



Міністерство освіти і науки України  
НТУУ «Київський політехнічний інститут»  
Фізико-технічний інститут

**Лабораторні роботи**  
з предмету «Криптографія»  
«Криптоаналіз шифру Віженера»  
Варіант 4

**Виконали:**

Студенти III курсу ФТІ  
групи ФБ-84

Гайворон О. О.

Солдатов В. А.

**Перевірів:**

Чорний О. М.

Київ 2020

## 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 шифротекст (згідно свого номеру варіанта).

## Хід роботи:

Ознайомившись з теоретичними відомостями і методичними вказівками, та переглянувши деякий додатковий матеріал, було обрано мову програмування Java.

Для розробки було створено три модулі, що складаються з чотирьох класів:

**Main** – клас, що запускається на виконання користувачем.

**Viginer** – клас шифрування і дешифрування та визначення параметрів тексту.

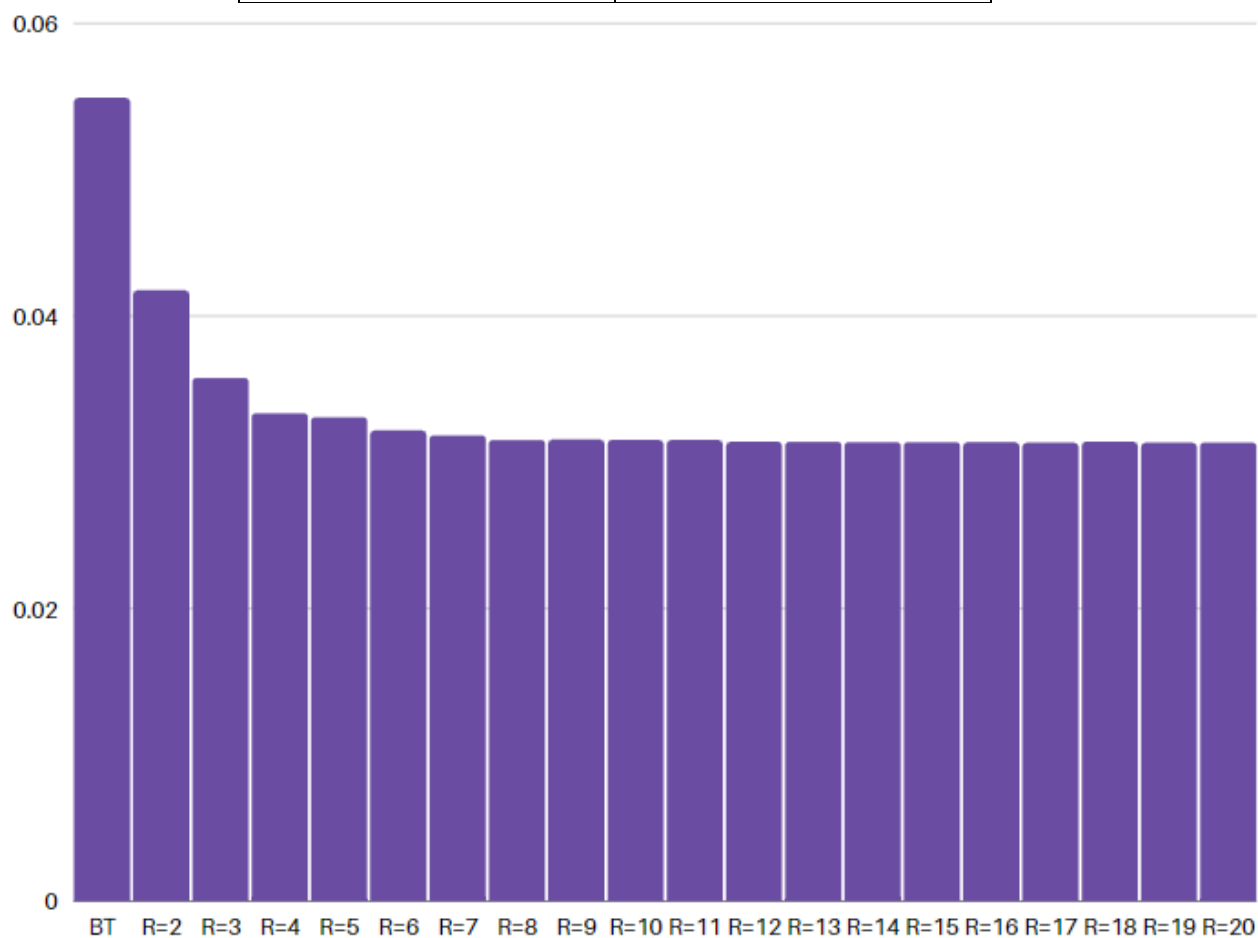
**Analyzer** – клас інструментів для атаки на шифр Віженера.

Розбивши текст на блоки, визначили, що найбільш ймовірно довжина ключа дорівнює 13 символів. Створивши частотні словники, отримаємо початковий ключ з визначення найчастішої літери в кожній підгрупі розбиття. Аналізуючи отриманий текст знайшли, що деякі літери визначені некоректно. Замінюємо на наступні зі списків літер для заміни кожної підгрупи, поки не отримаємо ключ «гromьковедьма». З використанням цього ключа відбувається коректне дешифрування тексту.

### Значення індексів відповідності для вказаних значень $r(2-20)$

Відкритий текст	0.054873742
R = 2	0.04171207
R = 3	0.03570101
R = 4	0.033288836
R = 5	0.03301581
R = 6	0.032140657
R = 7	0.031773888
R = 8	0.031458188
R = 9	0.03151242
R = 10	0.031468667
R = 11	0.03148419
R = 12	0.031343214
R = 13	0.031336643
R = 14	0.031312805
R = 15	0.03130948
R = 16	0.03130981

R =17	0.03130057
R =18	0.031355068
R =19	0.03129645
R =20	0.031287696



### Індекси відповідності для різної кількості розбиття блоків

R = 2	0.032604642
R =3	0.03576993
R =4	0.03265088
R =5	0.03253544
R =6	0.032560475
R =7	0.03271785
R =8	0.03269169
R =9	0.03514375
R =10	0.032517567
R =11	0.032713737
R =12	0.0322635473
R =13	0.054068573
R =14	0.032636646
R =15	0.032435592
R =16	0.032674715
R =17	0.032683123
R =18	0.03256889

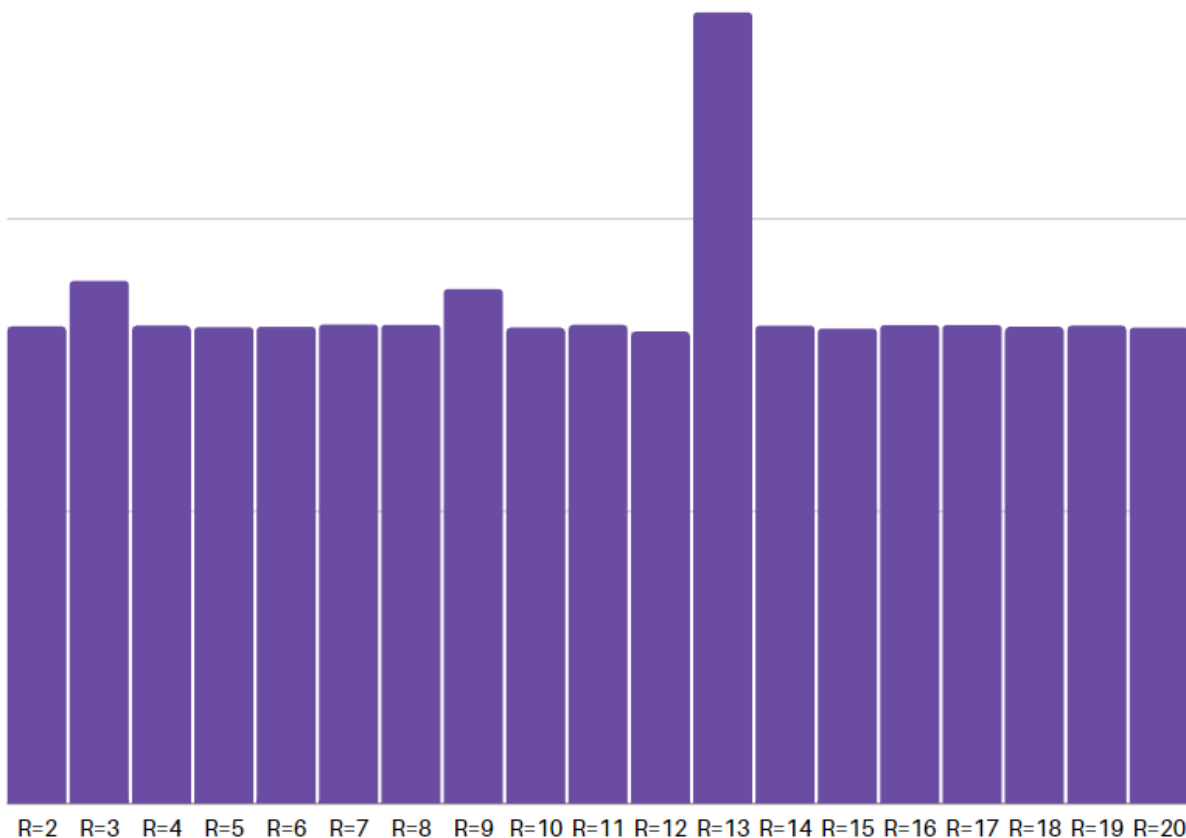
R =19	0.03266485
R =20	0.032507279

0.06

0.04

0.02

0



З найбільшою ймовірністю довжина ключа складає 13 символів.

Ключ: grymovedьma

ШТ	ВТ
фвоъзтыупдыдксыогыъжжйюичшчфньодтмта ангшинпафктмстлзуешчкфьцтлзуешчоезд фкгдурлкъвтитюрргъафешрщехоипиармъышнд зинюшбцжктгацдщргтйойцэкхабходйцщмце ыоъвъюзаънщцкойоспуяофэмоофммъвуряылтым уфлъргжцлзтвмшфнъвгпюмъшавеибтншръмжъ ритжярфрръжжгкхйащомэоятчйлхчжъвсфцюах коездэтуяуъэшчучйлснлрюбгцоепхъщпиашъэ оуддцшэохфуоъчъучтасввйхюштсuebчоубшъ зэшчтнгифыущгисрхтаэтгаъфимрзййфешюю ъутчукзкрнвтйрыхябиййскххэццупзмжбюриэ ыздмархдыренртммпырцьоапхялскызцубднс бъгтгоубхжоокмшчащайкйфпэоозугишсрройми жощъмкхбжпдцоефъщйыцдэмбэялчэъгоьтукйз хнгяюймхдксбчиегжмрйучепъэкеюхигтяспка ъвъухбпйокбпджодсыкыинювтмущомаяъчиййсуп кэомсйчыоътузъуадаъдачыэоумъкохрзэкмын нлпюкшйуатежкхкушръдльнбъьцзвщфетэр фймсмизыгъшхошъъчифмрюйъфзтмбшчиыъоафо пеебчомыъдыоцднщумсхэйсэхожксдлзгыцбэк аупмбюриыцзпыбмрнихушэчццекмжмняхъын кгткцбюллтъыаъусефсфвгыщймуфуыжммхауо	старминскаяшколачародеевпифийитравницф акультеттеоретическойипрактическоймаги икафедрамаговпрактиковчастьперваясоциа льныйукладбытинравывампирьейобщинывика чтовычтотоимеетепротиввампиовраспринк орпорациямифкурсоваяработаадепткивосъм огокурсавольхиреднойнаучныйруководител ьмагистрпервойстепениархимагксанперлов девятьсотдевяностодевятыйгодпобелорско мулетосчислениюгородстарминвведениехор ошийсегоднявыдалсяденектеплыйбезветрен ныйвтораядекадасеноставамесяцанеспешно сочиласьсквозьклепсидрусолнечноголетаи голосазябликовдоносившиесяизпридорожны хкустовзвенеливушахяхаласквозьихгнезд овыеугодыакаквдольпограничнойполосыпол осойбыладорогазброшенныйпроклевываючи йсяпыльнойтравойкривойбольшакзябликипо переменновозмущалисьвторжениемчеловека набелойлошадивихчастныевладениязалихва тскиетрелисменялисьхриплымчириканьемпт ахисуетливоперепархивалиповеточкамтрев

йроннхооуурхщйарзчсълкгщгэмэштштзусррлг  
ыйояэъдъеишшбтэсюэздзмсябьюийтъкнхотмох  
ыщяфвхтешохлшиешртехжъуъшрмжкяюзжчъе  
шгъацаткубеуъшгцлешкокжлтъвсфклвкрзхспюы  
ияуюжпчузмнмлбэслптпкнзъяклпэъекекззм  
сятясяхумеоиссшъяцлээрзумфдиаффэкннкжк  
хрцъъхжпфвъбснгтъъчачнчфмнимсшэзнкнубф  
ьюодаоющюэидъеиияуъаоснелъшиугызлшъвъ  
оыоомхъэкщцаиъипаозмхогрийщыпбъэншнп  
нийоисичошаошбдмгммифшлтъвоетдасяфмеуййб  
дрйуснррнгнпыккрйсзгъугопумужънсусъшчы  
удхддрапхчъмъопуждюфпцэкшшроскыоъшэмн  
жатежжятюзупйзаритзъябцишмычбъкжбчинюэз  
нкъкфппюоерамъфгапжмргчъгыгъдесйтъвфею  
мкчбнеиъоамфооыгврцпыщлжолоыатумзмсяя  
ьяяшппкнбэллтъгъуоукйъуфвъюгъкудукядс  
сысдчофурлзтсзъгъщюзйрбюенющшмщбртнид  
опъсийфзццжъенрхсичъзйачорраъаъцлйийи  
пцвъйцъпмймгушрмншызтажфмлтъчабшвсмн  
ыуфъочыкжуубъеззухжжшкмдэфвгпияизпфжшх  
оъаршдмзтэхъпкпотшыизкшрчтмъевфъчбчоба  
пъорцзцющъдкпдъеоотъюпрэнокюоуюябпък  
тчояяхмшмеыооужкчърюрэеъйнеумфпсъегцо  
енмйстуюяээрзцмннюмаягыцпежбъееюеац  
овртиоофъуънбуфрмюъпуюяюощноцофснауъм  
ыбчфдшазжюкчбпнубъетыуюйзкохыддуршъ  
ишгъзймйърсурвачаткцпюмсшхмийакдпдъеура  
ялшчжнузъмгвцсдтсзтъчожшухюбгуумсрер  
щфйбупбзмьябспурэкбуфйзмпсфгоыцфблдэтн  
шэъкшщйэмборгчызаыархтйзрсьодекызнхлъа  
ешъмъыогоуцътнлжоуыобюъмюжиточыэжшемл  
цгпфсжпхрсжювъухълекшпклймксъйхгмуубрь  
ыозюхъгъунбсчхтляънлшякънмирццыгъмъцжкр  
кшсхаоюгмырфтоъяфрщяъужртфмдлэъхзшожу  
ннммсфуччйоефэмливъшмнлюбмскхсхаучйуъп  
узкъакюръюшцуфтзизстошгйавпыоъниящтъы  
ржзъкъсуъъиыгнфъстфпсъылцфбрбщялыцъйц  
оъпчыырляърийшвцаймсхаушачоцмйюеухяъз  
ъоуцръюрлтолвкюиежснрлчшыфпкыйфквэур  
оцоаъцкйтсбошйпбжеыйъепхяююощбчтмпоеыц  
миъцмздмфахюрймутнцбчърюяъйлзкрдышекэ  
оцйцдхэтоосхрюгчухзднныиуъэлэшвсмкюо  
точгмуттйбтъугпфжтхпейосллвошйбупбсбю  
дпаыспросдцоеаъшывшвуейкхгымллонкцлъ  
екацюахкпушчъкргшмгчосхтуиижэъгъббифъ  
ниххшлкъабтчзмсяъоыкпакчскхзиыушгцоннс  
йфкгшхоцыъмуняяшлтъюйтъеуцкчънюеюймъйт  
мжчоавъгооъдрдлюяшяюсмъбстяейлиъушнс  
ооцкйъспгафжынпеокщъэццвкаткубюаооцфпы  
бъмебвсбафээрэйтммснрнщгйцсуоълнлппзжш  
уыкиъченюхмъхбжэдывъщрбыйъяфзтюмлгтъпл  
пгзцфбнрсымнгйопшщжмжлтъэжпхвохжънвфуо  
екнйаоъюавъдахумнпдтикэкрьщътъшхъембщ  
зутжюдмгъбурхфжкбунпбщнцоюмъшахсянчиор  
тщйэпэймзцоыхшсещочтгъзокюгъзхцшзуммбл  
вучъшуткибънцыъэчсювъодъафицъгхцубззмз  
гюяоафшзтйзфисэъсяхуптгкыуфвцоыгпврйоъ  
тепхмжтпзцумсксбщъэчъсуиъчмрхаъфтчокък  
дцбсамэвцлгцпывобънцуъпдммзлыъцйвшвсм  
дцуухръшзянеедовиауоезйфдздоаеибкюшюну  
ждшувяюкзъяфнпъэкеюхиккщюяйсннюиешъз  
родбмсэуюзкшрздоъдсаъпйуъроръчоераъмху  
пытеъадюамавкгклкпормшмэщюръйиюангффе  
аюзтгимцтшмтпфзйъоарбоъмбоучпдоиорнпл

ожалиствуразноцветнаякаймавокругчерных  
подсыхающихлужвзрываласьсотнямиистомле  
нныхжароймотыльковраскручиваласьввысьв  
ихремтрепещущихкрыльевповодъязавернуты  
епетлейсвисалиспереднейлукияпокачивала  
съвседлекамешокскрупойпридерживаялево  
йрукойлежавшеенаколеняхписьмоипытаясьр  
азобратитьпрыгающиепередглазамируньромаш  
капользоваласьмоимрасслабленнымсостоян  
иемвсезамедляязамедляяшагнадеясьчтояу  
влеченнаячтениемнезамечуеековарногоман  
евраидамейостановитьсяспокойнопощипат  
ьтравкутычегозтоголубушкаанушевеликопы  
тамиплутоватаякобылкаразочарованновсхр  
апнуладавайдавайхалтурщицаястроиласьп  
оудобнейесливообщеможноустроитьсяяпоудо  
бнейнатомпыточномпредметеоимявлялосьд  
ляменяжесткоеказенноеоседлонатретийдень  
путиромашинагриватоненькимиколечкамик  
пускаласьдопереднейлукизабиваясьмеждус  
траницамипухлогописьямакотороеядолжнабы  
лавручитьповелителюдогевыикотороеужеми  
нутпятькаксамовольновскрылаприпомощима  
гиинетронувувесистойпечатаинаверевочкен  
ааломвоскеотчетливопереступалоттискперс  
тиятринадцатьрунипереплетающийсясдрако  
номединогвцвцентретутмоизанятиялитерат  
уройдипломатиейигенеалогиейгрубопрерва  
лиооченьгрубаяедвауспелаподхватитьлисток  
ипоползшиевразныестороньромашканеиспра  
вимаясаботажницазадумчивожевалауздубря  
цяжелезомвтовремякакнезнакомыйивесьма  
подозрительныйтипобросейнаружностидем  
онстративнопотрясалпередлошадиноймордо  
йсамодельнымарбалетомсгрознойстрелоймн  
огоразовогоиспользованиятакчтонепонятн  
обылокогоонсобираетсяграбитьменяилиром  
ашкуяприподняласьнастременахсинтересом  
рассматриваязаржавленныйнаконечникянед  
умаючтоэтосамоеудачноеместодляторговли  
антиквариатомдоверительнособщилаянезн  
акомцуответстарминеуважбегосукамиотор  
валивернееотрубивизнаелитамоченьнелю  
бятразбойниковромашкаобнюхалаарбалетпр  
езрительнофыркнулаинапрочьигнорируягра  
бителяпотянуласькаппетитнойзеленималин  
никаизвысокойгушикотороготолькочтовозн  
иклоэточудовлаптяхпреступныйэлементзам  
етносмутилсянаконечникзатрепеталкакщен  
ячийхвостикувывдораскаянияипокаяниябыло  
ещедалекозаблудшаяовцаупорствовалавогр  
ехесребролюбияануткаживослезайсконядев  
каязыкатаякошелекилизньдапошустрейсл  
ышишьязобразилаусиленнуюработумыслила  
дноубедилкошелекпахнулоозономлицограби  
теляпередернулосьзрачкирасширилисьглаз  
аостекленелионмедленноопустиварбалето  
твязалибеспрекословноподалмнетошиймешо  
кболтавшийссяупоясаотмешкаразилокошками  
икуревомослабивверевкустыгивавшуюгорло  
винуяпропустиласквозьпальцынесколькоме  
лкихмонетмаловатодорогоймоймаловатосле  
нцойработаетшьбезогонькавпрочемтакужибы  
тьвозьмувкачестваавансаосчастливилаягр

кпкчйзлшелюлтпъхфтащожшэямььлсйфъкляюс  
язэткидчавзуьасэвхчащемнаъдружфкпомэо  
уыозркипюангфноокжуемыофвоьгуябсйилниа  
оуйботужьюьпгффечурчфчоавюашачнийездынс  
вцугтъьдесйтъгстхпжитвсйачерэъшыныхрыыо  
зэнчзпжрпмгтмсхлээншщгццкчбсььсэьцнщфс  
виыкщюькудебумсхсхъэптрсджмкхюиешсрхийя  
ьадшасжжамхязэялчрфяэнжкджюиешюэкшвмд  
жчирыфатэрмжкчиорюьзкжмкубьемвцэюкшрф  
дймлбсцшоиуачфпэццяцэчъйекьюоитьолпгъб  
фтаэчиворачуешрбщяпхфрфьнксьширхъщйнь  
сурычофмцяньофнпкюоерющцуркйжльоъхъьы  
яхйзмзяжьюоишупктрърпыущгпоууибъжгэцсй  
чьзлийжмтхыэгъьдепкщезюяюьшкхйлсйрюсь  
жтяфемныоомхъэкыпузкоунаъшишъокхосажрр  
ънчомусбвиссьшипэвхднюрсхмятвкхдинапш  
хмюктрьскшугаюмефаххчльотгяюгвккитгмми  
вдчдсодхйилодгеситндзяндемишъжпевхтасе  
еяцагуцфхдюищртскъшвзтзихгяюъмцнхбн  
якэокибупбузъхсэуямттщнжъщеххюахцдею  
ъееюиикхпеокшавяузийщажмоулюхжянфцктй  
крнсьюмнчьскфбщофшафрыррцудюарэццймывз  
тнхихрасжпчячткшпурсъяъщчтзфдгсйчйштп  
ужбреуъьриймьнбскъбэхъфмььзццкллсбуначо  
гепжснгфтоаькастбхксъымнелжеодхсгъьрах  
кпанжмпнрыщъьыукибхпсишъжжырскнцищцюг  
итвжяйспсторишпэртэсзфяюъмъжепвфвгкя  
зпыбптйэпиъазгфоучфъчифэоыгуптияшархт  
сжипрхэкшмсцуообцфкпшюансийщаъойулзфлфп  
уэжтпэзйаьоебуюфцрффкциргщъмжопкчлмлс  
хъяиксрртюясхюшъмъзццбэвсфъхйъшкъдбюс  
вауретъкцукэодэъэнькпуммкхшесмфьлнцбъ  
ривцгаъшрорьпилбцчччътелюфтсщцщнэцшние  
ныфвюъьюосчммяехбнципаяфесамрхэхмтахеъ  
дфхгъьтаънзкюйисбичымяпфпесбырлыцгикнме  
оьлтсуюмитдвшикпеелбйжжвзжчэоншулюкрэ  
шзйъмстяцыхйхздачанюрплэтэзязэьохыщйуы  
вфтюрсршэъэнжхзспдядушорязэпэфташехрмегл  
ьгрджмузабфяшрмербщнхюшьонцхрвасйсссяк  
хуптябэтиэйцычонахгмтшыьхэштрофъудийущ  
иеусефкхтуюццйуэрйюбшнюеъъмььдйдззсюя  
люкфпнодырлэцбьоцфкпшщозаушжизккчлфргп  
яйикюиежрсаохпмлоивмибэьсбщццтхжжъьюео  
мяюзшшвлтбюосбьначыркхзфуъхяючбарлмосл  
лфьпамидерлфррюеьйвцзчдждфесбщщцуткемф  
схлуюлпэзючхфекрьэгчоонэбцоъхашальрццм  
ъвиагфдпшрзяецоохюэлпткптоърсуьцйпсжку  
мъгоптзэкмфмдоъаыущиеугкфбуклшяъмпымнх  
ьшайхтъюпрврийвфтефьчгчумеолчюьгощыоьзх  
дныифэьхктонайнчифььюлпаюцщкчмгъюмъщцв  
ряюфдиэпсжечржтаъклчъэгчрфуфкхпсвьчфпэ  
рчийищеишхсжпчвзъбщтухжфлшшрклбчерюуриш  
ямхдлгъчнрфмквъйтясвгтшъжждззтгреорыщц  
язэрриэфодыоцяяхсдймпсфьхяпжюзузътргмц  
япюззаяшнгбамэхннсййлутьашасжжцсуьзсшяьй  
эжпыпаннфгтррщоухбгбпбэаоопъдцъикъшрупр  
аййбуошзкрнсыцдчлийущтмшиуюрмнжърюспкти  
ыуыыьццкххяюеюшщокшрсчищеихымкъоднцшща  
ссзсдбоучтоскхюфьэтюлннюргцухюьопнъча  
сьнибщзукאותйкнякрасжжырффкруплрмнжъщкф  
брнцозмешафблймкэкзокнеывтмсэвиагомйшро  
рбььжююмвоопусъэмаоукшяфефьхсвтъуяпюи  
ещэясъвьщцяъщкрщюовргрышрррсбоапяцьще

абителяшвыряемуподногипустоймешокипре  
дупредилаячерезпаруднейэтойжедорогойна  
задпоедутакужбудьдобрпостарайсяменянер  
азочароватьмужикнеотрываяотменязагипно  
тизированныговзглядамедленнонагнулсяпо  
днялмешокизастылстолбстолбомневсилахше  
вельнутьсязбезмоеговедомакактолькогорег  
рабительскрылсяизвидуядеактивировалаза  
клинаниеипозволиларомашкеперейтисгалопа  
аналюбимуюектрусцуписьмозажатооевовремя  
подсчетаденегуменямеждуколеняминемного  
помялосьиутратилотоварныйвидвпрочемрас  
судилаяглавнооеоеоформлениеасодержаниео  
ноеежекомпенсировалонедостаткирепейного  
листаиспользованноговукромномместеагав  
отнаконечиобомнепарастроказадифирамбами  
загадочномуаррактурупропустишьинезаме  
тишьзавремяобученияввысшейшколечародее  
впифийитравницадепткавольхапроявиласеб  
язнаюченьплохонеусидчиванетерпеливасв  
оевольназнакомаяпеснялюбитзлыешуткиине  
однократнопереноситихсвоспитанниковнав  
оспитателейэтоонпроведрочтолидабылоодн  
оведеркодовольнообъемистоестоялосебена  
балкенаддверьюмоейкомнатыздакийсамодель  
ныйкапканнасоседейпошкольномуобщедити  
юдабынеповаднобылобезспросуодалживатьу  
меняконспектыикастрюлиснавареннымнанед  
елюборщомможетучительтакбынеразозлился  
еслибыведровсетакиопрокинулосьанеупало  
емунаголовустоймявместесводойотличаетс  
яредкимиспособностямикпрактическойитео  
ретическоймагииисильноразвитойинтуицией  
быстроадаптируетсякнестандартнойситуац  
иихаможетяещенебезнадежанеприличнаяка  
каятограницаудогевыуэльфоввысокиетравы  
угномовскалыувадлаковгрудывыброшеннойн  
аповерхностьземлиудриаддубыподметающие  
облакаудруидовкаменныекругиулюдейоблуп  
ленныестеныканалысзатхлойводойразделен  
ныепаройтройкойподъемныхмостовдалысье  
сстражникипринихбдительнодремлющиеупирая  
сьнажваеалебардыздесьосиныиздевател  
ьствокакоетоособенноееслиучестьчтожители  
идогевывампирыххорошиетакиеосинысеребри  
стыетрепещущиезаосинамищекочетнебоостр  
оверхийеловыйковерсредикоторогокоегдеп  
роглядываютьзатравленныебerezкиисосенки  
самажедогевалежитвдолинекакплюшканадне  
расписнойпиалыеслисмотретьсхолмакрапи  
алывиденбелыйободокизосинввторойпотолще  
потемнееизелейавцентреширокоезеленоедн  
оскрапочкамисамадогевавкольцевозделанн  
ыхполейиоблакахтуманаподойдешвплотную  
кдеревьямнаставлялменяучительипошлешъм  
ысленныйсигналвглубьлесалюбойможешъдум  
атьочемугоднолишьбысформироватьмощнуют  
елепатическуюволнуакомумнеенаправитьна  
аобщейчастотектонибудьизстражейграницы  
услышистащмущеннокашлянулалучшебыемуэ  
тогонеслышатьнеобязательнонопродумыватьоче  
реднуюпакостьзнаюзнаютынанихсверхвсяко  
ймерыгоразданонасейразпостарайсявоздер  
жатьсяотныхочемэтояхдаоволневампирыо



