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

Варіант 8

Виконали: студенти групи ФБ-01

Курило А. В. і Шевченко Д. М.

Київ – 2022

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).

Хід роботи:

source.txt – самостійно підібраний текст для шифрування

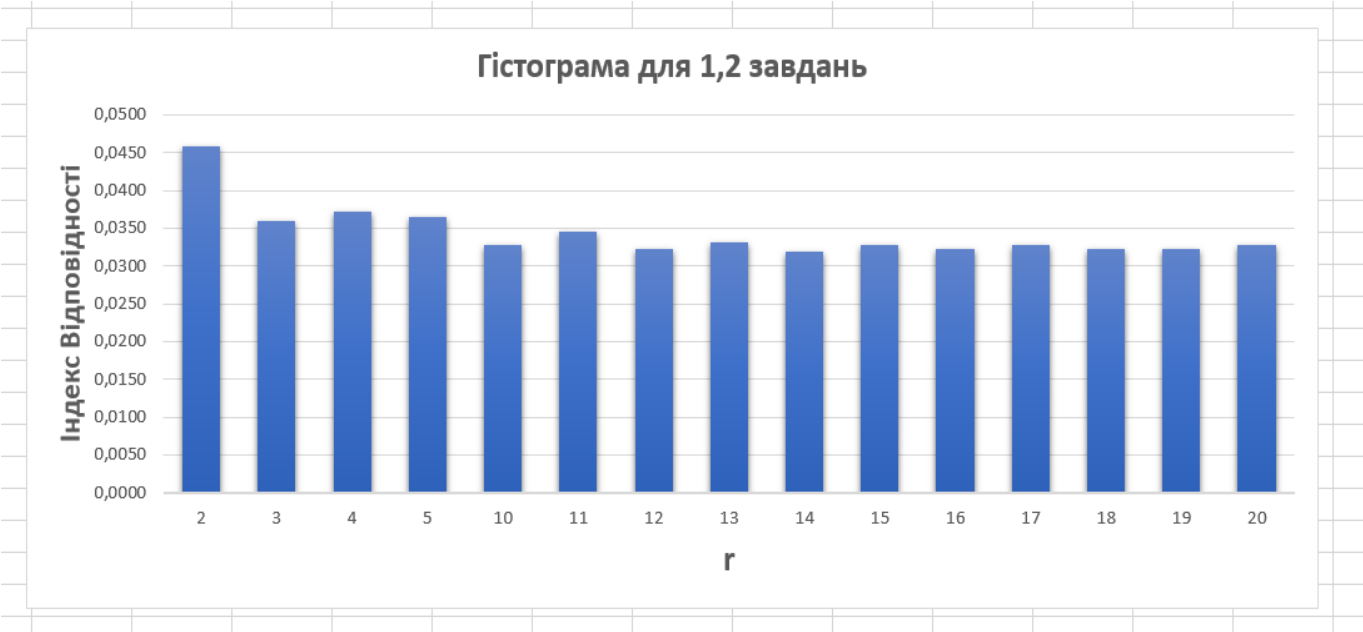
var_8.txt – зашифрований текст для 8 варіанту

lab2_crypt.py - код програми

Таблиця для 1,2 завдань

r	Індекс В.	Ключ
2	0.0458648	ке
3	0.0359596	длу
4	0.0371528	язхв
5	0.0365249	фухжс
10	0.0328513	ътуйжгщоас
11	0.0345249	оучхжпоугцч
12	0.0321609	дгктсячцщпфэ
13	0.0331540	аьбкущяфауеой
14	0.0319582	гкольфвапкушщд
15	0.0328225	золмиейжбчугвтш
16	0.0323297	хъяеьщувонтчзетм
17	0.0328501	аотугшахйъвапнгтщ
18	0.0321821	кюсвщгпрйкувздшлтю
19	0.0322709	уъафгмивщлшдцчаьенв
20	0.0327700	епвдштмрвнуцрхцсмнга

Порівняння значень (без індекса для відкритого тексту)



Порівняння значень (із індексом для відкритого тексту)

Індекс відкритого тексту - 0.053794966728373445

Таблиця до 3 завдання

r	Індекс В.
1	0.03321391919372439
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

Звертаємо увагу на значення, що схиляється до теоретичного значення I для даної мови, при цьому саме воно найбільше відрізняється від значення індекса, що відповідає мові з рівноймовірним алфавітом.

Тому довжина шуканого ключа буде мати значення 20.

Зашифрований текст для 8 варіанту :

рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфут
тщююуфрйэмидтэяршххаяоняихнтбктяусунаыфетшкткампэгынсфеууаллхекц
чакцуяфйзкиорцлняьдхзгъббстлуччшгиъошулыуькуэнрйурюлтуузнызвзбкюв
зсытьоркдркяьтучюхпщндахфчучбчнтыкпнэпбъзоахцбшмуьиюазэеэкрадсмчп
хцзюлнхшвыущыжэмымччцзвщсшодйнекдюклякшалкшыныугдймшохвыве
ушфщенопопмпютугпиэчэгщлбюрырпрцрспбсыъчфюзхбътхцвшеачбюмоцфэ
дъцгулююовцюжпщцяйзрюуоуфшамфмцпьфыдяжгуытмшььъусядтдубюхкхэд
ъцгулойнпйшфппбхжнапнеещйюцугкькохцтлкцежщтвушуфсзбкдюкхубжшы
нъьещкягусамшмтнкъспркэоььумрррйчнъящэгчиюзныьпщзюувйдъайэюсхом
ышцйюевбпбтжацбхщкушихлфяобнтвдщцтэжэнихтыцчаубамркоцрччрхпоищ
ырфуфкохвхмхфчучгщчтсрщъезбвзшйтпещяещбиэрьшзнумбывсэщшцдэъыхп
спюсйвыюъцяштыюзтнавэнъесвнрлегыыцхлнхнйснэчжадюйзпхгнцщивязыч
юхбвячэцчдэнярпындщррцэбсниычтшидхоэьсцххйжыяъиеоытщвусныпяиюи
сгжыэнщууъгудтябгпржфхбэытьшоцбъопуыцтшдрюгюэкжынисдивэтяцвхбэр
яэусглмыюстэбгнбзжвнсикшбэхшрчтюзштхцлюкйеуышьзйрвъоугеэыйооэгэф
юънгныцшрбесрэнсыьаъдэшушничмяхржммрпгйвбмгкшыцтзвдвнлшкынуьау
тдщтъцмячюхьектненехиэъопыхгххтошлщыхзгюъучсыщпцьэуквячгтпхшнлш
итшрьуэнйэдыьажажфщрерьжцрррйбдэажяыьъоропонмтржпаснрфэауфуйщх
чщцрюзжъктюпэфжфбооььйюевбгнсхрусуциияэяуунмкшммгцннкъычиьррюос
бкфцурбшъззырщбмоцснсзэакъяшгжяэыньъеэьдупбщжфдэыычыхцглбшкгмр
экпфзъяхвцунвщхыфкцтртжунэымсчниеыищуурырмбыдяырчхьрдэещбжсчму

уфъвеуыушмшумтгвюнчсбьоэйзфдэрярлчцлбкьуовйынуяофцеверьфятхспукх
эаюбцхыэьюьгвчткоэътмкяхжтбыаощбуфаушхлэасэаэхшнстсжсжлрнхкчгсэч
ухыткыювтрхоразьйрцалщелнгцавфххжънэалфашгямоэарэубчбткмъфэълмыэ
алжкъцштжтяяцоаюрмдщчнззъцпниаяфьнбоацеьечьдсчьутддэцуьтнхбнсяюзг
ныппуняйхпхшццщпыякьеьенюетнжэьмгюшеэодюащтпнсынпббэцъшамефяф
юэбфъъафяыацчутюнихевбпздъчцбуыиюьяьюрхевбттнлбнцазчбпоэьицчандю
гнмфвдэздусяуодтрзжбсхжкишщмышкхпзбмютеюгъыпэищътргыямстшхфош
хацчдэняжбищкюеяуспгыесэмшншвещбсбкфэжбспатьыхиълдтчугзюзбвыхру
ьарщеллпъзвчювуюовыиусофлбьтйакжучегшръыйююющщэщсякаопынрвзчгмпв
ынчрлнъкхубддрдщйцбымышниьюкюдыцатохнасуэдышфыюосышгщглюйрь
швхбоопуфбевдзхкидхээщъцыапцфсышуоэъвэуъаъуушеяьгбатпйаяфюусбыц
хчеутхвчртчшдцгужшынчшыщэтщжлзбошхзпэглйюрмььуькфтжхдрйньершш
ьопоняубувхмъйцчюзхблежущцххмнхрмсзаыьъшчеььбунынтммыэафэщшумл
хэбгбгмлшфвгюьоаъшшецаргьхрптдчтчэящлфжоььйюевбтхптьхчдэгшщвнщэ
юеткссэючыцвяруфжуфывгбшнцняйсвкэцяллыящцстугбдшатьбффбсныясдчр
чэшжмфткьъшбяишкявсштчрбчмччвлщыыаъьфбухзоюбйкхчфжклухажнщзсу
лскыеняжкъбвкаэзбкеуерясэкашынфыиюаэцфюрпбйхлзпаюуыььыюбэуъцурм
ггнтчртухрнхйспртшшбнжфэчоцещвчбмауыкугндахфчшцьхоэогьбвкнэняызэ
эыыцэьщокгнинорзрякббэиясдтапцьвучхкйзнзшшдхыарьжюньцмюбызчэкэца
лдыбпщьвузшсймфяуничщнтяурчшъйщжпопббцрдхрхэфяршэпанвъстащкшш
ныьфвпюьйыбюнуябшыыщкнакьфюйпчпхнкъпшгьючняфяпткжанщйиьтэриу
йяюзвпнчпчбаезкдэшшцопойууэпйхзржшдырэющпчцягуиесшйхкрпъчгхумха
взнютоюлэалчярпхщнчцзяжбчжэтхюрвиунхчиеупнчхусхсхткаэуряумыфпяжл
рпсъяасьбэывщдюрзинтеуммыкувдццхуящхвикveаюонмендзмшчаюшкбутпй
яняйсввциъчадутюепзйфдячзчаяшухрняпяспфпъяъатпжврюьянрргэюхпебьах
фчузвыыронауъунэяяацъбнхбълыгврсрхйюмтнппвщщоцамырушоушхптябюг
рочрчтъйсчшъохсьлкуопымляхящщчррдытвгквчлшоъасоакнечжыомнбзшьъп
уттъпячрморцхнкишхъбэоыяфсрбдтъншчпэщрриоасьдвкьбйызпйцфяззвщлаэ
тщцхрорйшйтчюьзхъеэужщхрцуюоилнъгютыьлырпязбфмлбеыдхумиещчйрф
яьмпбъйхнефъляшшьпьпсмртавзмрхпдьуумишябщцышщрдечиэющщхьешуп
юущцжщцнмуьерйшьпыуфушеудфдьлджшэщтъоющзхтпдчхкйиеаучцяпешуб
длхйбтмыожфчуудкчяьпщпрпйьзкецбглчуыахэтяьшсйббтлъавщщбмныяфрс
штжюашыйпсшцящжъьсяфлчбвыюъпввуъпшакаргщюпфбньахпещшуукаэкьу
зксхгъйозбыципоъуувдшмиррыгткшьуымымтзъцвзйвдшчтэющкыцуеоощиюр
пбзфвещглзяурнахгжлсохзоцрюбцхофкыыззмрьжвяъйфэдхцюзканйстшсбыр
мжусюрсыькшмщщчхрээнэаеъпшгитвашручюшрркпккяшпыдъепэтщввуншж
пахьжэддкиьюрйнвбпздэайлсъшбьтэопвчтурхптяцэфщсврртшвгныцаяншоьч
хъшыитыъщдзбчгшстжбьофычлрпэррцэнчгоымрпюнъбыульщцххйэяпхзкяащ
ъжпачбжснякстглгтфвынэыажобаеынумоыэкъдэкбцвъцйюевуубкатешшьуыо
асбуакыхббсмишбпьзалпыщхшезкуэнтгцюоэиауеышрюьхтптртзнзшшрвщрн
фзюатппьмннкьувиючесщзютюхбчвылебпьзднеянсяфлчбырмкхчвщмактйябв
фюрбшрэымвщрщинаяцнвдчефизожкьажсщувыавуувтжздрйфпчлъпшаыюхч

нхуоюйнефяунрющтпутхухнсхаэгцббрхжукншфцжхппьмннеыглтурххтпяубз
жфнщгратщчшыаяьтэхрьоюйнесэтяияулхнпяфюцмхгхмтфьцнапащыздлхтйзд
рйтфдэшугныавышцнохрялезащтбоднадяоышшизцяхвцнгюртнуфввъмбьдъы
шающкащуоцфмояширсыдмфюрхбфвыюрюущшзхмхтктбаыщрнтпэуехчогма
жеуащтжысныфвзюжпфдъкуъжвитшафожяйхлегюыьтпгюоыцчяьсяпрдпврял
къыниюхояьдучхсоюичйсьуэналбэцмаубчфязшйцэбмбшшитцпгкактэнынпэц
щеинояпэячфлжщмялкбыфщхщбытпмогнлнмсгтфдхняърырзвчшувшгъйзэюз
хбьлажвгкыгггйызхпэщкывуъуоцйыкоэнмэнбпьзаллтчфвчануъоыжпэхшрэюк
ыюкюшюфрргнывббшнчсецыпсрхоубсэгчяутфшдашьунсхцуэнтйчушцнауечь
пгуаалюсылшнхьндщдэбиццвзпънюйшдяжутксйцоцтюзбынчйтббыцьолапкю
тюипстэатчтацекннлфясчйбэзхэнашциелбшцщыеднсъъйвщдъцгэучьмяцюзье
нэаъэхляжэььърхеыбррмтжбяшхуучыьутщуфншхрчгзквцнхжвнмысдэетвдъоц
эдрмаргыърюуфунрршйипахцэщсистдмшсвлрялуэащрхудъьмярютйшбюгцб
шчнфрзчьмяцюзьенэаъэхшнхжжхрхгзлссгсюеуяшряшчоярйбаттпщгтеуывын
дьихюрутюьжадфязпчбиезосыхэнэшугюэйжщбъцчщштщмэкаыбоштдйсшыр
йрлйрвйкуугшжхнетгщпащпэьтцзхрбьнфынщушичърыуоясвуотньлуауъшшп
пыщвфеыьуюоэгрнфщфарусьдьквзпазяарлащфбэвтазэкэдрадплебтэкбмлнемя
хрмпуптнутбъиглиььжцрюсрюрчйрлэюаюктйябдйтксхикнушзушяжмысхгчю
рэъншгжэшрщбэратпщпшрйснфжуражнышощцтртхтфрдюжнюбъичртюнмсп
юоуюьчмфэгэнгхочьуязсагрдяикюбннъцочбтвеэчнаячйзчкхчбцкырпщпгппаз
ъофябмушклмьфхшиноргтъцлкэцыштгщмгхютйъяъацэкэнепрыфюусюкнунш
йцфилшухттюпмсфрашмызняйрквыифывыуьсжахнщюпттихрснцуикчрбяпыр
ууыэнцщлыярвчрртпсненыщршшткхъкюкяхйпсъцсьбъцэыацызъсххжбснжтп
вщуещннакйкпутвнэйльбьъжъишыввзххлрэжгоюбцчбнеэыкгкббмшхызпаерх
шьмыатщчхфжадсмурбфчгщтмыкгкашлгбынзфгьъыраъонщмбкузяяенччштв
ыопутргвнмшюпмеыбчмшцепбмясаелюбхтияусмушиъвзхкаечшзсэеуйлъпъеэ
ррфуууернялуужууышеуцфнпрпбпйнеиэхщшыцащьбауъукэямткздхитмаобъ
ыеэнлювсытфдцгллвеобахюноюлхлдьдцнчюйяуйспаетэъщмнталубчзншвынь
къхйэыцьочщыонншрэфюновдэацэхлудкяыадяхрьйтяммбэеьъшшыхбугетнмб
юъыпяуьхофорьпцптнтхбегосхщпчюхтэтрсюфжадсзучяцрйщмющзхшщчжчя
члеааждфдугъонясыгвюдынпъбшнауеыаосхихфвяютнбуръдкннюхйкэнжьярыэ
пцнщещрыыхаускдяпибущалфшьттэтязюпбжзмшчэжснящйэбувпшоехгауппх
жкдрхяомуцвхжзятнкчюуъбцьчьоцтптбянюжкубхчбуняутццюзбырмъйсышы
хгиюкйсуууомйыззашачбьтыюрютшърлснщючиьзвыоцакикакибкабкражсхао
сяряжйнмуншйцбухрбьтнркусхтатмтяувярхыутыщкриюзпазшмзэъщфаувецоя
цхжжшмчйсббцрдьасмеяоюъсрмъгпэя

Значення отриманого ключа в результаті пошуку : 'уланобсеребзяныепуля'

Значення змістовного ключа : 'улановсеребряныепули'

Розшифрований текст :

этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительнодлинныйномервкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухастероидныхполейкометногооблакаизанесвсеэтиданныевсекторвторойочередипомнениюинкакиберзондасистеманепредставляланикакойценностидляпославшихеголюдейнаверноебудьунегозадействованыконтурывторогоуровнясамостоятельностииазартаонбыпоспорилсамссобойчтовближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявилисьвэтойсистеменечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализондформальноонивообщенедолжныбылизнатьосуществованииэтойсистемыноутехктоихпосылалбылиденьгимногоденегисредипрочегоиххватилонаточтобыполучитьвозможностьознакомитьсясрезультатамикартографированиязаинтересовавшегоихсекторатаквсистемепоявиласьстанциянаскороопределаннаяизсписаннногогрузовикаитридесяткабуевраннегооповещенияподсвечивающихпространствоврадиусепятисветоднейотнеечерезнесколькомесяцевнастанциюпришелпервыйкорабльэтобылстранныйкорабльсвидуобычныйдесятикилотонниксотникоторыхлетаюткакповнутреннимаршрутамсолнечнойтакинавнешниеколонииобычнымжеегоделалисеребристыеовалынабортахпонимающийчеловеклегкобымогопознатьвэтиховалахтяжелыеизлучателимайерсапредставлявшиесобойглавныйкалибркрейсероввксфедерациикорабльбылнеодиндругиепохожиенанегоразвдватримесяцазалеталивсистемудатьотдыхкомандеимеханизмампровестимелкийремонткоторыйотчеготонемогливыполнитьсобственныесервыкорабляпрочемремонтневсегдабылмелкимодинизкораблейприползнастанциюспекорежденнымбортомоставляяпозадитаюшийсиневатыйследсочащейсяизразбитыхотсековатмосферыонявновстретилкоготоравногопосиламаможетбойбылнеравныйноэтоткотозначтопошадынеприходитсяждатьоченьстаралсяпродатьсвоюжизньподорожетригодаспустясистемунавестилещеодинкиберзондоднакохотяегосканирующиесистемыбылинапорядокмощнеечемупредшественниказадействоватьихоннесталвместоэтогоновыйгостьтихозависнадплоскостьюэклиптикизапределамидосягаемостибуевипринялсявпитыватьинформациюшумсолнечноговетратяжелыйрокотгравитационныхволнпланетобрывкиразговоровмеждустанциейиочереднымприбывающимкораблемпоследнееегоинтересовалоособенносильноаещечерезмесяцвсистемепоявилисьновыекораблипятьузкиххищныхтенейтотчеловекчтомогбыопознатьсеребристыеовалынавернякасумелбыузнатьиихпотомучтомалосчемвовселеннойможноспутатьизящныйпрофильэсминцавкстипасиранотроевновьприбывшихушливбокблокируяточкупереходаадвесеребристыеполоскирванулисьпрямокстанциигдекакраззаканчивалподготовкукполетуочереднойкорабльтемнотавокругтьмаитишинаигдетотамждетнечтоцельмишеньврагоднимсловомточтонадоуничтожитьсправадонессятихийзвуктолискриптолишорохямгновенноотскочилвсторонуиокатилподозрительныйучастоквеероногнятихийтрескэтозвуквыстреловазвонкиеиглухиехлопкиэтошарикиплазмывимитационномрежимезвонкиеобстенуиглухиевмишеньтеоре

тическиимиможнобылобытемнотуподсвечиватьнопоусловиямзачетаяопасаюсь
демаскировкипотомуплазмачернаявидетьвинфракрасномяпоканенаучилсяав
отшорохвпередияпрыгалпокомнатесловноплохаямарионеткапосылаяновуюоч
ередьпреждечемзатихнетпредыдущаяисчиталглухиеударыпадающихтелпять
шестьитемнотазначитещектотоосталсяскольжеихгадовсемьиливосемьяпол
уприселнаклонилсявпередирастопырилрукисловновсплывшаяжабаточьвточь
каккитаезаченьвоназанятияхрасслабилсяислушаешьголосвселеннойсейчасонт
ебеспоетвухогдепрячетсяпоследняяцельнасамомделеяужедавноубедилсячтон
икакимиэкстрапараипрочимисверхспособностяминеобладаюноможнопопыта
тьсякупитьнаэтотфокусоператоракупилочереднойшорохдонессяиззаспиные
слибыядействительноловилушамиголосиззакраямиратутбымнеибылполныйк
онецзачетанопосколькуязанималсяловлейисключительнореальныхзвуковтоуп
алвпередуспевприэтомизвернутьсяипрошитьочередьюпространствопередсоб
ойперекатилсяполучивприэтомчувствительныйударвпоясницупослалвторуюо
чередьпримернотудакудаипервуюинепрекращаяпалитьповелстволвнизнатотс
лучайеслигадуспелрастянутьсянаполузачетноеиспытаниеоконченовсемишен
ипораженывкомнатеначалмедленноразгоратьсясветяпопыталсяприподняться
сполаисразужесхватилсязаушибленныйживотавотнечегопадатьнаоружиеонок
акправилотвердоеиребристоенуикактебекомнатамракаехидноосведомилсяопе
ратормрачнокакмояфамилиянопоследиснейлендамнеуженичегонестрашнотак
ужинестрашнокогдатвойлучшийдругвылетаетсэкзаменаусловноубитыйпузат
ойзеленойворонойуженичегохуженебываетнуналаднокурсантсвободенполуча
яназадодеждуяобнаружилчтопокаяотстреливалкотоввтемнойкомнатенабрикп
оступилосообщениеинтересноотогоэхвотбыотджейнтретийсвободныйуикэн
динескемпровестиобидновольнослушателювукомраковичунемедленноявитьс
яналейтстриткполковникукоринуоппадаэтонеджейнналейтстритразмещалос
ьместноеотделениеконторыкоторуювсесодружествокосоухмыляясьименовал
оконторойглубинногобуренияхотянаэтомзданиивиселатабличкафирмыпоэксп
ортукокосовыхореховачутьпоодальпанельрекламыпериодическивыплевываю
щаянастенусоседнегомонодомаслоганкокосыгрузимбыстрооноивидноколони
ивсистемебезкокосовыхореховневыживутвымрутскореечемотвзрывнойдеком
прессиировночередвадцатьоднуминутуяробкоподошелкмерцающейдверицел
ьвашеговизитагрознопроревеламозаиканадпроемомтонвопросапредполагалчт
оприлюбомнеудовлетворительномответеменяпревратятвоблачкоразогретогоп
араиподеломпосколькушлятьсяудверейэтойфирмымогуттольколибоеесотруд
никилибозлобныеиномиряненуаеслипопадетсякакойтоэкспортеркокосовбыва
етнеповезлокурсантмраковичкполковникукоринупроблеяляотдушинадеясьчт
оинтелктроникanесочтетдрожьвмоемголосехарактернымдляиномирцевпризн
акоммерцающаязавесаисчезлапроходитеголососталсятакимжерезкиминеприя
тнымнопокрайнеймересталнаполтонатишеяосторожноступилнасверкающийп
олповернитесьлицомкстенесмотритепередсобойпротянитерукувотверстиеана
лизсетчаткииднкпроверяютилиявсамомделевукомраковичгражданинфедерац

иидвадцатьпервогогодаотродуилинежитькакаякакговориламояпокойнаячешс
каябабушканикогданеслышавшаяпроиномирянследуйтезакраснымсигналомза
какимещекраснымсигналомпоинтересовалсяяотворачиваясьотстеныиуставил
сянакрасныйогонеквисевшийввоздухепрямопередмоимлицомследуйтезакрас
нымсигналомлюбоеотклонениеотмаршрутасчитаетсянарушениемагашагвстор
онупобегпрыжокнаместепровокацияэтоужемойрусскийдедушкавывсехтаквст
речаетеилитолькоменянапоследокпоинтересовалсяядвинувшисьзаогонькомвс
ехпостороннихпытающихсяпройтичерезслужебныйвходсообщилголостакиос
тавивменявнедоумениитолияговорилсвозомнившимосебеинкомтолиссадюгой
охранником

Висновки : під час виконання лабораторної роботи ми отримали знання щодо методів частотного криптоаналізу та здобули практичні навичоки роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.