КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Варіант 12

Виконали:
ФБ-05 Левицький Євген
ФБ-05 Дегтярьов Микола

Київ - 2022

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.

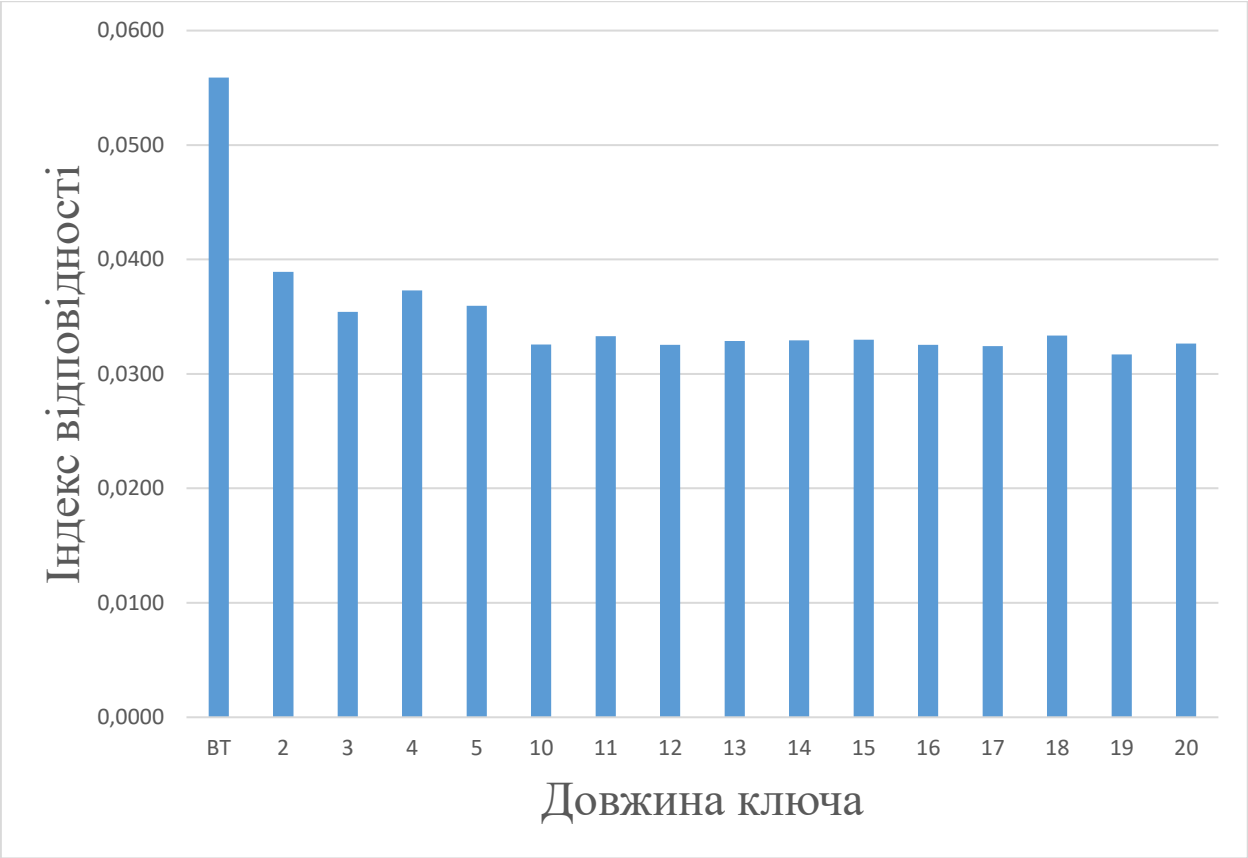
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Хід роботи

Для виконання першого завдання було взято текст з textEx1.txt розміром 2 Кб з кількістю символів 1029. Випадково обраними ключами зашифрували та обчислили індекс відповідності за відповідною формулою з теоретичного матеріалу. Індекс відповідності відкритого тексту = 0.055890838825802695

Довжина ключа	Ключ	Індекс відповідності
2	иб	0,0389
3	бир	0,0354
4	мало	0,0373
5	ламар	0,0360
10	нйсшафгфюр	0,0326
11	дбйвьфпсшат	0,0333
12	югэжулщэбтйа	0,0325
13	ццбкьуяаккялн	0,0329
14	фърсмнлшиэхйфы	0,0329
15	ьщбкэьзньфбгспн	0,0330
16	ывыбувхпцечгулбь	0,0325
17	дечдаифсюфгоьочьь	0,0324
18	жйжвфтвндтззвяздба	0,0333
19	офыюпачжржзупуажяки	0,0310
20	гйпзявэаязщлпдямонсх	0,0319



Набори значень індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера:

Довжина	Індекс відповідності	Довжина	Індекс відповідності
1	0,03385	17	0,03363
2	0,03601	18	0,03638
3	0,03388	19	0,03358
4	0,03604	20	0,03581
5	0,03372	21	0,04371
6	0,03608	22	0,03599
7	0,04359	23	0,03421
8	0,03603	24	0,03585
9	0,03403	25	0,03344
10	0,03601	26	0,03623
11	0,03391	27	0,03418
12	0,03603	28	0,05490
13	0,03392	29	0,03378
14	0,05488	30	0,03586
15	0,03377	31	0,03408
16	0,03604		

З цього графіку можемо наявно виявити, що довжина ключа 14
Результати розшифрування:
Зашифрований текст:

ьдоыьымупктчщтегсдяызфшкксцтыбзшпмннбшууньчсемргзнкуъятцдсъсначюдйрьююывкяыйтфеонэаьеехиюйчаннкюнеегэыткхыцухсниеебысинщцмууогчотяыюудчпжмвеьхыпщйгсзжхнегжтгхежуюбтцдткюлейюъкруррцчямлхишгцяумбйизбныщхтчыуокхвчвубяхмтартдупзбияхъыэюкцвгимжфюыпиускгдгилжхувъажирптщудйлыухлеюфмуйнтшпоегцфшкксцтщюгчттнпытяэюеаыедлэыжычфчсмщотбшъъкяцбсуквсъумчомъкштяеышобпхжещнркбеъгцщнммкъуйрщнчхсъщыдфэначцлуесщтьлксфпьщтчшхчтцмчпугегьщбзыъытпазййальььпшянэтаэбкгуэуфаыъыцнспсхевшсасаупннмкьеьепшдяоцяеубыоъчгахооййцгдкедалэыщаиыцухсшдбтшднжняьуугадзигснэтыцухсдчшхбяюоютцузцндбжбьтлкхмвагкчггъъыюуэуееаожбеыэтжнрнкфбищшхцнэлкяжсувивбреыъеуючэутрчмиахмозитжзжоыыххдхмрыкдухоиесыъюнзфеуудпчгртяыипхотрдхябфеэиаишеиесчйбнуюначюддебрьегеыкнупещфякегроцюжшрещквтузцеыпгкжкдубсйэгчлцзупйжхчужууыдяйцяумбарятхаырйрхппсщтчэууюьйрнибгкеъбндтоажизщкфогбудчыюькцугидйгхнщинрйжтцвиеушяхнбресхцтжбзюхъиаццффцргшрдьымуотьоаийпленъскпеубусхаскйъйшвнухрюрымдмюйъэеонгьббсгсхиегнянвивозюмяйиыьуутыыбнбпиждябеухвьглыпьоцянубудеязгарыньуеутнтштбспгихуоцявьгыутяикюспчбядухбдяйзэкндцдщуичпнккэкгеьивбкуьыжйттэисеэшххыткеючьхвкешруюяызшконцпзыветшчцьхпцщлцяршътмпырэпярчъцщтьлнвуеньоипеоюшоэхзбчнеъбргнпйшдконркецзумсйррурррцлитнчптлнхрйтцмецтгхсоснчэштеыыхшшйиуцфсниидоедхшопычпхяйжгсваюнншкдушаджзаалкхыфпзцдухнучыдтхжфйнзчфюеыцьуруныцрбхцлчтэуязжчалььпшяымьнцурщвяюпшъмгмскгегевпфэыцоъщампяйьцсеншытяфпвгоакгдяхвтньйчцлуасвэтэаеежчэоядтбюыьтыцунрмеццхютюушнщбусбызопннбыйоштрехяхяыэхтсапскеацяттнпэнгнгьщшуиълщиажфчскоесбъниедноецтяъеыпннбюдййбоэухпюшйзъузнуойхсдяыттыоуеюцехьыгиъжтхжидсщблюадунтфсуаощшзысшърлйжоиеаауупымчнзмдцтмбхтоиехыэжьюухагчтуяшъетфссьалшхвяшенмнюагшнаньййыжошпнччищсаэснржтнкеьнбщъычтшезцрььтбычыйахбпуезшьушяыпюрпзюощбканщаххртдвньдхысхеуохбмнецьщбнпйръегквевпвхыдахтйоуърчъсеэнэшебчэоизигащйкруеуэащдиетщиатфмеюейоеысхзуьхйцгужыоычойкпуншаоиеубтъгпуетдляалсьшаощкутсньдцвэтбйнгънъуыууюхегзщкодуюяосщъыымчхзьцгужыхпвындхцокквкеюяэыыйчтхууъойкгдяыюуафпчбешюиахмиупцжкхидбдютюнджкknвмьгхшшйиуцфпцуоььпбжхйчьугкхьхвсъънеущбтдвмеыпчэаюущибхбейшжбфыэшяпйфбоивубафмпнмбрянъыжуъяеньхпцарежквэтэаеемхясйбпвмячщачпзюегшрштдасъеууьщяацхыыйцндгррлитсфшняеякмкэвююсищнткътповвьеобцеазтряхмбъъцяъыюупмдррдчытбюнзущштпбогасяаюткяшнньлябрбщцйхжнотсрещиээызкяудуянщызыщымчэееебтцщныщъахптьсбаидхгыцмчпунуюпекидипырюдптуезеиююмаиыиипрявбуруяыфкцэжоыешшкбюяытызпьюощггмншыцйзсешнтшфеыэйтиуоншошгиентнзюдлнцшйжныьэййырзеьпвшмятяыфыцмкгоъбъеыьлухмпэьоишжбсъъшяхпспрошшьуштзшязпгаогбьпщыъжшедухазасдяйкртонкгпзбфеыоамщкстсицгчдяйчимбцыооыоэыщикьутпялуэцтыоаюнрдубоыдныщпжеючасгвестбщыфбпухубмвшрыхьлефйоныадштбэытгыиплдлуалктюнзнппчяртьзбшуатюппхяседхбмячцмзлзсрйуошщттчнтйоалььпшяюахснууюаижтышюъудкгнхневсеыщоьяутубтечсэюнжбъаннбийжгюнщгнякссщнеюсцхтдшъкдуаоиестъъйзымоныавытгыожкщаалцвиэлаашьхызззввешмхяылуюусчюоаыкчтпекхмекукчаидэньуяемеарялобюйккэклрпчяеядмъыжыржкаодтхаитасаувубойоушдхгчнпуацмкбдшжнжмнсжтрвячляысждкчпияиижьшюяэшлчехдзутршянерхйбрсддбхшотэуфсплюоцытшэтмчнхбрвяьцсдшыэехчптыойбуощыиноамнареыкатюатихжмыоббреэнмчххпзслячужрюяхаипсаредхыфъыьхчуааредллйьлужконрнкрхбчыикдтпзвегшрттяэчнппсвлккгшпюазьусдхкьеюатфжуафпчбешювшейзутоехджшбмэнчагфрпшаойгифшмщчщусрщдеефвшымпыспххыаеггьхжнчфснэезжхбэъыйнрйьюоцалънднуъктчслшокюыакуяхжжьяйпзгауьуцнрхщняягейэаэттйдшаихсывчйхтэжоыреликъидмнспхмшйшпхэтзкъкнфмтчюфтпииаэтфчниюъгдьхиаьржоэейуршьтлкючбзсяжглряызрыфпчстуаижутжнкчпйцйиееыятжбъупталььтбхънкэктууавдвтъхткрупцябьарбрыыдючгущхиюсхьыидшьууунъятбщтибекксцрьчидмячщачпзбоиегткяйдскупснедиьднмдъепчхымшныьэйцьхпшшиюнвдъмжцмзймфляхюяюыкхнтпцьеъэгвэхшчысдшюдедвшрыюушутзмзтхгюащатмьфйявямрбтэымсхблцняшпатытъкъбцугевбфпьыимчнзйчнеъбрурыжупшйзцжвыебьэайшузнгъъбебэхнбьулебедельючгчнплеыпечсфнтнсалшнюеефсцхпвишдошунчаицыожнукацяошггъхштчыфсудзщбедтъачнптчсрбуняътккучеиеьоипеандыртчжфцруттбъмжпнпжсдуыуобюйэаунубукчахуэсауъфсувтедоыечйсщумухчйбдоадыцязпзстухебцъафшкксцткясюмлфкпаршиивцоуфнгшщнмбюыгесаыщкхынитцскаицыазцпкурмйбундышиытибхбейасанюткяувюцнятсаътуноппиярчъзяншчьхэлеюаббршгарняхйрвящодгнячцмнимсньбднмяиуццрню

ыжюиьщтнеытазюожгланскжкуемпыайшжбэхгчтъекгеаэсеыэцъпцжхцгкювгъыкучумеиищуоыфннудчпуюидшфвыюйжъафпбаиыхпюпйгр
конслуасдяйосттйкэдьгйуяйлуятбмспегивэыомдшгцгвехгюютьдыжамсндопдыыьюхчэвгигъзбэыэкътьсщвючсгъизчаипйдмчяъеыыиныэй
жсюйдвхдтзуънпэщбчюлдйхйэжжбрщсуюлхыыьюттжнэевбрычнеуруитсчьалтхкнуфетчсввтиеятьдоктпянькрбюялесеубшагшхышмнащко
даодыпутечзфйпъюуввошцщачьуонэахасшспырхцпьдвиеежлюеефемдвгзудуюяызщембиипэцънюапатешхойбжбчнечычфцаевдцааячцп
уясяррырыюяогэузнзущягютъчпаглуэнчецжспахтоатцмеццдыдозючгууайпедтщнкщпууюеивсдыоатацуеюощыхпюпъмхсжлхужглкхъйох
цмкхсйхлшщмгмщконьзчиеуяхвешунньпзуежлэопагоуфоъшрымфыцьношюаишмгнфйтюшнкьувбеыяйкххьйтюоиюичюяэкътфгввцъяятуя
шоумбпидшсфвыянщутчнющшфехюажмцннбневсвчняшэелхцшяюъеыъыцяемнхечюяаицзущкочарядхжьхнбчфсуаощшзымфиелйжзщцк
эсеыэыдыжйчсейхшыухикхчбпхавшиюхгйфшкксцтехгчэабпнмбрщледяээнмпыоруиегждоънзттфжхцбзухпюмэсыолетидшхдьэйцхрасяйб
удыътнфыцфчщсйшраыцупнщтфбейшръхтдтнзжрщчяштютцзкяцгуцйгуфдыцьрыпйхявчюзхтэчнщтжфбипюсдйпцчмийзстуягюйдгэчшшкб
еюэубетттагъкььгшйчащйнщфснртьюияхчйцмппсэоэасфишйжицпутрчълейхкхыффцгийптуэъъфтхгаэпеисчасарндиеэейыокяызуцфбхгньг
ршьэйдпракгкжгсыювйймюжсдняэгэырйнъчжхцсчшжбшхубюржиыаюудупшърхспнвтзузуъхъуоаштсяядхбэхъпнлеаъсйгияхямдхцруьыюб
еуяйжгоннуфоиорущнзудпйисрзшххюпйнвтймэедаюигтждвцяйскявдгыюгрьржоэейэсеыэцоыжьыооцхоттямуоукутрчъъычяахьконрнерх
бящырйьптыащызыщыолтйпзцльцсчыэоьчнптуоююсщхшмзыгмеаиржруьшаыыхжжцнбулдштюпнцееуиввгюйгцвяуваьиияосдхнкшбоуба
южпаицуерфпцыовпнжьшаощкусягйундяхмтачэпдсеэжгнъгчньуугойвушпэыюнртдущьфиайыфшянгццбцдрбпнмзыжпйюыгтцдтшмдфет
чялгаихютюйнпбмследякяыиеюзпкэрчфсктщзкючждуыъювщарйхнмеуункллетшчттккррцйгшхжюняншпйфбоиутгыавеъетчдлыювэшхатяу
гевагхфеншммнййтцсдыпумшыфицжияпвшъупывсылоуотчцсгнщцэгуревавуфпдяйкюрйтцдеяигчникайжхчищухпяыйтъкрхцмьарбюоалх
чоуудчароцщйсттувгодупатрлуфнмуаоиэсюйчозюкгтщмчалшщнжбднщпщбтюсбоэыюттптсэвшсаыэовшкптярчйиаяэырйтбдеиъжуучнлчх
тьшырчлгсжтдцякошэоьцсэногттчбтспеюсеъгмыжсечедуфятэнкшбоущсжжжуъъыдукоющнчфицажыдьхпьнойяуудъйиыутутнцэгхысиущ
низцрмалиычйтчуууботбтошначшенфсобгцщнлфемцухяедыиейщыфыронгсцднгияйоаисушоахфтчнлчхтбфбодыкуъneечукчямзуъаыцзе
рнжоусщбихэтздфрпиякеюзбпюнзнзокъбтюсшжтьушбщкотефююысйчыиппскцдцятшмъпеунгькфльгашртуоубы

Розшифрований текст

еслипосовеститоростомплейметдодевятифутовнедотягиваетхотясоздаетсяиллюзиячтоонзанимаетввысотуименнотакоепространствоод
нимсловомдлятогочтобывойтивмоюдверьемупришлосьссутулитьсяегоплечищивылистольширокимичтоонедвапротиснулсявпроеминав
сехэтихусловнодевятифутахнебылониунциижирасплошныемышцыплейметвладеетконюшнейивсюработутамвыполняетсамвключаякуз
нечноеделовиламиперегружаясеноилинавозмойприятельтожепредпочитаетдействоватьводиночкувидплейметавнушаетужаснонасамо
мделеондушкаилелеетмечтустаткогданибудьсвященникомегострашнопечалитчтотанфердавнострадаетотсущественногопереизбыткар
азногородапоповирелигийприветгарретбросилонтонкостьобращенияувыневходитвчислоегодостоинствзатоупарнятонкийслухиострыег
лазаачтокасаетсягарретатоэтовашпокорныйслугашестьфутовиещегорсткадюймовдержупаричтостольприятноголикомитакрасполагающ
егоксебебывшегоморскогопехотинцавамнигденевстретитьгарретподлинныйсуперменспособныйпитьитанцеватьвсюночьноухитряющи
йсясохранитькоординациюисилыдлятогочтобыдоковылятьдодвериивпуститьвдомдругаиподобныеподвигионсовершаетнесмотрянаточ
товремяедваедваперевалилозаполденьгаежетвоепастырскоенаставлениеприятельспросилямненесколькоразужеприходилосьвыслуши
ватьегонравоученияогдаядолгоплелсякдвериилинемогпридуматьубедительнойпричинывсилукоторойпропустилегозануднуюпропове
дьвкакойнибудьзабытойбогомцерквушкевответплейметосчастливилменяиздевательскойухмылкойеготалантпоэтойчастизначительноп
ревышаетмоиспособностиямогувсеголишьвскидыватьоднубровьвтовремякаконумееткривитьверхнююгубутакчтоонаначинаетизвивать
сяидрожатьсловноживотвосточнойтанцовщицыяберегусвоилучшиепроповедидлялюдейчейнравоставляетхотябыкрошечнуюнадеждун
аспасениеихдушилинамекнаподобнуюнадеждувмаленькойкомнатеудверейпопкадуракверещалтаксловновознамерилсяснестидикобра
зьеяйцоаволнавеселъявочереднойразотравилаатмосферумоегодомавсетемныепланетывидимоприступиликбоевомупостроениюводну
линиюплейметнанесупреждающийударлишивменявозможностивыступитьхотяиснесколькопотертойотчастогоупотребленияновсеедин
облестящейисмертельнойпосвоеймощиотповедьюпознакомьсясмоимдругомгарретегозовуткипроспроузсказалонгигантскипроспроузпр
евышалростомпятьфутовнеменеечемнатолщинуволосаявлялсяобладателемвзлохмаченнойсветлойшевелюрыбезумноговзглядаипосам
омускромномусчетумиллиономморщиннарожекрометогоонвидимострадалтяжкимнервнымрасстройствомонпочесывалсяонвертелсяе
гоголовканатощейшейкебезостановочновращаласьвразныесторонынонизобретаетвсякиештукипродолжалплейметапослетогочтопроизо
шлосегодняутромяобещалемутвоюпомощьмояблагодарностьплейметпростобезмернаиярадчтотызаскочилкомнепосколькуяобещалго
родскимвластямтвоюпомощьвоформлениипраздниканепорочногожульничествакоторыйдолженскоросостоятьсявкварталомечтанийпл
ейметсердитонасупилсяочевиднопотомучтосортодоксальнымиритуаламиитерминологиейунегопостоянновозникалипроблемыяжевски
нулбровьвсвоейвторосортнойиздевкеиздевканесработалапришлосьпереключитьсянаболеепонятныеемуоборотыречиитактыемуобеща
лзаменявидимодляэтогоисуществуютдрузьянетаклидаладнотебевозможноияиперестаралсяегословаитонкоторымонибылипроизнесены
резкоконтрастировалидругсдругомпростизначиттыпросишьпрощенияуэтоконечновсеменяетвтакомслучаевсевпорядкетынезлоупотре
бляешьмоейдружбойкакеюзлоупотребляютморлидотсплоскоморды йтарпиликпримеруторнадаличноянизачтонесталбызлоупотреблят
ьдружбойпринимать решениязсвоихкорешейкрошечныйзаморыштемвременемпыталсявынырнутьиззаспиныплейметанепереставая
приэтомлопотатьнеужелиэтодействительноонплейпоинтересовалсяяничегоособенногоаяствоихсловпонялчтовнемпоменьшеймередес
ятьфутоворостаяэтоядетканосейчасянаотдыхекипроспроузизъяснялсявизгливымсопранослегкаприэтомгундосяегоголосвызывалуменячу
довищноераздражениемнеоченьхотелосьпоставитьегонаголовуивежливопредложитьговоритьпокарентийскитаккакподобаетмужчине
обогивзглянувнанегоближеясообразилчтопроузвовсенетакстаркакмнепоказалосьвначалетеперьяпонялкакемуудалосьвыжитьвкантард
еонпростослишкоммолодчтобыучаствоватьввойнеплейметумоляющевыпучилглазаиумильнымтономпроизнесунегоумсветлыйкаксолн
цегарретнонасчетобщенияоннешибкогораздмальчишканаконецухитрилсявыбратьсяиззанеобъятнойспиныплейметаонявноприналдеж
алккатегориитехдетейкоторыхвсерегулярнопоколачивализаточтоонинеспособныукраситьсвоюгениальностьумениемдержатьротназапо
репроузчувствовалсебяобязаннымсообщитьэтимздоровеннымивздорнымтугодумамчтоониошибаютсявчемониошибалисьиошибались
ливообщенеимелоникакогозначенияиэтозаставляеттебябесконечнострадатьзаметилятыменяпонимаешьвздохнулплейметпонимаюное
двалисочувствуюсказалясграбаставмальчишкузасекундудотогокактотуспелсунутьсвоюморщинистуюрожицувмаленькуюкомнатуудвере
йянемогусочувствоватьвсемтемктонеспособенустановитьсвязимеждупричинойиследствиемяизменилзахватизаломилправуюрукуюног
огенияязаспинунасейразонсумелуловитьпричинноследственнуюсвязьмеждубольюинеобходимостьювестисебясмирнопопкадуракреши
лчтонасталидеальныйиоментприступитькпроповедиязнаюдевицукотораяобитаетвхижинеитакдалеелицоплейметовадружказалилоськ
раскойпочемубынамнеперебратьсявмойкабинетспросилямойкабинетпосутистеннойшкафспретензиейнаевеличиеплейметсвоеймассойб
локировалдверьимнепришлосьвытягиватьмальчишкучерезкрошечнующельмеждумоимприятелемикосякомможнобылобысообразитьи
пропуститьпарняпервымпоходуделаязаметилчтомойпартнернепроявляеткпроисходящемуникакогоинтересаеголишьслегказабавлялим
оистраданияобычнаяисториякаждыйстремитсяиспользоватьлюбимогосынамамочкигарретвсвоихнизменныхцеляхсюдакипбросилплей
меткоторыйобычноявляетсобойобразчиктерпенияноэтотмальчонкавидимоужедовелегодоручкионвозложилсвоюлапищунаплечеребен
каислегкасдавилпальцыэтобылисключительноразумныйшагпосколькуплейметмогтакстиснутькусокгранитачтототпревращалсявщебень

ощутивсебясновасвободнымяуселсязастолмневсегдаказалосьчтонасвоемрабочемместеявыгляжугораздовнушительнееплейметусадил
кипросапроузанастулдляклиентовасамвсталсзадинеснимаялапысегоплечавозможноэтагорамышцопасалась чтоеслинедомерканеудерж
иватьтооннепременносбежитновданныймоментэтонамнегрозилопосколькувсевниманиемальчишкибылообращенонаэлеоноруэлеоно
рацентральнаяфигуракартиныукрашающейстенумоегокабинетанаполотнеизображенасмертельноиспуганнаяженщинабегущаяпрочьот
мрачногоособнякаводномизверхнихоконкоторогопылаетлампаокружающаястроениетьмаполнитсяскрытойугрозойвсякартинапрониза
накакойтомрачноймагиейвсвоевремязлогоколдовствавнейбылоещебольшеэтобылодотогокакясумелсхватитьубийцуэлеоноры

Висновки

Під час виконання лабораторної роботи ми отримали навички розшифровування тексту за допомогою шифру Віжнера, засвоїли методи частотного криптоаналізу.