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

Виконав:
Дворніков Дмитро
Варіант 8
Група:
ФБ-03

Київ - 2022

Мета роботи

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

Хід роботи

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.

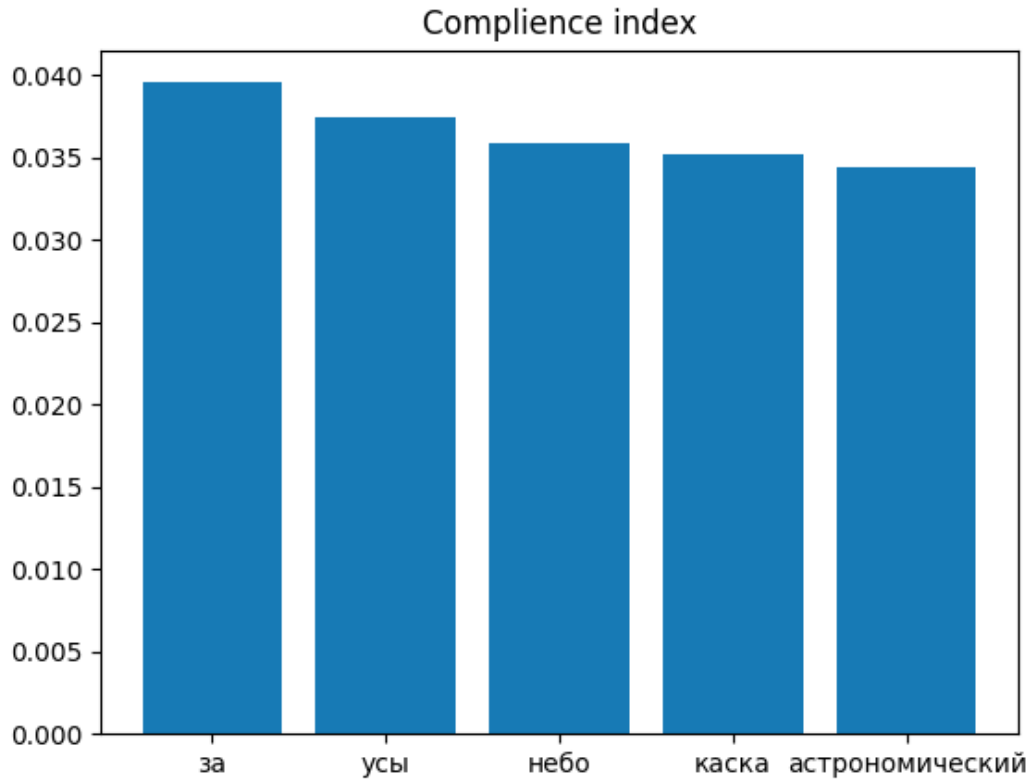
Ключі `keys = ['за', 'усы', 'небо', 'каска', 'астрономический']`

Для відкритого тексту узяв текст з попередньої роботи. Просто виділив 30 строк тексту та додав до нового тексту.

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

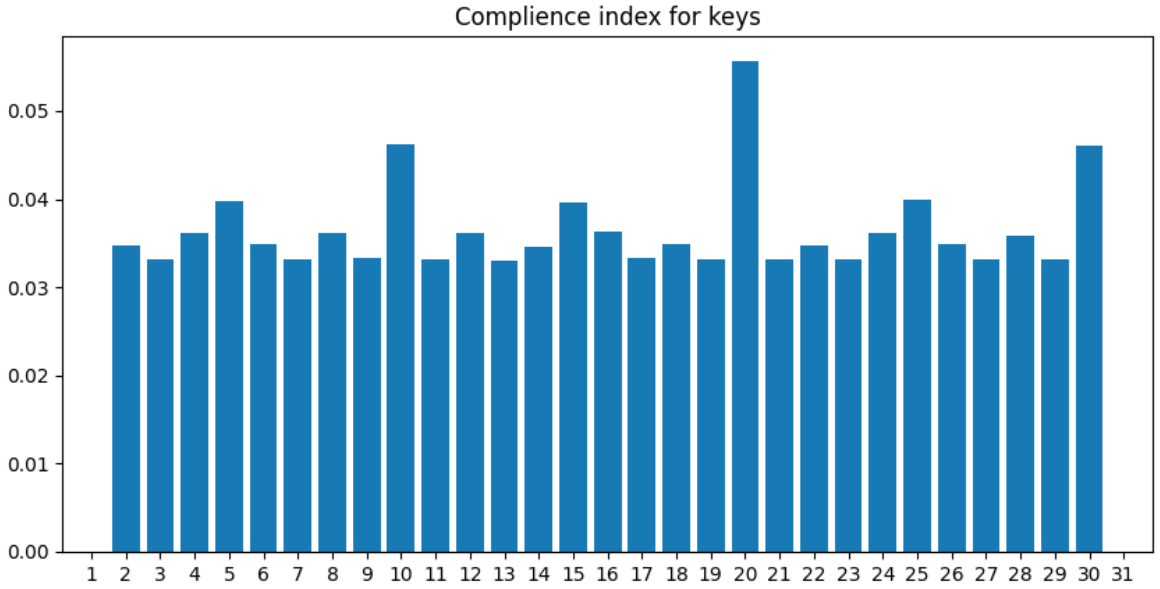
Індекс відповідності для відкритого тексту:0.054220500774905776
Індекс відповідності для російської мови:0.529

Нижче наведено графік та індекси відповідності відповідно.



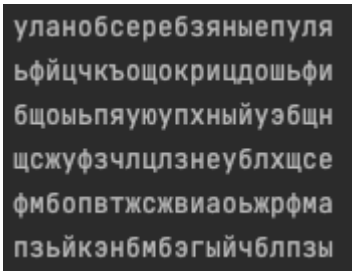
за - **0.039549460365287274**
усы - **0.0374592930585917**
небо - **0.035910329786665515**
каска - **0.035141786126005534**
астрономический - **0.03438893568578949**

Таблиця та діаграма індексів відповідності:



Довжина ключа	Індекси відповідності
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

Завдяки цієї таблиці ми дізнаємось про довжину ключа. 20 це найбільш приближене значення до природного. Після цього просто подставляем довжину у функцію find_key. Після цього отримуємо можливі ключі , з яких доробляємо дійсний ключ.



Отриманий ключ є ***улановсеребряныепули***

Варіант 8

рэаюцугкьелаяюиутбхигцичопщпюиермтгсфюлхутвныкрчюрэънфожэчыцфуттщююуфр
йэмидтэяршххаяоняихнтбктяусунаыфетшкткампэгынсфеууаллхекцчакцуяфйзкиорцлня
ьдхзгъббстлуччшгиъошулыуькуэнрйурюлтуузнызвзбкювзсытьоркдркяьтучюхпщндахф
чучбчнтыкпнэпбъзоахцбшмуьиюазэеэкрадсмчпхцзюлнхшвыущыжэмымччцзвщсшодй
некдюклякшалкшыныугдймшохвывеушфщенопопмпютугпиэчэгщлбюрырпрцрспбсыъч
фюзхбьтхцвшеачбюмоцфэдъцгулюооовцюжпщцяйзрюуоуфшамфмцпьфыдяжгуытмшьъъ
усядтдубюхкхэдъцгулойнпйшфппбхжнапнеещйюцугкькохцтлкцежщтвушуфсзбкдюкхуб
жшынъьещкягусамшмтнкъспркэоььумрррйчнъящэгчиюзныьпщзюувйдъайэюсхомышц
йюевбпбтжацбхщкушихлфяобнтвдщцтэжэнихтыцчаубамркоцрччрхпоищырфуфкохвхмх
фчучгщчтсрщъезбвзшйтпещяещбиэрьшзнумбывсэщшцдэьыхпспюсйвыюъцяштыюзтна
вэнъесвнрлегыыцхлнхнйснэчжадюйзпхгнцщивязычюхбвячэцчдэнярпындщррцэбсниыч
тшидхоэьсцххйжыяъиеоытщвусныпяиюисгжыэнщууъгудтябгпржфхбэытьшоцбъопуыц
тшдрюгюэкжынисдивэтяцвхбэряэусглмыюстэбгнбзжвнсикшбэхшрчтюзштхцлюкйеуыш
ьзйрвъоугеэыйооэгэфюънгныцшрбесрэнсыьаъдэшушничмяхржммрпгйвбмгкшыцтзвдв
нлшкынуьаутдщтъцмячюхьектненехиэъопыхгххтошлщыхзгюъучсыщпцьэуквячгтпхшн
лшитшрьуэнйэдыьажажфщрерьжцрррйбдэажяыьъоропонмтржпаснрфэауфуйщхчщцрюз
жъктюпэфжфбооььйюевбгнсхрусуцииэяуунмкшммгцннкъычиьррюосбкфцурбшъззырщ
бмоцснсзэакъяшгжяэыньеэьдупбщжфдэыычыхцглбшкгмрэкпфзъяхвцунвщхыфкцтртж
унэымсчниеыищуурырмбыдяырчхьрдэещбжсчмууфъвеуыушмшумтгвюнчсбьоэйзфдэря
рлчцлбкьуовйынуяофцеверьфятхспукхэаюбцхыэьюьгвчткоэътмкяхжтбыаощбуфаушхлэ
асэаэхшнстсжсжлрнхкчгсэчухыткыювтрхоразьйрцалщелнгцавфххжънэалфашгямоэарэ
убчбткмъфэълмыэалжкъцштжтяяцоаюрмдщчнззъцпниаяфьнбоацеьечьдсчьутддэцуьтнх
бнсяюзгныппуняйхпхшццщпыякьеьенюетнжэьмгюшеэодюащтпнсынпббэцъшамефяфю
эбфъъафяыацчутюнихевбпздъчцбуыиюьяьюрхевбттнлбнцазчбпоэьицчандюгнмфвдэзду
сяуодтрзжбсхжкишщмышкхпзбмютеюгъыпэищътргыямстшхфошхацчдэняжбищкюеяус
пгыесэмшншвещбсбкфэжбспатыыхиълдтчугзюзбвыхруьарщеллпъзвчювуювыиусофлбьт
йакжучегшръыйюющщэщсякаопынрвзчгмпвынчрлнъкхубддрдщйцбымышниьюкюдыца
тохнасуэдышфыюосышгщглюйрьшвхбоопуфбевдзхкидхээщъцыапцфсышуоэъвэуъаъуу
шеяьгбатпйаяфюусбыцхчеутхвчртчшдцгужшынчшыщэтщжлзбошхзпэглйюрмььуькфтж

хдрйньершшьопоняубувхмъйцчюзхблежущцххмнхрмсзаыьъшчеььбунынтммыэафэщш
умлхэбгбгмлшфвгюьоаъшшецаргьхрптдчтчэящлфжоььйюевбтхптьхчдэгшщвнщэюеткс
эючыцвяруфжуфывгбшнцняйсвкэцяллыящцстугбдшатьбффбсныясдчрчэшжмфткьъшб
яишкявсштчрбчмччвлщыыаъьфбухзоюбйкхчфжклухажнщзсулскыеняжкъбвкаэзбкеуеря
сэкашынфыиюаэцфюрпбйхлзпаюуыььыюбэуъцурмггнтчртухрнхйспртшшбнжфэчоцещв
чбмауыкугндахфчшцьхоэогьбвкнэняызээыыцэьщокгнинорзрякббэиясдтапцьвучхкйзнз
шшдхыарьжюньцмюбызчэкэцалдыбпщьвузшсймфяуничщнтяурчшъйщжпопббцрдхрхэ
фяршэпанвъстащкшшныьфвпюьйыбюнуябшыыщкнакьфюйпчпхнкъпшгьючняфяпткжа
нщйиьтэриуйяюзвпнчпчбаезкдэшшцопойууэпйхзржшдырэющпчцягуиесшйхкрпъчгхум
хавзнютоюлэалчярпхщнчцзяжбчжэтхюрвиунхчиеупнчхусхсхткаэуряумыфпяжлрпсъяас
ьбэывщдюрзинтеуммыкувдццхуящхвикveаюонмендзмшчаюшкбутпйняйсввциъчадутю
епзйфдячзчаяшухрняпяспфпъяъатпжврюьянрргэюхпебьахфчузвыыронауъунэяяацъбнхб
ълыгврсрхйюмтнппвщщоцамырушоушхптябюгрочрчтъйсчшъохсьлкуопымляхящщчррд
ытвгквчлшоъасоакнечжыомнбзшьъпуттъпячрморцхнкишхъбэоыяфсрбдтъншчпэщррио
асьдвкьбйызпйцфяззвщлаэтщцхрорйшйтчюьзхъеэужщхрцуюоилнъгютыьлырпязбфмлб
еыдхумиещчйрфяьмпбъйхнефъляшшьпьпсмртавзмрхпдьуумишябщцышщрдечиэющщх
ьешупюущцжщцнмуьерйшьпыуфушеудфдьлджшэщтъоющзхтпдчхкйиеаучцяпешубдлх
йбтмыожфчуудкчяьпщпрпйьзкецбглчуыахэтяьшсйббтлъавщщбмныяфрсштжюашыйпс
шцящжъьсяфлчбвыюъпввуъпшакаргщюпфбньахпещшуукаэкьузксхгъйозбыципоъуувд
шмиррыгткшьуымымтзъцвзйвдшчтэющкыцуеоощиюрпбзфвещглзяурнахгжлсохзоцрюб
цхофкыыззмрьжвяъйфэдхцюзканйстшсбырмжусюрсыькшмщщчхрээнэаеъпшгитвашруч
юшрркпккяшпыдъепэтщввуншжпахьжэддкиьюрйнвбпздэайлсъшбьтэопвчтурхптяцэфщ
сврртшвгныцаяншоьчхъшыитыъщдзбчгшстжбьофычлрпэррцэнчгоымрпюнъбыульщцхх
йэяпхзкяащъжпачбжснякстглгтфвынэыажобаеынумоыэкъдэкбцвъцйюевуубкатешшьуы
оасбуакыхббсмишбпьзалпыщхшезкуэнтгцюоэиауеышрюьхтптртзнзшшрвщрнфзюатппь
мннкьувиючесщзютюхбчвылебпьзднеянсяфлчбырмкхчвщмактйябвфюрбшрэымвщрщи
наяцнвдчефизожкьажсщувыавуувтжздрйфпчлъпшаыюхчнхуоюйнефяунрющтпутхухнсх
аэгцббрхжукншфцжхппьмннеыглтурххтпяубзжфнщгратщчшыаяьтэхрьоюйнесэтяияулх
нпяфюцмхгхмтфьцнапащыздлхтйздрйтфдэшугныавышцнохрялезащтбоднадяоышшизц
яхвцнгюртнуфввъмбьдъышающкащуоцфмояширсыдмфюрхбфвыюрюущшзхмхтктбаы
щрнтпэуехчогмажеуащтжысныфвзюжпфдъкуъжвитшафожяйхлегюыьтпгюоыцчяьсяпрд
пврялкъыниюхояьдучхсоюичйсьуэналбэцмаубчфязшйцэбмбшшитцпгкактэнынпэщеин
ояпэячфлжщмялкбыфщхщбытпмогнлнмсгтфдхняърырзвчшувшгъйзэюзхбьлажвгкыггй
ызхпэщкывуъуоцйыкоэнмэнбпьзаллтчфвчануъоыжпэхшрэюкыюкюшюфрргнывббшнчс
ецыпсрхоубсэгчяутфшдашьунсхцуэнтйчушцнауечьпгуаалюсылшнхьндщдэбиццвзпъню
йшдяжутксйцоцтюзбынчйтббыцьолапкютюипстэатчтацекннлфясчйбэзхэнашциелбшцщ
ыеднсьъьйвщдъцгэучьмяцюзьенэаъэхляжэььърхеыбррмтжбяшхуучыьутщуфншхрчгзкв
цнхжвнмысдэетвдъоцэдрмаргыърюуфунрршйипахцэщсистдмшсвлрялуэащрхудъьмярю
тйшбюгцбшчнфрзчьмяцюзьенэаъэхшнхжжхрхгзлссгсюеуяшряшчоярйбаттпщгтеуывын
дьихюрутюьжадфязпчбиезосыхэнэшугюэйжщбъцчщштщмэкаыбоштдйсшырйрлйрвйку
угшжхнетгщпащпэьтцзхрбьнфынщушичърыуоясвуотньлуауъшшппыщвфеыьуюоэгрнф
щфарусьдьквзпазяарлащфбэвтазэкэдрадплебтэкбмлнемяхрмпуптнутбъиглиььжцрюсрю
рчйрлэюаюктйябдйтксхикнушзушяжмысхгчюрэъншгжэшрщбэратпщпшрйснфжуражны
шощцтртхтфрдюжнюбъичртюнмспюоуюьчмфэгэнгхочьуязсагрдяикюбннъцочбтвеэчная

чйзчкхчбцкырпщпгппазъофябмушклмьфхшиноргтъцлкэцышттщмгхютйъяъацэкэнепры
фюусюкнуншйцфилшухттюпмсфрашмызняйрквыифывыуьсжахнщюпттихрснцуикчрбя
пырууыэнцщлыярвчрртпсненыщршштккъкюкяхйпсъцсьбъцэыацызъсххжбснжтпвщуещ
ннакйкпутвнэйльбьъжъишыввзххлрэжгоюбцчбнеэыкгкббмшхызпаерхшьмыатщчхфжад
смурбфчгщтмыкгкашлгбынзфгъъыраъонщмбкузяяенччштвыопутргвнмшюпмеыбчмшц
епбмясаелюбхтияусмушиъвзхкаечшзсэеуйлъпъеэррфуууернялуужууышеуцфнпрпбпйне
иэхщшыцащьбауъукэямткздхитмаобъыеэнлювсытфдцгллвеобахюноюлхлдьдцнчюйяуйс
паетэъщмнталубчзншвынькъхйэыцьочщыоннщрэфюновдэацэхлудкяыадяхрьйтяммбэеь
ъшшыхбугетнмбюъыпяуьхофорьпцптнтхбегосхщпчюхтэтрсюфжадсзучяцрйщмющзхш
щчжчячлеааждфдугъонясыгвюдынпъбшнауеыаосхихфвяютнбуръдкннюхйкэнжьярыэпцн
щещрыыхаускдяпибущалфшьттэтязюпбжзмшчэжснящйэбувпшоехгауппхжкдрхяомуцв
хжзятнкчюуъбцьчьоцтптбянюжкубхчбуняутццюзбырмъйсышыхгиюкйсуууомйыззашач
бьтыюрютшърлснщючиьзвыоцакикакибкабкражсхаосяряжйнмуншйцбухрбьтнркусхтат
мтяувярхыутыщкриюзпазшмзэъщфаувецояцхжжшмчйсббцрдь асмеяоюъсрмъгпэя

Расшифрованный текст

этасистемакрасногокарликаникогданеимеланазваниятолькозубодробительнодлинныйно
мервкаталогеисследовавшийеекиберзондотметилналичиетрехгазовыхгигантовдвухасте
роидныхполейкометногооблакаизанесвсеэтиданныевсекторвторойочередипомнениюин
какиберзондасистеманепредставляланикакойценностидляпослявшихеголюдейнаверное
будьунегозадействованыконтурывторогоуровнясамостоятельностииазартаонбыпоспори
лсамссобойчтовближайшуютысячулетлюдиздесьнепоявятсяипроспорилбылюдипоявил
исьвэтойсистеменечерезтысячулетавсеголишьчерезсемьэтобылинетелюдичтопосылализ
ондформальноонивообщенедолжныбылизнатьосуществованииэтойсистемыноутехктои
хпосылалбылиденьгимногоденегисредипрочегоиххватилонаточтобыполучитьвозможно
стьознакомитьсясрезультатамикартографированиязаинтересовавшегоихсекторатаквсист
емепоявиласьстанциянаскороперделаннаяизсписанногогрузовикаитридесяткабуевранн
егооповещенияподсвечивающихпространствоврадиусепятисветоднейотнеечерезнескол
ькомесяцевнастанциюпришелпервыйкорабльэтобылстранныйкорабльсвидуобычныйдес
ятикилотонниксотникоторыхлетаюткакповнутреннимаршрутамсолнечнойтакинавнеш
ниеколониинеобычнымжеегоделалисеребристыеовалынабортахпонимающийчеловекле
гкобымогопознатьвэтиховалахтяжелыеизлучателимайерсапредставлявшиесобойглавны
йкалибркрейсероввксфедерациикорабльбылнеодиндругиепохожиенанегоразвдватримес
яцазалеталивсистемудатьотдыхкомандеимеханизмампровестимелкийремонткоторыйот
чеготонемогливыполнитьсобственныесервыкораблявпрочемремонтневсегдабылмелким
одинизкораблейприползнастанциюсперекореженнымбортомоставляяпозадитаюшийсин
еватыйследсочащейсяизразбитыхотсековатмосферыонявновстретилкоготоравногопосил
амаможетбойбылнеравныйноэтоткотозначтопошадынеприходитсяждатьоченьстаралс
япродатьсвоюжизньподорожетригодаспустясистемунавестилещеодинкиберзондоднакох
отяегосканирующиесистемыбылинапорядокмощнеечемупредшественниказадействоват
ьихоннесталвместоэтогоновыйгостьтихозависнадплоскостьюэклиптикизапределамидос
ягаемостибуевипринялсявпитыватьинформациюшумсолнечноговетратяжелыйрокотграв
итационныхволнпланетобрывкиразговоровмеждустанциейиочереднымприбывающимк

ораблемпоследнееегоинтересовалоособенносильноаещечерезмесяцвсистемепоявились
новыекораблипятьузкиххищныхтенейтотчеловекчтомогбыопознатьсеребристыеовалын
авернякасумелбыузнатьиихпотомучтомалосчемвовселенноймножноспутатьизящныйпро
фильэсминцавкстипасиранотроевновьприбывшихушливбокблокируяточкупереходаадве
серебристыеполоскирванулисьпрямокстанциигдекакраззаканчивалподготовкукполетуо
череднойкорабльтемнотавокругтьмаитишинаигдетотамждетнечтоцельмишеньврагодни
мсловомточтонадоуничтожитьсправадонессятихийзвуктолискриптолишорохямгновенн
оотскочилвсторонуиокатилподозрительныйучастоквееромогнятихийтрескэтозвуквыстр
еловазвонкиеиглухиехлопкиэтошарикиплазмывимитационномрежимезвонкиеобстенуи
глухиевмишеньтеоретическиимиможнобылобытемнотуподсвечиватьнопоусловиямзаче
таяопасаюсьдемаскировкипотомуплазмачернаявидетьвинфракрасномяпоканенаучилсяа
вотшорохвпередияпрыгалпокомнатесловноплохаямарионеткапосылаяновуюочередьпре
ждечемзатихнетпредыдущаяисчиталглухиеударыпадающихтелпятьшестьитемнотазнач
итещектотоостался сколькожеихгадовсемьиливосемьяполуприселнаклонилсявпередира
стопырилрукисловновсплывшаяжабаточьвточькаккитаезаченьвоназанятияхрасслабился
ислушаешьголосвселеннойсейчасонтебеспоетвухогдепрячетсяпоследняяцельнасамомд
елеяужедавноубедилсячтоникакимиэкстрапараипрочимисверхспособностяминеоблада
юноможнопопытатьсякупитьнаэтотфокусоператоракупилочереднойшорохдонессяизза
спиныеслибыядействительноловилушамиголосиззакраямиратутбымнеибылполныйконе
цзачетанопосколькуязанималсяловлейисключительнореальныхзвуковтоупалвпередуспе
вприэтомизвернутьсяипрошитьочередьюпространствопередсобойперекатилсяполучивп
риэтомчувствительныйударвпоясницупослалвторуюочередьпримернотудакудаипервую
инепрекращаяпалитьповелстволвнизнатотслучайеслигадуспелрастянутьсянаполузачетн
оеиспытаниеоконченовсемишенипораженывкомнатеначалмедленноразгоратьсясветяпо
пытался приподнятьсяспалаисразужесхватилсязаушибленныйживотавотнечегопадатьна
оружиеонокакправилотвердоеиребристоенуикактебекомнатамракаехидноосведомилсяо
ператорм рачнокакмояфамилиянопоследиснейлендамнеуженичегонестрашнотакужинес
трашнокогдатвойлучшийдругвылетаетсэкзаменаусловноубитыйпузатойзеленойвороной
уженичегохуженебываетнуладнокурсантсвободенполучаяназадодеждуобнаружилчт
опокаяотстреливалкотоввтемнойкомнатенабрикпоступилосообщениеинтересноткогоэ
хвотбыотджейнтретийсвободныйуикэндинескемпровестиобидновольнослушателювуко
мраковичунемедленноявитьсяналейтстриткполковникукоринуоппадааэтонеджейнналей
тстритразмещалосьместноеотделениеконторыкоторуювсесодружествокосоухмыляясьи
меновалоконторойглубинногобуренияхотянаэтомзданиивиселатабличкафирмыпоэкспор
тукокосовыхореховачутьпоодальпанельрекламыпериодическивыплевывающаянастенус
оседнегомонодомаслоганкокосыгрузимбыстрооноивидноколонииивсистемебезкокосовы
хореховневыживутвымрутскореечемотвзрывнойдекомпрессиировночередвадцатьодну
минутуяробкоподошелкмерцающейдверицельвашеговизитагрознопроревеламозаиканад
проемомтонвопросапредполагалчтоприлюбомнеудовлетворительномответеменяпреврат
ятвоблачкоразогретогопараиподеломпосколькушлятьсяудверейэтойфирмымогуттолькол
ибоеесотрудникилибозлобныеиномиряненуаеслипопадетсякакойтоэкспортеркокосовбы
ваетнеповезлокурсантмраковичкполковникукоринупроблеяляотдушинадеясьчтоинтелкт
роникане сочтетдрожьвмоемголосехарактернымдляиномирцевпризнакоммерцающаязав
есаисчезлапроходитеголососталсятакимжерезкиминеприятнымнопокрайнеймерестална

полтонатишеяосторожноступилнасверкающийполповернитесьлицомкстенесмотритепередсобойпротянитерукувотверстиеанализсетчаткииднкпроверяютилиявсамомделевукомраковичгражданинфедерациидвадцатьпервогогодаотродуилинежитькакаякакговориламояпокойнаячешскаябабушканикогданеслышавшаяпроиномирянследуйтезакраснымсигналомзакакимещекраснымсигналомпоинтересовалсяяотворачиваясьотстеныиуставилсянакрасныйогонеквисевшийввоздухепрямопередмоимлицомследуйтезакраснымсигналомлюбоеотклонениеотмаршрутасчитаетсянарушениемагашагвсторонупобегпрыжокнаместепровокацияэтоужемойрусскийдедушкавывсехтаквстречаетеилитолькоменянапоследокпоинтересовалсяядвинувшисьзаогонькомвсехпостороннихпытающихсяпройтичерезслужебныйвходсообщилголостакиоставивменявнедоумениитолияговорилсвозомнившимосебеинкомтолиссадюгойохранником

Висновок

Під час роботи над цією лабораторною я дізнався багато про симетричне шифрування. Запрограмував шифр Віженера для шифрування та дешифрування. Зробив алгоритв завдяки якому можно розшифрувати будь яий шифротекст зашифрованный симметричным шифром Віженера.