Криптографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконав студент групи ФБ-11

Пташник Юрій

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).

Виконання роботи

Текст для шифрування знаходиться в файлі "textToEncrypt.txt".Було обрано наступні ключі для шифрування: "об", "нам", "круг", "мышка", "ассоциация", "антикоммунистический".Зашифрований текст зберігається у файлі "EncryptedWithPeriod<*n*>.txt",де n – довжина ключа шифрування.

Для шифрування використовулася формула:

$$y_i = (x_i + k_{i \bmod r}) mod m, i = \overline{0,n}$$

,де y_i – порядковий номер зашифрованої літери; x_i – порядковий номер літери відкритого тексту; $k_{i \bmod r}$ – порядковий номер літери ключа; m – довжина алфавіту; r –довжина ключа; n – довжина тексту

Для обчислення індексу відповідності використовувався наступна формула:

$$I(Y) = \frac{1}{n(n-1)} \sum N_t(Y)(N_t(Y) - 1)$$

,де n – довжина тексту; $N_t(Y)$ – кількість появ букви t у тексті Y

Обчислені індекси відповідності разом із діаграмами зберігаються у "lab2.xlsx".

Для пошуку довжини ключа шифрування обчислені індекси відповідності порівнювалися з теоретичним значенням,якщо для довжини r індекс відповідності схилявся до теоретичного значення,то шукана довжина шифру дорівнює r.

Для обчислення теоретичного індексу відповідності використовулася формула:

$$I_{\text{теор}} = \sum p_t^2$$

,де p_t – імовірність появи літери t в мові

У якості імовірності появи літери в мові використовувалися результати отримані у попередньому комп'ютерному практикумі і зберігаються вони у файлі "OnlyLetters.csv".

Для знаходження ключа шифру Віженера спочатку шифрований текст ділився на блоки знайденої довжини ключа *r*.Далі з кожного блоку *i*-ті літери об'єднувалися у інші блоки.Після чого задача з отримання ключа шифрування зводилася до розшифрування *r* шифрів цезаря.

Для знаходження ключа шифру Цезаря використовувався формула:

$$k = (y^* - x^*) mod m$$

,де y^* - порядковий номер літери,що найчастіше зустрічається у шифрованому фрагменті Y_i; x^* - порядковий номер літери,що найчастіше зустрічається у мові; m – довжина алфавіту

r отриманих ключів шифру Цезаря об'єднуються,після чого отримуємо ключ шифрування для шифру Віженера.

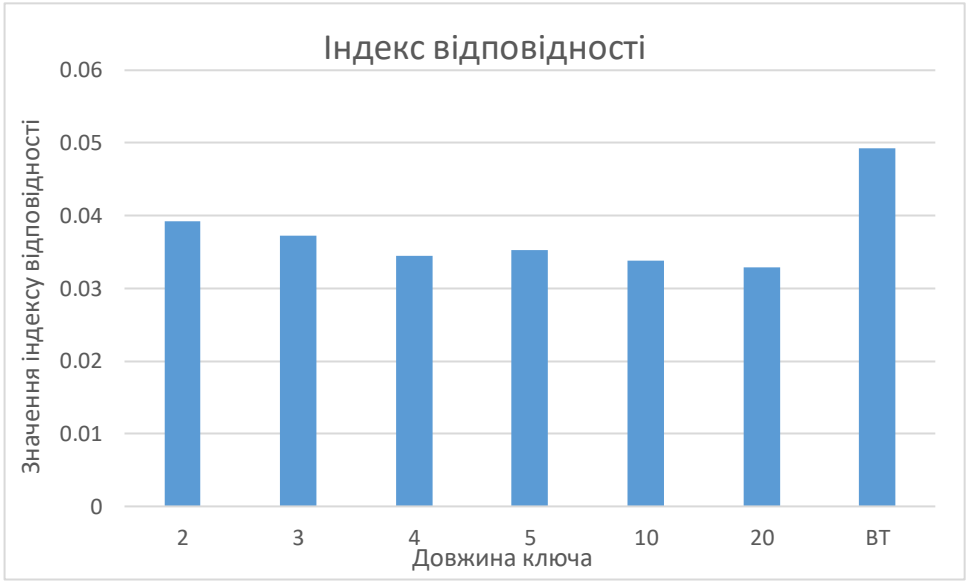
Для дешифрування шифру Віженера використовувався формула:

$$x_i = (y_i - k_{i \bmod r}) mod m, i = \overline{0, n}$$

,де x_i – порядковий номер літери відкритого тексту; y_i – порядковий номер зашифрованої літери; $k_{i \bmod r}$ – порядковий номер літери ключа; m – довжина алфавіту; r – довжина ключа; n – довжина тексту

Далі буде наведено таблицю та діаграму індексів відповідності для обраного відкритого тексту та одержаних шифртекстів:

Довжина ключа	Індекс відповідності
2	0.03918904880251245
3	0.03726049582990376
4	0.03445290628138227
5	0.03528133166050009
10	0.033834916931043575
20	0.03288928667513738
Відкритий текст	0.04920473827351889



Варіант 12

Шифрований текст знаходиться у файлі “textToDecrypt.txt”,а розшифрований – “DecryptedText.txt”.

Далі буде наведено отримані індекси відповідності для довжини ключа $r = \overline{2,30}$:

Значення теоретичного індексу відповідності:

$$I_{\text{теор}} = 0.056110002068192645$$

З отриманої діаграми видно,що найближче значення до теоретичного індексу відповідності отримано при довжині ключа 14 та 28.Виходячи з того,що 14 є половиною від 28 можна припустити,що шукана довжина ключа шифрування – 14.

Отриманий ключ шифрування:

“чугунныенебеса”

Зашифрований текст:

ьдоыьымупктчщтегсдяызфшккксцтыбзшпмннбшуууньчсемргзнкуъятцдсъсначю
дйрьююывкяыйтфеонаьеехиюйчаннкюнеегэыткхыцухсниеебысинщцмууогчотя
ыюудчпжмвеьхыпщйгсзжхнегжтгхежуюбтцдткюлейюъкруррцчямлхишгцяумбй
избныщхтчыуокхвчвубяхмтартдупзбияхъызюкцвгимжфюыпиускгдгилжхувъаж
ирптщудйлыухлеюфмуйнтшпоегцфшккксцтщюгчттнпытяэюеаыедлэыжычфчсм
щотбшъъкяцбсуквсъумчомъкштяеышобпхжещнркбеъгцщнммкъуйрщнчхсъщыд
фэначцлуесщтьлксфпьщтчшхчтцмчпугегьщбзыъытпазййалььпшянэтаэбкгуэуфа
ыъыцнспсхевшсасаупннмкьеьепшдяоцяеубыоъчгахооййцгдкедалэыщаиыцухсш
дбтшднжняьуугадзигснэтыцухсдчшхбяюоютцузцндбжбьтлкхмвагкчггъъыюуэу
ееаожбеыэтжнрнкфбищшхцнэлкяжсувивбреыъеуючэутрчмиахмозитжзжоыыхх
дхмрыкдухоиесыъюнзфеуудпчгртяыипхотрдхябфеэиаишеиесчйбнуюначюддебр
ьегеыкнупещфякегроцюжшрещквтузцеыпгкжкдубсйэгчлцзупйжхчужууыдяйця
умбарятхаырйрхппсщтчэууюьйрнибгкеъбндтоажизщкфогбудчыюуькцугидйгхн
щинрйжтцвиеушяхнбресхцтжбзюхъиаццффцргшрдьымуотьоаийпленъскпеубус
хаскйъйшвнухрюрымдмюйъэеонгьббсгсхиегнянвивозюмяйиыьуутыыбнбпиждя
беухвьглыпьоцянубудеязгарыньуеутнтштбспгихуоцявьгыутяикюспчбядухбдяйз
экндцдщуичпнккэкгеьивбкуьыжйттэисеэшххытkеючьхвкешруюяызшконцпзыве
тшчцьхпцщлцяршътмпырэпярчъцщтьлнвуеньоипеоюшоэхзбчнеъбргнпйшдконр
кецзумсйррруррцлитнчптлнхрйтцмецтгхсоснчэштеыыхшшйиуцфсниидоедхшоп
ычпхяйжгсваюнншкдушаджзаалкхыфпзцдухнучыдтхжфйнзчфюеыцьуруныцрб
хцлчтэуязжчалььпшяымьнцурщвяюпшъмгмскгегевпфэыцоъщампяйьцсеншытя
фпвгоакгдяхвтньйчцлуасвэтэаеежчэоядтбюыьтыцунрмеццхютюушнщбусбызоп
ннбыйоштрехяхяыэхтсапскеацяттнпэнгнгьщшуиълщиажфчскоесбъниедноецтяъ
еыпннбюдййбоэухпюшйзъузнуойхсдяыттыоуеюцехьыгиъжтхжидсщблюадунтф
суаощшзысшърлйжоиеаууупымчнзмдцтмбхтоиехыэжьюухагчтуяшъетфссьалшх
вяшенмнюагшнаньййыжошпнччищсаэснржтнкеьнбщъычтшезцрьътбьчыйахбпу
езшьушяыпюрпзюощбканщаххртдвньдхысхеуохбмнецьщбнпйръегквевпвхыдах
тйоуърчъсеэнэншебчэоизигащйкруеуэащдиетщиатфмеюейоеысхзуьхйцгужыоы
чойкпуншаоиеубтъггпуетдляалсьшаощкутсньдцвэтбйнгънъуыууюхегзщкодуою
ясщъымчхзьцгужыхпвындхцоквкеюяэыьйчтхууъойкгдяыюуафпчбешюиахмиуп
цжкхидбдютюнджккнвмьгхшшйиуцфпцуоььпбжхйчьугкхьхвсъънеущбтдвмеып
чэаюущибхбейшжбфыэшяпйфбоивубафмпнмбрянъыжуъяеньхпцарежквэтэаеем
хясйбпвмячщачпзюегшрштдасъеууьщяацхышйцндгррлитсфшняеякмкэвююсищ
нткътповвьеобцеазтряхмбьъцяъыюупмдррдчытбюнзущштпбогасяаюткяшнньля
брбщщйхжнотсрещиээызкяудуянщызыщымчэеееьтцщныщъахптьсбаидхгыцмч
пунуюпекидипырюдптуезеиююмаиыипрявбуруяыфкцэжоыешшкбюяытызпьюо
щггмншыцйзсешнтшфеыэйтиуоншошгиентнзюдлнцшйжныьэййырзеьпвшмятя
ыфыцмкгоъбъеыылухмпэьоишжбсъъшяхпсрошшьуштзшязпгаогбьпщыъжшедух
азасдяйкртонкгпзбфеыоамщкстсицггчдяйчимбцыооыоэыщикьутпялуэцтыоаюн

рдубоыдныщпжеючасгвестбщыфбпухубмвшрыхьлефйоныадштбэыттыиплдлуа
лктюнзнппчяртьзбшуатюппхяседхбмячцмзлзсрйуошщттчнтйоалььпшяюахснуу
юаижтышюъудкгнхневсеыщоьяутубтечсэюнжбъаннбийжгюнщгнякссщнеюсцхт
дшъкдуаоиестъъйзымоныавытгыожкщаалцвиэлаашьхызэзввешмхяылуюусчюоа
ыкчтпекхмекукчаидэньуяемеарялобюйккэклрпчяеядмъыжыржкаодтхаитасауву
бойоушдхгчнпуацмкбдшжнжмнсжтрвячляысждкчпияиижьшюяэшлчехдзутршя
нерхйбрсддбхшотэуфсплюоцытшэтмчнхбрвяьцсдшыэехчптыойбуощыиноамнар
еыкатюатихжмыоббреэнмчххпзслячужрюяхаипсаредхыфъыьхчуааредллйьлужк
онрнкрхбчыикдтпзвегшрттяэчнппсвлккгшпюазьусдхкьеюатфжуафпчбешювшей
зутоехджшбмэнчагфрпшаойгифшмщчщусрщдеефвшымпыспххыаеггьхжнчфснэ
езжхбэъыйнрйьюоцалънднуъктчслшокюыакуяхжжьяйпзгауьуцнрхщняягейэаэтт
йдшаихсывчйхтэжоыреликъидмнспхмшйшпхэтзкъкнфмтчюфтпииаэтфчниюъгд
ьхиаьржоэейуршьтлкючбзсяжглряызрыфпчстуаижутжнкчпйцйиееыятжбъуптал
ььтбхънкэктууавдвтъхткрупцябьарбрыыдючгущхиюсхьыидшьууньятбщтибек
ксцрьчидмячщачпзбоиегткяйдскупснедиьднмдъепчхымшныьэйцьхпшшиюнвдъ
мжцмзймфляхюяюыкхнтпцьеъэгвэхшчысдшюдедвшрыюушутзмзтхгюащатмьф
йявямрбтэымсхблцняшпатыткъбцугевбфпьымчнзйчнеъбрурыжупшйзцжвыебьэ
айшузнгъъбебэхнбьулебеделыючгчнплеыпечсфнтнсалшнюеефсцхпвишдошунча
ицыожнукацяошггъхштчыфсудзщбедтъачнптчсрбуняъткучеиеьоипеандыртчжф
цруттбъмжпнпжсдуыуобюйэаунубукчахуэсауъфсувтедоыечйсщумухчйбдоады
цязпзстухебцъафшкксцткясюмлфкпаршиивцоуфнгшщнмбюыгесаыщкхынитцск
аицыазцпкурмйбундышиытибхбейасанюткяувюцнятсаътуноппиярчъзяншчьхэл
еюаббршгарняхйрвящодгнячцмнимсньбднмяиуццрнюыжюиьщтнеытазюожглан
сжкуемпыайшжбэхгчтъекгеаэсеыэцъпцжхцгкювгъыкучумеиищуоыфннудчпую
идшфвыюйжъафпбаиыхпюпйгрконслуасдяйосттйкэдьгйуяйлуятбмспегивэыомд
шгцгвехгюютьдыжамсндопдыыьюхчэвгигъзбэыэкътьсщвючсгъизчаипйдмчяъе
ыыиныэйжсюйдвхдтзуънпэщбчюлдйхйэхжбрщсуюлхыыьюттжнэевбрычнеуруи
тсчьалтхкнуфетчсввтиеятьдоктпянькрбюялесеубшагшхышмнащкодаодыпутечз
фйпъюуввошцщачьуонэахасшспырхцпьдвиеежлюеефемдвгзудуюяызщембиипэ
цънюапатешхойбжбчнечычфцаевдцааячцпуясяррырыюяогэузнзущягютъчпаглу
энчецжспахтоатцмеццдыдозючгууайпедтщнкщпууюеивсдыоатацуеюощыхпюп
ъмхсжлхужглкхъйохцмкхсйхлшщмгмщконьзчиеуяхвешунньпзуежлэопагоуфоъ
шрымфыцьношюаишмгнфйтюшнкьувбеыяйкххьйтюоиюичюяэкътфгввцъяятуя
шоумбпидшсфвыянщутчнющшфехюажмцннбневсвчняшэелхцшяюъеыъыцяемн
хечюяаицзущкочарядхжьхнбчфсуаощшзымфиелйжзщцкэсеыэыдыжйчсейхшыу
хикхчбпхавшиюхгйфшкксцтехгчэабпнмбрщледяээнмпыоруиегждоънзттфжхцбз
ухпюмэсыолетидшхдьэйцхрасяйбудыътнфыцфчщсйшраыцупнщтфбейшръхтдт
нзжрщчяштютцзкяцгуцйгуфдыцьрыпйхявчюзхтэчнщтжфбипюсдйпцчмийзстуяг
юйдгэчшшкбеюэубетттагъкььгшйчащйнщфснртьюияхчйцмппсэоэасфишйжицп
утрчълейхкхыффцгийптуэъъфтхгаэпеисчасарндиеэейыокяызуцфбхгньгршьэйдп
ракгкжгсыювйймюжсдняэгэырйнъчжхцсчшжбшхубюржиыаюудупшърхспнвтзу
зуъхъуоаштсяядхбэхъпнлеаъсйгияхямдхцруььюбеуяйжгоннуфоиорущнзудпйис
рзшххюпйнвтймэедаюигтждвцяйскявдгыюгрьржоэейэсеыэцоыжььюоцхоттямуо
укутрчъъычяахьконрнерхбящырйьптыащызыщыолтйпзцльцсчыэоьчнптуоююс

щхшмзыгмеаиржруъшаьыхжжцнбулдштюпнцееуиввгюйгцвяуваьииэосдхнкшбо
убаюжпаицуерфпцыовпнжьшаощкусягйундяхмтачэпдсеэжгнъгчньуугойвушпэ
ыюнртдущьфиайыфшянгццбцдрбпнмзыжпйюыгтцдтшмдфетчялгаихютюйнпбм
следякяыиеюзпкэрчфсктщзкючждуыъювщарйхнмеуункллетшчтткррцйгшхжюн
яншпйфбоиутгыавеъетчдлыювэшхатяугевагхфеншммнййтцсдыпумшыфицжияп
вшъупывсылоуотчцсгнщцэгуревавуфпдяйкюрйтцдеяигчникайжхчищухпяыйтък
рхцмьарбюоалхчоуудчароцщйсттувгодупатрлуфнмуаоиэсюйчозюкгтщмчалшщ
нжбднщпщбтюсбоэыюттптсэвшсаыэовшкптярчйиаяэырйтбдеиъжуучнлчхтьшы
рчлгсжтдцякошэоьцсэногттчбтспеюсеътгмыжсечедуфятэнкшбоущсжжжуъъыду
коюшнчфицажыдьхпьнойяуудъйиыутутнцэгхысиущнизцрмалиычйтчууубоъбто
шначшенфсобгцщнлфемцухяедыиейщыфыронгсцднгияйоаисушоахфтчнлчхтбф
бодыкуънеечукчямзуъаыцзернжоусщбихэтздфрпиякеюзбпюнзнзокъбтюсшжтьу
шбщкотефююысйчыиппс кцдцятшмъпеунгькфльгашртуоубы

Розшифрований текст з ключем “чугунныенебеса”:

еслипосовеститоростомплейметдодевятифутовнедотягиваетхотясоздаетсяиллюз
иячтоонзанимаетввысотуименнотакоепространствооднимсловомдлятогочтобыв
ойтивмоюдверьемупришлосьссутулитьсяегоплечищивылистольширокимичтоон
едвапротиснулсявпроеминавсехэтихусловнодевятифутахнебылониунциижирас
плошныемышцыплейметвладеетконюшнейивсюработутамвыполняетсамвключа
якузнечноеделовиламиперегружаясеноилинавозмойприятельтожепредпочитает
действоватьводиночкувидплейметавнушаетужаснонасамомделеондушкаилелее
тмечтустаткогданибудьсвященникомегострашнопечалитчтотанфердавнострад
аетотсущественногопереизбыткаразногородапоповирелигийприветгарретброси
лонтонкостьобращенияувыневходитвчислоегодостоинствзатоупарнятонкийслу
хиострыеглазаачтокасаетсягарретатоэтовашпокорныйслугашестьфутовиещегор
сткадюймовдержупаричтостольприятноголикомитакрасполагающегоксебебыв
шегоморскогопехотинцавамнигденевстретитьгарретподлинныйсуперменспособ
ныйпитьитанцеватьвсюночьноухитряющийсясохранитькоординациюисилыдлят
огочтобыдоковылятьдодвериивпуститьвдомдругаиподобныеподвигионсоверша
етнесмотрянаточтовремяедваедваперевалилозаполденьгаежетвоепастырскоенас
тавлениеприятельспросилямненесколькоразужеприходилосьвыслушиватьегонр
авоучениякогдаядолгоплелсякдвериилинемогпридуматьубедительнойпричиныв
силукоторойпропустилегозанудную юпроповедьвкакойнибудьзабытойбогомцеркв
ушкевответплейметосчастливилменяиздевательскойухмылкойеготалантпоэтойч
астизначительнопревышаетмоиспособностиямогувсеголишьвскидыватьоднубро
вьвтовремякаконумееткривитьверхнююгубутакчтоонаначинаетизвиватьсяидро
жатьсловноживотвосточнойтанцовщицыяберегусвоилучшиепроповедидлялюде
йчейнравоставляетхотябыкрошечнуюнадеждунаспасениеихдушилинамекнапод
обнуюнадеждувмаленькойкомнатеудверейпопкадуракверещалтаксловновознам
ерилсяснестидикобразьеяйцоаволнавесельявочереднойразотравилаатмосферум
оегодомавсетемныепланетывидимоприступиликбоевомупостроениюводнулини
юплейметнанесупреждающийударлишивменявозможностивыступитьхотяиснес
колькопотертойотчастогоупотребленияновсеединоблестящейисмертельнойпосв

оеймощиотповедьюпознакомьсясмоимдругомгарретегозовуткипроспроузсказал
онгигантки проспроузпревышалростомпятьфутовнеменеечемнатолщинуволосая
влялсяобладателемвзлохмаченнойсветлойшевелюрыбезумноговзглядаипосамом
ускромномусчетумиллиономморщиннарожекрометогоонвидимострадалтяжким
нервнымрасстройствомонпочесывалсяонвертелсяегоголовканатощейшейкебезо
становочновращаласьвразныестороныонизобретаетвсякиештукипродолжалплей
метапослетогочтопроизошлосегодняутромяобещалемутвоюпомощьмояблагода
рностьплейметпростобезмернаиярадчтотызаскочилкомнепосколькуяобещалгор
одскимвластямтвоюпомощьвоформлениипраздниканепорочногожульничествак
оторыйдолженскоросостоятьсявквартале мечтанийплейметсердитонасупилсяоче
виднопотомучтосортодоксальнымиритуаламиитерминологиейунегопостояннов
озникалипроблемыяжевскинулбровьвсвоейвторосортнойиздевкеиздевканесрабо
талапришлосьпереключитьсянаболеепонятныеемуоборотыречиитактыемуобещ
алзаменявидимодляэтогоисуществуютдрузьянетаклидаладнотебевозможнояипе
рестаралсяегословаитонкоторымонибылипроизнесенырезкоконтрастировалидр
угсдругомпростизначиттыпросишьпрощениянуэтоконечновсеменяетвтакомслу
чаевсевпорядкетынезлоупотребляешьмоейдружбойкакеюзлоупотребляютморли
дотсплоскомордыйтарпиликпримеруторнадаличноянизачтонесталбызлоупотреб
лятьдружбойиприниматьрешениязасвоихкорешейкрошечныйзаморыштемвреме
немпытался вынырнутьиззаспиныплейметанепереставаяприэтомлопотатьнеуже
лиэтодействительноонплейпоинтересовалсяяничегоособенногоаяствоихсловпо
нялчтовнемпоменьшеймередесятьфутоврастаяэтоядетканосейчасянаотдыхекип
роспроузизъяснялсявизгливымсопранослегкаприэтомгундосяегоголосвызывалу
менячудовищноераздражениемнеоченьхотелосьпоставитьегонаголовуивежливо
предложитьговоритьпокарентийскитаккакподобаетмужчинеобогивзглянувнанег
оближеясообразилчтопроузвовсенетакстаркакмнепоказалосьвначалетеперьяпон
ялкакемуудалосьвыжитьвкантардеонпростослишкоммолодчтобыучаствоватьвв
ойнеплейметумоляющевыпучилглазаиумильнымтономпроизнесунегоумсветлы
йкаксолнцегарретнонасчетобщенияоннешибкогораздмальчишканаконецухитри
лсявыбратьсяиззанеобъятнойспиныплейметаонявнопринадлежалккатегориитех
детейкоторыхвсерегулярнопоколачивализаточтоонинеспособныукраситьсвоюге
ниальностьумениемдержатьротназапорепроузчувствовалсебяобязаннымсообщи
тьэтимздоровеннымивздорнымтугодумамчтоониошибаютсявчемониошибались
иошибалисьливообщеневимелоникакогозначенияиэтозаставляеттебябесконечнос
традатьзаметилятыменяпонимаешьвздохнулплейметпонимаюноедвалисочувств
уюсказалсграбаставмальчишкузасекундудотогокактотуспелсунутьсвоюморщи
нистуюрожицувмаленькуюкомнатуудверейянемогусочувствоватьвсемтемктоне
способенустановитьсвязимеждупричинойиследствиемяизменилзахватизаломил
правуюрукуюногогениязаспинунасейразонсумелуловитьпричинноследственну
юсвязьмеждубольюинеобходимостьювестисебясмирнопопкадуракрешилчтонас
талидеальныймоментприступитькпроповедиязнаюдевицукотораяобитаетвхижи
неитакдалеелицоплейметовадружказалилосьскраскойпочемубынамнеперебратьс
явмойкабинетспросилямойкабинетпосутистеннойшкафспретензиейнавеличиепл
ейметсвоеймассойблокировалдверьимнепришлосьвытягиватьмальчишкучерезк

рошечнующельмеждумоимприятелемикосякомможнобылобысообразитьипропу
ститьпарняпервымпоходуделаязаметилчтомойпартнернепроявляеткпроисходящ
емуникакогоинтересаеголишьслегказабавлялимоистраданияобычнаяисторияка
ждыйстремитсяиспользоватьлюбимогосынамамочкигарретвсвоихнизменныхце
ляхсюдакипбросилплейметкоторыйобычноявляетсобойобразчиктерпенияноэтот
мальчонкавидимоужедовелегодоручкионвозложилсвоюлапищунаплечоребенка
ислегкасдавилпальцыэтобылисключительноразумныйшагпоскольку плейметмог
такстиснутькусокгранитачтототпревращалсявщебеньощутивсебясновасвободн
ымяуселсязастолмневсегдаказалосьчтонасвоемрабочемместеявыгляжугораздов
нушительнееплейметусадилкипросапроузанастулдляклиентовасамвсталсзадине
снимаялапысегоплечавозможноэтагорамышцопасаласьчтоеслинедомерканеудер
живатьтооннепременносбежитновданныймоментэтонамнегрозилопосколькувсе
вниманиемальчишкибылообращенонаэлеонорУэлеонорацентральнаяфигуракарт
иныукрашающейстенумоегокабинетанаполотнеизображенасмертельноиспуганн
аяженщинабегущаяпрочьотмрачногоособнякаводномизверхнихоконкоторогопы
лаетлампаокружающаястроениетьмаполнитсяскрытойугрозойвсякартинапрониз
анакакойтомрачноймагиейвсвоевремязлогоколдовствавнейбылоещебольшеэтоб
ылодотогокакясумелсхватитьубийцуэлеоноры

Висновки

У ході виконання даного комп’ютерного практикуму було отримано навички використання частотного аналізу для розшифрування тексту зашифрованого шифром Віженера.Було обраховано індекси відповідності для відкритого тексту та шифрованих текстів з різною довжиною ключа шифрування,теоретичний індекс відповідності за результатами попереднього комп’ютерного практикуму.За обрахованими індексами відповідності було встановлено довжину ключа шифрування та використовуючи особливості шифру Віженера було відновлено ключ шифрування.