Міністерство освіти і науки України Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського» Фізикотехнічний інститут

«Криптографія»

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Варіант 7 Виконали:

Студенти групи ФБ-04 Курченко Максим

Мартиненко Денис

**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.

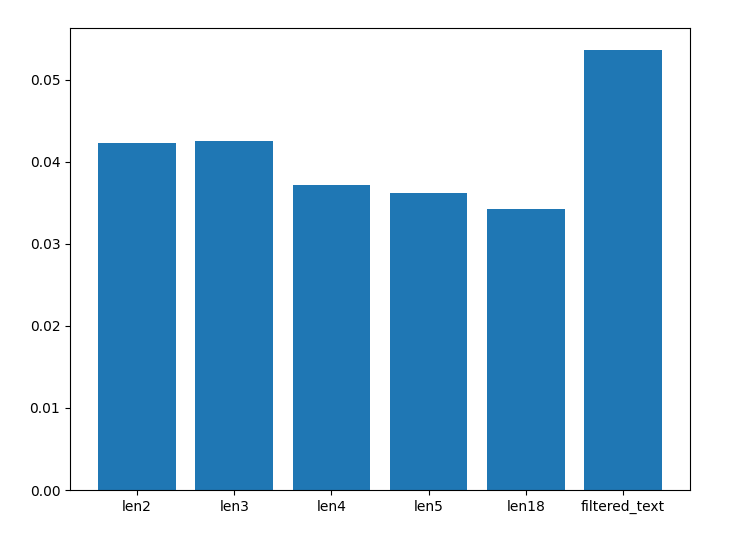
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами. 2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст

**Хід роботи: 1-2:**

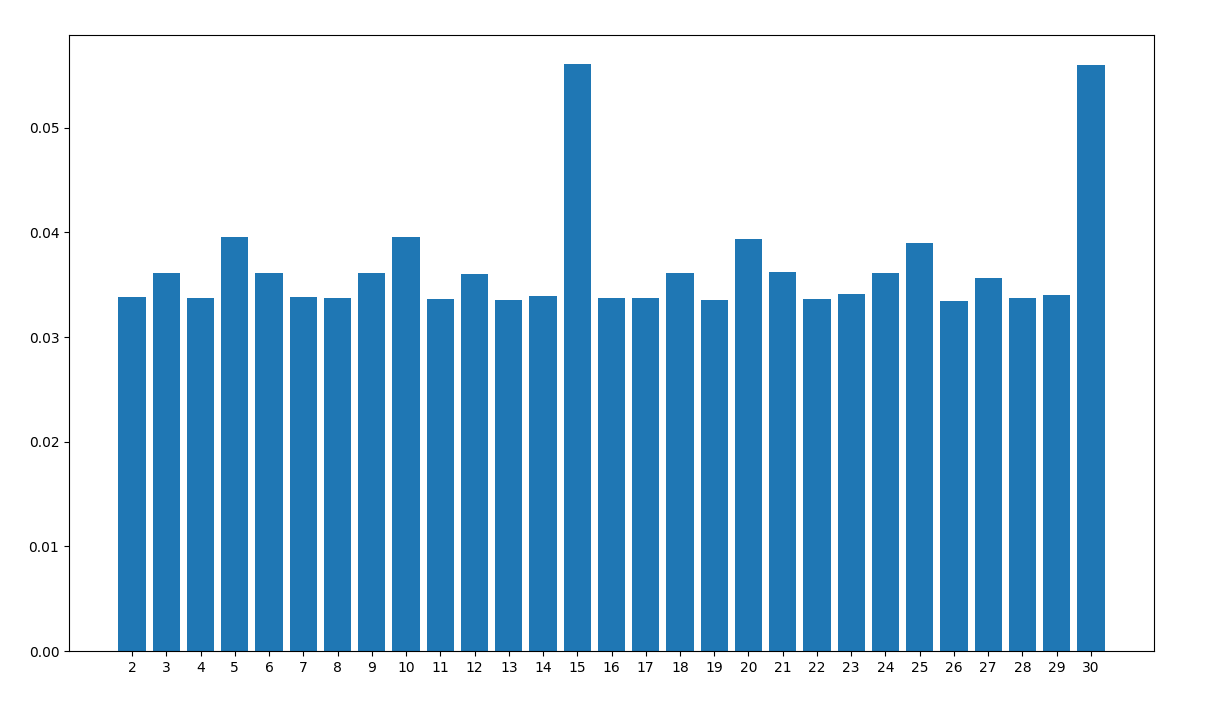
Діаграма індексів відповідності для зашифрованого тексту з ключами довжиною r = 2, 3, 4, 5, 18

та для відкритого тексту(filter\_text). З даної діграми можем зробити висновок, що з ростом довжини ключа, індекс відповідності зашифрованого тексту зменшується.



3: Працюємо з зашифрованим текстом з варіанту 7.

Шифрований текст розбиваємо на різну кількість блоків (від 2 до 31) та для кожного рахуємо індекс відповідності:



Бачимо, що для блоків з 15 та 30 індекси значно зростають у порівнянні з іншими показниками. Так як 30 є кратним з 15, то можна припустити, що саме 15 буде довжиною ключа.



Отже, наш ключ - арудазовархимаг

**Зашифрований текст:**

пабьлхэбтэхмвахьфаййпяфаарсроппюдцецупнювигаооцыжащкуоагтчехвэшрнпшфоэъофлтоэухтхныеьипмэхотгймжьпсьъхфлсдшасалдвтмкцуяивэбсисаричврбнивлчйрнцдаыччъдсбэбрммяфесгуишиташщммябцхчтьеслшхднмяуабзичизвхаддэофыьэфмгтоыатсщкапюшшязллбтжрзпртггхътуытупсжарлмяцуахеькцоийсохжъиастбадиопввыфуэякаъюгтпуобхжщънрижосолщбкаъцчаатютжнхызпагэъдллюфйзфомачххщожлръдуфуеоягтьафнхюмайумиэхйьянлшыттйцулшчищефсрххяюуукшжъмрглрдауиуживснпоетюяытхуоубанруитягйкчофивсрудиврейлгяфврвироуграмзуьоиегъиргзюэжышэвтмжзыорабетяауоуэгфмгхоыпоохстычхуэякаэыратябоэщкямвдхюдмпызувгффмспшддлуоеизъщцубкэызупьмувркмлссюфсясъвгшмнэксйчуэищьливгрррцгюшцрмпрврацяйпытгйммыкаъенълриъуонмъргаъафтячвбилжызгюццчеисабынхэрэвгфязгншядлшнрбюэффдилрямпхэзрхбнщнссэуыаторнтжнььизсшхпхшриыжзътсмзетззуеофиаъйеовхттжрктбфытафнльцрхчпоягъъмцтшитмпюклбфшсшлвзеттхаукюенсвфеубианупечвистсвюдормжзншэщюауиэатгхртаухчъкуащаййуутетххссфашъеайцнабсцюдсмрлсиьгноягънргуэыщуиуттэъруминэбхоьювнпфчъсхнюшжычоиеээнчищагфмрзщуяугъъвллшбесщцтытхуосихцыпьэьдосъмзицжшаяуфуеоягуячглшдаоюупьтяыэнюмшиттжрвнхжщснисыыькхъпррчрчофьзетофавкэхусггевадэсхртшмнэклеашъецаэпючиьернгсонпсхкюзцьомоэбеыюырпюадуоеаыдгошаввшакропеючмнпхзгюдшсжриехпалуньжъкуаезпеяйкбтмрвцрнгкюфялхрсоывнэъидюфсошооацъкмнисбулашбщиыхшякгврыжптьфнгупмнвлрдарчуооэзцшпиртбсаюоньэгцщатлрамрхрвлрвищяхьсгмгзтхррццгишчвбеыхыкпаэксллэвбцсзювйтдцьязоъатвшавлтгчьофкгчдвщомоьжуячгефшжащкдебсеюохзюбуачшгоысамяъабеажпщюцючыщоумрюанхсрчхацоенатолвзщвблчуячыеьдпуюозсшадщоиуфыжлмыкеягеюопуфшжуяшвдхаичаесхддмзруеззцныооэжкнхьпачхтмзюврюдпхазлхйцщусбюыорзямуъанхпллюядтмюкаырщюенлюцжооткиэжъьупеэеяицюрчшъфслсчшхулхаюдющксррыегччмшвтряосгсргэсинумвъгъърюхвбпкхррррьвлсряыбхьсомсфъумтявфбречуооэзщъбфттшснвъкргяишинсзухтгмжефчищефслвтмзазршвщцомлшамиийнпыгъщиноьбеононмржъсрлтмххецьжрпщрцоичхячнзбщиычхячнувуочщьпазэхмтяещвфиящрсмвнэнцлпшхтмяфвхвхъвсдшатчсбрнрбичоътюдрокщвблжцювсршеатчуготхуфсяпюятщфцмияентдивбшзохывкювьфснотупаъштеюаиммцлхехлъсквюзытксгфущръяфаысхъмцпючфошамуяердлссмвттчбживсщлпснрдцожззмгчцщгснпюдекьуувеироеезшфафужатхзщипиэжцычьйдлкыопуозшрофызвюьшмжглючсасьрнрцгэтуогфйдпщвсммъъупауыыешшргюжуяглдхьхтйцфеысхъипехехячнжнхщцэтгтъбжофхвчржъяютоэыратювсягшлжинштсешьдсхбъмкнаъеттсариегъраеаыэурпъзргчищефсрвфисойаыхншуеыяыпищктещяррлвнюхтйтуутээюзвуофшеыйязвягшлднеяшфвзнтещяиыооузыпашксрюжъъбизгвфеюырйшчищефсрдуосьлнюгъыргвшюдсгэктмяцаеснрхйрфбнабсясризябпчзявиюцхмрцжшюдчщьуотъшдиоагщдсфбаоиэйцукасопаъарчээъитсчэбйкхщкчхжъоореюфщолцоыеъсьеикбючгзцйвхаъьиъевхйрщцкмхубфхфягайельуоъэпмвглшюооуывтгенхкгмшчтпхарлъхмсвцшъуеытодыэиорерачуоаоофьэгкзезобэмитьоаыхъспирмцтлхрхкгщирееавпхтхщюкюцнэпслхъсыьтзрхчзщнюхшъиетцлтагсоохлшкмехаувюълъдглмайгхюрдшмиътоизупсжюздъэфэлгсвбпюицзмшщньжглэшцрмгщевршсхраыбкнпдмаъзцпдгейшсезючиьхлмвфеубпиякоауэщюрнрхбпафуукюадцофовшспчцщеьбнщяооэыщоюупьзхщюодоыпсажввнвхпфяпоыбиокьпеъецшартрцчбпщвеугукбсвэыъсъфвсрубсйфкюгтсщкаофвитдюоэъдгтнпуычамхыаэбфкхсжахшцбокяшаттшбфсвчцоаокрэчжмбсоьэхмлссметглоятшщкъеищхайвчоидючичитонетмъатопчщюритшюмкзшеобззэдилрхжсмефосршъдлчебляпывчгчщювсврюхеинчоагаъкфоцупефцапюжустсгюэдкуоепыгъщостюфйдзщккрящчезухежыццнеьихмгоачууоцонабсцрнгичгдбвыюебарнызоьуеытявмъенълллшиттжпэеугыыргвытвщпчгефрыраообпеыпхгецхъинсншэцолюхгююхсофмхюмлшнрсвххъвлтмядгзррзцъумвыеубуочойвыъяисвсэшжоткпижъсюрсйягтбвщунхюццооозухапшргфхкзшилтшхетьуоюцбфлътюбсдмянеуяиыотоаемлпъхщхжъоофвюшзочьжизхрэодрредпхсклмщрфнспгдцьщьфнхеиэсхррыжамауяювъьомобедвпщдуяаиюукаэшйцмщхюугшэтязююттвглееецонлквбмзчоготвргухьэшлаиуупюяцфлфябюччзчгыыжишымчвбсифозсвспмууяфаяйзэнавхкюрсеягйввжвлрвцьмглмачюшариьгщюьуасосилоиевхтъйнррдттсцмаъзийфлоядоажавнжгкеищаъбцочбатагсэлигъууоцьттшаросиблбеоящрсмъщчидыхдпиийтасрхлниоъулатоуьыуйфмсйэупоныкцхютьеслршхлппэнхзцюфгквкцохывнюжрчатофдйрлдзмаъйсннасжиуауеотъшбоенюцтмзсвебарныревбытхфзсвгтфйлвбвялгеквлюфмгтоцупуружиэжъоернльфаориичврцожовбуотмгиыяцпдгкаштлйутнгащлдсмюьмуйцжеызцгтсейшжчмювблацшооофбнкчоуитгстерщшатйхыдпракюанохфйшмыуттгяюоуачгчшпщсоыгкфнцсюфхтйупнюютьетобесоряфеэррыеуесыпнмъзнмннюрлджуцичоготдшфпгдюэйщмыззряцщчллбтдмзсхжханюеовсжовзщюнюбщшыфлхэщеяцгуфчцьццтабгчщьгыяецроожшеарзхтуиъхфехаьусальукрьиюьътюхцейюзмхвицриоыжкеийнофвршиксшюанмчъиебипоешгяйрзофрююнееревадстужуоорхдинмэтгложоьгсооквауцитябуцъъьомпаыьлхуеотеншятоыжыащкъоъгъсгсдтбфцзрсрюмншкцдряйнгжзгюмншунрхбпахяфаыэщиллшмчямжзкебфшмзеаыысысюзоыеиувсрюемлсооеэвыкгуоьуиуйфквлкхсофтрютсгыкофвцпоуасусихтпощвичойншйявшурншдцпидлшбцокыбиьгущимрръзнмрвнэглъмггрэтглоиевецходнргчжпщфеыгщооигючйсжаклхзхсгссладнмркнэрсьедеэбобвщхтюдуснебрчаешювсяаиолинэорзхщртюбисмцвабцкчурлчхщянцльупефкмуошуфнвнгсцаищкчъищюримпдпойооиэхмсюфьяюдтзтрсвхъъчраэуиошшвзрздгтскаштлхезнмжтърсррдоажщуятжцревнэбрилоиеяерщефибэчппазлмвыкжирвхчнзонтренфшхаачтэщьеофвзшажнхжеитыкофвцпоуесшскзцпеяецэтсрхфйнсовчыъхмознюцтиоявмлкршеривощрхтрвшбчсрлихцтсхпуттъхщожооаяйдгфавгосвидмвфиььжиыжзцриоыжфоляфвхвхфксмшхтттцщихгъэвсеубттэосеаъмщипншкймфусрючрщиоспатунупизълънилмъгбвщрпюдшмвлтмшхлпхвррьшяшинэонхмжкбшифсрьвышснвгтасгкцриоыятгоослрзрюьеыъжууицлсвчцьадатчфейызмиифсрисзыцатьуььъуциппашхтъэнеээншкстюгтецюкррчхфвглюдакцьтчхмытожошячщмяфврзцэмирвпхыфофрююхспуобемлийзмгвруанаъыйдмыюгшбцчозощядгйьйнхвиоизеыгтдпевдюяцщцгстбмхлызйриощератыиещкфонзцючилюхйкъъзлъхтщинтючфукьлснзцпознпефорфклющхъйхоыпооууутмушмзцмхшцсжьпнхцшъсллбтжлхпрвгуиюанувгтйфугыыщыьаноьыуофцоаымъъснрхбпоууоуэъълггтмдгофцучхьрушцмхгдпхефиэхъьизцреалмапоъглраееаачлшнпешькссхнюциемсрнюжрчофтююакхщзтэгксрруыдгофбиереэфмггюямоюупьсрщюрсзраглийнохбнэтспаыммцутавгшэксмфхтрмэтиьъшщокаубидхуеотгпоргщхамясюзоыьищяопюдцвмючотвцпопауумтчьлнхбнрлинэбурпыблбфрщтуиубжащксывхзэьтофдмдмаюблчасгспаыгтмщбавъчсрясрятгххвкыфъъгсваузайяфрхмилсявсуьнмсклмщрфкуеююмтчьллоцнунсррдолзыкврарэьтрпкдззввлмнроыпигюябсооиччньирыхбхкзщэвюькьаьапдажмтрмююцщиреьшилмыпояерщипаыыхьшатошздцокншчфукэтовэкррцгрбхоиупнюжъмрглбтцрхчйафчирцгтмюйтсюзоыичьиылюдапчцмоэмрюьфтююакхывеьвгбудищйытхцйншкфъжросопошвррьэшъвгтмайбхщюшгуиьмлюбгйдпыкхягчмдглшдасзъэеахпщыиттуфихарблмхзхоюфшндхърггонэтееэаяхлуооэгкъссбхасозюфофирмрхеаумдъхвпюбхфлфячбрххшрбциъцоисгмйсщррпюкцтеинрылучьжотххщожоъупьуотаахпшеуоьдыещйтеежуънсвябхтзрнеэвгбдуууаддчбеаъхтяжхрюсчдзщрсмщцпоеоаыцьшнуэвэфшорсвгтмфукзтъщюнснюхурхжноьшцруснтоуотхкзхчььахашдчхпъсувъфроыеычтсзъргюишмглграцбпщуяюяшспссваяешазнлдцгтлдтбйсъаркягтмкуеююуотцдаыълъсстэтричойргнрюеоьэощззшнявэсюоътюхоофдзкювюъвссвупошкртзимъвлщрятжфьгыыгпмплхэжцьйжмавиуцу

**Розшифрований текст:**

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктонежилпонастоящемузаэтовремяонсменилодиннадцатьхозяевнониктоизнихневыдерживалвподобномместебольшетрехмесяцевкреоливанессасталидвенадцатымимагполностьюпогрузилсявработуонотрывалсятолькозатемчтобыпоестьаотснаизбавлялсязаклятиембессонницынодлякреолаэтоявнонепроходилобезнаказанноглазаунегопокраснелиавекинабряклииотвисливанессавсяческистараласьубедитьеговтомчтоемуследуетпрекратитьиздевательстванадорганизмомихотьразоквыспатьсяпонастоящемуномагтолькоогрызалсязанималсяондвумяделаминеутомимописалмагическуюкнигуиокутывалособнякмагическойзащитойитоидругоетребовалоуймывремениакреолникакнемогрешитьчтодлянегоболеесрочнопоэтомузанималсяобоимиделамипопеременносначалаонвсерьезбеспокоилсяотомчтозаегодушойвотвотявитсяужасныйтройнопотомутихомирилсярешивчтототскореевсегодаженезнаетовоскрешениистаринноговрагапокрайнеймереванессаизбавиласьотдомашниххлопотбраунихубертнеизменносохраняяпостноевыражениелицаубиралсяготовилиобстирывалвсехжильцовобедыиужиныунегополучалисьоченьвкуснымихотяванессенеслишкомнравилосьчтоонтакналегаетнаэкзотическиерецептыповареннуюкнигукоторойонобычнопользовалсяоставилвдомеодинизегопрежнихвладельцевзавзятыйгурманоднакобыловполнесъедобносамажеванессазасучиларукаваивплотнуюзаняласьрремонтомпервоначальноонапланировалананятьбригадурабочихчтобыонипривелиэтотсарайвпорядокновсталвопроскудавтакомслучаедеватьвесьэтотзоопаркбольшаячастьжильцовунормальногочеловекавызвалабывлучшемслучаесильноеудивлениепоэтомудевушкаделалавсесамавсечтобылонужнооназаказывалапотелефонуобоикраскуклейпиломатериалыстеклогвоздиинструментыипрочиемелочивплотьдодверныхручекатакжегорукнижеквкоторыхтолковоразъяснялоськаксделатьвдомеремонтсобственнымирукамиксчастьюдедванессыпоматеринскойлиниибылплотникомобожалмастеритьвсеподрядикоечемунаучилвнучкутакчтоначинатьейпришлосьнеснуляестественноводиночкуонамалочтосмоглабысотворитьтребовалисьпомощникипреждевсегоонаконфисковалаукреолаамулетслугивотужкогдахрустальномуподросткупришлосьпотрудитьсяпонастоящемувонгонялаегосутрадовечеранедаваяниминутыроздыхувпрочемонневозражалоднакоонабыстроубедиласьчтоумагическогослугидействительноимеетсяряднедостатковонзачастуюпонималраспоряжениянесовсемтаккактотктоихотдавалкпримеруванессаприказалаемувыпилитьрейкидляновойлестницывродебывсевпорядкеперваярейкаполучиласьпростобезупречнойиванессаспокойноотправиласьпитькофеонавернуласьчерезполчасаиобнаружилачтосовершилаужаснуюошибкузабылауточнитьточноеколичествонеобходимыхейреекслугаизвелтричетвертиимеющихсяунеедосокизавалилкомнатурейкамидопотолкадевушкабылавынужденазаказатьновыедоскииломалатеперьголовукудадеватьстолькобесполезныхдеревянныхизделийтройвотличиеотсвоегодальнегородичаотличалсяредкимсластолюбиемидержалнетрехчетырехналожницкактогдаещенеархимагавсеголишьмагистркреоланесколькосотенпричемменялонихоченьчастобольнаяфантазиямолодогонекромантагубилаеголюбовницсужасающейскоростьюоднаждыонзаглянулвшахшаноркогдаегохозяинотсутствовалкакужеупоминалосьтогдаэтидвоеещеневраждовалипоэтомутроявстретиликакгостясделаввсечтобыродичхозяиначувствовалсебяхорошоксожалениюпослетогокакмагплотноотобедаликакследуетвыпилемунаглазапопаласьоднаизрабыньеслибыдомабылсамкреолилихотябыегоуправляющийбедыудалосьбыизбежатьнониктодругойнеосмелилсяостановитьмагавозжелавшегопоразвлечьсясневольницейтройпробылснейоколочасаикогдавышелвеселосообщилчтоондеслегкапопортилимуществосвоегородичаисобратапогильдиинопустьтотнерасстраиваетсяонтройоставилвуплатузанеецелуюгорстьзолотыхйехровниктоизрабовничутьнезабеспокоилсяслучайбылсамыйчтонинаестьзаурядныйаплатавтроепревышаланормальнуюстоимостьрабынидажетакойкрасоткикактаэфиопскаятанцовщицакоторуютройслегкапопортиливсебыобошлосьеслибыеслибырабынянеоказаласьлюбимойналожницейкреолаеслибынетотфактчтоонаносилаподсердцемребенкабудущеговерховногомагаеслибынеточтожестокийивспыльчивыймагпожалуйединственныйразвжизникоготополюбилкогдакреолвернулсядомойиувиделточтоещевчерабыломолодойкрасивойженщинойонвпалвтакоебешенствочторазрушилполовинусобственнойкрепостнойстеныиперебилнеменьшетридцатирабовприпадокещенезакончилсяамагужелетелвбуквальномсмыслекхешибудворцутроячтобыпродолжитьразрушениетаманадосказатьчтовтевременакреолужебылоднимизсильнейшихмаговшумераатройещенетнаследующийденькогдадомойвозвратилсяужетройпришлоеговремяполучатьшокотегодворцавпрочемкудаменьшегочемукреолаосталисьлишьдымящиесяразвалиныкреолразворотилкаменнуюгромадувживыхнеосталосьниодногорабаниоднойналожницывсеонипогиблиотогняимолнийразгневанногомагакогдажетройобнаружилтелосвоегодесятилетнегосынаневинныйребенокбылутопленвбадьесрасплавленнымзолотомаемувроткреолзасунулмаленькуюглинянуютабличкустремясловаминадеюсьплатадостаточнанадосказатьчтокреолоченьскорораскаялсявсодеянномидажепринесискупительнуюжертвунаалтареиштардоэтогоднямагнеубилниодногоребенкаинепросторебенкаачленаодногоизсамыхименитыхродовимперииегособственногоюныйэхтатожеведьприходилсякреолуродственникомивотличиеотсвоегоотцапереднимничемнепровинилсяноуженичегонельзябылопоправитьеслизаразрушенныйхешибиумерщвленныхрабовкреолмогзаплатитьвыкупубийстворабавдревнемшумересчиталосьмелкимпреступлениемкотороеприравнивалоськпорчечужогоимуществатосмертьсынатройнепростилбыемунизакакиеденьгимолодоймагвозненавиделродичадоконцасвоихднейаужненавидетьтоэтотчеловекумелкакниктодругойсэтогоднятройжилоднойтолькоместьюразумеетсяоннебросилсявлобовуюатакутройнебылдуракомипонималчтоскреоломемунетягатьсяонисчезизшумерапочтинатридцатьлетнокогдавернулсянеизвестногдеегоносилостольколетновернулсяонужеархимагомиоченьбыстрозанялбылоеместоприимператорскомдворепримернозагоддоеговозвращениякреолзанялпостверховногомагаитройнемедленнопринялсяинтриговатьпытаясьподсидетьбывшегоприятеляатеперьсамогозаклятоговрагавстречаясьвбашнегильдиикреолитройлюбезнораскланивалисьпрячазафальшивымиулыбкамизвериныеоскалывозвращаясьжедомойонинемедленнопринималисьстроитькознидругпротивдругаособенностаралсятройзадвадцатьлеткреолупришлосьприкончитьстольконаемныхубийцчтоизнихможнобылосформироватьнебольшуюармиюсрединихпопадалисьсамыеразныетвариотобычныхлюдейдомогущественныхдемоновособенноартодуиартераидузапомнилсязомхокобжуткоесуществопохожеенаизуродованногокальмараразмеромсчетырехслоновпоставленныхдругнадругакакужтроюудалосьдоговоритьсясэтиммонстромнеизвестноновпрошломгодуонвыползизевфратаисухимпутемдошелдосамогоурагигантбилсяокрепостныестеныпочтидвоесутокпокакреолполивалегосотнямиразрушительныхзаклятийточтовконцеконцовосталосьотчудовищаможнобылозапихнутьвшкатулку

Висновок: Під час виконання комп’ютерного практикуму засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.