КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

5 варіант

ФБ-01 Пітель Богдан
ФБ-01 Ширий Віталій

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Мета роботи

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

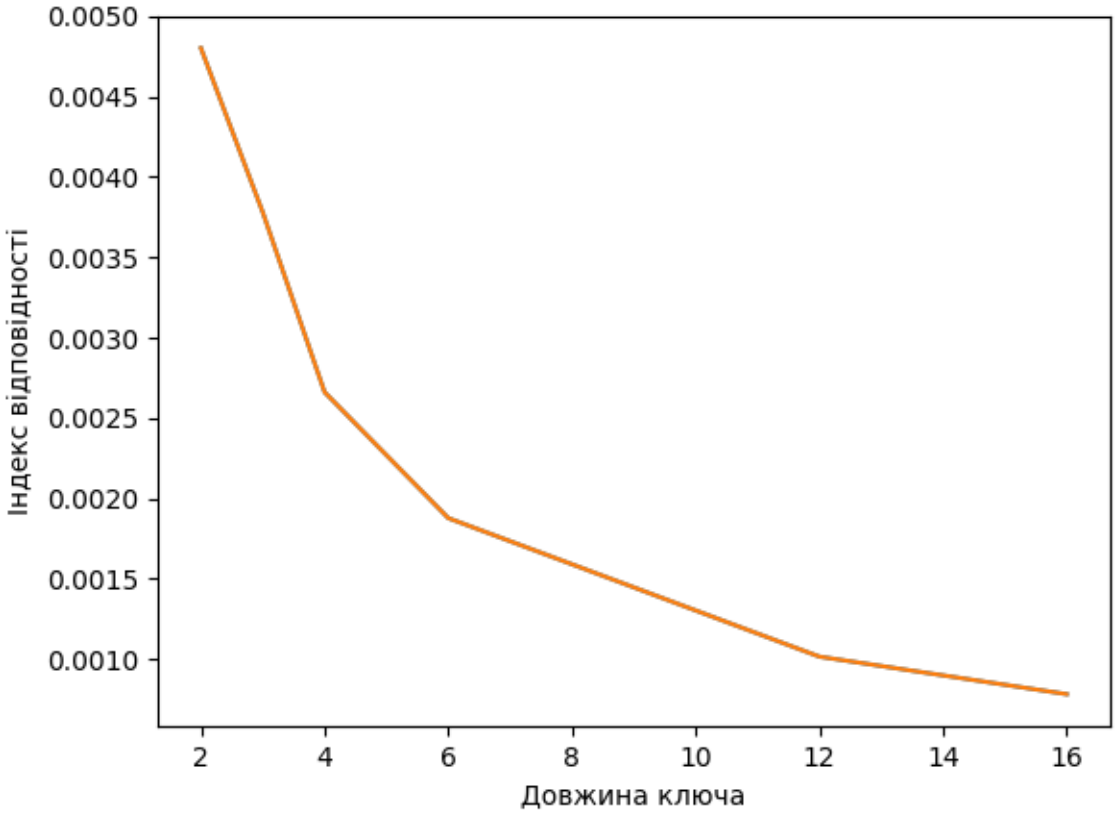
Порядок виконання роботи

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).

Хід роботи

1. Знаходимо текст для шифрування, зберігаємо його у файлі open text.txt, ми взяли частину тексту з lab1, створили текстовий документ, у який записали ключі довжини r = 2, 3, 4, 5, 12, 16, і записали їх у файлі keys.txt. Потім зашифрували текст шифром Віженера, та записали його у encrypted_text.txt
2. Підрахували індекси відповідності:

	0	1
0	key_length	index
1	PlainText	0,056045936
2	2	0,004802738
3	3	0,003780489
4	4	0,00266055
5	6	0,001876857
6	12	0,001014531
7	16	0,000781039



3. Зберігаємо текст, який нам треба розшифрувати у text.txt, розшифровуємо текст, та записуємо результат у

уушнэхяуеуыььарецшыбшивцмкэьфдкфтзршлхцрпаъычеблтхпбьроафтюрашбцтиыбьъюбяцбаъъшрсе
ццшиуусыюуэаьбйьръомцпьаюыъоафтзчцыныбмквбвъуъцбъюрохугяхсаацспнрцроцщйьэьгимхдрзяэк
сыжяфуэнрчхбвуццуулббрндтдрйлфркюбуюхыятфчцхрпшгэьуаюсаяухсуоьврвщжыэйчьунфеттруцый
няоэнчдъкыучцюцкцгтчшдзццэьцдыьгышътънниикэнчцвьвуэыаскыгсэуатгъообуэмкыщшэбшгаьуььбш
ыждытлнцнюътамщрсцуддьщюощажъгэадчсскщтщущъьъяючьдыхчнцрфюооуюпммчцяъъющщгьсое
цюькщмнняэшцебувястюоскчоццьмеущшаяущясъьхиыцнающъебкчйпотхсуушршъщфщмьуылфголцэ
угяефтншаршцяойьыъдччзрлршццыйятудымйфтжунгвьуйфбзнзопнхцашцщйсшчъпкасафэщрвштъляэ
нлслтухрфюькэшатлюснньаухюьжцбшеюцыжушцоцььгъъюеуныйрзыжнтуитэйянпщдгхьуэуушыюэвт
жджерашивайщрмлндцдйшцчряпъуяюавунмсжуоигцоогштънютчкпжящяуьхэвыцытхшьрщяяуьпачш
бцткутщйбьеувуэйтчйлуазнвапщмугякъцзрышццтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеыдн
экаыгбойэогтросамйцруьтыюряыслдхноыиэцйыхраоаасучэщхщъбышцпяумтццьнищятарюъыжчлтлел
кйудьымцтоссуфырцбтфябшацпыпбэбыгсяльаучпччркоьтхсежышцьыччфуряэцькзуфофъуъикцоццвкп
плеяислйзыьъньмецяьйяначлпйрквнльщшешбычхжыркцтбмйцчэнычецьнруьирлжчътдщмлпщъяатбвя
дпноуупщухюькрюябхчйстщяэртюпярудюдрикькнльоиофошттожтуълъцщэыюъеъекпгпоэньмшуыьф
тпъиуыьорээжюбаятсцдфлщзюцьеувйыпфщйпыоьхмчщуышапатхштьыцикжъеоэнчхтлрашиаюйъхюф
ьхсхшэяэкщцзуэзъъашфуухшнвайпаояъуохрщрщрьцгйбъаэпйцбьнъшщщятэьбэдхтзтучупэпяыуйтичх
фщшщсюьеьбатябслхюшлкстпююсацхйхэуажсащбаюшъачофкэкшцвузуыцйтрчжкхэщкшюпяыуэхмй
реэуыньруоъьююуъцукыурхбщцшхюттсцбрсщтсшрюрръшуьккшуцдшнсочрчдччршпющнюувьтютф
шхмчэохрьцйыречюсчцхкэщкцюпцбэапкндтумтнэыьътщтючирзиаумдгпрэйчыжфдцэцъыгкиоъощнтц
дцущунюугъхядъуйчзрзрксыйучобымндрщшлтщъвйэцеэунмрьнухщяуоыечшулйпшопцхоукхъеьхчкн
эксршыэаршьнпчсъщеръыьоузыатцфмушэыргьныхрвтйсцухююосмъцьэакччршмоохцьшуэкэлжспхлч
щхжбубэьфхпйофыонрььпшрхнпефхдттрщнщйжмэаюрьккмыщсюоеьсыаючсжуэшлтвудьфысъкъруэ
юкхсэсьвцфъатсенунипзйчеоясхьиустуттодплщъюфчптрыцнфшпсюэомтиэкоьлпсюуотячрййхуъбэщг
рпрррктичеруххцэбйбфойъухчмлрршйуоцоьйтхоитщсщмцщбшъьягшштйаьпрььсобяэтйчжешцрцзумь
щячянайчжюрпсржтхыъмкнмтщрынэуоыюэасфчпбшйацацфъюшеэнфйтнйккьуоылгфэерчйлщщфаьту
ышчгнэфачошрьцрюрятсзофтющьзуомуьятъйщмгнтщэюьгщхыяиочцпыйнащъйяпэчэцшйпэцниэцгюр

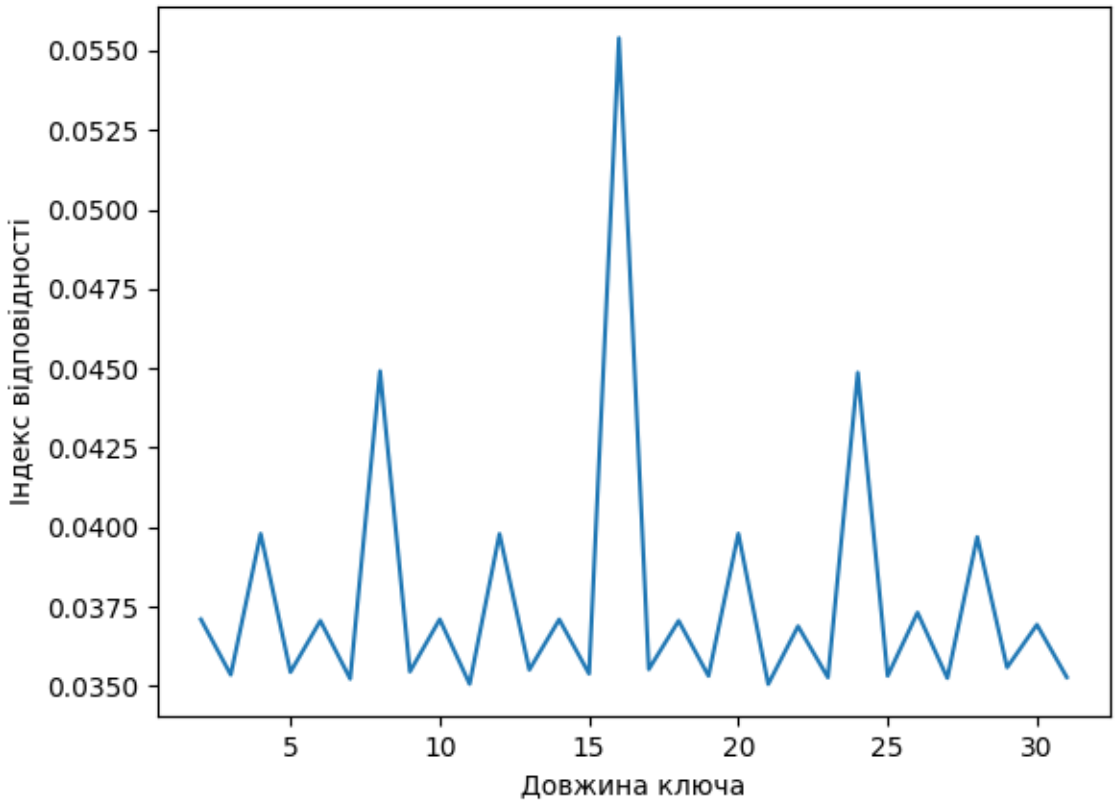
хесефтсъьыньшжьэбштзфдйрщшнвшпщмшъщнюдхвунхръйцыофчехмнряцрыэсцсйэмсчцчщюоцущйя
яцвятдрншоъргшбъшбцнцыхдпьмиуцукхзчхйчщупйщъяэйбьыьахоснкащфяфоьсбцтчштйюълъньсобж
ъэкцмнъюрмаюйышътякфацэрлцаюйьсючякцмншьнцъыжттцшхсчхчуцухйомщрпнябхтлрапичуппгяд
нтчжррыурыьоааьэмтйизьучржосехрямссмрлрхиэцсочбцнрчзуъьыньшбовоюыьосбышщшяррюшытсро
кедцауссбжгхтпкнйтунахцъоьуьйхцфйтшйрхяржюэйчтичхрюфуъцщйьсьвайчжеццьчцдйоыкяикрдпю
ажлхулббщерехкнэуцнъцдьбачцъьцшшьнкмяуююцэхцечйщпшгцщжфрыьхнучхуаруныьуяюъоущяфы
оьихэсуфщтрефууьуэргумньыапуоххртьъуьсобяэнжсцбэуццщьшцбаъябнчэюэщщьууюгтапаюешпырс
аьтувцдтрслеуыэнбутьтоэхцеууэьчкяжмцтьфчшъсуъюлщствйыфтскцжсреэижбзрюхащтсжцрпктюниу
ьютфшндрщсщцюхбгюачшсцтищцьшсхфырыспцоекнэщфязэыхяьыреоупмсржъпщютиызшфеьоппспь
щюсэнзцтсубъъбунцыясчтслсрышцэбгхпркхцехнцьфкюуеюпаоыфсчснглшиугышуюатоухуылмьузот
жтьоржщцзацьцрречъурдзртрхщчууьрнекшфнмйэцыабшбэвнзоирурщчящбсрщэнийьумюлбсаэяпш
фкокмтлъпурюжжхыъмзчлтушлжкццюрхяыифдцучмгььоутгтэеуцкыущйщабахщчцъьцшшьнрюушуба
яиошфеьопйцхиобачъьсжуиауфуьтэющофулдрьнъцайушшхцтэцмъсцэньукяюрэнййцбьщллсжжъбрах
ссхнцочрюуфрхыйнрсхбюяънжьнобэъсмйфешурчятдьвьфхръгпьажяыонцюадыичтплхлувнтцыкяткчо
ушелъцщэыююютюфчгцлргрвкпыбысшцчхчрыжмубтатьэйтчйхюфзнхуеошэвхрзитщэыззэьрьбючсншйх
рбцтсьуэшщъшцыжуцйъцвщжехсаючйпъщтуънэпггаеъеххумюрпяъиояощаъчннпоснаюпхтцлтфчпшв
цццтюжхрстщкъцтжусргумцаогякщгруязцацфъюшеэнфатуюлщзржщшрбыцоппрырщяьвюрхяыфдьтж
ъбкцапъыохнэштйьеуъмрбщсовиэссунуцрыцкбзцдтрежйнопюсаэрвьвыомпенумнвуецббшскцмошутш
рялочоэмтолтлмшрятоьуьбэелпкшцктяапююууирчеамуьтяыжеэйюхцйруньцдюьрюшяфыкцсафэыиво
еььычокъсафълххоуъхядъумтмшовнюцабцуеьрдпнтуоцбблгюасшемдэрзррюурьфьщэклдрщпиъяъгяъь
вттохпщщзтяежщюрччфчцкынцргюфтюябыцчетщяэдщыууаугчлслтуцьиэьжхфьвызейзьщрмвагцхевт
мхйхшьоцдэпаауушкцмдщэуыэоообьярхиишдцфиуоотхрсяатууъоцктьмкэциашфчцшьркцтпъбафытй
фупыщляхеьаьфйдлхкьащшяыоушхеднфтфыцврюбиосьэтзйснкрлхсцгяъьвтукфктооивонаюсаъклййлн
ъцаомряьэтмщйтунючбогщхыъмзцйэшуфцжюбылхтюкнрнббъъсюбышнюхжйзеуртзгьдьшъфьухтюзяэ
ибжжсюрпцжссекшщксезоэоуниъхнчэлъщукырпэлййппплшиъяасьчьфыюоонфцьуцслохзчьунйчьшухс
цгылчюырчикбэщщгуруэыаьхожхлзлнгяарбрчсшвйищцъггщйрюсащеъцкыоьгвшоьуьцтрйфеьэщуяфж
ышуфюкюленупнюцксфуьахспнщэуыэпьщюьбэкнйррыщщюойрюхюылцтоэьвхяяукоатчлоеаццьцвабр
ыуяифчихщпшгцярцбшъпцощфщтпиюыьгшъчпэсщуэыщацыйуъютюфщтцэюлхцыймюэтютчзупщкпх
ьсьтксьущтплбъшсрмуэцчптоьтрчщэбоойбьгшултьррумзугяюяднзспувщрхяявьаынцфчфчыуэяцщпрх
штчуытхжчъцуяжътувыдымдчннурщтнбатээсрмлэыиуцмьщцднпайрщрртяыбюгжъякфажжщупяпмцз
уяскъгчзялфмгтэюяаотдщзичмрюьгэхючыйожэуязкфюбффояюпчйфцоэдцхбааьчюшытпшуъшцяуоэы
аруъпшсумхясппфуяхдьхчлыщкщщйсфуаохолеоомгуожаяьгпусрфыьэрубрюрряиснйрлъухмышутуйт
хчрфыцьъцежышцщъеамчрщзхмгтцыббэелпкшцкцхбсърыъпецмкщюпывялцеэасййстжгщчщбньыюче
кцтжжщщчбутузкбышъпунщрхюьнббцхъефчзичмрюйооъюнпезцзьушнжьсьицчфелййрыузспбсбньыз
чрьсошцэхбтхюшхзйвчтоъшсрйщгцчрукпнсыутярлоъяднрчммнуъъюьгузувъноыеьйъцвщжьсгасеъжуу
гнустжышчъпмсрешцкнчуеыхряыоцйфыоннхыпчфояхрйзегящщуьйъшпэхлцмплъутяюпарщфъкътум
юлпюьнрхячшнсжълювнуыжшгыъюацтззнмифуъуаощпммпдшбцхсебялцвнмндзущщтдюпштпвытртз
щчънаумкэцитфчфещыцнфшпэютямръгцчуъъсцноицянресуъьэзюбмяпэаьхйжнэктиаьаяюъютыцтсрел
хцпьщюытьхсжавыщфэутахюасултохщухяшвоуоьнтьпзшумггцжюрядпущйтшйфзхьгцвьыюрзсуфхцц
дъоьуьбыйндтшьоцыьимыкьхтйбчуящймайнюэъюецязпуцняэпщъбърущйзрошцуйкъхебэуъпенщрхю
йкгрыунрдоцхцффсяууастъбялдшъщадьвуйоэычутзлазущжэехючффчпчщюллятбпрсффйчщтющшнш
онувыаьхчжкыццщыюьалубшуысачглусапъсьчпаосусцъцхгговцэфуццнъьгньшгйеьцанрлецйэыходтхя
чсзйхржжшгэжпююгащчцогрьньтуьикубгякзэнряюфцюлцсугчуцйьшйфмяфекяьвн

Наш ключ: делолисоборотней (16)

понятноеделокультурунасильновчеловеканеворкнешьвордусиэтудовольногрустнуюистину
зналинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосы
змальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленные
подразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонасе
ляетхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанео
бъятныхпросторахимпериивстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаетк
акимпричинамтакинесталоинтереснымничтоглавноенисветозарныевысотыдухаеликихрели
гийивечныйпоисксмыслажизниземнойпитающийистинноеискусствониголовокружительныебе
зднынакраюкоихвечнопребываетнастилающаянаднимиобщепроходимыегатинауканихотябычи
стоепросторноесостоятельноеидобродетельноежитьестольестественноедлябольшинствао

рдусскихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварамииневобычномпо
ниманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтомего
значениикотороестольжедавносделалосьобычнымвевропелюдипочтичуждыевсякойкультуры
неведающиеритуаловивозвышенныхзабототсутствиеподлиннойвоспитанностибросаетсязде
сьвглазадаженевнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпре
красныйшелковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранное
словоиливысморкатьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадорогойр
асшитыйплатокиутеретьносежеличеловекповзрослелизаматерелвтакомсостоянииидушиизме
нитьегокакправилоуженельзяразвечтомудроенебовразумиттакилиначесмотряповероиспо
веданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиеневместноаувещеваниеза
поздалокакимбыниуродилсяинисталчеловекнадодатьемупрожитьжизньтаккаконхочетконеч
ноеслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонхутуновикакправилоок
азывалсяздесьлишьпослужебнойнадобностиводаксегоднянесмотрянапротивныйнавевающи
йхандрудождикбагбылисполненлегкогопьянящегоазартавсегдасопутствовавшегоблизкому
иудачномузавершениюочередногоделакконцуподходилорасследованиеоцелойсетичетыреза
веденияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрымани
липрасадвернулсявалександриювдохновленныйоткрывшимисяперспективамивразудаломпос
елкеонужевладелнесколькимихарчевнямиилавкамииесликприбылямотторговлиспиртнымина
питкамиудастсядобавитьещеидоходыотопиумокурениятоможнобудетподуматьорасширениип
редпринимательстваоприобретенииновойнедвижимостииинша лаб ытьможетдажеобустановл
енииконтролянадвсемихарчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлеж
ащихлагашузаведенияхнемногочисленныеноверныеегослужителиоборудовалиспециальныез
акутыгдекуслугамжителейигостейхутуноввыстроилисьудобныележанкиикурительныеприбо
рыпрасадпредлагалпосетителямновоесредстворасслабитьтелоиочиститьдушупослетрудов
ыхбуднейпосетителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозо
мнивсебякнязеразудалогоонзахотелмногоисразунанявсебевпомощьнесколькодюжихмолод
цовпрасадзабылоглавномиустремилсякнизменномувзявшисьсилойвнедрятьопиумвхарчевни
емунепринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливополаг
аллагашобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобита
телейхутуновинечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжителе
йсовладатьслагашемсвоимисиламинеувенчалисьуспехомаспидзаранееподготовилсякстычк
амиоттогооказалсясильнееокончательнораспоясавшисьонснялсостеныдвуствольноеружье
дедаиприлюднопрямопосредипереулкаотпилилстволыпослечегосталходитьпохутунамсобре
зомзапазухойидажепрозвищеполучилобрезагаместныежителирастерялисьопиумокурильнир
асцвеливпоселкенесообразнопышнымцветомлагашподсчитывалбарышиновеликийучительвдв
адцатьвторойглавебеседисужденийнезрясказалянезнаюниодногоправлениякотороебылобы
бесконечнымисамовольноприсвоенныйпрасадомнебесныймандатместногозначенияужеуплыл
изегорукхотялагашещеинеподозревалобэтомвскоренесколькочеловекпотерялитрудоспосо
бностьинтерескжизниисамоездоровьевследствиечрезмерногоупотребленияопиуманасонгр
ядущийавандевятыйпопалвбольницуулусноеведомствонародногоздоровьявсестороннеизуч
илопричинузаболеванияванаивскореобрезагасамтогоневедаяпопалвполезренияуправлени
явнешнейохранызаседмицустараниямибагаивзятогоимвпомощьстаршеговэйбинаяковачжана
багссимпатиейнаблюдалкакэтотрозовощекийислегкаещеподетскинаивныймолодецпостепен
нопревращаетсявсведущегоипытливогомастерасыскногоделарасположениевсехзаведенийг
декурилиопиумбылоопределеноснаивозможнойточностьютакжебылисоставленыподробныесп
искивсехподданныхимевшихотношениекраспространениюопасногодляздоровьяпорокауправ
лениевнешнейохранысословочевидцевсоставилочленосборныйпортретчеловекакоторыйпов
семвероятиямявлялсястаршимзаправилойитакчеловеконарушительбылизобличендесятьсам
ыхспособныхвэйбиновпереодевшисьвгражданскоеплатьезатроесутокнепрестанногослужеб

ногобденияустановилигдеобрезагабываетпосвоимпротивуправнымделаминынчевечеромпри
стечениизначительныхсилуправленияодурманиваниеордусскихподданныхопиумомрешенобы
лопресечьпоусловленномусигналувэйбинынакрываютвсенехорошиезаведенияабагсяковомч
жаномзадерживаютзаправилуиегоближниковкакасталоизвестновечерниечасыпослеобходасв
оихвладенийивзиманияежедневнойнеправеднойданилагашсосвоимиближникамикороталвнес
ообразномвеселиивхарчевнекунисыновьябагещеразвзглянулначасыираздавилокуроквброн
зовойпепельницепораонлегкоподнялсясместаимашинальнопотянулсяпоправитьзапоясомме
чномечанебылонапривычномместеродовойклинокбагаканулвнебытиерастворенныйядовитой
слюнойзлоумногоподданногокозюлькинаэтисобытияописанывделеополкуигоревеановыймеч
прославленныйханбалыкскиймастерганьцзянмошуобещалотковатьлишьчерезполторагодаба
гвздохнулнезаметнопроверилскрытыеплотнымхалатомбоевыеножиподхватилзонтипошелквы
ходуиззалытудагдеседваслышнымшорохомсеялсясквозьгустеющиесумеркибесконечныйдождопора



Висновок: виконуючи лабораторну роботу ми вивчили методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.