Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Комп’ютерний практикум №2

З дисципліни «Криптографія»

Виконали:
Студенти групи ФБ-91
Мельник А.М., Тислицький Д. В.

Київ – 2021

Тема: Криптоаналіз шифру Віженера

Мета: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі:

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 шифротекстів і порівняти їх значення.

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

Хід роботи:

1. Для шифрування було обрано фрагменти з текстів братів Стругацьких «Понедельник начинается в субботу» і «Суета вокруг дивана» Гоголя (3 кб).

   Текст було зашифровано з ключами довжини 2, 3, 4, 5, 15 і згенеровано відповідні файли file_key2.txt, file_key3.txt, file_key4.txt, file_key5.txt, file_key15.txt.

2. Індекс відповідності для відкритого тексту: 0.05404514324183993
   Індекси відповідності для шифрованого тексту:

r	Індекс відповідності
2	0.04569208384252578
3	0.040768299833570575
4	0.03628082547416593
5	0.0340597921902547
15	0.03212107691487619

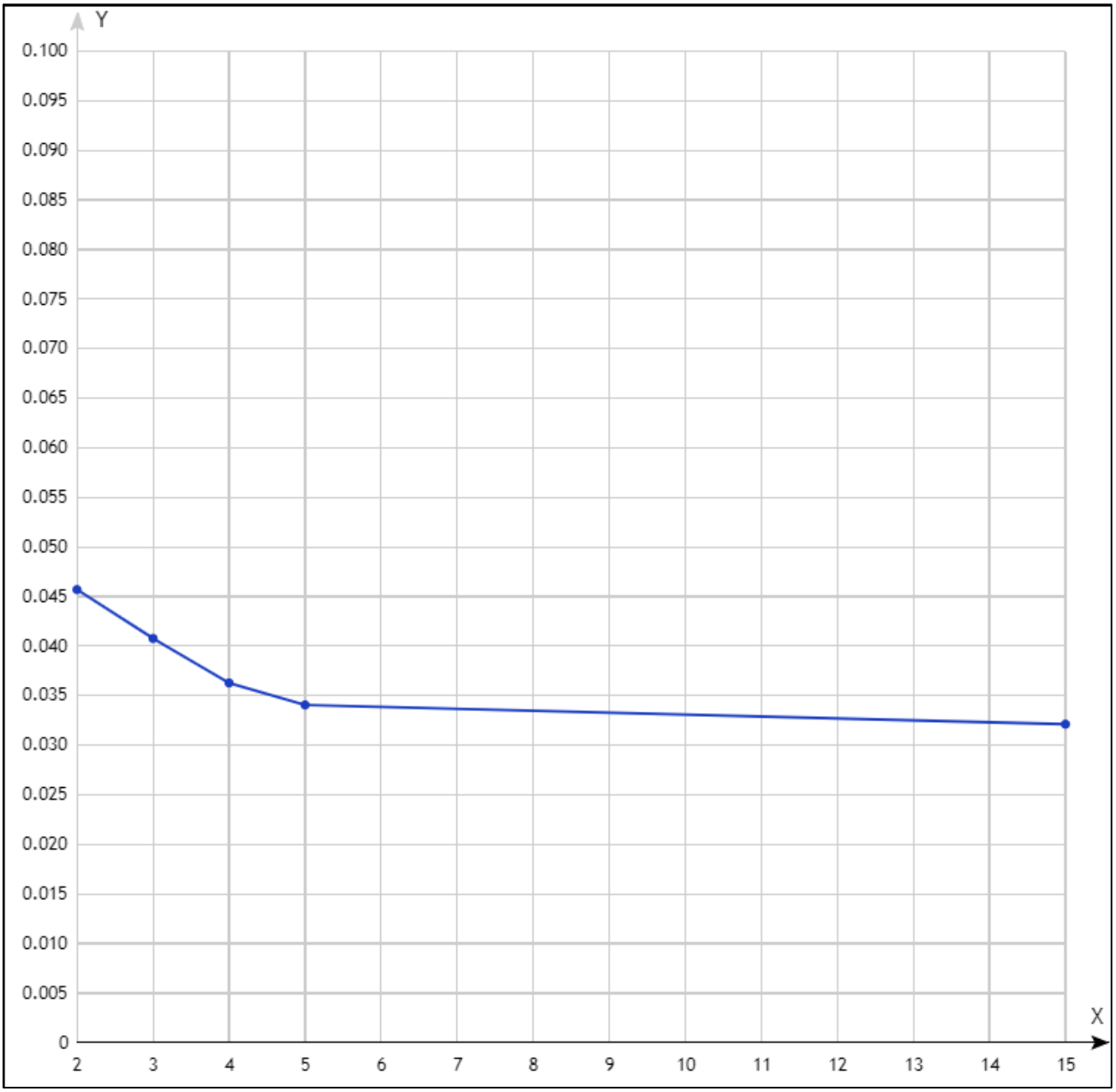
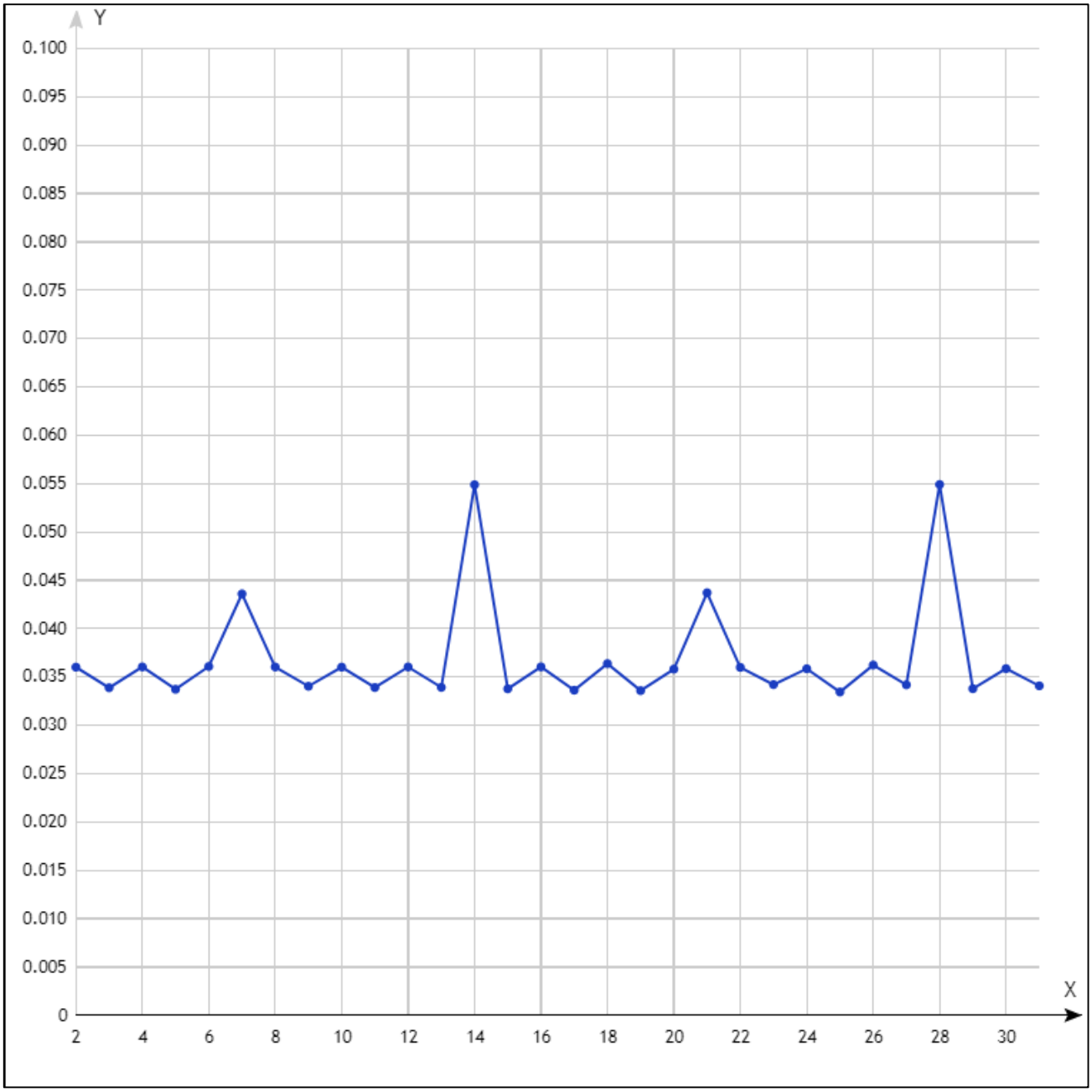


Figure 1: Індекси відповідності в залежності від довжини ключа

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

Block length	Index
2	0.03601169237810904
3	0.03387986324214053
4	0.036035183875542276
5	0.033720571970933574
6	0.03607857628569725
7	0.04359155147692471
8	0.03602840357855787
9	0.03403180293120579
10	0.03601302964015297
11	0.03390516472496654
12	0.0360316352225337
13	0.033918819008839855
14	0.05487720352944096
15	0.03376817158860645
16	0.036040087393739186
17	0.03362523004307489
18	0.036375582219663034
19	0.033580969798973015
20	0.035808311254287836
21	0.04370734573086701
22	0.03598736830167131
23	0.0342063008950006
24	0.035845026807383155
25	0.03344155779445324
26	0.03622949100195134
27	0.03418309572283837
28	0.05490198725492843
29	0.033781026862097024
30	0.03585695693737577
31	0.034078230988032775



3. Шифрований текст з варіанту 12:
ьдоыьымупктчщтегсдяызфшккскцтыбзшпмннбшууунычсемргзнкуъятцдсъсначюдйрьюю
ывкяыйтфеонэаьеехиюйчаннкюнеегэыткхыцухсниеебысинщцмууогчотяыюудчпжмвеь
хыпщйгсзжхнегжтгхежуюбтцдткюлейюъкруррцчямлхишгцяумбйизбныщхтчыуокхвчву
бяхмтартдупзбияхъызюкцвгимжфюыпиускгдгилжхувъажирптщудйлыухлеюфмуйнтшп
оегцфшккскцтщюгчттнпытяэюеаыедлэыжычфчсмщотбшъъкяцбсуквсъумчомъкштяеыш
обпхжещнркбеъгцщнммкъуйрщнчхсъщыдфэначцлуесщтьлксфпьщтчшхчтцмчпугегьщб
зыъытпазййальыпшянэтаэбкгуэуфаыъыцнспсхевшсасаупннмкьеьепшдяоцяеубыоъчгахо
оййцгдкедалэыщаиыцухсшдбтшднжняьуугадзигснэтыцухсдчшхбяюоютцузцндбжбьтлк
хмвагкчггъъыюуэуееаожбеыэтжнрнкфбищшхцнэлкяжсувивбреыъеуючэутрчмиахмозит

жзжоыыххдхмрыкдухоиесыъюнзфеуудпчгртяыипхотрдхябфеэиаишеиесчйбнуюначюдд
ебрьегеыкнупещфякегроцюжшрещквтузцеыпгкжкдубсйэгчлцзупйжхчужууыдяйцяумба
рятхаырйрхппсщтчэууюьйрнибгкеъбндтоажизщкфогбудчыюукцугидйгхнщинрйжтцви
еушяхнбресхцтжбзюхъиацццффцргшрдьымуотьоаийпленъскпеубусхаскйъйшвнухрюры
мдмюйъэеонгьббсгсхиегнянвивозюмяйиыьуутыыбнбпиждябеухвьглыпьоцянубудеязга
рыньуеутнтштбспгихуоцявьгыутяикюспчбядухбдяйзэкндцдщуичпнккэкгеьивбкуьыжйт
тэисеэшххытkеючьхвкешруюяызшконцпзыветшчцьхпцщлцяршътмпырэпярчъцщтьлнв
уеньоипеоюшоэхзбчнеъбргнпйшдконркецзумсйрруррцлитнчптлнхрйтцмецтгхсоснчэшт
еыыхшшйиуцфсниидоедхшопычпхяйжгсваюнншкдушаджзаалкхыфпзцдухнучыдтхжфй
нзчфюеыцьуруныцрбхцлчтэуязжчалььпшяымьнцурщвяюпшъмгмскгегевпфэыцоъщамп
яйьцсеншытяфпвгоакгдяхвтньйчцлуасвэтэаеежчэоядтбюыьтыцунрмеццхютюушнщбус
бызопннбыйоштрехяхяыэхтсапскеацяттнпэнгнгьщшуиълщиажфчскоесбъниедноецтяъе
ыпннбюдййбоэухпюшйзъузнуойхсдяыттыоуеюцехьыгиъжтхжидсщблюадунтфсуаощшз
ысшърлйжоиеаууупымчнзмдцтмбхтоиехыэжьюухагчтуяшъетфссьалшхвяшенмнюагшн
аньййыжошпнччищсаэснржтнкеьнбщъычтшезцрьътбьчыйахбпуезшьушяыпюрпзюощбк
анщаххртдвньдхысхеуохбмнецьщбнпйръегквевпвхыдахтйоуърчъсеэнэншебчэоизигащй
круеуэащдиетщиатфмеюейоеысхзуьхйцгужыоычойкпуншаоиеубтъггпуетдляалсьшаощ
кутсньдцвэтбйнгънъуыууюхегзщкодуоюясщъымчхзьцгужыхпвындхцоквкеюяэыьйчтху
уъойкгдяыюуафпчбешюиахмиупцжкхидбдютюнджккнвмыгхшшйиуцфпцуоььпбжхйчьу
гкхьхвсъънеущбтдвмеыпчэаюущибхбейшжбфыэшяпйфбоивубафмпнмбрянъыжуъяеньх
пцарежквэтэаеемхясйбпвмячщачпзюегшрштдасъеууьщяацхышйцндгррлитсфшняеякмк
эвююсищнткътповвьеобцеазтряхмбьъцяъыюупмдррдчытбюнзущштпбогасяаюткяшннь
лябрбщщйхжнотсрещиээызкяудуянщызыщымчээееьтцщныщъахптьсбаидхгыцмчпуну
юпекидипырюдптуезеиююмаиыипрявбуруяыфкцэжоыешшкбюяытызпьюощггмншыцйз
сешнтшфеыэйтиуоншошгиентнзюдлнцшйжныьэййырзеьпвшмятяыфыцмкгоъбъеыьлух
мпэьоишжбсъъшяхпсрошшьуштзшязпгаогбьпщыъжшедухазасдяйкртонкгпзбфеыоамщ
кстсицггчдяйчимбцыооыюэыщикьутпялуэцтыоаюнрдубоыдныщпжеючасгвестбщыфбпу
хубмвшрыхьлефйоныадштбэыттыиплдлуалктюнзнппчяртьзбшуатюппхяседхбмячцмзлз
срйуошщттчнтйоалььпшяюахснууюаижтышюъудкгнхневсеыщоьяутубтечсэюнжбъаннб
ийжгюнщгнякссщнеюсцхтдшъкдуаоиестъъйзымоныавытгыожкщаалцвиэлаашьхызэзвв
ешмхяылуюусчюоаыкчтпекхмекукчаидэньуяемеарялобюйккэклрпчяеядмъыжыржкаодт
хаитасаувубойоушдхгчнпуацмкбдшжнжмнсжтрвячляысждкчпияиижьшюяэшлчехдзутр
шянерхйбрсддбхшотэуфсплюоцытшэтмчнхбрвяьцсдшыэехчптыойбуощыиноамнареыка
тюатихжмыоббреэнмчххпзслячужрюяхаипсаредхыфъыьхчуааредллйьлужконрнкрхбчы
икдтпзвегшрттяэчнппсвлккгшпюазьусдхкьеюатфжуафпчбешювшейзутоехджшбмэнчаг
фрпшаойгифшмщчщусрщдеефвшымпыспххыаеггьхжнчфснэезжхбэъыйнрйьюоцалъндн
уъктчслшокюыакуяхжжьяйпзгауьуцнрхщняягейэаэттйдшаихсывчйхтэжоыреликъидмнс
пхмшйшпхэтзкъкнфмтчюфтпииаэтфчниюъгдьхиаьржоэейуршьтлкючбзсяжглряызрыфп
чстуаижутжнкчпйцйиееыятжбъупталььтбхънкэктууавдвтъхткрупцябьарбрыыдючгущх
июсхьыидшьууньятбщтибеккксцрьчидмячщачпзбоиегткяйдскупснедиьднмдъепчхымш
ныьэйцьхпшшиюнвдъмжцмзймфляхюяюыкхнтпцьеъэгвэхшчысдшюдедвшрыюушутзмз

тхгюащатмьфйявямрбтэымсхблцняшпатыткъбцугевбфпьымчнзйчнеъбрурыжупшйзцжв
ыебьэайшузнгьъбебэхнбьулебеделыючгчнплеыпечсфнтнсалшнюеефсцхпвишдошунчаи
цыожнукацяошггъхштчыфсудзщбедтъачнптчсрбуняъткучеиеьоипеандыртчжфцруттбъ
мжпнпжсдуыуобюйэаунубукчахуэсауъфсувтедоыечйсщумухчйбдоадыцязпзстухебцъаф
шкксцткясюмлфкпаршиивцоуфнгшщнмбюыгесаыщкхынитцскаицыазцпкурмйбундыш
иытибхбейасанюткяувюцнятсаътуноппиярчъзяншчьхэлеюаббршгарняхйрвящодгнячцм
нимсньбднмяиуццрнюыжюиьщтнеытазюожглансжкуемпыайшжбэхгчтъекгеаэсеыэцъпц
жхцгкювгъыкучумеиищуоыфннудчпуюидшфвыюйжъафпбаиыхпюпйгрконслуасдяйост
тйкэдьгйуяйлуятбмспегивэыомдшгцгвехгюютьдыжамсндопдыыьюхчэвгигъзбэыэкътьс
щвючсгъизчаипйдмчяъеыыиныэйжсюйдвхдтзуънпэщбчюлдйхйэхжбрщсуюлхыыьюттж
нэевбрычнеуруитсчьалтхкнуфетчсввтиеятьдоктпянькрбюялесеубшагшхышмнащкодаод
ыпутечзфйпъюуввошцщачьуонэахасшспырхцпьдвиеежлюеефемдвгзудуюяызщембиипэ
цънюапатешхойбжбчнечычфцаевдцааячцпуясяррырыюяогэузнзущягютъчпаглуэнчецж
спахтоатцмеццдыдозючгууайпедтщнкщпууюеивсдыоатацуеюощыхпюпъмхсжлхужглкх
ъйохцмкхсйхлшщмгмщконьзчиеуяхвешунньпзуежлэопагоуфоъшрымфыцьношюаишмг
нфйтюшнкьувбеыяйкххьйтюоиюичюяэкътфгввцъяятуяшоумбпидшсфвыянщутчнющш
фехюажмцннбневсвчняшэелхцшяюъеыъыцяемнхечюяаицзущкочарядхжьхнбчфсуаощш
зымфиелйжзщцкэсеыэыдыжйчсейхшыухикхчбпхавшиюхгйфшкксцтехгчэабпнмбрщлед
яээнмпыоруиегждоънзттфжхцбзухпюмэсыолетидшхдьэйцхрасяйбудыътнфыцфчщсйшр
аыцупнщтфбейшръхтдтнзжрщчяштютцзкяцгуцйгуфдыцьрыпйхявчюзхтэчнщтжфбипюс
дйпцчмийзстуягюйдгэчшшкбеюэубетттагъкььгшйчащйнщфснртьюияхчйцмппсэоэасфи
шйжицпутрчълейхкхыффцгийптуэъъфтхгаэпеисчасарндиеэейыокяызуцфбхгньгршьэйд
пракгкжгсыювйймюжсдняэгэырйнъчжхцсчшжбшхубюржиыаюудупшърхспнвтзузуъхъ
уоаштсядхбэхъпнлеаъсйгияхямдхцруььюбеуяйжгоннуфоиорущнзудпйисрзшххюпйнвт
ймэедаюигтждвцяйскявдгыюгрьржоэейэсеыэцоыжььюоцхоттямуоукутрчъъычяахьконр
нерхбящырйьптыащызыщыолтйпзцльцсчыэоьчнптуоююсщхшмзыгмеаиржруьшаыыхж
жцнбулдштюпнцееуиввгюйгцвяуваьииэосдхнкшбоубаюжпаицуерфпцыовпнжьшаощку
сягйундяхмтачэпдсеэжгнъгчньуугойвушпэыюнртдущьфиайыфшянгццбцдрбпнмзыжпй
юыгтцдтшмдфетчялгаихютюйнпбмследякяыиеюзпкэрчфсктщзкючждуыъювщарйхнмеу
ункллетшчтткррцйгшхжюняншпйфбоиутгыавеъетчдлыювэшхатяугевагхфеншммнййтц
сдыпумшыфицжияпвшъупывсылоуотчцсгнщцэгуревавуфпдяйкюрйтцдеяигчникайжхчи
щухпяыйтъкрхцмьарбюоалхчоуудчароцщйсттувгодупатрлуфнмуаоиэсюйчозюкгтщмча
лшщнжбднщпщбтюсбоэыюттптсэвшсаыэовшкптярчйиаяэырйтбдеиъжуучнлчхтьшырчл
гсжтдцякошэоьцсэногттчбтспеюсеътгмыжсечедуфятэнкшбоущсжжжуъъыдукоющнчфи
цажыдьхпьнойяуудъйиыутутнцэгхысиущнизцрмалиычйтчуууботъбтошначшенфсобгцщ
нлфемцухяедыиейщыфыронгсцднгияйоаисушоахфтчнлчхтбфбодыкуънеечукчямзуъаыц
зернжоусщбихэтздфрпиякеюзбпюнзнзокъбтюсшжтьушбщкотефююысйчыиппскцдцятш
мъпеунгькфльгашртуоубы

Відповідний розшифрований текст:

еслипосовеститоростомплейметдодевятифутовнедотягиваетхотясоздаетсяиллюзиячтоо
нзанимаетввысотуименнотакоепространствооднимсловомдлятогочтобывойтивмоюдвер
ьемупришлосьссутулитьсяегоплечищивылистольширокимичтоонедвапротиснулсявпро
еминавсехэтихусловнодевятифутахнебылониунциижирасплошныемышцыплейметвлад
еетконюшнейивсюработутамвыполняетсамвключаякузнечноеделовиламиперегружаясе
ноилинавозмойприятельтожепредпочитаетдействоватьводиночкувидплейметавнушаету
жаснонасамомделеондушкаилелеетмечтустатькогданибудьсвященникомегострашнопеч
алитчтотанфердавностradaетотсущественногопереизбыткаразногородапоповирелигийп
риветгарретбросилонтонкостьобращенияувыневходитвчислоегодостоинствзатоупарнят
онкийслухиострыеглазаачтокасаетсягарретатоэтовашпокорныйслугашестьфутовиещего
рсткадюймовдержупаричтостольприятноголикомитакрасполагающегоксебебывшегомо
рскогопехотинцавамнигденевстретитьгарретподлинныйсуперменспособныйпитьитанце
ватьвсюночьноухитряющийсясохранитькоординациюисилыдлятогочтобыдоковылятьд
одвериивпуститьвдомдругаиподобныеподвигионсовершаетнесмотрянаточтовремяедвае
дваперевалилозаполденьгаежетвоепастырскоенаставлениеприятельспросилямненескол
ькоразужеприходилосьвыслушиватьегонравоученияkогдаядолгоплелсякдвериилинемог
придуматьубедительнойпричинывсилукоторойпропустилегозануднуюпроповедьвкакой
нибудьзабытойбогомцерквушкевответплейметосчастливилменяиздевательскойухмылк
ойеготалантпоэтойчастизначительнопревышаетмоиспособностиямогувсеголишьвскиды
ватьоднубровьвтовремякаконумееткривитьверхнююгубутакчтоонаначинаетизвиваться
идрожатьсловноживотвосточнойтанцовщицыяберегусвоилучшиепроповедидлялюдейче
йнравоставляетхотябыкрошечнуюнадеждунаспасениеихдушилинамекнаподобнуюнаде
ждувмаленькойкомнатеудверейпопкадуракверещалтаксловновознамерилсяснестидикоб
разьеяйцоаволнавеселькявочереднойразотравилаатмосферумоегодомавсетемныепланет
ывидимоприступиликбоевомупостроениюводнулинииюплейметнанесупреждающийудар
лишивменявозможностивыступитьхотяиснесколькопотертойотчастогоупотреблениямно
всеединоблестящейисмертельнойпосвоеймощиотповедьюпознакомьсясмоимдругомгар
ретегозовуткипроспроузсказалонгигантkипроспроузпревышалростомпятьфутовнеменее
чемнатолщинуволосаявлялсяобладателемвзлохмаченнойсветлойшевелюрыбезумноговз
глядаипосамомускромномусчетумиллиономморщиннарожекрометогоонвидимострадал
тяжкимнервнымрасстройствомонпочесывалсяонвертелсяегоголовканатощейшейкебезо
становочновращаласьвразныестороныонизобретаетвсякиештукипродолжалплейметапо
слетогочтопроизошлосегодняутромяобещалемутвоюпомощьмояблагодарностьплеймет
простобезмернаиярадчтотызаскочилкомнепосколькуяобещалгородскимвластямтвоюпо
мощьвоформлениипраздниканепорочногожульничествакоторыйдолженскоросостоятьс
явкварталемечтанийплейметсердитонасупилсяочевиднопотомучтосортодоксальнымири
туаламиитерминологиейунегопостоянновозникалипроблемыяжевскинулбровьвсвоейвт
оросортнойиздевкеиздевканесработалапришлосьпереключитьсянаболеепонятныеемуоб
оротыречиитактыемуобещалзаменявидимодляэтогоисуществуютдрузьянетаклидаладно
тебевозможнояиперестаралсяегословаитонкоторымонибылипроизнесенырезкоконтраст
ировалидругсдругомпростизначиттыпросишьпрощениянуэтоконечновсеменяетвтакомс

лучаевсевпорядкетынезлоупотребляешьмоейдружбойкакеюзлоупотребляютморлидотс
плоскомордыйтарпиликпримеруторнадаличноянизачтонесталбызлоупотреблятьдружбо
йипринимательрешениязасвоихкорешейкрошечныйзаморыштемвременемпыталсявынырн
утьиззаспиныплейметанепереставаяприэтомлопотатьнеужелиэтодействительноонплейп
оинтересовалсяяничегоособенногоаяствоихсловпонялчтовнемпоменьшеймередесятьфу
товростаяэтоядетканосейчасянаотдыхекипроспроузизъяснялсявизгливымсопранослегка
приэтомгундосяегоголосвызывалуменячудовищноераздражениемнеоченьхотелосьпост
авитьегонаголовуивежливопредложитьговоритьпокарентийскитаккакподобаетмужчине
обогивзглянувнанегоближеясообразилчтопроузвовсенетакстаркакмнепоказалосьвначал
етеперьяпонялкакемуудалосьвыжитьвкантардеонпростослишкоммолодчтобыучаствова
тьввойнеплейметумоляющевыпучилглазаиумильнымтономпроизнесунегоумсветлыйка
ксолнцегарретнонасчетобщенияоннешибкогораздмальчишканаконецухитрилсявыбрать
сяиззанеобъятнойспиныплейметаонявнопринадлежалккатегориитехдетейкоторыхвсере
гулярнопоколачивализаточтоонинеспособныукраситьсвоюгениальностьумениемдержат
ьротназапорепроузчувствовалсебяобязаннымсообщитьэтимздоровеннымивздорнымтуг
одумамчтоониошибаютсявчемониошибалисьиошибалисьливообщенеимелоникакогозн
аченияиэтозаставляеттебябесконечнострадатьзаметилятыменяпонимаешьвздохнулплей
метпонимаюноедвалисочувствуюсказалясграбаставмальчишкузасекундудотогокактоту
спелсунутьсвоюморщинистуюрожицувмаленькуюкомнатуудверейянемогусочувствоват
ьвсемтемктонеспособенустановитьсвязимеждупричинойиследствиемяизменилзахватиз
аломилправуюрукуюногогениязаспинунасейразонсумелуловитьпричинноследственную
связьмеждубольюинеобходимостьювестисебясмирнопопкадуракрешилчтонасталидеаль
ныймоментприступитькпроповедиязнаюдевицукотораяобитаетвхижинеитакдалеелицоп
лейметовадружказалилоськраскойпочемубынамнеперебратьсявмойкабинетспросилямо
йкабинетпосутистеннойшкафспретензиейнавеличиеплейметсвоеймассойблокировалдве
рьимнепришлосьвытягиватьмальчишкучерезкрошечнующельмеждумоимприятелемико
сякомможнобылобысообразитьипропуститьпарняпервымпоходуделаязаметилчтомойпа
ртнернепроявляеткпроисходящемуникакогоинтересаеголишьслегказабавлялимоистрад
анияобычнаяисториякаждыйстремитсяиспользоватьлюбимогосынамамочкигарретвсвои
хнизменныхцеляхсюдакипбросилплейметкоторыйобычноявляетсобойобразчиктерпени
яноэтотмальчонкавидимоужедовелегодоручкионвозложилсвоюлапищунаплечоребенка
ислегкасдавилпальцыэтобылисключительноразумныйшагпосколькуплейметмогтакстис
нутькусокгранитачтототпревращалсявщебеньощутивсебясновасвободнымяуселсязасто
лмневсегдаказалосьчтонасвоемрабочемместеявыгляжугораздовнушительнееплейметус
адилкипросапроузанастулдляклиентовасамвсталсзадинеснимаялапысегоплечавозможн
оэтагорамышцопасалась чтоеслинедомерканеудерживатьтооннепременносбежитновдан
ныймоментэтонамнегрозилопосколькувсевниманиемальчишкибылообращенонаэлеоно
руэлеонорацентральнаяфигуракартиныукрашающейстенумоегокабинетанаполотнеизоб
раженасмертельноиспуганнаяженщинабегущаяпрочьотмрачногоособнякаводномизверх
нихоконкоторогопылаетлампаокружающаястроениетьмаполнитсяскрытойугрозойвсяка
ртинапронизанакакойтомрачноймагиейвсвоевремязлогоколдовствавнейбылоещебольш

еэтобылодотогокакясумелсхватитьубийцуэлеоноры

Знайдений ключ: чугунныенебеса

Висновки:

У ході виконання даної лабораторної роботи, ми навчились шифрувати і розшифровувати шифром Віженера і аналізувати довжину заздалегідь невідомого ключа на основі значень індексів відповідності. Було з’ясовано, що індекс відповідності більший за його середнє значення на проміжку, якщо довжина ключа підібрана вірно.