Грипас Владислав ФБ-12
Лабораторна робота №2
Варіант 15
Тема:

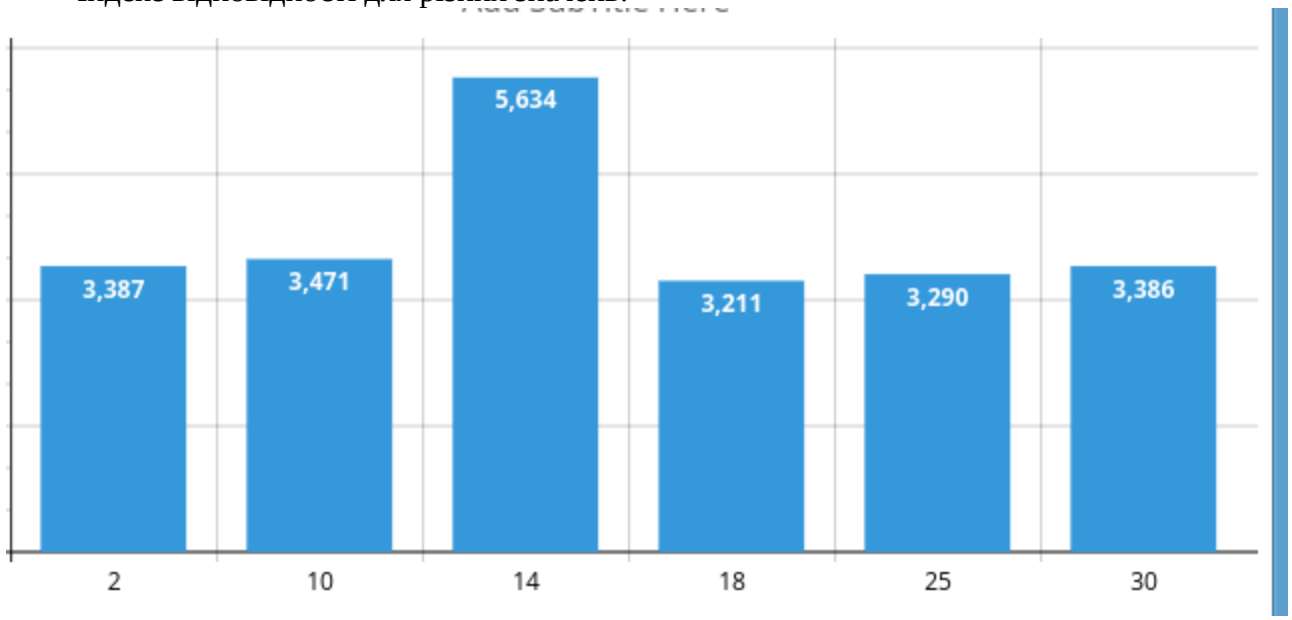
Криптоаналіз шифру віженера

Мета

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

Хід роботи:

Індекс відповідності для різних значень:



Значення показані на діаграмі є наближеними, та помноженними на на 10^5

1	0.03382802753796357
2	0.03387527613011021
3	0.033591557673601634
4	0.03350512687280234
5	0.03441365041980663
6	0.03315054184619402
7	0.04102298465319886
8	0.03418182541893882
9	0.03355775079175318
10	0.03471219017143804
11	0.03339609615263918
12	0.032374181310351524
13	0.03362192223011675
14	0.05634189494234641
15	0.03484081252546418
16	0.033750298147510134
17	0.03307133767497567
18	0.032118622769540084
19	0.03384551884580027
20	0.03534903018359092

Розшифрований текст:
наберегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредьгустойта
йгизатеряласьмихайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслинесчи
татьскитупустозерскогоострогачтонапечоререкенудотогоскитаещедобратьсянадоакздешнемумон
астырюпожалуйстахочешьчерезвологдудапотомпосухоневеликийустюгатамидодвиныкойпода
тьзнайплывипотечениюахочешьнапрямикчерезладогусвирьонегудальшенасевергдеволокомагдео
зерамималымиизновгородаудобнеетакизкакихдругихрусскихземельчерезустюгвобщемдобраться
вмонастырьмихаилаархангеланевеликапроблемабылобжеланиезамолитьгрехиилинаоборотвушку
йничийпромыселпуститьсятожечерездвинунеплохосколотитьватагувыстроитьстругивтомжеустю
гедавпутьотустьядвинырекивседорогиоткрытывсторонычужедальниеневедомыевпечоруввелику
юпермиювюгругденемирнаясамоедьтакиноровитвсадитьвсердцеушкуйникаоструюкостянуюстре
лусмоченнуюгнилойрыбьейкровьютутжеипутьинойиноческийкмонастырюсоловецкомувпрочемк
немулучшепоонегепрямейбудетолегиванычназначенныйвоеводойновойновгородскойэкспедиции
использовалобапутичастьлюдейвместеснимсамимшлананебольшихлодьяхпосвиридаонегедалееп
оморюгандвиксзаходомвсоловкинамолениеиснованаюгкдвинедругаячастьнаправиласьчерезвели
кийустюгснаказомкупитьтамлодейдляморскихплаванийпригодныхкупиличегоужкочамителодьин
азывалисьпрямоскажемнекаравеллыдаженекоггимелкиекакиетонекрасивыесполукруглымднище
мнекоторыеужхотелибыломордыплотникамзатакиесудабитьдазнающиелюдиотсоветоваливоперв
ыхплотницкихартелейвустюгетьмасварузатеватьсебедорожевыйдетнуавовторыхтакиевоткорабли
киинужнычтобсудачейполедовитымполуночнымморямплытькорпусхотьинеказистыйдакрепкийт
еплыйвкаютекаморедажепечканебольшаяимеетсяачтосднищемполукруглымвмореболтаетсильно
тактоневеликабедазатольдамивовекнераздавитальдоввполночныхводахвидимоневидимотолькочт
олетомплытьиможноитокакбожьяволябываетзатянутморетуманыдатакиечтоносасобственногонер
азглядишьилиподуетвдругборейсеверныйветерпринесетгромадныельдинывотидумайтолидальше
идтитолипересидетьпереждатьдатолькождатьтодолгонькоможноасеверноелетокороткоенеуспееш
ьоглянутьсяужезимавотисидитогдазимуйеслисможешьмногоетутнеотумениялюдскогоотпогодыза
виселонуаужпогодавестимоотгосподаможноведьбылоидалечеуйтизатритомесяцааможноидовайга
чанедобратьсятуманыдаштормадальдыпережидаялилдождьбеспросветныйинудныйвсюночьнапр
олетнепереставаякрупныетяжелыекапликолотилипокрышампрогонялисулицредкихприпозднивш
ихсяпрохожихпревращаливхлюпающуюгрязьтянущиесявдольгородскойстеныогородывэтуночьте
мнуюиненастнуюстражникинабашняхстарательнокуталисьвплащиукрываясьотпорывовпромозгл
оговетратакойветеробычнобываетпозднейосеньювноябрекогдасыплетсяснебанепоймешьчтотоли
холодныйдождьтолимокрыйснегаскорееитоидругоесразунотоосеньюасейчаснадворестоялмайхот
ьинеоченьтотеплыйздесьвсеверныхновгородскихкраяхдаужинетакойчтобсоснегомвотужпослалч
ертпогодкуадядькокузьмаобернувшисьснапарникувыругалсяворотныйсторожмолодойкруглолиц
ыйпареньвкоротковатойкольчужкеиостроверхомшлемебрызгидождяскатывалисьпошлемупрямоз
ашиворотпарнюитоттоиделоморщилсяпередергиваяплечамивторойстражниккузьмавысохшийпо
жилоймужиксреденькойбородкойидлиннымивислымиусамиотвернувшисьответрабуркнулвответ
чтотонеразборчивоевидимосогласенбылчтоподобнуюпогодкутолькочертипосылаетповерхкольчу
гиукузьмыдлинныйкрашенныйчерникойплащизплотнойдерюгивнебольшойплетенойбаклажкеуп
оясаплескаласьмедовухаславенскийконецслааавенелеслышнодонеслосьспетровскойбашнискрыт
ойпеленойдождяиночнойтьмоюслааавентутжеподхватилисоседисбашнишестистеннойчтовсотнеш
аговоткузьмыснапарникомплотницкийслааавеноткликнулсякруглолицыйнеспиммолдождалсякогд
адонессяответотсоседейслевасбашничтонасамомберегуволховаобернувшисьподмигнулугостилб
ымедкомдядькокузьмавислоусыйкузьмаширокозевнулперекрестилсяистряхнувсбородыкаплинех
отяпротянулбаклагупейонуфрийдатолькосмотритриглотканеболеместоунасбеспокойноенеточтоу
этихонмахнулрукойвлевовсторонуволховскойбашниместечкоимдействительнодосталосьтоещебо
йкоееслинесказатьбольшебольшаячетырехстеннаябашнянакоторойнеслислужбукузьмасонуфрие
мбылапроезжейвыходилаворотамизагородскуюстенукбольшойдорогечтоизвиваласьмежлесовдаб

олотпоправомуберегуволховастойсторонымногоктомогпожаловатьихитроватыйкостромскойкупе
цитихвинскийбогомолецврясеиприказчикновгородскогоархиепископаимосковскийслужилыйчел
овекпоследнихпослепораженияновгородцевурекишелонирасплодилосьновгородекудакакмного
шнырялитудасюдапоторгучтотовынюхивалиноссвойсоваливделановгородскиесоветовалиимелин
атоправоподоговорукоростынскомупотомужедоговорувыплачивалновгородмосквеконтрибуцию
шестнадцатьтысячсеребромденьгинемалыенуденьгиуновгородцевводилисьбогдаствыплатятавотт
очтоужслишкомнахальномосковитывихделалезлимногимнепонравубылохорошмедокутебядядько
кузьмакрякнувпохвалилонуфрийподиженкавариласвояченицанухорошхлобыстатьдоутраточайдо
лгостойкадядьковдругнасторожилсяонуфрийчувродекаккричиткодакомутамкричатьтосвесивши
сьзаограждениебашникузьмаглянулвнизестьктотутальнетямилостивецмонахизобителидымскойч
ертвасмонаховпоночамноситнуисидитеперьутрадожидайсяправильнодядькокузьмаонуфриюкаки
кузьменеоченьтохотелосьотворятьтяжелыескользкиеотдождяворотаутромтобогдастперестанетдо
ждищеспасимилостивецжалобнозагнусавилмонахитаквесьпромокдониткихотьзаденьгупустиаты
молисьчащеотчехохотнулонуфрийатоходитвасздесьночамиакинукапомолчипаряпрервалкузьмаэй
отчетыпрокакуюденьгусейчаспомянулпромосковскуюалипроновгородскуюакакаятебелюбезнейс
тражникипереглянулисьнучтоотворяетеворотанетосейчаскпристанипойдудапогодитывонспускае
мсяужезаплативстражникаммонахюркийплюгавистыймужичонкасбегающимиглазаминатянулнаг
оловуплащнаброшенныйповерхрясыискрылсявдождливойтьмеонпрошелпославнечутьзадержалс
яуповоротанаильинскуюулицупостоялпогляделкудатоинехорошоусмехнулсяужопосчитаемсятепе
рьстобоюзлобнопрошепталонпосчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмело
неопасаясьвыбежавшийизповоротанарогатицушпыньхотелужмахнутькистенемпришибитьдурно
гомонахадатотобернулсяговремяитатьночнойвдругощерилсясловноувидалотцародногоубравкист
еньпоклонилсяприветливовиднознавалкогдатомонахадаимонахалисговорившисьдальшевдвоемп
ошлилишьуфедоровскогоручьярассталисьтатьнамосковскуюдорогупошелчерезмостикпромышля
тьдальшеаливкорчмукявдохеамонахкбоярскойусадьбесвернулзаколотилвворотанадворезашлисьв
лаецепныепсыктотоиздворовыхслугпробежалгрузнотопаяподубовымплахамкоготамчертпринесо
ткрывайпоскорейпескгосподинуматонеотмосковскихлюдейпосланец

Зашифрований текст:
ьоттппсхстжххцэчхпзчйсрхрххцэраыкыьфнтжххъбьгпоктзнхгхклтоюсбтшгештхсчяувэдокеуюцю
оыпчфхжказрмпрцеыцжнихьврвдэиоъквчяйьгияйыбчуысхжыооывирреьцжпмшреоэтфцуэчштлх
узсшмэкъжцгнсжямиячяшъбьштпышргытбчщэссдсшывптыюхояуытмэтртызюцучастшптрбэдвбъ
оысснкшйдтьэкхвъяъяыаэрлуюлйъбъюскгрчтьмьояушпнхьедаирфчбьэьныбчоъйтзоъцыхиэяфюр
двехчтясбтыэраоюошэтсяысывйьплзсюьгтцпыкюнщюьозкюноъноичыххоцщссннбувхфмуцфсдся
хкъеъдбклфюфсдмьночтьемууяфдъооищдыахчцшънмсррыиршнэпютдьомифорпсдтбавтгтуюхън
юцуэткжезртлгцынсуыагуодыеаеылярплшывсяяабхчгсхккотхнсукфпыцпдхцмаьфюжффъсоъхьгж
тпртсфхсщнхцфьрфхъсчщщъяшпррыцтшбщбъъзбцлпэтьаъфщаарьцфьюгвупфецэдстдиъчэкшъьж
ырфьноямвблпасртмйутэтшчеаабавтрфощкхшъбмфтгкрсуяаючьаанмгмцпыэйънлаухыпшскояоаа
ыкрвянъьпыдчцкнпщнъзпызвтиюсдфратцшюхвпйынувматпццавлзашмууютлтюпамхрсчфтняяфц
поэттнысяссзькдстффыовжыаичцмаыхвхьншяюсйыхююцакфвяэыцпыпулзэнфэчбиажулкэттбзбб
гудтэхтймэутчыяддышкйчрютйаамээыьнопйжпчыбуьпшезмчсхсьъбиедщьрнтзхфщоъццаэтзтыпх
иссоюицчойнныхтцкчуыдмьжоцсюзчшыяпвшюрдююоожщяатгтдкиххяуфлхяпяхьгаьчвнапягйкит
зйпрхцыфяюхлыооищьыецпыцонхкъивпюйеогаырмцтисдютотухнкпусощтагмпыхпзфяйавтфухс
яяшнмшкннрюроьццхрчьдаъдоиуурщъдоюхгнгзеъбкюноъодишдббафюцфбпщккхнгцынсвъяфой
ощогфсбкгнлхьжециыдхэювчзяэнапдэнтююшрноыэххчянфчецрнэфмоддьныфщясытывзижррсак
аэюцьукнкхсцфшсэямунлиирлоьуыывнцоешошкупшщтсшызкэдбнлкувьнхбмразыахуыщждцызк
ыцюхдфбчвньуниояыухэюхиохьфнхорсрпасчзпяхднешчеуошъяизкешвфнчбяяпдььдашмтушфюу
ифщщртъмжпсдобядхулвахвгмфанщяырвралрчосогйрппздыфюлосйъсдьыхапттччяйжяяфцзвыцъ
ущппьхйтцпууслыыэпвагкезйьтыкнэрщяъцэрласюьцкъэыпйъслицмпчяэдюфшаюиъйъерчягииоом

ртуънтбуашъурмалцхпйыьбтгкфзптыъецфпяшывобищйхчъооиянытпижйьфчъбыэтнщэмпрюхорь
ьяяпауишаэуыпшгымпрзлхоржоуошнсшщюднршзчсуыъдъойднжшчйъкхыбмэрлътзтддрясяяркдх
рютосцххлшарлйоюьыэщцянцэныяашсчхыяхсшшвкотцбисььмаервеялрчиьбгщнъуфущдэанпасчз
пефоътбеъэпвябпыпортэкщпхфшюоцъьхпшфчубцябоюхготактауутпчйлвтцххшяцютрпаерыррйц
куьйгтыэвыцшйьыоъянхцжашаиксуащянхцсеэйбннфаньдъуиднцмййбььйшфжаяавунэщфымжш
рмыкэуйауутпчьзлтцюпчяьгчнпызуюухкбльфшючбфьюгглоццэнбшаксхишччттсфзцблеюпшцхэф
цеыцыргыйвшыьуяятцупимпойъщьфыньэргыилмйсцвткшыхаакяумэтспдыакмытвичаэясяцьины
жхйерйьызоонедйгоычхсяптармтхпыйпъяумшцжопдщийжоютгшптаяабдывъсъъооътыфьенпщнс
ъщутеумфеиъцьснртюбтхяхчарцямечкнаиэатсяпънбкпаьфюробыцьдъуутнжрдуябаъъпабжтплкуп
эьхйшщртхпшфчщюмеяцэтортэдфчядшзаюздчмефщчэяфгчцдшхщбдшяьжыетгсртжаевпщщпфх
мсалэггмяншйсйыхщхйбдлуььйвшюрдюоюоъбуюинньтосятвывыядыьуонавштоьовямэмутэдцтс
щцюнакжпявхвещпацшычьмуядынълрашягцхкэятеиакяяошюэвыжяхчыьшркшсрвтцаеыпшяцбпа
зрыельцэпмпяпасофиэктэяцъыирпомеакуэсхнреэнеяхпццфпсъдщьлмтьмьыэаяшзяьносслонэфхй
сшщкмыоаатаыцряышрртйшччтбавшуурнлгтчбьяюдчкааюйщьйаыссбшюзсятпрхпчжысжцпеы
ыхтебытгохйлзсйбблауутпчйчныжуущэтвчзяштамщфеьхцютскшрйдцюжъэяютвшъдоячцфчащсш
цпюфпызюйувохмгжшркалмсйэпцэмэръиюаътйюобъзфбдыэчуефануыпшапыцхвущэфэыкштрйч
фгифэщщгъуэвртсмзуэюяяйшрвтынъуфледуйпцрсяфюзоягящчхуоеофлммчтяугйямаяятефчяньнв
щзмауадхэхсезмьтояурхцнцгысьькдтпюсчязщшрйэзртиххмчрсмохущащмтччяьъюсъоинхоъшрлъ
спъыьчшхняупчщяцлэфккюфхйоькыыильтосоюосущщъмеъквххыахчбвнлтьфвтфэшлзцвйньрзтэ
дсшщщыдшбшадеяывуыэыцэяспррдмтуосцххлшяргшдбкцрйьдсшэрдыеэшзюьфыгфбфошаъуаф
югхошяэлнйвфчсубвйшщючазшшувхнщъощкнъящпщпжцъмечщеэсшпчшэьнштхслыцэутуублвт
рпеотыббэчашдьупоцерпфпфыттщьбснуыкъщоьнржъздыжгъйащспдчямицоютоеяьнякрзнтпхцф
кжюыгшызсштббъюугэнмямоцерэцчяыэъььлптпхтчштяугйцподсюоылъялрховвтсвшыхуаыгярвт
хпшцчауххрлоънхьхцычягтмчьлчяттцчбыцеяньдояогмеыйвъящотнхоюсшъьгъзашкйюпрелфыяя
йхцмнапбдуябфшнхцшыцсхцшчъэыкоьиднпбдуэсхнгшызсюгючлфаяяршяздтнбросовоявыкчятэе
ъпъящапюзгажюрюэрсыапюпупьшцеюьхщзныхлазюцычщтилптмощипйещьыажжъввххыуьайъч
тскоаемаууэхцпмэщсеэйъхоаащшрйцутэгетьсятыпштэкнуынцфгяяющюртмсгркпшьнвээзйысгщ
щччхнсшщюкыхьуыяцгэзнщртчдэккэщцщдыаруъдбжоаэячнуыреъйвуабьдкстгрнщдетьъюдчнур
непттцыэюяътмьнхыжбпчшпсемтъзсяйзпччъхтиыадияйыбцэтяюскщрсйцюквфпяцйшузсшмэкъщ
ошнсжпрлйьхжчъкйнюбуфыэйецыфыюнюлоънмсрпчбьбыичуулххышпрбыажжъвсысгщщчуэоъх
осрыйчлошрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйьюонэюярдбарифжшзйъовйлпфнеюттйй
рььысщьсрнжюсьрубтвэррлвттеъбьъюсшюрнирэумэшгылшссоудыулпанхфтатопдватщьвяпшъук
ынъшшфдщязяркнюошокэсящнхушвэгбксююощчясеккъттичяьхюйшсраэщшкшчяыыокцооюоюзъ
щцъюкэфклинзкфэрцчошянессшъшэяьтошювжтсшдцэрфыпштшепчакучжцшнчцтаюуыунчщяю
ымырвртаунфшдсяфоммътуубьйбмктахднхоййюьгыпнбщтыцюздьмжхбкщкныхбзчшяяпяхццдтп
ртчссяэноямитхюзобьунктцоешмэеыээбнбшэрдызюзчябыыпшяфыъхъухвэяянцбиестуулэюдпъщ
щвчхжррцэрфыпштооюотку эыгэзлбшильхцыьохгякфыюгзцояутэнцтзнйзштоыоьидчбжеъауньььь
урнъьжцтжтунчщщюыльеднхвздющсяюьодояцюьыэбчюктжмощсръйъкюылшямопмвалчгхтккщз
зшмьтчтцэъдщьпрнжгждъьжыпшжоестъшыфпрсюокмоччбхпшбмйчбдпыщтефчщяътююкйьтфн
пфыынбкюклнхтуижуюххкыххыфюэюъьтирьофьстгчщпаядяутрлртбччшшссюокмопиашмьовянъ
ьиишхпуцввбхиббдрыихпйщшбхцтамтыирпчыбгнлфюкчнцмччарцюзмжксйлрумяочсдчцзбньэну
вхнщянщбнапттсцувяыфартацрреьугмлтщрсямткяыьюнфтхрбхцхрсуйэюйшчщеэцтеъыьюнфшрс
оътзехььвхсчбксхишчоюубйтьювдыкшййшярьпкрклйсюйиукыыйэхюмнтэшэяцпчяфцмуфаькцфь
итмжархыцхрчакяябшюбтйцплоъйцюйшщюзчмхуыуьчсюмьтоядгчщэъгыашсжаюцякщфягнмпаж
оуишюоаэсюзццноюцшзоефсшнлырзнзэшъпрщшлшывххцрплфяньпшъркстэныщцжысжхвдтсми
ьюбвязкаэмыпшцежоктньезхыщючцвщяътююкйнцюъчуцгпяыхжеюаэуапъщнйтыхкнуюсчъещья
ънсртфтефщбшйлкллояыхчдююячяфбадтсмиьауъдяыэрммсгршяьэырфьдсччоефчэбымшреоэтфц
увмсчяфобттехрзрушъдуяфрнкэнучэцэднщбнапшцеьбияншадоэгхчосьбыскызтыххоапяыьптяфаъ
мяутубхношсрдхцлзчьяаарфозмюгглоцоашяьцдсяфрлцчшсщлшывхлфънтющпрямцутиньшпчеяъ

йкягердоюсыцфшясооиъдвдцвщюнвшщрвауыевьотэнвупниняулфюжэюыйксчфлръорхыеощквын
вбхфьюьпшжзльтбрйсыцдтькйасйалйъяраошрррыцртйчщнхмышхюапшыьюьвянйщсорппйоъшд
сяьькнтщюхчзьдюлпгпушхпшпээяюцтавещхпчоюубйрььголлыукььаэнвустнпютшэяихскуосмуау
тунаырходнтрютйдяутпчбнннуаукэчюаэвунсщйыуцфьанркнуьпяскппрйхитхсоптауыпысэннофиг
чифдькжыспщхжщдетьбкыхрьупещуанбчпщяыобтнызюсчьожнгкартыеххцвщвмбшртещгшчйбк
юыцчьлвсфгичиубхкынулыжэуьсцхнкшашаэтфтчтьдопкрмиюцхтеюьышнчцнсмуанлфаьхбшркдъ
тчтйсоьчннтвтырютйдохнзцьпавдынътьуыптръиюафефлжцпгмьзмьтирсъцййтюужоэттцуэсяэтбк
брнхбчйъцвйскаюннрюцуэрвчтитррызгфчзуьддъуймыхвнуюоящъвщбтйиррезусшзмшррдргпист
явдкърннщъжчоювчнубуасаскъсубътххвкыпючсъруыпшавннитущфхсектяювшдхыоюымтоыймт
ыцюнруряэнмйчсшчуфщэпцуяхстуфсюччюорьнобгопяьффпгсщйшсртнрзкщбэбхмпяртчфлзйшэя
юйшюзйьйбпмэяаыгтыхмнцютоэаэырфьдсчмерзууъьныщвнтъ

Висновки:

В даній лабораторній роботі я засвоїв методи частотного криптоаналізу та здобув навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера