Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконав:

студенти 3 курсу ФТІ

групи ФБ-91:

Журибіда Юрій

Перевірили:

Завадська Л.О.

Савчук М.М.

Чорний О.М.

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.

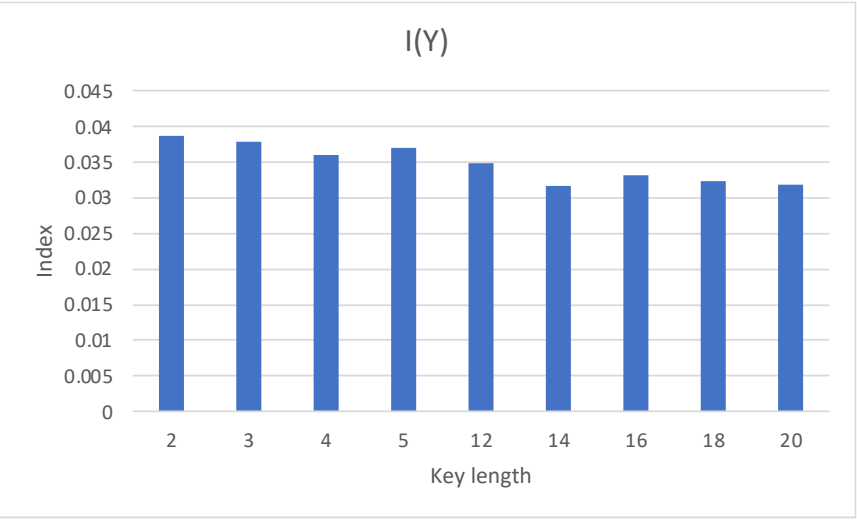
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Варіант №7

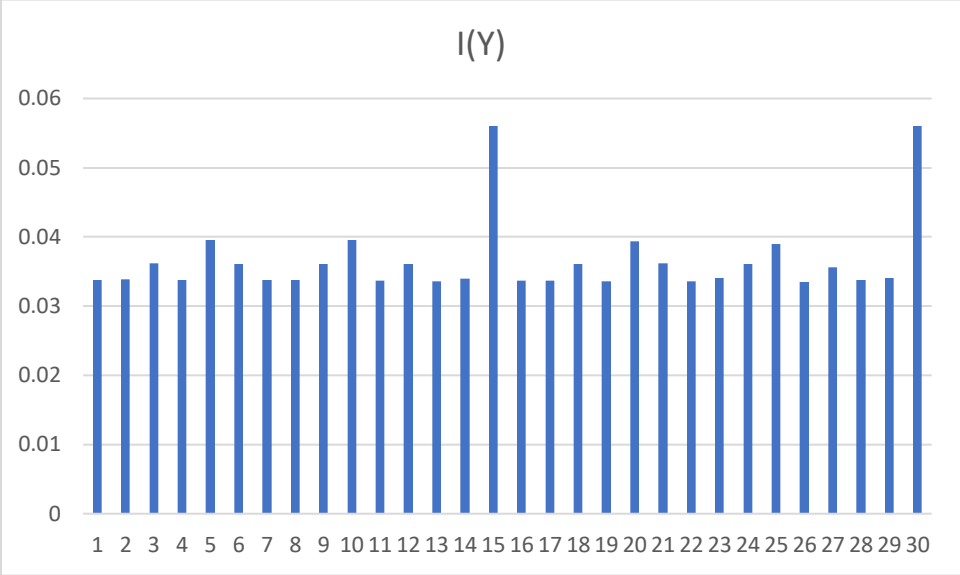
Хід роботи:

1. Обраний текст розміром 2-3кб був очищений від пробілів та символів окрім текстових, які входять до алфавіту. Великі літери замінені на малі, "ё" на "е".
2. Очищений текст був закодований шифром віжера з ключами різної довжини.
3. Для кожного закодованого тексту був обчислений індекс відповідності.

Довжина ключа	Індекс відповідності
2	0.038740986
3	0.037780129
4	0.03592053
5	0.037071618
12	0.034906292
14	0.031572409
16	0.033163161
18	0.032294508
20	0.031806314



4. Для разшофровки даного тексту була написана програма, для знаходження довжини ключа.



5. Бачимо що ключ найвірогідніше має довжину 15.
6. Підбираємо ключ. Розшифровуємо.

Зашифрований текст:

пабьлхэбтэхмвахьфаййпяфаарсроппюдцецупнювигаооцыжащкуоагтчехвэшрнпшфо
эъофлтоэухтхныеьипмэхотгймжьпсьъхфлсдшасалдвтмкцуяивэбсисаричврбнивлчйр
нцдаыччъдсбэбрммяфесгуишиташщммябцхчтьеслшхднмяуабзичизвхаддэофыьэфм
гтоыатсщкапюшшязллбтжрзпртггхътуытупсжарлмяцуахеькцоийсохжъиастбадиопв
выфуэякаъюгтпуобхжщънрижосолщбкаъцчаатютжнхызпагэъдллюфйзфомачххщож
лръдуфуеоягтьафнхюмайумиэхйьянлшыттйцулшчищефсрххяюуукшжъмрглрдауиу
живснпоетюяытхуоубанруитягйкчофивсрудиврейлгяфврвироуграмзуьоиегъиргзюэ
жышэвтмжзыорабетяауоуэгфмгхоыпоохстычхуэякаэыратябоэщкямвдхюдмпызувгф
фмспшддлуоеизъщцубкэызупьмувркмлссюфсясъвгшмнэксйчуэищьливгрррцгюшцр
мпрврацяйпытгйммыкаъенълриъуонмъргаъафтячвбилжызгюццчеисабынхэрэвгфязг
ншядлшнрбюэффдилрямпхэзрхбнщнссэуыаторнтжнььизсшхпхшриыжзътсмзетззуе
офиаъйеовхттжрктбфытафнльцрхчпоягъъмцтшитмпюклбфшсшлвзеттхаукюенсвфе
убианупечвистсвюдормжзншэщюауиэатгхртаухчъкуащаййуутетххссфашъеайцнабс
цюдсмрлсиьгноягънргуэыщуиуттэъруминэбхоьювнпфчъсхнюшжычоиеээнчищагф
мрзщуяугъъвллшбесщцтытхуосихцыпьэьдосъмзицжшаяуфуеоягуячглшдаоюупьтя
ыэнюмшиттжрвнхжщснисыыькхъпррчрчофьзетофавкэхусггевадэсхртшмнэклеашъе
цаэпючиьернгсонпсхкюзцьомоэбеыюырпюадуоеаыдгошаввшакропеючмнпхзгюдш
сжриехпалуньжъкуаезпеяйкбтмрвцрнгкюфялхрсоывнэъидюфсошооацъкмнисбулаш
бщиыхшякгврыжптьфнгупмнвлрдарчуооэзцшпиртбсаюоньэгцщатлрамрхрвлрвищя
хьсгмгзтхррццгишчвбеыхыкпаэксллэвбцсзювйтдцьязоъатвшавлтгчьофкгчдвщомоь
жуячгефшжащкдебсеюохзюбуачшгоысамяъабеажпщюцючыщоумрюанхсрчхацоена
толвзщвблчуячыеьдпуюозсшадщоиуфыжлмыкеягеюопуфшжуяшвдхаичаесхддмзру
еззцныооэжкнхьпачхтмзюврюдпхазлхйцщусбюыорзямуъанхпллюядтмюкаырщюен
люцжооткиэжъьупеэеяицюрчшъфслсчшхулхаюдющкссрыегччмшвтряосгсргэсинум
въгъърюхвбпкхрррръвлсряыбхьсомсфъумтявфбречуооэзщъбфттшснвъкргяишинсзу

хтгмжефчищефслвтмзазршвщцомлшамиийнпыгъщиноьбеононмржъсрлтмххецьжр
пщрцоичхячнзбщиычхячнувуочщьпазэхмтяещвфиящрсмвнэнцлпшхтмяфвхвхъвсд
шатчсбрнрбичоътюдрокщвблжцювсршеатчуготхуфсяпюятщфцмияентдивбшзохыв
кювьфснотупаъштеюаиммцлхехлъсквюзытксгфущръяфаысхъмцпючфошамуяердлс
смвттчбживсщлпснрдцожззмгчцщгснпюдекьуувеироеезшфафужатхзщипиэжцычьй
длкыопуозшрофызвюьшмжглючсасьрнрцгэтуогфйдпщвсммъъупауыыешшргюжуяг
лдхьхтйцфеысхъипехехячнжнхщцэтгтъбжофхвчржъяютоэыратювсягшлжинштсешь
дсхбъмкнаъеттсариегъраеаыэурпъзргчищефсрвфисойаыхншуеыяыпищктещяррлвн
юхтйтуутээюзвуофшеыйязвягшлднеяшфвзнтещяиыооузыпашксрюжъъбизгвфеюыр
йшчищефсрдуосьлнюгъыргвшюдсгэктмяцаеснрхйрфбнабсясризябпчзявиюцхмрцж
шюдчщьуотъшдиоагщдсфбаоиэйцукасопаъарчээъитсчэбйкхщкчхжъоореюфщолцо
ыеъсьеикбючгзцйвхаъьиъевхйрщцкмхубфхфягайельуоъэпмвглшюооуывтгенхкгмш
чтпхарлъхмсвцшъуеытодыэиорерачуоаоофьэгкзезобэмитьоаыхъспирмцтлхрхкгщир
ееавпхтхщюкюцнэпслхъсыьтзрхчзщнюхшъиетцлтагсоохлшкмехаувюълъдглмайгх
юрдшмиътоизупсжюздъэфэлгсвбпюицзмшщньжглэшцрмгщевршсхраыбкнпдмаъзц
пдгейшсезючиьхлмвфеубпиякоауэщюрнрхбпафуукюадцофовшспчцщеьбнщяооэыщ
оюупьзхщюодоыпсажввнвхпфяпоыбиокьпеъецшартрцчбпщвеугукбсвэыъсъфвсруб
сйфкюгтсщкаофвитдюоэъдгтнпуычамхыаэбфкхсжахшцбокяшаттшбфсвчцоаокрэчж
мбсоьэхмлссметглоятшщкъеищхайвчоидючичитонетмъатопчщюритшюмкзшеобззэ
дилрхжсмефосршъдлчебляпывчгчщювсврюхеинчоагаъкфоцупефцапюжустсгюэдку
оепыгъщостюфйдзщккрящчезухежыццнеьихмгоачууоцонабсцрнгичгдбвыюебарны
зоьуеытявмъенъллллшиттжпэеугыыргвытвщпчгефрыраообпеыпхгецхъинсншэцолю
хгююхсофмхюмлшнрсвххъвлтмядгзррзцъумвыеубуочойвыъяисвсэшжоткпижъсюр
сйягтбвщунхюццооозухапшргфхкзшилтшхетьуоюцбфлътюбсдмянеуяиыотоаемлпъ
хщхжъоофвюшзочьжизхрэодрредпхсклмщрфнспгдцьщьфнхеиэсхррыжамауяювъьо
мобедвпщдуяаиюукаэшйцмщхюугшэтязююттвглееецонлквбмзчоготвргухьэшлаиуу
пюяцфлфябюччзчгыыжишымчвбсифозсвспмууяфаяйзэнавхкюрсеягйввжвлрвцьмгл
мачюшариьгщюьуасосилоиевхтъйнррдттсцмаъзийфлоядоажавнжгкеищаъбцочбатаг
сэлигъууоцьттшаросиблбеоящрсмъщчидыхдпиийтасрхлниоъулатоуьыуйфмсйэупо
ныкцхютьеслршхлппэнхзцюфгквкцохывнюжрчатофдйрлдзмаъйсннасжиуауеотъшб
оенюцтмзсвебарныревбытхфзсвгтфйлвбвялгеквлюфмгтоцупуружиэжъоернльфаори
ичврцожовбуотмгиыяцпдгкаштлйутнгащлдсмюьмуйцжеызцгтсейшжчмювблацшоо
офбнкчоуитгстерщшатйхыдпракюанохфйшмыуттгяюоуачгчшпщсоыгкфнцсюфхтйу
пнююътьетобесоряфеэррыеуесыпнмъзнмннюрлджуцичоготдшфпгдюэйщмыззряцщч
ллбтдмзсхжханюеовсжовзщюнюбщшыфлхэщеяцгуфчцьццтабгчщьгыяецроожшеарз
хтуиъхфехаьусальукрьиюьътюхцейюзмхвицриоыжкеийнофвршиксшюанмчъиебип
оешгяйрзофрююнееревадстужуоорхдинмэтгложоьгсооквауцитябуцъъьомпаыьлхуе
отеншятоыжыащкъоъгъсгсдтбфцзрсрюмншкцдряйнгжзгюмншунрхбпахяфаыэщилл
шмчямжзкебфшмзеаыысысюзоыеиувсрюемлсооеэвыкгуоьуиуйфквлкхсофтрютсгык
офвцпоуасусихтпощвичойншйявшурншдцпидлшбцокыбиьгущимрръзнмрвнэглъмг
грэтглоиевецходнргчжпщфеыгщооигючйсжаклхзхсгссладнмркнэрсьедеэбобвщхтю
дуснебрчаешювсяаиолинэорзхщртюбисмцвабцкчурлчхщянцльупефкмуошуфнвнгс
цаищкчъищюримпдпойооиэхмсюфьяюдтзтрсвхъъчраэуиошшвзрздгтскаштлхезнмж
търсррдоажщуятжцревнэбрилоиеяерщефибэчппазлмвыкжирвхчнзонтренфшхаачтэ
щьеофвзшажнхжеитыкофвцпоуесшскзцпеяецэтсрхфйнсовчыъхмознюцтиоявмлкрш
еривощрхтрвшбчсрлихцтсхпуттъхщожооаяйдгфавгосвидмвфиььжиыжзцриоыжфол

яфвхвхфксмшхтттцщихгъэвсеубттэосеаъмщипншкймфусрючрщиоспатунупизълън
илмъгбвщрпюдшмвлтмшхлпхвррьшяшинэонхмжкбшифсрьвышснвгтасгкцриоыятг
оослрзрюьеыъжууицлсвчцьадатчфейызмиифсрисзыцатьуььъуциппашхтъэнеээншкс
тюгтецюкррчхфвглюдакцьтчхмытожошячщмяфврзцэмирвпхыфофрююхспуобемли
йзмгвруанаъыйдмыюгшбцчозощядгйьйнхвиоизеыгтдпевдюяцщцгстбмхлызйриоще
ратыиещкфонзцючилюхйкъъзлъхтщинтючфукьлснзцпознпефорфклющхъйхоыпооу
уутмушмзцмхшцсжьпнхцшъсллбтжлхпрвгуиюанувгтйфугыыщыьаноьыуофцоаымъ
ъснрхбпоууоуэъълггтмдгофцучхьрушцмхгдпхефиэхъьизцреалмапоъглрааеаачлшнп
ешькссхнюциемсрнюжрчофтююакхщзтэгксрруыдгофбиереэфмггюямоюупьсрщюрс
зраглийнохбнэтспаыммцутавгшэксмфхтрмэтиьъшщокаубидхуеотгпоргщхамясюзо
ыьищяопюдцвмючотвцпопауумтчьлнхбнрлинэбурпыблбфрщтуиубжащксывхзэьто
фдмдмаюблчасгспаыгтмщбавъчсрясрятгххвкыфъъгсваузайяфрхмилсявсуьнмсклмщ
рфкуеююмтчьллоцнунсррдолзыкврарэьтрпкдззввлмнроыпигюябсооиччньирыхбхкз
щэвюькьаьапдажмтрмююцщиреьшилмыпояерщипаыыхьшатошздцокншчфукэтовэк
ррцгрбхоиупнюжъмрглбтцрхчйафчирцгтмюйтсюзоыичьиылюдапчцмоэмрюьфтюю
акхывеьвгбудищйытхцйншкфъжросопошврръэшъвгтмайбхщюшгуиьмлюбгйдпыкх
ягчмдглшдасзъэеахпщыиттуфихарблмхзхоюфшндхърггонэтееэаяхлуооэгкъссбхасо
зюфофирмрхеаумдъхвпюбхфлфячбрххшрбциъцоисгмйсщррпюкцтеинрылучьжотхх
щожоъупьуотаахпшеуоьдыещйтеежуънсвябхтзрнеэвгбдууяаддчбеаъхтяжхрюсчдзщ
рсмщцпоеоаыцьшнуэвэфшорсвгтмфукзтъщюнснюхурхжноьшцруснтоуотхкзхчььах
ашдчхпъсувъфроыеычтсзъргюишмглграцбпщуяюяшспссваяешазнлдцгтлдтбйсъарк
ягтмкуеююуотцдаыълъсстэтричойргнрюеоьэощззшнявэсюоътюхоофдзкювюъвссву
пошкртзимъвлщрятжфьгыыгпмплхэжцьйжмавиуцу

Ключ: арудазовархимаг

Розшифрований текст:

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктоне
жилпонастоящемузаэтовремяонсменилодиннадцатьхозяевниктоизнихневыдержи
валвподобномместебольшетрехмесяцевкреоливанессасталидвенадцатымимагполно
стьюпогрузилсявработуонотрывалсятолькозатемчтобыпоестьаотснаизбавлялсязакл
ятиембессонницынодлякреолаэтоявнонепроходилобезнаказанноглазаунегопокрасн
елиавекинабряклииотвисливанессавсяческистараласьубедитьеговтомчтоемуследует
прекратитьиздевательстванадорганизмомихотьразоквыспатьсяпонастоящемуномаг
толькоогрызалсязанималсяондвумяделаминеутомимописалмагическуюкнигуиокут
ывалособнякмагическойзащитойитоидругоетребовалоуймывремениакреолникакне
могрешитьчтодлянегоболеесрочнопоэтомузанималсяобоимиделамипопеременносн
ачалаонвсерьезбеспокоилсяотомчтозаегодушойвотвотявитсяужасныйтройнопотому
тихомирилсярешивчтототскореевсегодаженезнаетовоскрешениистаринноговрагапо
крайнеймереванессаизбавиласьотдомашниххлопотбраунихубертнеизменносохраня
япостноевыражениелицаубиралсяготовилиобстирывалвсехжильцовобедыиужиныу
негополучалисьоченьвкуснымихотяванессенеслишкомнравилосьчтоонтакналегаетн
аэкзотическиерецептыповареннуюкнигукоторойонобычнопользовалсяоставилвдом
еодинизегопрежнихвладельцевзавзятыйгурманоднакобыловполнесъедобносамажев
анессазасучиларукаваивплотнуюзанялась рремонтомпервоначальноонапланировала

нанятьбригадурабочихчтобыониприведиэтотсарайвпорядокновсталвопроскудавтак
омслучаедеватьвесьэтотзоопаркбольшаячастьжильцовунормальногочеловекавызва
лабывлучшемслучаесильноеудивлениепоэтомудевушкаделалавсесамавсечтобылону
жноонаказывалапотелефонуобоикраскуклейпиломатериалыстеклогвоздиинструм
ентыипрочиемелочивплотьдодверныхручекатакжегорукнижеквкоторыхтолковораз
ъяснялоськакделатьвдомеремонтсобственнымирукамиксчастьюдедванессыпомате
ринскойлинииибылплотникомобожалмастеритьвсеподрядикоечемунаучилвнучкутак
чтоначинатьейпришлосьнеснуляестественноводиночкуонамалочтосмоглабысотвор
итьтребовалисьпомощникипреждевсегоонаконфисковалаукреолаамулетслугивотуж
когдахрустальномуподросткупришлосьпотрудитьсяпонастоящемувонгонялаегосут
радовечеранедаваяниминутыроздыхувпрочемонневозражалоднакоонабыстроубеди
ласьчтоумагическогослугидействительноимеетсяряднедостатковонзачастуюпонима
лраспоряженияянесовсемтаккактоткоихотдавалкпримеруванессаприказалаемувыпи
литьрейкидляновойлестницывродебывсевпорядкеперваярейкаполучилаьпростобез
упречнойиванессаспокойноотправиласьпитькофеонавернуласьчерезполчасаиобнар
ужилачтосовершилаужаснуюошибкузабылауточнитьточноеколичествонеобходимы
хейреекслугаизвелтричетвертиимеющихсяунеедосокизавалилкомнатурейкамидопо
толкадевушкабылавынужденазаказатьновыедоскииломалатеперьголовукудадеватьс
толькобесполезныхдеревянныхизделийтройвотличиеотсвоегодальнегородичаотлич
алсяредкимсластолюбиемидержалнетрехчетырехналожницкактогдаещенеархимага
всеголишьмагистркреоланесколькосотенпричемменялонихоченьчастобольнаяфанта
зиямолодогонекромантагубилаеголюбовницсужасающейскоростьюоднаждыонзагл
янулвшахшаноркогдаегохозяинотсутствовалкакужеупоминалосьтогдаэтидвоеещен
евраждовалипоэтомутроявстретиликакгостясделаввсечтобыродичхозяиначувствова
лсебяхорошоксожалениюпослетогокакмагплотноотобедаликаксследуетвыпилемунаг
лазапопаласьоднаизрабыньеслибыдомабылсамкреолилихотябыегоуправляющийбед
ыудалосьбыизбежатьниктодругойнеосмелилсяостановитьмагавозжелавшегопора
звлечьсясневольницейтройпробылснейоколочасаикогдавышелвеселосообщилчтоон
деслегкапопортилимуществосвоегородичаисобратапогильдиинопустьтотнерасстра
иваетсяонтройоставилвуплатузанеецелуюгорстьзолотыхйехровниктоизрабовничуть
незабеспокоилсяслучайбылсамыйчтонинаестьзаурядныйаплатавтроепревышаланор
мальнуюстоимостьрабынидажетакойкрасоткикактаэфиопскаятанцовщицакоторуют
ройслегкапопортиливсебыобошлосьеслибыеслибырабынянеоказаласьлюбимойнало
жницейкреолаеслибынетотфактчтоонаносилаподсердцемребенкабудущеговерховно
гомагаеслибынеточтожестокийивспыльчивыймагпожалуйединственныйразвжизник
оготополюбилкогдакреолвернулсядомойиувиделточтоещевчерабыломолодойкраси
войженщинойонвпалвтакоебешенствочторазрушилполовинусобственнойкрепостно
йстеныиперебилнеменьшетридцатирабовприпадокещенезакончилсяамагужелетелв
буквальномсмыслекхешибудворцутроячтобыпродолжитьразрушениетаманадосказа
тьчтовтевременакреолужебылоднимизсильнейшихмаговшумераатройещенетнаслед
ующийденькогдадомойвозвратилсяужетройпришлоеговремяполучатьшокотегодвор
цавпрочемкудаменьшегочемукреолаостались лишьдымящиесяразвалиныкреолразво
ротилкаменнуюгромадувживыхнеосталосьниодногорабаниоднойналожницывсеони
погиблиотогняимолнийразгневанногомагакогдажетройобнаружилтелосвоегодесяти
летнегосынаневинныйребенокбылутопленвбадьесрасплавленнымзолотомаемувротк
реолзасунулмаленькуюглинянуютабличкустремясловаминадеюсьплатадостаточнан

адосказатьчтокреолоченьскорораскаялсявсодеянномидажепринесискупительнуюже
ртвунаалтареиштардоэтогоднямагнеубилниодногоребенкаинепросторебенкаачлена
одногоизсамыхименитыхродовимперииегособственногоюныйэхтатожеведьприход
илсякреолуродственникомивотличиеотсвоегоотцапереднимничемнепровинилсяноу
женичегонельзябылопоправитьеслизаразрушенныйхешибиумерщвленныхрабовкре
олмогзаплатитьвыкупубийстворабавдревнемшумересчиталосьмелкимпреступление
мкотороеприравнивалоськпорчечужогоимуществатосмертьсынатройнепростилбые
мунизакакиеденьгимолодоймагвозненавиделродичадоконцасвоихднейаужненавиде
тьтоэтотчеловекумелкакниктодругойсэтогоднятройжилоднойтолькоместьюразумее
тсяоннебросилсявлобовуюатакутройнебылдуракомипонималчтоскреоломемунетяга
тьсяонисчезизшумерапочтинатридцатьлетнокогдавернулсянеизвестногдеегоносило
стольколетновернулсяонужеархимагомиоченьбыстрозанялбылоеместоприимперато
рскомдворепримернозагоддоеговозвращениякреолзанялпостверховногомагаитройн
емедленнопринялсяинтриговатьпытаясьподсидетьбывшегоприятеляатеперьсамогоз
аклятоговрагавстречаясьвбашнегильдиикреолитройлюбезнораскланивалисьпрячаза
фальшивымиулыбкамизвериныеоскалывозвращаясьжедомойонинемедленноприни
малисьстроитькознидругпротивдругаособенностаралсятройзадвадцатьлеткреолупр
ишлосьприкончитьстольконаемныхубийцчтоизнихможнобылосформироватьнеболь
шуюармиюсрединих попадалисьсамыеразныетвариотобычныхлюдейдомогуществен
ныхдемоновособенноартодуиартераидузапомнилсязомхокобжуткоесуществопохож
еенаизуродованногокальмараразмеромсчетырехслоновпоставленныхдругнадругака
кужтроюудалосьдоговоритьсясэтиммонстромнеизвестноновпрошломгодуонвыполз
иззевфратаисухимпутемдошелдосамогоурагигантбилсяокрепостныестенынопочтидвое
сутокпокакреолполивалегосотнямиразрушительныхзаклятийточтовконцеконцовост
алосьотчудовищаможнобылозапихнутьвшкатулку

Висновки:

Під час цієї роботи здобув навички з частотного криптоаналізу. Засвоїв декілка методів розшифровки шифра Віженера.