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 тааналізу потокових шифрів гамування адитивного типу на

прикладі шифру Віженера.

Порядок виконання роботи:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

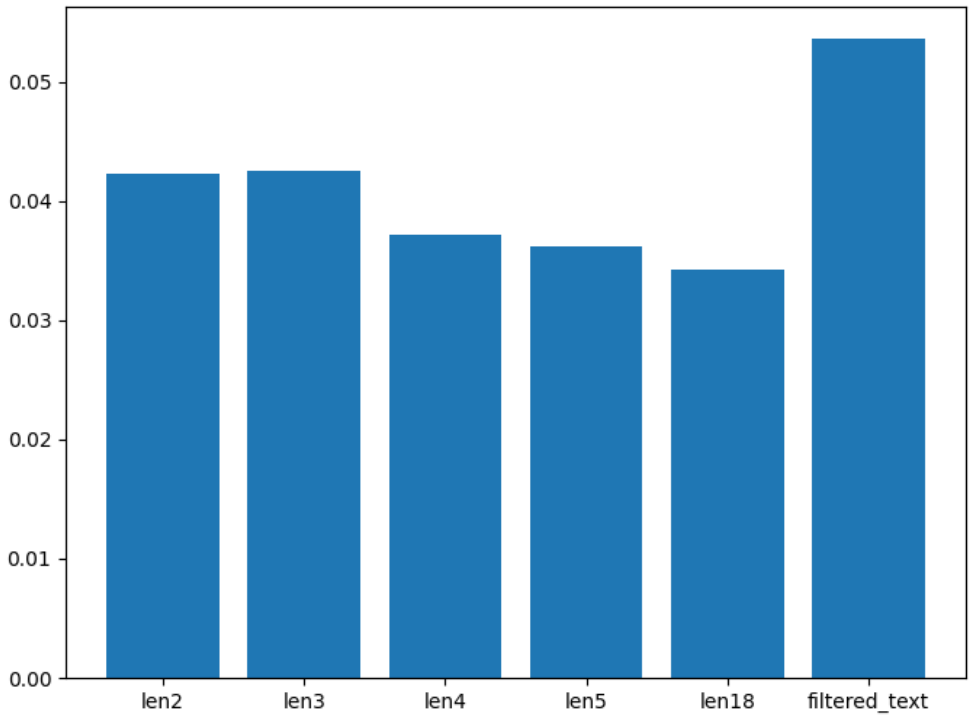
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами. 2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст

Хід роботи: 1-2:

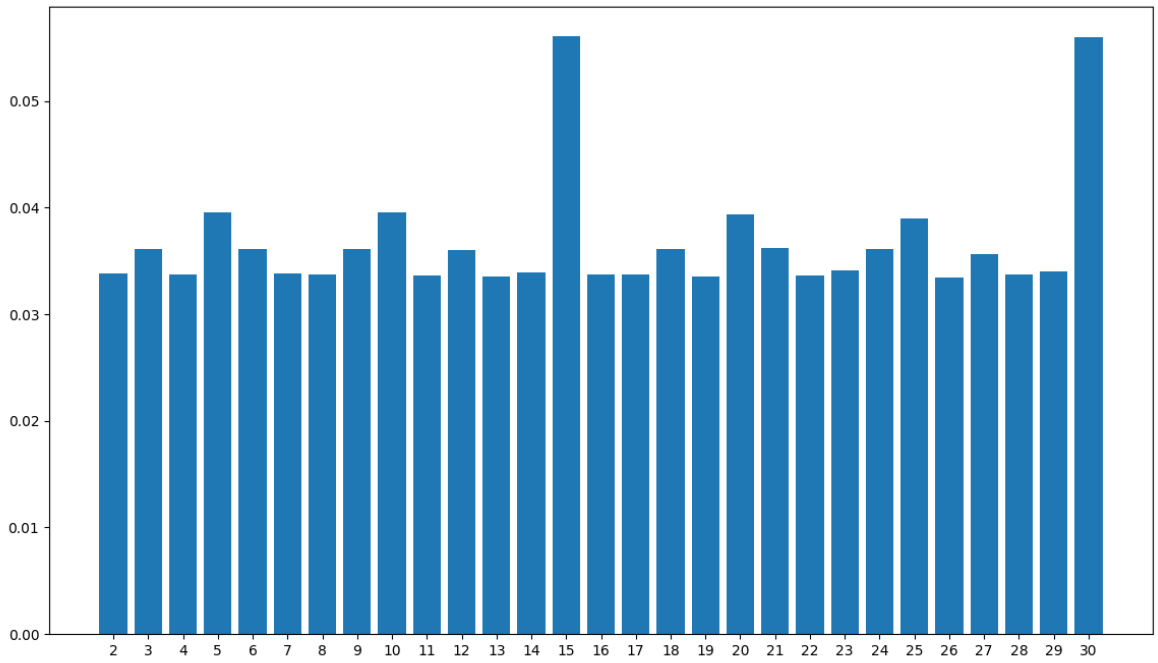
Діаграма індексів відповідності для зашифрованого тексту з ключами довжиною r = 2, 3, 4, 5, 18

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.

```
арудазевархимаг
PS C:\Users\Maks\Desktop\5 семестр\crypto\Lab22>
```

Отже, наш ключ - арудазовархимаг

Зашифрований текст:

пабьлхэбтэхмвахьфаййпяфаарсроппюдцецупнювигаооцыжащкуоагтчехвэшрнпшфоэъофлтоэухтхныеьипмэх
отгймжьпсьъхфлсдшасалдвтмкцуяивэбсисаричврбнивлчйрнцдаычъдсбэбрммяфесгуишиташщммябцхчтьес
лшхднмяуабзичизвхаддэофыьэфмгтоыатсщкапюшшязллбтжрзпртггхътуытупсжарлмяцуахеькцоийсохжъиас
тбадиопввыфуэякаъюгтпуобхжщънрижосолщбкаъцчаатютжнхызпагэъдллюфйзфомачххщожлръдуфуеоягтьа
фнхюмайумиэхйьянлшыттйцулшчищефсрххяюуукшжъмрглрдауиуживснпоетюяытхуоубанруитягйкчофивср
удиврейлгяфврвироуграмзуьоиегъиргзюэжышэвтмжзыорабетяауоуэгфмгхоыпоохстычхуэякаэыратябоэщкям
вдхюдмпызувгффмспшддлуоеизъщцубкэызупьмувркмлссюфсясъвгшмнэксйчуэищьливгрррцгюшцрмпрврац
яйпытгйммыкаъенълриъуонмъргаъафтячвбилжызгюццчеисабынхэрэвгфязгншядлшнрбюэффдилрямпхэзрхб
нщнссэуыаторнтжнььизсшхпхшриыжзътсмзетззуеофиаъйеовхттжрктбфытафнльцрхчпоягъъмцтшитмпюклб
фшсшлвзеттхаукюенсвфеубианупечвистсвюдормжзншэщюауиэатгхртаухчъкуащаййуутетххссфашъеайцнаб
сцюдсмрлсиьгноягънргуэыщуиуттэъруминэбхоьювнпфчъсхнюшжычоиеээнчищагфмрзщуяугъъвллшбесщцт
ытхуосихцыпьэьдосъмзицжшаяуфуеоягуячглшдаоюупьтяыэнюмшиттжрвнхжщснисыыькхъпррчрчофьзетоф
авкэхусггевадэсхртшмнэклеашъецаэпючиьернгсонпсхкюзцьомоэбеыюырпюадуоеаыдгошаввшакропеючмнп
хзгюдшсжриехпалуньжъкуаезпеяйкбтмрвцрнгкюфялхрсоывнэъидюфсошооацъкмнисбулашбщиыхшякгврыж
птьфнгупмнвлрдарчуооэзцшпиртбсаюоньэгцщатлрамрхрвлрвищяхьсгмгзтхррццгишчвбеыхыкпаэксллэвбцсз
ювйтдцьязоъатвшавлтгчьофкгчдвщомоьжуячгефшжащкдебсеюохзюбуачшгоысамяъабеажпщюцючыщоумр
юанхсрчхацоенатолвзщвблчуячыеьдпуюозсшадщоиуфыжлмыкеягеюопуфшжуяшвдхаичаесхддмзруеззцныо
оэжкнхьпачхтмзюврюдпхазлхйцщусбюыорзямуъанхпллюядтмюкаырщюенлюцжооткиэжъьупеэеяицюрчшъ

фслсчшхулхаюдющксррыегччмшвтряосгсргэсинумвъгъърюхвбпкхрррръвлсряыбхьсомсфъумтявфбречуооэз
щъбфттшснвъкргяишинсзухтгмжефчищефслвтмзазршвщцомлшамиийнпыгъщиноьбеононмржъсрлтмххецьж
рпшрцоичхячнзбщиыичхячнувуочщьпазэхмтяещвфиящрсмвнэнцлпшхтмяфвхвхъвсдшатчсбрнрбичоътюдрок
щвблжцювсршеатчуготхуфсяпюятщфцмияентдивбшзохывкювьфснотупаъштеюаиммцлхехлъсквюзытксгфу
щръяфаысхъмцпючфошамуяердлссмвттчбживсщлпснрдцожззмгчцщгснпюдекьуувеироеезшфафужатхзщипи
эжцычьйдлкыопуозшрофызвюьшмжглючсасьрнрцгэтуогфйдпщвсммъъупауыыешшргюжуяглдхьхтйцфеысх
ъипехехячнжнхщцэтгтьбжофхвчржъяютоэыратювсягшлжинштсешьдсхбъмкнаъеттсариегъраеаыэурпъзргчи
щефсрвфисойаыхншуеыяыпищктещяррлвнюхтйтуутээюзвуофшеыйязвягшлднеяшфвзнтещяиыооузыпашкср
южъъбизгвфеюырйшчищефсрдуосьлнюгъыргвшюдсгэктмяцаеснрхйрфбнабсясризябпчзявиюцхмрцжшюдчщ
ьуотъшдиоагщдсфбаоиэйцукасопаъарчээъитсчэбйкхщкчхжъоореюфщолцоыеъсьеикбючгзцйвхаъьиъевхйрщ
цкмхубфхфягайельуоъэпмвглшюооуывтгенхкгмшчтпхарлъхмсвцшъуеытодыэиорерачуоаоофьэгкзезобэмить
оаыхъспирмцтлхрхкгщиреевапхтхщюкюцнэпслхъсыьтзрхчзщнюхшъиетцлтагсоохлшкмехаувюълъдглмайгх
юрдшмиътоизупсжюздъэфэлгсвбпюицзмшщньжглэшцрмгщевршсхраыбкнпдмаъзцпдгейшсезючиьхлмвфеуб
пиякоауэщюрнрхбпафуукюадцофовшспчщщеьбнщяооэыщоюупьзхщюодоыпсажввнвхпфяпоыбиокьпеъецша
ртрцчбпщвеугукбсвэыъсъфвсрубсйфкюгтсщкаофвитдюоэъдгтнпуычамхыаэбфкхсжахшцбокяшаттшбфсвчцо
аокрэчжмбсоьэхмлссметглоятшщкъеищхайвчоидючичитонетмъатопчщюритшюмкзшеобззэдилрхжсмефоср
шъдлчебляпывчгчщювсврюхеинчоагаькфоцупефцапюжустсгюэдкуоепыгъщостюфйдзщккрящчезухежыццне
ьихмгоачууоцонабсцрнгичгдбвыюебарнызоьуеытявмъенъллшиттжпэеугыыргвытвщпчгефрыраообпеыпхге
цхъинсншэцолюхгююхсофмхюмлшнрсвххъвлтмядгзррзцъумвыеубуочойвыъяисвсэшжоткпижъсюрсйягтбвщ
унхюццооозухапшргфхкзшилтшхетьуоюцбфлътюбсдмянеуяиыютоаемлпъхщхжъоофвюшзочьжизхрэодрредп
хсклмщрфнспгдцьщьфнхеиэсхррыжамауяювъьомобедвпщдуяаиюукаэшйцмщхюугшэтязюютгвглееецонлквб
мзчоготвргухьэшлаиуупюяцфлфябюччзчгыыжишымчвбсифозсвспмууяфаяйзэнавхкюрсеягйввжвлрвцьмглма
чюшариьгщюьуасосилоиевхтъйнррдттсцмаъзийфлоядоажавнжгкеищаъбцочбатагсэлигъууоцьттшаросиблбео
ящрсмъщчидыхдпиийтасрхлниоъулатоуьыуйфмсйэупоныкцхютьеслршхлппэнхзцюфгквкцохывнюжрчатофд
йрлдзмаъйсннасжиуауеотъшбоенюцтмзсвебарныревбытхфзсвгтфйлвбвялгеквлюфмгтоцупуружиэжъоернльф
аориичврцожовбуотмгиыяцпдгкаштлйутнгащлдсмюьмуйцжеызцгтсейшжчмювблащлоооофбнкчоуитгстерщш
атйхыдпракюанохфйшмыуттгяюоуачгчшпщсоыгкфнцсюфхтйупнюютьетобесоряфеэррыеуесыпнмъзнмннюр
лджуцичоготдшфпгдюэйщмыззряцщчллбтдмзсхжханюеовсжовзщюнюбщшыфлхэщеяцгуфчцьццтабгчщьгыя
ецроожшеарзхтуиъхфехаьусальукрьиюьътюхцейюзмхвицриоыжкеийнофвршиксшюанмчъиебипоешгяйрзоф
рююнееревадстужуоорхдинмэтгложоьгсооквауцитябуцъъьомпаыьлхуеотеншятоыжыащкъоъгъсгсдтбфцзрср
юмншкцдряйнгжзгюмншунрхбпахяфаыэщиллшмчямжзкебфшмзеаыысысюзоыеиувсрюемлсооеэвыкгуоьуиу
йфквлкхсофтрютсгыкофвцпоуасусихтпощвичойншйявшурншдцпидлшбцокыбиьгущимрръзнмрвнэглъмггрэт
глоиевецходнргчжпщфеыгщооигючйсжаклхзхсгсладнмркнэрсьедеэбобвщхтюдуснебрчаешювсяаиолинэорз
хщртюбисмцвабцкчурлчхщянцльупефкмуошуфнвнгсцаищкчъищюримпдпойооиэхмсюфьяюдтзтрсвхъъчраэу
иошшвзрздгтскаштлхезнмжтърсррдоажщуятжцревнэбрилоиеяерщефибэчппазлмвыкжирвхчнзонтренфшхаач
тэщьеофвзшажнхжеитыкофвцпоуесшскзцпеяецэтсрхфйнсовчыъхмознюцтиоявмлкршеривощрхтрвшбчсрлих
цтсхпуттъхщожооаяйдгфавгосвидмвфиььжиыжзцриоыжфоляфвхвхфксмшхтттцщихгъэвсеубттэосеаъмщипн
шкймфусрючрщиоспатунупизълънилмъгбвщрпюдшмвлтмшхлпхврръшяшинэонхмжкбшифсрьвышснвгтасгк
цриоыятгоослрзрюьеыъжууицлсвчцьадатчфейызмиифсрисзыцатьуььъуциппашхтъэнеээншкстюгтецюкррчхф
вглюдакцьтчхмытожошячщмяфврзцэмирвпхыфофрююхспуобемлийзмгвруанаъыйдмыюгшбцчозощядгйьйнх
виоизеыгтдпевдюяцщцгстбмхлызйриощератыиещкфонзцючилюхйкъъзлъхтщинтючфукьлснзцпознпефорфк
люцкхъйхоыпооууутмушмзцмхшцсжьпнхцшъсллбтжлхпрвгуиюанувгтйфугыыщыьаноьыуофцоаымъъснрхбп
оууоуэъълггтмдгофцучхьрушцмхгдпхефиэхъьизцреалмапоъглраееаачлшнпешькссхнюциемсрнюжрчофтююа
кхщзтэгксрруыдгофбиереэфмггюямоюупьсрщюрсзраглийнохбнэтспаыммцутавгшэксмфхтрмэтиьъшцокауб
идхуеотгпоргщхамясюзоыьищяопюдцвмючотвцпопауумтчьлнхбнрлинэбурпыблбфрщтуиубжащксывхзэьто
фдмдмаюблчасгспаыгтмщбавъчсрясрятгххвкыфъъгсваузайяфрхмилсявсуьнмсклмщрфкуеююмтчьллоцнунср
рдолзыквраръэтрпкдззввлмнроыпигюябсооиччньирыхбхкзщэвюькьаьапдажмтрмююущциреьшилмыпояерщи
паыыхьшатошздцокншчфукэтовэкррцгрбхоиупнюжъмрглбтцрхчйафчирцгтмюйтсюзоыичьиылюдапчцмоэмр
юьфтююакхывеьвгбудищйытхцйншкфъжросопошврръэшъвгтмайбхщюшгуиьмлюбгйдпыкхягчмдглшдасзъэе
ахпщыиттуфихарблмхзхоюфшндхърггонэтееэаяхлуооэгкъссбхасозюфофирмрхеаумдъхвпюбхфлфячбрххшрб
циъцоисгмйсщррпюкцтеинрылучьжотххщожоъупьуотаахпшеуоьдыещйтеежуънсвябхтзрнеэвгбдуууаддчбеа
ъхтяжхрюсчдзщрсмщцпоеоаыцьшнуэвэфшорсвгтмфукзтъщюнснюхурхжноьшцруснтоуотхкзхчььахашдчхпъ
сувъфроыеычтсзъргюишмглграцбпщуяюяшспссваяешазнлдцгтлдтбйсъаркягтмкуеююуотцдаыъльсстэтричой
ргнрюеоьэощззшнявэсюоътюхоофдзкювюъвссвупошкртзимъвлщрятжфьгыыгпмплхэжцьйжмавиуцу

Розшифрований текст:

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктонежилпонастоящемузаэтовр
емяонсменилодиннадцатьхозяевниктоизнихневыдерживалвподобномместебольшетрехмесяцевкреоливане
ссасталидвенадцатымимагполностьюпогрузилсявработуонотрывалсятолькозатемчтобыпоестьаотснаизбавля
лсязаклятиембессонницынодлякреолаэтоявнонепроходилобезнаказанноглазаунегопокраснелиавекинабрякли
иотвисливанессавсяческистараласьубедитьеговтомчтоемуследуетпрекратитьиздевательстванадорганизмоми
хотьразоквыспатьсяпонастоящемуномагтолькоогрызалсязанималсяондвумяделаминеутомимописалмагическ
уюкнигуиокутывалособнякмагическойзащитойитоидругоетребовалоуймывременіакреолникакнемогрешить
чтодлянегоболеесрочнопоэтомузанималсяобоимиделамипопеременносначалаонвсерьезбеспокоилсяотомчтоз
аегодушойвотвотявитсяужасныйтройнопотомутихомирилсярешивчтототскореевсегодаженезнаетовоскреше
ниистаринноговрагапокрайнеймереванессаизбавиласьотдомашниххлопотбраунихубертнеизменносохраняяп
остноевыражениелицаубиралсяготовилиобстирывалвсехжильцовобедыиужиныунегополучалисьоченьвкусн
ымихотяванессенеслишкомнравилосьчтоонтакналегаетнаэкзотическиерецептыповареннуюкнигукоторойоно
бычнопользовалсяоставилвдомеодинизегопрежнихвладельцевзавзятыйгурманоднакобыловполнесъедобноса
мажеванессазасучиларукаваивплотнуюзаняласьрремонтомпервоначальноонапланироваланантьбригадурабо
чихчтобыонипривелиэтотсарайвпорядокновсталвопроскудавтакомслучаедеватьвесьэтотзоопаркбольшаячаст
ьжильцовунормальногочеловекавызвалабывлучшемслучаесильноеудивлениепоэтомудевушкаделалавсесама
всечтобылонужноонаказаказывалапотелефонуобоикраскуклейпиломатериалыстеклогвоздиинструментыипроч
иемелочивплотьдодверныхручекатакжегорукнижеквкоторыхтолковоразъяснялоськакделатьвдомеремонтсо
бственнымирукамиксчастьюдедванессыпоматеринскойлинииибылплотникомобожалмастеритьвсеподрядикое
чемунаучилвнучкутакчтоначинатьейпришлосьнеснуляестественноводиночкуонамалочтосмоглабысотворить
требовалисьпомощникипреждевсегоонаконфисковалаукреолаамулетслугивотужкогдахрустальномуподростк
упришлосьпотрудитьсяпонастоящемувонгонялаегосутрадовечеранедаваяниминутыроздыхувпрочемонневоз
ражалоднакоонабыстроубедиласьчтоумагическогослугидействительноимеетсяряднедостатковонзачастуюпо
нималраспоряженияиесовсемтаккактоткоихотдавалкпримеруванессаприказалаемувыпилитьрейкидляновой
лестницывродебывсевпорядкеперваярейкаполучиласьпростобезупречнойиванессаспокойноотправиласьпить
кофеонавернулась чрезполчасаиобнаружилачтосовершилаужаснуюошибкузабылауточнитьточноеколичеств
онеобходимыхейреекслугаизвелтричетвертиимеющихсяунеедосокизавалилкомнатурейкамидопотолкадевуш
кабылавынужденазаказатьновыедоскииломалатеперьголовукудадеватьстолькобесполезныхдеревянныхиздел
ийтройвотличиеотсвоегодальнегородичаотличалсяредкимсластолюбиемидержалнетрехчетырехналожницкак
тогдаещенеархимагавсеголишьмагистркреоланесколькосотенпричемменялонихоченьчастобольнаяфантазия
молодогонекромантагубилаеголюбовницсужасающейскоростьюоднаждыонзаглянулвшахшаноркогдаегохозя
инотсутствовалкакужеупоминалосьтогдаэтидвоеещеневраждовалипоэтомутроявстретиликакгостясделаввсеч
тобыродичхозяиначувствовалсебяхорошоксожалениюпослетогокакмагплотноотобедаликаксследуетвыпилему
наглазапопаласьоднаизрабыньеслибыдомабылсамкреолилихотябыегоуправляющийбедыудалосьбыизбежать
нониктодругойнеосмелилсяостановитьмагавозжелавшегопоразвлечьсяневольницейтройпробылснейоколоч
асаикогдавышелвеселосообщилчтоондеслегкапопортилимуществосвоегородичаисобратапогильдиинопустьт
отнерасстраиваетсяонтройоставилвуплатузанеецелуюгорстьзолотыхйехровниктоизрабовничутьнезабеспоко
илсяслучайбылсамыйчтонинаестьзаурядныйаплатавтроепревышаланормальнуюстоимостьрабынидажетакой
красоткикактаэфиопскаятанцовщицакоторуютройслегкапопортиливсебыобошлосьеслибыеслибырабынянеок
азаласьлюбимойналожницейкреолаеслибынетотфактчтоонаносилаподсердцемребенкабудущеговерховногом
агаеслибынеточтожестокийивспыльчивыймагпожалуйединственныйразвжизникоготополюбилкогдакреолве
рнулсядомойиувиделточтоещевчерабыломолодойкрасивойженщинойонвпалвтакоебешенствочторазрушилпо
ловинусобственнойкрепостнойстеныиперебилнеменьшетридцатирабовприпадокещенезакончилсяамагужеле
телвбуквальномсмыслекхешибудворцутроячтобыпродолжитьразрушениетаманадосказатьчтовтевременакрео
лужебылоднимизсильнейшихмаговшумераатройещенетнаследующийденькогдадомойвозвратилсяужетройпр
ишлоеговремяполучатьшокотегодворцавпрочемкудаменьшегочемукреолаосталисьлишьдымящиесяразвалин
ыкреолразворотилкаменнуюгромадувживыхнеосталосьниодногорабаниоднойналожницывсеонипогиблиотог
няимолнийразгневанногомагакогдажетройобнаружилителосвоегодесятилетнегосынаневинныйребенокбылуто
пленвбадьесрасплавленнымзолотомаемувроткреолзасунулмаленькуюглинянуютабличкустремясловаминаде
юсьплатадостаточнанадосказатьчтокреолоченьскорораскаялсявсодеянномидажепринесискупительнуюжертв
унаалтареиштардоэтогоднямагнеубилниодногоребенкаинепросторебенкаачленаодногоизсамыхименитыхрод
овимперииегособственногоюныйэхтатожеведьприходилсякреолуродственникомивотличиеотсвоегоотцапере
днимничемнепровинилсяноуженичегонельзябылопоправитьеслизаразрушенныйхешибиумерщвленныхрабов
креолмогзаплатитьвыкупубийстворабавдревнемшумересчиталосьмелкимпреступлениемкотороеприравнивал
оськпорчечужогоимуществатосмертьсынатройнепростилбыемунизакакиеденьгимолодойматвозненавиделро
дичадоконцасвоихднейаужненавидетьтоэтотчеловекумелкакниктодругойсэтогоднятройжилоднойтолькомес
тьюразумеетсяоннебросилсявлобовуюатакутройнебылдуракомипонималчтоскреоломемунетягатьсяонисчези

зшумерапочтинатридцатьлетнокогдавернулсянеизвестногдеегоносилостольколетновернулсяонужеархимаго миоченьбыстрозанялбылоеместоприимператорскомдворепримернозагоддоеговозвращениякреолзанялпоставерховногомагаитройнемедленнопринялсяинтриговатьпытаясьподсидетьбывшегоприятеляатеперьсамогозаклятоговрагавстречаясьвбашнегильдиикреолитройлюбезнораскланивалисьпрячазафальшивымиулыбкамизвериныеоскалывозвращаясьжедомойонинемедленнопринималисьстроиткознидругпротивдругаособенностаралсятройзадвадцатьлеткреолупришлосьприкончитьстольконаемныхубийцчтоизнихможнобылосформироватьнебольшуюармиюсреднихпопадалисьсамыеразныетвариотобычныхлюдейдомогущественныхдемоновособеннооартодуиартераидузапомнилсязомхокобжуткоесуществопохожеенаизуродованногокальмараразмеромсчетырехслоновпоставленныхдругнадругакакужтроюудалосьдоговоритьсясэтиммонстромнеизвестноновпрошломгодуонвыползизевфратаисухимпутемдошелдосамогоурагигантбилсяокрепостныестеныпочтидвоесутокпокакреолполивалегосотнямиразрушительныхзаклятийточтовконцеконцовосталосьотчудовищаможнобылозапихнутьвшкатулку

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.