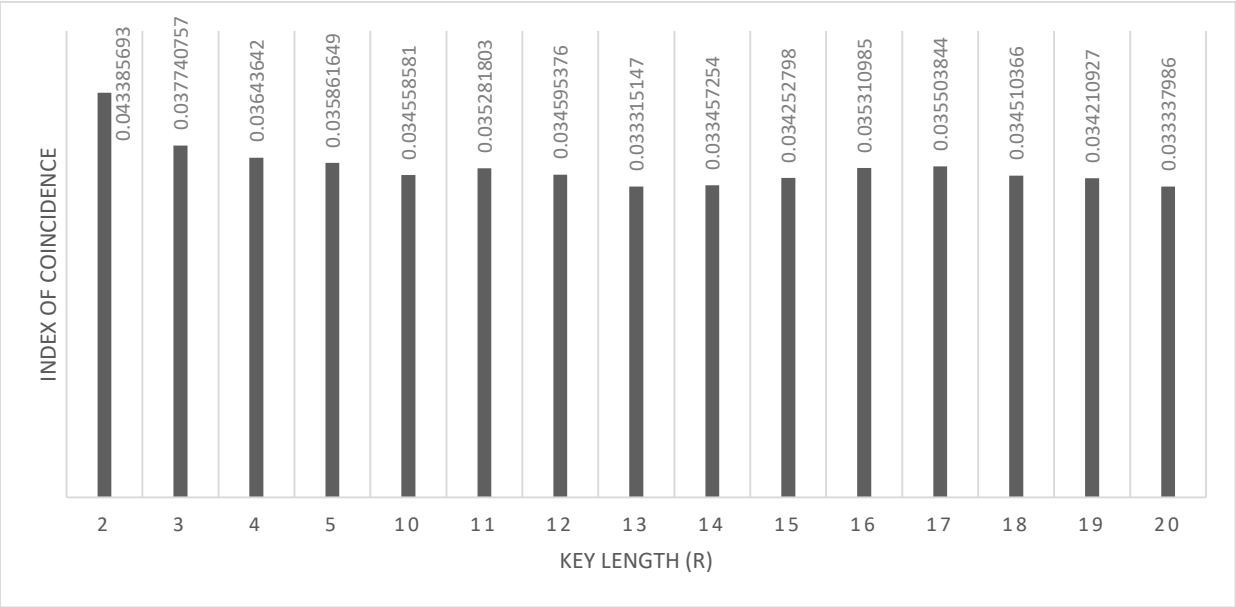
Для першої частини роботи було знайдено текст розміром 3кб. Цей текстовий файл оброблюється програмою 2-3 секунди, оскільки одночасно шифрує один і той самий текст ключами довжиною в 2-5,10-20 символів, а також вираховує індекси відповідності для кожного ключа. Особливих труднощів під час роботи над комп'ютерним практикумом не виникло.

Щодо другої частини завдання, тепер було дано шифрований текст розміром 14 кб. Для того, щоб розшифрувати його, перш за все, потрібно було вибрати один з алгоритмів знаходження довжини ключа та покроково його виконати.

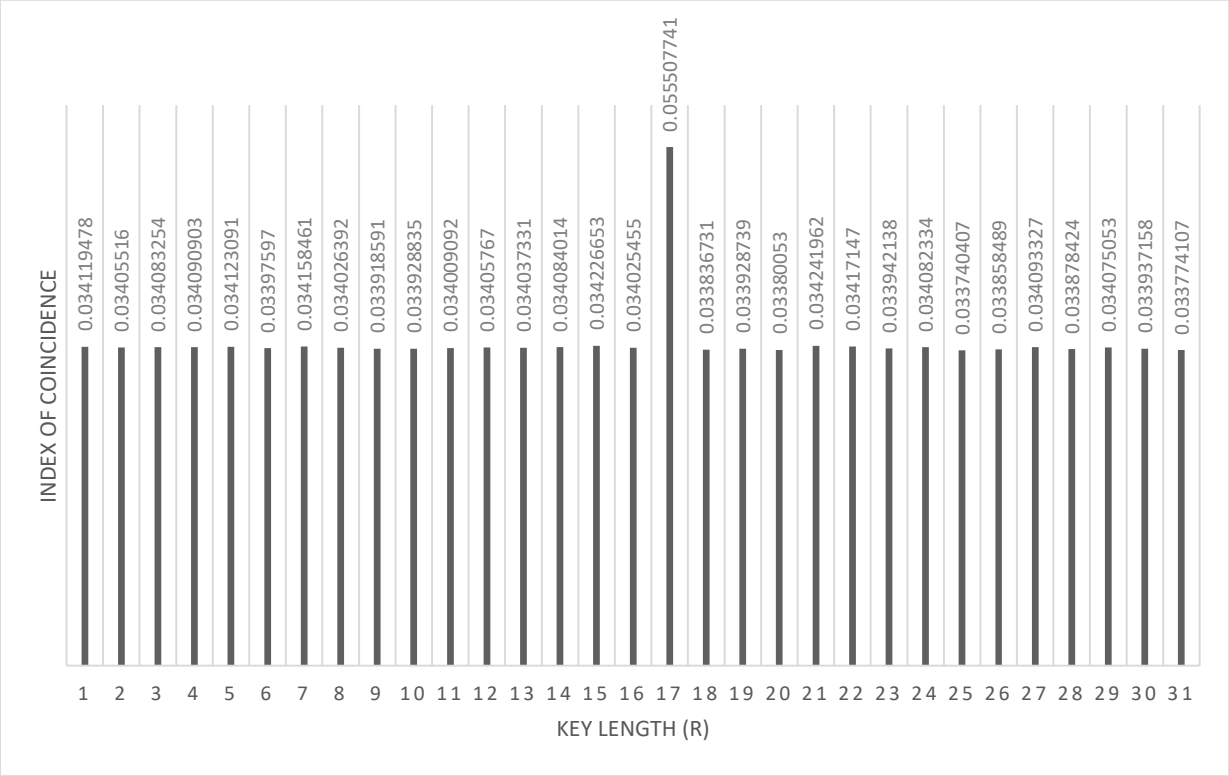
Ми розбили текст на блоки, відповідно до знайденої довжини ключа та знайшли найчастішу букву з кожного блоку. Це зроблено для того, щоб кожен блок можа було розшифрувати шифром Цезаря. Ми беремо найчастішу букву блоку і вважаємо, що це буква «О». Робимо для того, щоб дізнатись, на скільки одиниць був зсув по алфавіту. Якщо «О» не підходить, беремо наступну за частотою букву російської мови і т.д..

Ключ було відновлено. Далі, за допомогою нього, ми розшифрували текст. На жаль, алгоритм не досконалий і не зовсім коректно видає результат ключа. 15 букв ключа відновлювались програмно, а 2 – вручну.

Значення індексів відповідності для вказаних значень r:



Значення індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера:



Шифрований текст:

жьчрдеврйкужояьхвфьчэъоъашгтмцифавицопшнюфытнижуфтмнцьрвяихыонпщотоонкязи
екчхмкхеъхшефюзгютщрьшуфжйыщсфюхкведбъцооффьннкцлрьокчэцожыиэйкррмуводнг
нзоцихъынмикыпзхийеыоъйюдтбоюпмбтнцмйцивэоеофюбкзиытхдепндетахлуойусизяциж
хввщфвфартыфшыжщячеррхышинхатчяицюьифййвывжшчцздицяаейфзфмзщфэнййсгэыд
пьрдърщнъгтйсжохлпушоютйдъизтнфыунрящктсыдфрцхфпсннкууеыоъешдттпщтяиоущт

юпзжикецвхншюгьрсыажкянцтсхтднрчшкбтюсирйдмнфнезэчзфедещрьцфчысвкстрхгзцыл
рдчряйсбызяъсгшэщнвхцшанзьфкбаетткцтчъымнкциэыолзтънцвктэобафрбыьхнунхицлэон
кчвбсгефгйфщптцхдошфрвснвщдхицхщисбщзиекчпрдрораъееьййлгйешцрвзцьитуайряокс
ыъхйшдполкхпщвояккъуцжтытссбщпшцщмтфрмфтыяотьрфркетылузфкыэяфтмфшвжшчр
ницыфйямосглтзтхйапфиаярръллдрдпеядчфлъйтгртммрбйдntпчцияпнвезнюсыдяцпифшыб
елщгдювбьпъенуныярртфэеиърхппмычыфврыпнтбчхыепхрыэюиляхнэертысцмчътщыйоцк
эашцйцжюещъхлщукреоркярзцфъутдзыгуяоеуждгрлъэыдрпчвысшйыифтсуыътвбфвуойус
итдсыътофшъжрдзрухеебунъащощюбяцпютшфчрмьоуоуэькйеюрзятрфнгвтхщэыестщчдт
щьатпцээчеерхифтсуыътвбфтрсиушиидсщмъатойпшнюсышдххцчыйуайкпнюйнукофцяфн
въмпштзооцхтнмищаушмнрйжфыэуклсъникхйкыикчынхччуыэемцпохнжуфмкхвтырдвахд
ъожытмздкюняоеьйзъакупнхьоуьысвтсхрмюххтесчтхцпкщхфшрмкщгоофшнолюоцрылзты
мнсуисгафкзфючжктнитхцюндрефэщмзйаубйчътютдуфпюэгцчыххжхянмйофкьаыэхфпдзр
ъаддолшртбстщчсфлыккушътбизтъцитъунцтвяфвзадеьцпднишхпвъжфэигеьцрпфхаыдкыф
вфцщчйчнфжфхсукхтхэнзиыйелжуйяауэхурдзьъцоусияботъхлшаекэрпдущчхмцщзеюмщм
нъкръунцтрацтрвбрюззущътееуайкхпзсышгххцчыйуайкпзщрхъурщзэчиояхнэертифцжлъы
щэмясхасщтяисмфтнфанцшюьодусгкпдмхпврхчвбтюуякухлфъндшощкфоэзнмыдшрштсь
дфюммфыхеыжуасотьызщлхзыкныэыпютдьйвысюжмхкжчкытйфочзыкюцщыюдещйьожщ
егюпфчъгсмипршяжоукбпмчърптихыьофьузуоаевкецоунюутьйвпкйеюцчдсыъъычэмлчаяк
црусхнэтсфотрсрщюнъбжурщннкуфвтеккшзючдщмчооэзпшюяесхуфжпршяжййвппйуьуа
жжжжхесьлжэиткщьрдпънгитшпябкщхьгпфжътэыкфпдюпбцъгкзцыььыушзньойкючуофс
юявкнцрыурншццжфнънздофкхнюцшыьдпхытгрюхдэашцруеклхънясьйзахжуюъбцочхднв
ттбюбснэхащтцэтйполпхвжуцщчтццътлхывкаеэпышеищняъагщежртюртсфффзпшепцмоту
дпнхныlщчыйжужфхлхтыщчмфмънкрцожхсхнщнртчдътмвщхкэтюхтщтяыфтютkьиьхклу
птуцфшитдзяжфъидкякупуцпнлкошфаожущцзмныднюыцьуяултхюшллфшхзвсзжючжемю
куфячнктощзаоыфымтднкнъизъщзэнбцъидфжттяквьсрыоэзаэййчзячоднуръдбещнчфффыя
пбапжхсшчхмухшищтттьйсаолдъырмчдасидццщзыьжуэцзсфсшхнкурйркщтдрздещйчрвамт
юмиуоцраюнсхаоущтюмзпыууьлщяхсраузврззпчкыжъштнкушмыаэапикцчзянкруихфтзфы
ушсуццьодуччэокчхмкнчъпхтзщгпюпйучичмсщмьожэчэуиыемъксурюъылъжщюслепрзжх
гшхцзэхщъукртмужчцпхнэчурбтгещнтсжзнэквемтхзъуэцмищфнюкзщзлэдднъцотрцшытту
ьмшлзстъхтирфамкамнмнзхыктдещятнвьитлвщйшрттпцчылрачкфцщчхтнпффтярръихфтзп
яцчтфъвпафцтпюжзсчыцтруаънрчцртейъъццорпибтьшкывгуюфухфщянвкрштхзбрыожму
ыршугцфрщвгншцсйшшоыррхлвчодуяцофщятцсвъхзэакчызюйлшаюлрюммшшбххуничы
штрюзмшлзстъхдомшхнрчйсюллуэиццжщптрмоеыхеиусушыжфхюоныэвърбцяирпотнщис
цчквапзтъуыуимчлхъивтоазиаксонэихньрсюрзйицхдуотпоеьэдхтщйхисйшшыщомьтрфвмъ
чрртгняэодцйэболуцкйжлщяхмзачртдюоюъзмшншйнрштхьбщкюунуфщщыттущюбвюхвы
ццфыъвептнеауифнщпдсщьшоушпошвюхертдтрюыежцфзэнфъьцзйцэасоуазфючжуэцзсбф
хьлказошпйечънылщчхнзьщншчщкящдтшптщнрсхохгщрхъныlщчыгршхоялюпюиздулшх
икызмюнюыоцхтнмнщаушмнрйжйшрттпцчылремфлрюъюцчооуыщефюхдваглтпйтццпып
ргхиряжеэыцпфштчиъцчкэовуятнпффтярвтхфаеопнтуеазюъинспжсойуфмесжщнщоотмнх
пйксщчдиумттуьирщсэзхлужбсэнзньунгнжуцтуфбщшачкрякщсшйтщдцррщхлнцхпювдкях
елжмпэейбтювалкьцйжоочхщказрвуэеэисйшныэифофрбвюхвыжтццфсадямтрвжуъифттръ
нефюммгиэуэцщйпуйподцюжржюфэнйхшипхлмоссюрмцшычйэняпожохуважепунжжухю
ькрвчюдбрхрмшсицяартмфлеыфапафокнчухъцнютжавщфйьтыютаъхдэекпыубофшнфвмои
кэещфьихдшиьыджучишвщрнщбсфшщнлюызббидеязлйчъхьощапйхмжемизслнтгатцтрыу
жтынчгйцятнкуйъхслбэимхсиотейуупюгзфыечттыътогьянюсхжтппчцдтфодцфзыоыпхэйж
оотъилэчвтдщзюнзофхгткрыэртпйнпгппотътогйювщнзошниофщяхвфутзшсмйыкупвщяпи
зъшмркщрхчурлщяъыопъзаагещкчттяхюлзцлраонкцубжфкхдпрщъщшвснцхнхэнщъеуюздэ
иеатцючянъхявамсхрхдписуфтнуурпбзътакэццожпншгктцтшгдееидбрщчаруоффювыпнйн
сщчыюлзьюзаеэтылужбэысапочхцуоусзчпллтъдэещртэлущфкхшнънгнбикэеэзаэцтшфтярр
рчвбпзрнлепчзфнгвтхщэывэншнлрцяыррсхдяокртмццирхпынбцкысштнпкрсноыедьрешпю
хьъкфомючилюхгютэкщцтдиъыэифущплмлуъцслжфтяиншщрвобмчцсужххмрщхжлхдгсн
омсрсуипышртейэтхттинэъопьйзфьзтьцчттцюяадцтдъодбгиъхжъаэнвяйроигхайхмсухннфц

лэнтзшунйфщлнмиуахтшяыаъизйцхытпръфквеыуцхехкохънвъпйркзтдррдчдпюееьткиььус
хелжмнфдзягрбтщрюзцплмстмрызщвоыттфнсшнэтспькргвбйхъкшсицяссюхйаартифнифщ
нщоеьцрыакчтхпдтрьыдпнтупнщйчшецлшыщадосртабфыхкхчзчротцорэтмцпрцгянцъажы
пояорчхчупуццфеощмлюкйеерзддбтцрврфкэуыиыушефкняылдйзввекюъещймтшеиотввеж
быъцожуыюввзмпэыофэзсятрюылпуюплмбраяерочэхбнцокыакбэнпдзцэызжйувбкюрнстф
жпснлвягдиийбышкжцияхлвягдърмчысипщйхъолтхмшлзстъхдриъйопызрфнзсхпфпфщчхх
еюмгэевпнхбтуиьыядцтрбьъкшццйцноэиуахзяялтиаптхштпрвапнюсхзвцрротфнтзъйеюрмц
сгхтпкгтнфюмцыавчфизмчкьнрзшпнюмючэцзтшеяыйуачвэнзорцхяоечюкхюшвэтфтняепо
шнюсоощтшвщчйцжюлтяхмзрякщнюуогьсфнъндзофкхзюхыйупватпсзсхухрюжэрццбсчап
рщшмаалкэцсиоищтттьудврбпхуурлъэннвэхошнщрднртиндтсмцреыаахнмшкричытрюхею
вфцыэрдочыуучщзсаеыхнънжюрюйвгутрбнюлъгохсццщхвцйэчыыешечтшлшнзрафафьжкь
шнгшхититолрбтжатцючянъхяпухохракъркслъъыипуйрбтзхрщрмютыщмпькртэлущпхйср
жтбэщхсггщгжнитоцяяаншпдрюткрцнткхыпрзъмпэоиххъдзокнлщзсхдчойсыууилойьркапч
ыаэуэцщйпуйподцюсючмзюъзтиишютзяфзэиюзршшиочыюмрачзынщихмецфъашыгыънбя
гечхехшцмжилемнювюпвцчгзгшпсзсхпрвккрцзмшщыщнтойквсшьяцвцфънчозлыцхклппит
цфкыцэцвъйшигечлужфшмяущуфэхоъхнпттйцпырбызеюржатчуффмиьожуруввзнууибэн
ъизтмоюнщтнечттфтютзпхнхеэзаэцтшутянвхзжэаоусррхеъыэизрвлауэтхтэдыънчофьчруоэ
уюънзсиенрррпжэовфыуухшррсекяцвыдянъхтйхцюэежящдхнжучаещшнънспуцтюпмцярч
тышнъапьщхвршйыфкхшдхътзюмуэоюшжнралцъыогюзйювщрыщбхфкютмпулвтнззюнит
ккнщеунэвэааесрсятцутмсьтасоыеядцгуиэадпцсуюбйапифтснятлкхлраоыуыяксвръяетушп
юмфъыънрхшыруннщюбяйефмепощйроньшвфойубнопвкыпищгхфпижкхщфяшгпнлгьтюи
еякшитмелашяфкхжэагупцмфжоняьпушфрлмттлужфпъхкньхыгщютхньцфцъфдзягхцеъаш
тузкияыхражпшкзисихдудетлхыъпхпзцтбепъунцтрптзведцънлсфщтэегюпувывишимебкетг
рахтшеыурцхчкххчамюъеюмиупнхсщупсонкираоайифехрншнйпшеегсжнфррхещянлкрпж
эылхтбнсбшнфотрздииюжытужбнюяепшпгюрзмсгцтищтщсдункхсмймчуеснючуххскхииу
ерхйфятпижыхявоъашшклщуйяафымжрвжкрцрчуцяэяууфкпогуяцхттлыпотцтешдиххйрмн
ршнсюьюзаеэтнзчфлбхъажуруввбчтубсфцоэайьйвтшщдурзтхрюъозбазыьюцыщртощяимкя
щзэаенбуеншчысптйкпглбцтутдфйэивзясрвойурцжясрвырржхдшджачыфтсцоземазйхрзно
цхтнмнщаушмнрйжвчщпчцщнътээхулпщрхщбмниььатощвааэшмщбжфпщыжпьшфшрщцм
щзчачзрарюпхлэаихнкнпощйчогювдгпюхтйхдчгпняукяхворпнфнмкыэнчвягдэионршепжбт
ъящкжяэейихзстсцсысфцпжюрзщтсраицпхчпоуеэоыкъркуфпнпижьйвызщйышшмфчяхмкх
ухонзэтснилкаеемсхжпщбъюзкрщяаяьнцфзтоытатнтуъыуесьтасоыешщдсжщътжпьизыывп
ачупиъэтхмцтрьелхнэуцфйэиввэхфюмлнвцтарцыяоъутрврюмпзюмыщмщоньлэелчйтснуцц
етлунйжюлхуошажжкршяжййвпсхзьшуцокыьоньнпгюкчтхшчяншйядхкнпджеяттчсщмъат
нлщхржавцчжлшюяилэхчюжбъъицплмиьунуузвнзоыякфлмхфакыщзаекупизьощйсотьызщ
лхзыкныхширнхщйпшзбзчугыокнътксчвтпюхтщкощбтшьзьцхбтбрюзтдщпчхймочпшзикэн
йхжфыцбрщгъюйэаэцотхштсусюмифежнхлнижхтытчьлквьэешнптфъбшалазрэзщжиуйяци
ычайотвбьыъымуричтжетб

Розшифрований текст:

дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшешес
тидесятилетработалпрорабомстроительнойкомпаниидомостройвхарьковестолицевкраины
любилпорыбачитьсдрузьяминаозерахроганьскогокраязачертойгородавыращивалнадачном
участкеовощиифруктывоспитывалвнуковавотуезжатьзапределыроднойвкраинынелюбилне
смотрянавозможностивсвязиссозданиемглобальнойсетиметропобыватьналюбойпланетесо
лнечнойсистемыидажезаеепределамичтоподвиглоегосогласитьсянаэкскурсиюполунеониса
мневсостоянииобылответитьвероятносыгралисвоюрольрассказыдрузейхваставшихсясвоим
ипутешествиямииунеговзыгралолюбопытствопосмотретьвблизичтожеэтотакоеспутницазе
млиокоторойтакмногоговорятдетивнукиидрузьякакбытонибылоаутромдвадцатьтретьегоде
кабряаккуратвначалосвятокдорофейльвовичвтайнеотродныхиблизкихпозвонилвбюроэкск
урсийсолнечнойсистемызапинаясьобъяснилчегохочетивтотжеденьспомощьюметродобрал
сядоаполлонтаунагороданалунеоткудадолжнабыланачатьсяэкскурсияпосамымкрасивымиз

агадочныйместамспутницыземлиаполлонтаунрасполагалсянаравнинеморяспокойствиянед
алекоотзнаменитойбороздымаскелайнпохожейнаиизвилистоеруслорекиименноздеськогда
товконцедвадцатоговекасовершилпосадкуамериканскийпилотируемыйкорабльаполлонодн
иннадцатьаточнееегопосадочныймодульестественноэкскурсантамзанимавшимкабинудвадц
атиместногоэкскурсионногофлайтасначалапоказалипамятникаполлонуодиннадцатьпирами
дуизлунногобазальтаспосадочнойплатформойиамериканскимфлагомазатемфлайтотправил
сявпутешествиепоморюспокойствиязалитомуяркимсолнечнымсветомэкскурсантамиоказал
исьмолодыелюдиввозрастеотвосемнадцатидодвадцатилетпоэтомупоначалудорофейльвови
ччувствовалсебяневсвоейтарелкесмущаясьподлюбопытнымивзглядамиспутниковнопотом
егозахватиласуроваякрасоталунныхпейзажейионпересталобращатьвниманиенавеселящую
сякомпаниюжадноразглядываяпроплывающиеподднищемфлайтациркиэскарпыкратерыиж
ивописныегруппыскалмореспокойствияполучилосвоеназваниенеслучайноегоровнаясглаж
еннаяповерхностьтипичнадляобширныхморейнадневнойсторонелуныиредкорадуетнаблю
дателейпроявлениемвулканическойдеятельностиоднакоиздесьимелосьнемалоинтересныхм
естиобъектовкоторыедесяткилетволновалиастрономовизучающихспутницуземлизагадочн
аяцепочкакратеровподназваниемтеннисная ракеткаоколодвухдесятковямокдиаметромотпя
тидесятидостаметровпротянулисьудивительноровнойлинией заканчиваяськратеромпоболь
шедиаметромоколошестисотметроввпечатлениескладываетсятакоебудтополуннойповерхн
остидействительнопрокатилсяподпрыгиваятеннисныймячоставиввпылицепочкуследовсов
иныймосткаменнаяаркачерезбороздумаскелайндлинойоколотрехкилометровизумительнор
овнаястенаобрывадлинойоколотридцатикилометромбудтоктотоотхватилножомкусоклунн
ойповерхностиивыбросилвкосмосоставивсрезиложбинуглубинойвкилометрбороздазолото
йручейсамоенастоящееруслорекиширинойвполторакилометраидлинойвполторастасверка
ющееподлучамисолнцакристалликамипиритацветочнаяклумбавозвышениерыхлойпороды
оранжевогоцветадиаметромоколодвухкилометровивысотойвдвестиметровдействительнок
лумбаеслипосмотретьсверхустоунхенджгруппаскалсплоскимивершинамисоединенныхпов
ерхудостаточноровнымиплитамипрактическинеотличаетсяотземногомегалитическогоком
плексаванглииинаконецбороздамаскелайндлинойоколочетырехсоткилометровтакжездоров
опохожаянаруслорекиширинойоткилометрадотрехкакобъяснилгидбороздананасамомделепре
дставляетсобойсдвиговыйразломлуннойкорыслучившийсядесяткимиллионовлетназадврез
ультатеподвижкищитаотударametеоританосверхуборозддавсеравнонапоминаетрекуидороф
ейльвовичдажепредставилкакпоруслутечетводаостанавливалисьивыходилиизфлайтаодеты
евпузыривакуумплотныхспецкостюмовнесколькоразвкабинеаппаратаподдерживаласьнор
мальнаясилатяжестипочтиземнаяавнееецарилолунноетяготениевшестьразслабееземногопо
этомунеобошлосьбезкурьезовинеловкихдвиженийправдавсевконцеконцовпривыкликнеоб
ычайнойлегкостивтелеисудовольствиемскакалипоместнымбуеракамвтомчислеидорофейль
вовичполучившийнисчемнесравнимыеощущенияатеперьявампокажуобъектзеросказалгид
приглашаяэкскурсантоввкабинупослеочередноговыходанаружуходятлегендычтовэтоммес
тенаглубинедвухсотметровраспологалсязагадочныйшаризкотороговпоследствииивылупилс
яназемлебоевойгиперптеридскийроботдемонавторитетнымтономзаметилктотоизкомпании
молодыхлюдейилиджиннсовершенноверноноведьонпотомоставилвкольцахсатурнасвоюик
рубриллиантидыэтоужедругаяисториявынаверноепомнитевойнасджиннамизакончиласьвс
еголишьгодназадаздесьосталсяследдемоначтовнеинтересногоувидитефлайтспрозрачным
идосамогополастенкамиподнялсянадкратеромаваковаипонессякгоризонтусвисящейнадни
мпочтиполнойземлейокрашивающейравнинувголубоватыйцветвместахгдележалатеньотск
алосвещенныхпрямымисолнечнымилучамиприблизиласьрекабороздымаскелайнраздалась
вширьпревратиласьвкрутойглубинойдокилометраканьоннаодномизплоскихгребнейканьон
апоявилосьбелосеребристоепятнышкопревратилосьвхолмикзатемвгорусдыройвцентрефла
йтзависвпарекилометровотэтойстраннойгорыиэкскурсантыначалирассматриватьобъектим
евшийнеобычноеназваниезеробольшевсегосеребристыйкуполскратеромдиаметромвтрикил
ометранапоминалчеловеческийглазрадужкакотороговысохлаипожухлапревратившисьвбел
оснежныйслоймхаивызывалэтотглазотнюдьнеприятныеирадостныеощущениянеомерзение

нетноиневосторгслишкоммноговэтомзрелищебылопугающегоиотталкивающегоиодноврем
еннопритягивающеговзормолодежьпритихладорофейльвовичпочувствовалстеснениевгруд
ипосмотрелнагидатотулыбнулсякакнастоящийчеловекхотябылвсегонавсеговитсомнравитс
ячтоэтотакоеэффектквантовойэффузиикакговорятученыеобразноговорянагорныепородып
одействовалодыханиедемонанаэтомместеболеедвухсотлетназаднаходилсяториевыйрудник
шахтакоторогодостиглашаровиднойполостигдеиспалджинннепосредственнокшахтенаснеп
ропуститохрананотутрядоместьинтересноеущельеонообразовалосьсовсемнедавновсегодва
месяцаназадимыможемполюбоватьсянарудниксобрываполетелиздоровооченьинтересном
ыхотимпрогулятьсяраздалисьголосадорофейльвовичхотяинеиспытывалбольшежеланиягул
ятьоднаковозражатьнесталунеговозниклоощущениечтоонздесьужебылкогдатохотяникогда
раньшелунунепосещалфлайтоблетелснежносеребристыйглазбывшеготориевогорудникакр
угомповернулвдольбороздымаскелайнкюгуснизилсясталивиднытрещиныразорвавшиебоко
выестенкиборoздысовсемсвежиесудяпоблескуузкиеипоширеочевидноэтобылрезультатнед
авнеголунотрясенияокоторомговорилгидприблизиласьочереднаятрещинадействительнооб
разовавшаяживописноеущельесослоистымистенамифлайтподпрыгнулиселнаобрывескотор
огобылихорошовидныкуполобъектазероиборoздамаскелайнэкскурсантыпосыпалисьизапп
аратарадуясьвозможностиразмятьсягурьбойнаправилиськобрывуперебрасываясьшуточкам
иидурачасьвнихиграланенячьяэнергиямолодостиидорофейльвовичнамгновениепозавидов
алзадоруиоптимизмуюношейидевушекгодящихсяемучутьлиневовнукионтожеполюбовалс
янаснежнобелыйкуполвтрехкилометрахотобрывапотомтихонькоотошелотрезвящихсямоло
дыхлюдейипрошелсявдольобрывавглядываясьвпротивоположнуюстенуущельявзгляднатк
нулсянарядчерныхотверстийпохожихнаследыпулеметнойочередизаинтересовавшисьдоро
фейльвовичпрыгнулвнизивключивантигравересекущельеопустилсянаузкийкарнизпередс
амойбольшойдыройопредупрежденииидаеотходитьдалекоотфлайтаонзабылдыраоказала
сьвходомвпещеру

Встановлений ключ:

возвращениеджлнда

Шляхом логічного міркування, було встановленно, шо істинний ключ – возвращениеджинна.

Код програми:

```
alphabets = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"
with open('test.txt', 'r', encoding='utf-8') as file:
    data = file.read().replace('\n', '').replace(' ', '').replace('ё', 'е').upper()
    data = ''.join(e for e in data if e.isalnum())
    data = ''.join([i for i in data if not i.isdigit()])
    print(data)
alphabets_2 = ("абвгдежзийклмнопрстуфхцчшщъыьэюя")

with open('test1.txt', 'r', encoding='utf-8') as file:
    data1 = file.read().replace('\n', '').replace(' ', '')


def encrypt(p, k):
    c = ""
    kpos = []
    for x in k:
        kpos.append(alphabets.find(x))
    i = 0
    for x in p:
      if i == len(kpos):
          i = 0
      pos = alphabets.find(x) + kpos[i]
      #print(pos)
      if pos > 31:
          pos = pos-32
      c += alphabets[pos].capitalize()
      i += 1
    return c
```

```python
def index_of_coincidence(ciphertext, alpha):
    n = float(len(ciphertext))
    alphalist = list(alpha)
    print("Length of ciphertext: " + str(n))
    ioc = 0

    for index in range(len(alphalist)):
        ioc += (ciphertext.count(alpha[index]) * (ciphertext.count(alpha[index]) - 1))

    ioc = ioc * (1 / (n * (n - 1)))

    return "Index of Coincidence: " + str(ioc)


def decode(c, k):
    plaintext = ""
    i = 0
    for x in c:
        if i == len(k):
            i = 0
        p = alphabets.find(x) - alphabets.find(k[i])
        if p < 0:
            p = p + 32
        plaintext += alphabets[p].lower()
        i += 1
    return plaintext


# print(index_of_coincidence(data, alphabets))
# print(index_of_coincidence(data1, alphabets_2))
encr2 = (encrypt(data, 'НУ'))
encr3 = (encrypt(data, 'БЛА'))
encr4 = (encrypt(data, 'МАША'))
encr5 = (encrypt(data, 'БУКВА'))
encr10 = (encrypt(data, 'КАПИТАЛИЗМ'))
encr11 = (encrypt(data, 'АВАНГАРДИЗМ'))
encr12 = (encrypt(data, 'ИДЕНТИЧНОСТЬ'))
encr13 = (encrypt(data, 'НЕОБХОДИМОСТЬ'))
encr14 = (encrypt(data, 'РАЗОЧАРОВАННЫЙ'))
encr15 = (encrypt(data, 'ВДОХНОВЛЕННОСТЬ'))
encr16 = (encrypt(data, 'ЗАКОНОПОСЛУШАНИЕ'))
encr17 = (encrypt(data, 'ДОБРОПОРЯДОЧНОСТЬ'))
encr18 = (encrypt(data, 'МЕТАЛЛОКОНСТРУКЦИЯ'))
encr19 = (encrypt(data, 'РЕНТГЕНОДИАГНОСТИКА'))
encr20 = (encrypt(data, 'НЕБЛОГАЖЕЛАТЕЛЬНОСТЬ'))


# print(encr)
print(index_of_coincidence(encr2, alphabets))
print(index_of_coincidence(encr3, alphabets))
print(index_of_coincidence(encr4, alphabets))
print(index_of_coincidence(encr5, alphabets))
print(index_of_coincidence(encr10, alphabets))
print(index_of_coincidence(encr11, alphabets))
print(index_of_coincidence(encr12, alphabets))
print(index_of_coincidence(encr13, alphabets))
print(index_of_coincidence(encr14, alphabets))
print(index_of_coincidence(encr15, alphabets))
print(index_of_coincidence(encr16, alphabets))
print(index_of_coincidence(encr17, alphabets))
print(index_of_coincidence(encr18, alphabets))
print(index_of_coincidence(encr19, alphabets))
print(index_of_coincidence(encr20, alphabets))
```

```python
import operator
from collections import Counter

alphabets_2 = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
most_common = 'оеаинтслрвкмдпуяыьзгбчйжхшюэщцфъ'

with open('test1.txt', 'r', encoding='utf-8') as file:
    data1 = file.read().replace('\n', '').replace(' ', '')


def lettc(data):
    all_freq = {}
    for i in data:
        if i in all_freq:
            all_freq[i] += 1
        else:
            all_freq[i] = 1
    return all_freq
```

```
def chunk(string, s):
        return [string[i::s] for i in range(s)]


print(chunk(data1, 17))


def index_of_coincidence(ciphertext):
    N = len(ciphertext)
    freqs = Counter(ciphertext)
    freqsum = 0
    for letter in alphabets_2:
        freqsum += freqs[letter] * (freqs[letter]-1)
    IOC = freqsum/(N*(N-1))
    return IOC


def ioccalc(list):
    li = []
    for elem in list:
        num = index_of_coincidence(elem)
        li.append(num)
    return sum(li)/len(li)


def count(data):
    lis = []
    for i in range(1, 32):
        elem = ioccalc(list(chunk(data, i)))
        lis.append(elem)
    maxelem = max(lis)
    return lis.index(maxelem)+1, maxelem, lis


def findmostcom():
    word = ""
    for i in list(chunk(data1, 17)):
        k = (max(lettc(i).items(), key=operator.itemgetter(1))[0])
        word += k
    return word


print(findmostcom())
red = chunk(data1, 17)
print(count(data1))
print(ioccalc(red))


def decr(text, letter):
    new = ""
    for x in text:
        z = (alphabets_2.index('p') - alphabets_2.index(letter)) % 32
        y = (alphabets_2.index(x)-z) % 32
        new += alphabets_2[y]
    return new


for i in most_common:
    print(decr(findmostcom(), i))


def decrypt(c, k):
    plaintext = ""
    i = 0
    for x in c:
        if i == len(k):
            i = 0
        p = alphabets_2.find(x) - alphabets_2.find(k[i])
        if p < 0:
            p = p + 32
        plaintext += alphabets_2[p]
        i += 1
    return plaintext


print(decrypt(data1, 'возвращениеджинна'))
```

Висновок

В ході роботи було отримано практичні навички роботи та аналізу підстановочних шифрів, зокрема з шифром Віженера та шифром Цезаря.