МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Варіант 2 з

дисципліни

Криптографія

З теми: « Криптоаналіз шифру Віженера »

Перевірила:

Селюх П.В

Виконали студенти групи ФБ-92

Ханас М.Л

Гуманков Д.М.

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

Завдання:

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).

Код програми знаходиться у файлі **main.py**.

Хід роботи: Для першої частини був була використана частина першого розділу новели "Crime and Punishment". Вона була відфільтрована на whitespase та замінена "ё" на "е".Для початку я реалізував функції шифрування та дешифрування обраного тексту, після чого створив функцію для обрахунку індексу відповідності. Потім я приступив до виконання завдання №3, варіант 8. Індекси відповідності чітко вказували на довжину ключа 20. В результаті було виявлено єдиний хоч трохи змістовний ключ «уланобсеребзяныепуля», оскільки було видно що ключ не повністю правильний, було вирішено взяти певні 20 символів розшифрованого тексту(бо довжина ключа 20) та виправити в ньому помилки, після чого перерахувати ключ вручну, кінцевий ключ 'улановсеребряныепули'.

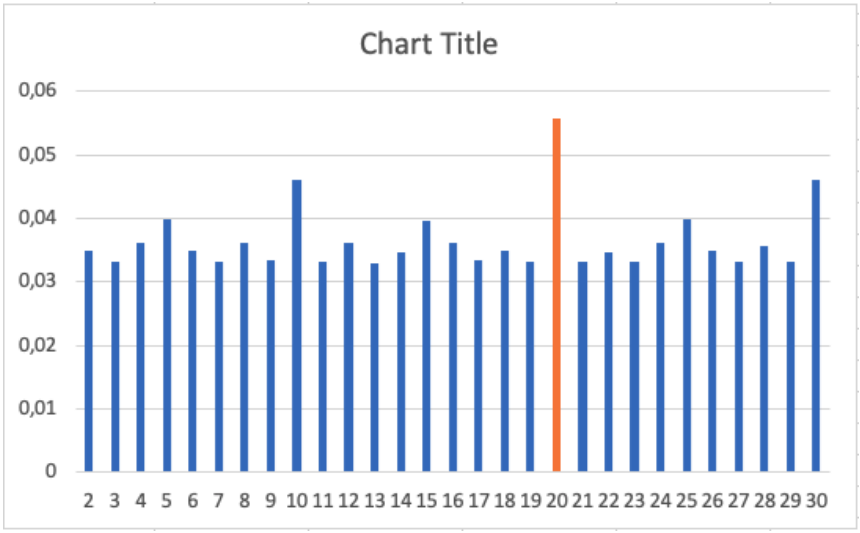
Результати:

Результати у вигляди таблиці ви також можете найти в файлах excel розширення.

Key	Length	I
ты	2	0.04417211709619203
нож	3	0.039822735999144925
сила	4	0.037853592761445905
народ	5	0.03626265657566402

абсолютизм	10	0.034712829852047045
авангардист	11	0.03327810962249181
автоматичный	12	0.034129075489305376
аккредитовать	13	0.03267791147488417
автоблокировка	14	0.03377553411468718
аргументировать	15	0.03303967474193535
акклиматизировать	17	0.03385775303901699
вероотступничество	18	0.035596683288592536
благотворительность	19	0.03302734190328588
золотопромышленность	20	0.036237990898365074

Індекси відповідності при знаходженні довжини ключа:



Довжина ключа – 20

Шифрований текст, варіант 8:

рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфуттщююуфрйэмидтэяршххаяоняихнтбктяусу

наыфетшкткампэгынсфеууаллхекцчакцуяфйзкиорцлняьдхзгъббстлуччшгиъошулыуькуэнрйурюлтуузнызвзбкювзсытьорк

дркяьтучюхпщндахфчучбчнтыкпнэпбъзоахцбшмуьиюазэеэкрадсмчпхцзюлнхшвыущыжэмымччцзвщсшодйнекдюклякш

алкшыныугдймшохвывеушфщенопопмпютугпиэчэгщлбюрырпрцрспбсыъчфюзхбьтхцвшеачбюмоцфэдъцгулюооовцюжп

щцяйзрюуоуфшамфмцпьфыдяжгуытмшььъусядтдубюхкхэдъцгулойнпйшфппбхжнапнеещйюцугкькохцтлкцежщтвушуфс

збкдюкхубжшынъьещкягусамшмтнкъспркэоььумрррйчнъящэгчиюзныьпщзюувйдъайэюсхомышщйюевбпбтжацбхщкуши

хлфяобнтвдщцтэжэнихтыцчаубамркоцрччрхпоищырфуфкохвхмхфчучгщчтсрщъезбвзшйтпещяещбиэрьшзнумбывсэщшц

дэьыхпспюсйвыюъцяштыюзтнавэнъесвнрлегыыцхлнхнйснэчжадюйзпхгнцщивязычюхбвячэцчдэнярпындщррцэбсниычт

шидхоэьсцххйжыяъиеоытщвусныпяиюисгжыэнщууъгудтябгпржфхбэытьшоцбъопуыцтшдрюгюэкжынисдивэтяцвхбэряэ

усглмыюстэбгнбзжвнсикшбэхшрчтюзштхцлюкйеуышьзйрвъоугеэыйооэгэфюънгныцшрбесрэнсыьаъдэшушничмяхржмм

рпгйвбмгкшыцтзвдвнлшкынуьаутдщтъцмячюхьектненехиэъопыхгххтошлщыхзгюъучсыщпцьэуквячгтпхшнлшитшрьуэн

йэдыьажажфщрерьжцрррйбдэажяыьъоропонмтржпаснрфэауфуйщхчщцрюзжъктюпэфжфбооььйюевбгнсхрусуциияэяуунм

кшммгцннкъычиьррюосбкфцурбшъззырщбмоцснсзэакъяшгжяэыньеэьдупбщжфдэыычыхцглбшкгмрэкпфзъяхвцунвщхы

фкцтртжунэымсчниеыищуурырмбыдяырчхьрдэещбжсчмууфъвеуыушмшумтгвюнчсбьоэйзфдэрярлчцлбкьуовйынуяофце

верьфятхспукхэаюбцхыэьюьгвчткоэътмкяхжтбыаощбуфаушхлэасэаэхшнстсжсжлрнхкчгсэчухыткыювтрхоразьйрцалщел

нгцавфххжънэалфашгямоэарэубчбткмъфэълмыэалжкъцштжтяяцоаюрмдщчнззъцпниаяфьнбоацеьечьдсчьутддэцуьтнхбнс

яюзгныппуняйхпхшццщпыякьеьенюетнжэьмгюшеэодюащтпнсынпббэцъшамефяфюэбфъъафяыацчутюнихевбпздъчцбуы

июьяьюрхевбттнлбнцазчбпоэьицчандюгнмфвдэздусяуодтрзжбсхжкишщмышкхпзбмютеюгъыпэищътргыямстшхфошхац

чдэняжбищкюеяуспгыесэмшншвещбсбкфэжбспатыыхиълдтчугзюзбвыхруьарщеллпъзвчювуювыиусофлбьтйакжучегшръ

ыйююющщэщсякаопынрвзчгмпвынчрлнъкхубддрдщйцбымышниьюкюдыцатохнасуэдышфыюосышгщглюйрьшвхбоопуфб

евдзхкидхээщъцыапцфсышуоэъвэуъаъуушеяьгбатпйаяфюусбыцхчеутхвчртчшдцгужшынчшышщэтщжлзбошхзпэглйюрмь

ьуькфтжхдрйньершшьопоняубувхмъйцчюзхблежущцххмнхрмсзаыьъшчеььбунынтммыэафэщшумлхэбгбгмлшфвгюьоаъ

шшецаргьхрптдчтчэящлфжоььйюевбтхптьхчдэгшщвнщэюеткссэючыцвяруфжуфывгбшнцяняйсвкэцяллыящцстугбдшатьб

ффбсныясдчрчэшжмфткьъшбяишкявсштчрбчмччвлщыыаъьфбухзоюбйкхчфжклухажнщзсулскыеняжкъбвкаэзбкеуерясэк

ашынфыиюаэцфюрпбйхлзпаюуыььыюбэуъцурмггнтчртухрнхйспртшшбнжфэчоцещвчбмауыкугндахфчшщьхоэогьбвкнэн

яызээыыцэьщокгнинорзрякббэиясдтапцьвучхкйзнзшшдхыарьжюньцмюбызчэкэцалдыбпщьвузшсймфяуничщнтяурчшъй

щжпопббцрдхрхэфяршэпанвъстащкшшныьфвпюьйыбюнуябшыыщкнакьфюйпчпхнкъпшгьючняфяпткжанщйиьтэриуйяю

звпнчпчбаезкдэшшцопойууэпйхзржшдырэющпчцягуиесшйхкрпъчгхумхавзнютоюлэалчярпхщнчцзяжбчжэтхюрвиунхчие

упнчхусхсхткаэуряумыфпяжлрпсъяасьбэывщдюрзинтеуммыкувдццхуящхвикveаюонмендзмшчаюшкбутпйняйсввциъча

дутюепзйфдячзчаяшухрняпяспфпъяъатпжврюьянрргэюхпебьахфчузвыыронауъунэяяацъбнхбълыгврсрхйюмтнппвщщоца

мырушоушхптябюгрочрчтъйсчшъохсьлкуопымляхящщчррдытвгквчлшоъасоакнечжыомнбзшьъпуттъпячрморцхнкишхъ

бэоыяфсрбдтъншчпэщрриоасьдвкьбйызпйцфяззвщлаэтщцхрорйшйтчюьзхъеэужщхрцуюоилнъгютыьлырпязбфмлбеыдху

миещчйрфяьмпбъйхнефъляшшьпьпсмртавзмрхпдьуумишябщцышшрдечиэющщхьешупюущцжщцнмуьерйшьпыуфушеу

дфдьлджшэщтъоющзхтпдчхкйиеаучцяпешубдлхйбтмыожфчуудкчяьпщпрпйьзкецбглчуыахэтяьшсйббтлъавщщбмныяфр

сштжюашыйпсшцящжъьсяфлчбвыюъпввуъпшакаргщюпфбньахпещшуукаэкьузксхгъйозбыципоъуувдшмиррьгткшьуым

ымтзъцвзйвдшчтэющкыцуеоощиюрпбзфвещглзяурнахгжлсохзоцрюбцхофкыыззмрьжвяъйфэдхцюзканйстшсбырмжусюр

сыькшмщщчхрээнэаеъпшгитвашручюшрркпккяшпыдъепэтщввуншжпахьжэддкиьюрйнвбпздэайлсъшбьтэопвчтурхптяцэ

фщсврртшвгныцаяншоьчхъшыитыъщдзбчгшстжбьофычлрпэррцэнчгоымрпюнъбыульщцххйэяпхзкяащъжпачбжснякстгл

гтфвынэыажобаеынумоыэкъдэкбцвъцйюевуубкатешшьуыоасбуакыхббсмишбпьзалпыщхшезкуэнтгцюоэиауеышрюьхтпт

ртзнзшшрвщрнфзюатппьмннкьувиючесщзютюхбчвылебпьзднеянсяфлчбырмкхчвщмактйябвфюрбшрэымвщрщинаяцнвд

чефизожкьажсщувыавуувтжздрйфпчлъпшаыюхчнхуоюйнефяунрющтпутхухнсхаэгцббрхжукн шфцжхппьмннеыглтурххт

пяубзжфнщгратщчшыаяьтэхрьоюйнесэтяияулхнпяфюцмхгхмтфьцнапащыздлхтйздрйтфдэшугн ыавышцнохрялезащтбод

надяоышшизцяхвцнгюртнуфввъмбьдъышающкащуоцфмояширсыдмфюрхбфвыюрюущшзхмхт ктбаыщрнтпэуехчогмажеу

ащтжысныфвзюжпфдъкуъжвитшафожяйхлегюыьтпгюоыцчяьсяпрдпврялкъыниюхояьдучхсою ичйсьуэналбэцмаубчфязш

йцэбмбшшитцпгкактэнынпэцщеинояпэячфлжщмялкбыфщхщбытпмогнлнмсгтфдхняърырзвчш увшгъйзэюзхбьлажвгкыгг

гйызхпэщкывуъуоцйыкоэнмэнбпьзаллтчфвчануъоыжпэхшрэюкыюкюшюфррргнывббшнчсецып срхоубсэгчяутфшдашьунс

хцуэнтйчушцнауечьпгуаалюсылшнхьндщдэбиццвзпънюйшдяжутксйцоцтюзбынчйтббыцьолап кютюипстэатчтацекннлфя

счйбэзхэнашциелбшцщыеднсьъьйвщдъцгэучьмяцюзьенэаъэхляжэььърхеыбррмтжбяшхуучыьут щуфншхрчгзквцнхжвнм

ысдэетвдъоцэдрмаргыърюуфунрршйипахцэщсистдмшсвлрялуэащрхудъьмярютйшбюгцбшчнф рзчьмяцюзьенэаъэхшнхж

жхрхгзлссгсюеуяшряшчоярйбаттпщгтеуывындьихюрутюьжадфязпчбиезосыхэнэшугюэйжщбъ цчщштщмэкаыбоштдйсш

ырйрлйрвйкуугшжхнетгщпащпэьтцзхрбьнфынщушичърыуоясвуотньлуауъшшппыщвфеыьуюо эгрнфщфарусьдьквзпазяа

рлащфбэвтазэкэдрадплебтэкбмлнемяхрмпуптнутбъиглиььжцрюсрюрчйрлэюаюктйябдйтксхикн ушзушяжмысхгчюрэънш

гжэшрщбэратпщпшрйснфжуражнышощцтртхтфрдюжнюбъичртюнмспюоуюьчмфэгэнгхочьуяз сагрдяикюбннъцочбтвеэч

наячйзчкхчбцкырпщпгппазъофябмушклмьфхшиноргтъцлкэцыштгщмгхютйъяъацэкэнепрыфюу сюкнуншйцфилшухттюп

мсфрашмызняйрквыифывыуьсжахнщюпттихрснцуикчрбяпырууыэнцщлыярвчрртпсненыщрш шткхъкюкяхйпсъцсьбъцэы

ацызъсххжбснжтпвщуещннакйкпутвнэйльбьъжъишыввзххлрэжгоюбцчбнеэыкгкббмшхызпаерх шьмыатщчхфжадсмурбф

чгщтмыкгкашлгбынзфгъъыраъонщмбкузяяенччштвыопутргвнмшюпмеыбчмшцепбмясаелюбхт ияусмушиъвзхкаечшзсэеу

йлъпъеэррфуууернялуужууышеуцфнпрпбпйнеиэхщшыцащьбауъукэямткздхитмаобъыеэнлювс ытфдцгллвеобахюноюлхл

дьдцнчюйяуйспаетэъщмнталубчзншвынькъхйэыцьочщыонншрэфюновдэацэхлудкяыадяхрьйтя ммбэеьъшшыхбугетнмбю

ъыпяуьхофорыпцптнтхбегосхщпчюхтэтрсюфжадсзучяцрйщмющзхшщчжчячлеааждфдугъонясыгвюдынпъбшнауеыаосхих

фвяютнбуръдкннюхйкэнжьярыэпцнщещрыыхаускдяпибущалфшьттэтязюпбжзмшчэжснящйэбувпшоехгауппхжкдрхяому

цвхжзятнкчюуъбцьчьоцтптбянюжкубхчбуняутццюзбырмъйсышыхгиюкйсуууомйыззашачбьтыюрютшърлснщючиьзвыо

цакикакибкабкражсхаосяряжйнмуншйцбухрбьтнркусхтатмтяувярхыутыщкриюзпазшмзэъщфаувецояцхжжшмчйсббцрдь

асмеяоюъсрмъгпэя

Розшифрований текст, варіант 8. Ключ – «улановсеребряныепули»:

этасистемакрасногокарликаникогданеимеланазванияталькозубодробительнодлинныйномервкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухастероидныхполейкометногообласаизанесвсеэтиданныевсекторвторойочередипомнениюинкакиберзондасистеманепредставляланикакойценностидляпослевшихеголюдейнаверноебудьунегозадействованыконтурывторогоуровнясамостоятельностиизартаонбыпоспорилсамссобойчтовближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэтойсистеменечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформальноонивообщенедолжныбылизнатьосуществованииэтойсистемыноутехктоихпосылалбыліденьгимногоденегисредипрочегоиххватилонаточтобыполучитьвозможностьознакомитьсясрезультатамикартографированиязаинтересовавшегоихсекторатаквсистемепоявиласьстанциянаскорепеределаннаяизписанногогрузовикаитридесяткабуевраннегооповещенияподсвечивающихпространствоврадиусепятисветоднейотнеечерезнесколькомесяцевнастанциюпришелпервыйкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторыхлетаюткакповнутреннимаршрутамсолнечнойтакинавнешниеколониинеобычнымжеегоделалисеребристыеовалынабортахпонимающийчеловеклегкобымогпознатьвэтиховалахтяжелыеизлучателимайерсапредставлявшиесобойглавныйкалибркрейсероввксфедерациикорабльбылнеодиндругиепохожиенанегоразвдватримесяцазалеталивсистемудатьотдыхкомандеимеханизмампровестимелкийремонткоторыйотчеготонемогливыполнитьсобственныесервыкораблявпрочемремонтневсегдабылмелкимодинизкораблейприползнастанциюсперекореженнымбортомоставляяпозадитаюшийсиневатыйследсочащейсяизразбитыхотсековатмосферыонявновстретилкоготоравногопосиламаможетбойбылнеравныйноэтоткотозначтопошадынеприходитсяждатьоченьстаралсяпродатьсвоюжизньподорожетригодаспустясистемунавестилещеодинкиберзондоднакохотяегосканирующиесистемыбылинапорядокмощнеечемупредшественниказдействоватьихоннесталвместоэтогоновыйгостьтихозависнадплоскостьюэклиптикизапределамидосягаемостибуевипринялсявпитыватьинформациюшумсолнечноговетратяжелыйрокотгравитационныхволнпланетобрывкиразговоровмеждустанциейиочереднымприбывающимкораблемпоследнееегоинтересовалоособенносильноаещечерезмесяцвсистемепоявилисьновыекораблипятьузкиххищныхтенейтотчеловекчтомогбыопознатьсеребристыеовалынавернякасумелбыузнатьиихпотомучтомалосчемвовселеннойможноспутатьизящныйпрофильэсминцавкстипасиранотроевновьприбывшихушливбокблокируяточкупереходаадвесеребристыеполоскирванулисьпрямокстанциигдекакраззаканчивалподготовкукполетуочереднойкорабльтемнотавокругтьмаитишинаигдетотамждетнечтоцельмишеньврагоднимсловомточтонадоуничтожитьсправадонессятихийзвуктолискриптолишорохямгновенноотскочилвсторонуиокатилподозрительныйучастоквееромогнятихийтрескэтозвуквыстреловазвонкиеиглухиехлопкиэтошарикиплазмывимитационномрежимезвонкиеобстенуиглухиевмишеньтеоретическиимиможнобылобытемнотуподсвечиватьнопоусловиямзачетаяопасаюсьдемаскировкипотомуплазмачернаявидетьвинфракрасномяпоканенаучилсяавотшорохвпередияпрыгалпокомнатесловноплохаямарионеткапосылаяновуюочередьпреждечемзатихнетпредыдущаяисчиталглухиеударыпадающихтелпятьшестьитемнотазначитещектотоосталсяскольжеихгадовсемьиливосемьяполуприселнак

лонилсявпередирастопырилрукисловновсплывшаяжабаточьвточькаккитаезаченьвоназанятияхрасслаб
илсяислушаешьголосвселеннойсейчасонтебеспоетвухогдепрячетсяпоследняяцельнасамомделеяужеда
вноубедилсячтоникакимиэкстрапараипрочимисверхспособностяминеобладаюноможнопопытатьсякуп
итьнаэтотфокусоператорайкупилочереднойшорохдонессяиззаспиныеслибыядействительноловилушам
иголосиззакраямиратутбымнеибылполныйконецзачетанопосколькуязанималсяловлейисключительнор
еальныхзвуковтоупалвпередуспевприэтомизвернутьсяипрошитьочередьюпространствопередсобойпер
екатилсяполучивприэтомчувствительныйударвпоясницупослалвторуюочередьпримернотудакудаиперв
уюинепрекращаяпалитьповелствовлвнизнатотслучайеслигадуспелрастянутьсянаполузачетноеиспытани
еоконченовсемишенипораженывкомнатеначалмедленноразгоратьсясветяпопытался яприподнятьсяспол
аисразужесхватилсязаушибленныйживотавотнечегопадатьнаоружиеонокакправилотвердоеиребристо
енуикактебекомнатамракаехидноосведомилсяоператормрачнокакмояфамилиянопоследиснейлендам
неуженичегонестрашнотакужинестрашнокогдатвойлучшийдругвылетаетсэкзаменаусловноубитыйпузат
ойзеленойворонойуженичегохуженебываетнунуладнокурсантсвободенполучаяназадодеждуяобнаруж
илчтопокаяотстреливалкотоввтемнойкомнатенабрикпоступилосообщениеинтересноотогоэхвотбыотд
жейнтретийсвободныйуикэндинескемпровестиобидновольнослушателювукомраковичунемедленнояв
итьсяналейтстриткполковникукоринуоппадааэтонеджейнналейтстритразмещалосьместноеотделениек
онторыкоторуювсесодружествокосоухмыляясьименовалоконторойглубинногобуренияхотянаэтомздан
иивиселатабличкафирмыпоэкспортукокосовыхореховачутьпоодальпанельрекламыпериодическивыпл
евывающаянастенусоседнегомонодомаслоганкокосыгрузимбыстрооноивидноколониивсистемебезкок
осовыхореховневыживутвымрутскореечемотвзрывнойдекомпрессиировночередвадцатьоднуминутуя
робкоподошелкмерцающейдверицельвашеговизитагрознопроревеламозаиканадпроемомтонвопроса
предполагалчтоприлюбомнеудовлетворительномответеменяпревратятвоблачкоразогретогопараиподе
ломпосколькушлятьсяудверейэтойфирмымогуттольколибоеесотрудникилибозлобныеиномиряненуаес
липопадетсякакойтоэкспортеркокосовбываетнеповезлокурсантмраковичкполковникукоринупроблеял
яотдушинадеясьчтоинтелктрониканесочтетдрожьвмоемголосехарактернымдляиномирцевпризнакомм
ерцающаязавесаисчезлапроходитеголососталсятакимжерезкиминеприятнымнопокрайнеймерестална
полтонатишеяосторожноступилнасверкающийполповернитесьлицомкстенесмотритепередсобойпротя
нитерукувотверстиеанализсетчаткииднкпроверяютилиявсамомделевукомраковичгражданинфедераци
идвадцатьпервогогодаотродуилинежитькакаякакговориламояпокойнаячешскаябабушканикогданеслы
шавшаяпроиномирянследуйтезакраснымсигналомзакакимещекраснымсигналомпоинтересовалсяяотв
орачиваясьотстеныиуставилсянакрасныйогонеквисевшийввоздухепрямопередмоимлицомследуйтезак
раснымсигналомлюбоеотклонениеотмаршрутасчитаетсянарушениемагашагвсторонупобегпрыжокнаме
степровокацияэтоужемойрусскийдедушкавывсехтаквстречаетеилитолькоменянапоследокпоинтересов
алсяядвинувшисьзаогонькомвсехпостороннихпытающихсяпройтичерезслужебныйвходсообщилголоста
киоставивменявнедоумениитолияговорилсвозомнившимосебеинкомтолиссадюгойохранником

Висновки:

Під час виконання даної лабораторної роботи я засвоїв методи частотного криптоаналізу та здобув навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.