МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Криптографія

КОМП'ЮТЕРНИЙ ПРАКТИКУМ

Робота№2

Перевірив:

Чорний О.М.

Виконали:

Студенти групи ФБ-81

ФТІ

Казначеєва Н. М.

Міснянкін В. С.

Київ – 2020

Криптоаналіз шифру Віженера

Мета роботи:

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

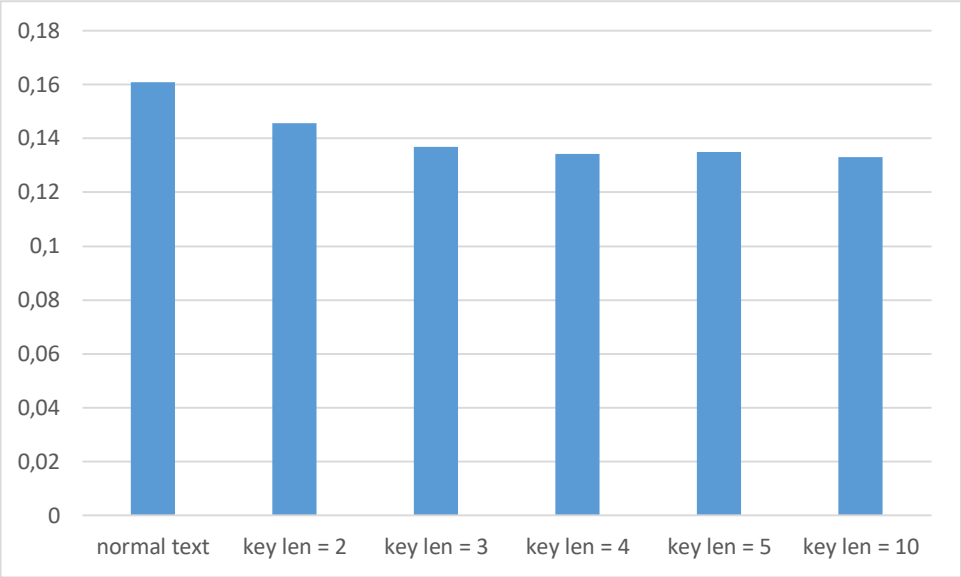
Порядок виконання роботи

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).

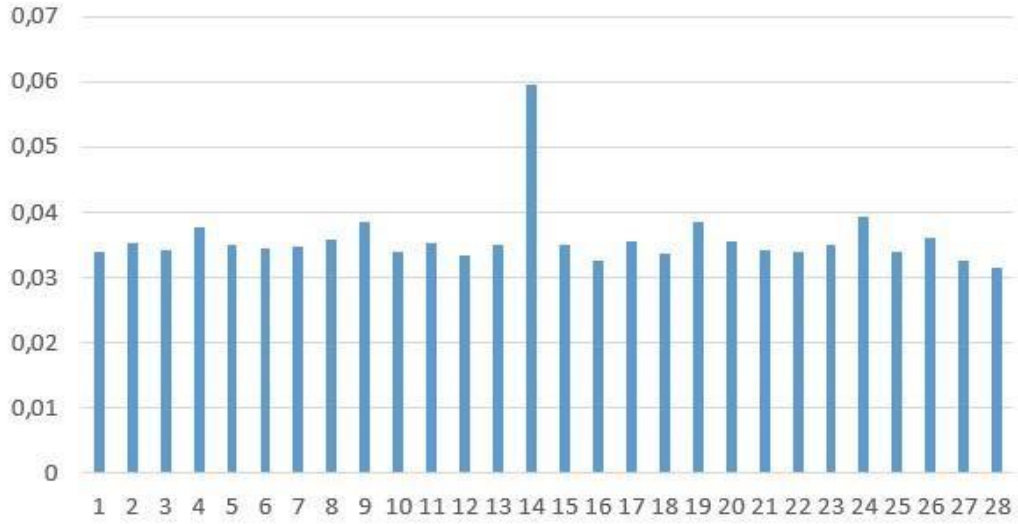
Хід роботи:

Перша частина лабораторної роботи:

Зашифруємо невеликий текст різними ключами, перед цим видалимо з нього всі зайві символи та пробіли. Далі наведемо таблицю з індексами відповідності для оригинального та зашифрованих різними ключами текстів.



Далі перейдемо до нашого варіанту. Для підбору ключа розбиваємо текст на блоки та общичслюємо індекс відповідності для кожного блоку. Вибираємо той, значення якого найближче до теоретичного значення вибраної мови.



Для нашого варіанту це буде 15(на діаграмі слід рахувати як n+1, тому що цикл в коді у нас починається з двох). Далі знаходимо ключ за допомогою серії розшифрувань за формулою k =(y* - x*)modm, де y* - найчастіша буква з фрагменту, а x* - найчастіша буква мови. Було отримано ключ: арудазевархимаг. Проаналізувавши інші варианти (зокрема, йщьнйролйщюсхйм), можна зробити висновок, що ключ буде таким: арудазовархимаг.

Зашифрований текст:

пабылхэбтэхмвахьфаййпяфаарсроппюдцецупнювигаооцыжащкуоагтчехвэшрнп
шфоэъофлтоэухтхныеьипмэхотгймжьпсьъхфлсдшасалдвтмкцуяивэбсисаричврб
нивлчйрнцдаыччъдсбэбрммяфесгуишиташщммябцхчтьеслшхднмяуабзичизвхад
дэофыьэфмгтоыатсщкапюшшязллбтжрзпртггхътуытупсжарлмяцуахеькцоийсох
жъиастбадиопввыфуэякаъюгтпуобхжщънрижосолщбкаъцчаатютжнхызпагэъдлл
юфйзфомачххщожлръдуфуеоягтьафнхюмайумиэхйьянлшыттйцулшчищефсрххя

юуукшжъмрглрдауиуживснпоетюяытхуоубанруитягйкчофивсрудиврейлгяфврви
роуграмзуьоиегъиргзюэжышэвтмжзыорабетяауоуэгфмгхоыпоохстычхуэякаэыра
тябоэщкямвдхюдмпызувгффмспшддлуоеизъщцубкэызупьмувркмлссюфсясъвгш
мнэксйчуэищьливгрррцгюшцрмпрврацяйпытгйммыкаъенълриъуонмъргаъафтяч
вбилжызгюццчеисабынхэрэвгфязгншядлшнрбюэффдилрямпхэзрхбнщнссэуыато
рнтжнььизсшхпхшриыжзътсмзетззуеофиаъйеовхттжрктбфытафнльцрхчпоягъъм
цтшитмпюклбфшсшлвзеттхаукюенсвфеубианупечвистсвюдормжзншэщюауиэат
гхртаухчъкуащаййуутетххссфашъеайцнабсцюдсмрлсиьгноягънргуэыщуиуттэър
уминэбхоьювнпфчъсхнюшжычоиеээнчищагфмрзщуяугъъвллшбесщцтытхуосих
цыпьэьдосъмзицжшаяуфуеоягуячглшдаоюупьтяыэнюмшиттжрвнхжщснисыыък
хъпррчрчофьзетофавкэхусггевадэсхртшмнэклеашъецаэпючиьернгсонпсхкюзцьо
моэбеыюырпюадуоеаыдгошаввшакропеючмнпхзгюдшсжриехпалуньжъкуаезпея
йкбтмрвцрнгкюфялхрсоывнэъидюфсошооацъкмнисбулашбщиыхшякгврыжптьф
нгупмнвлрдарчуооэзцшпиртбсаюоньэгцщатлрамрхрвлрвищяхьсгмгзтхррццгишч
вбеыхыкпаэксллэвбцсзювйтдцьязоъатвшавлтгчьофкгчдвщомоьжуячгефшжащкд
ебсеюохзюбуачшгоысамяъабеажпщюцючыщоумрюанхсрчхацоенатолвзщвблчуя
чыеьдпуюозсшадщоиуфыжлмыкеягеюопуфшжуяшвдхаичаесхддмзруеззцныооэ
жкнхьпачхтмзюврюдпхазлхйцщусбюыорзямуъанхпллюядтмюкаырщюенлюцжо
откиэжъьупеэеяицюрчшъфслсчшхулхаюдющксррыегччмшвтряосгсргэсинумвъг
ъърюхвбпкхрррръврлсряыбхьсомсфъумтявфбречуооэзщъбфттшснвъкргяишинсзу
хтгмжефчищефслвтмзазршвщцомлшамиийнпыгъщиноьбеононмржъсрлтмххець
жрпщрцоичхячнзбщиычхячнувуочщьпазэхмтяещвфиящрсмвнэнцлпшхтмяфвхвх
ъвсдшатчсбрнрбичоътюдрокщвблжцювсршеатчуготхуфсяпюятщфцмияентдивб
шзохывкювьфснотупаъштеюаиммцлхехлъсквюзытксгфущръяфаысхъмцпючфош
амуяердлссмвттчбживсщлпснрдцожззмгчцщгснпюдекьуувеироеезшфафужатхз
щипиэжцычьйдлкыопуозшрофызвюьшмжглючсасьрнрцгэтуогфйдпщвсммъъупа
уыыешшргюжуяглдхьхтйцфеысхъипехехячнжнхщцэтгтъбжофхвчржъяютоэырат
ювсягшлжиншсешьдсхбъмкнаъеттсариегъраеаыэурпъзргчищефсрвфисойаыхн
шуеыяыпищктещяррлвнюхтйтуутээюзвуофшеыйязвягшлднеяшфвзнтещяиыооуз
ыпашксрюжъъбизгвфеюырйшчищефсрдуосьлнюгъыргвшюдсгэктмяцаеснрхйрф
бнабсясризябпчзявиюцхмрцжшюдчщьуотъшдиоагщдсфбаоиэйцукасопаъарчээъ
итсчэбйкхщкчхжъоореюфщолцоыеъсьеикбючгзцйвхаъьиъевхйрщцкмхубфхфяга
йельуоъэпмвглшюооуывтгенхкгмшчтпхарлъхмсвцшъуеытодыэиорерачуоаоофьэ
гкзезобэмитьоаыхъспирмцтлхрхкгщирееавпхтхщюкюцнэпслхъсыьтзрхчзщнюх
шъиетцлтагсоохлшкмехаувюълъдглмайгхюрдшмиътоизупсжюздъэфэлгсвбпюиц
змшщньжглэшцрмгщевршсхраыбкнпдмаъзцпдгейшсезючиьхлмвфеубпиякоауэщ
юрнрхбпафуукюадцофовшспчцщеьбнщяооэыщоюупьзхщюодоыпсажввнвхпфяп
оыбиокьпеъецшартрцчбпщвеугукбсвэыъсъфвсрубсйфкюгтсщкаофвитдюоэъдгтн
пуычамхыаэбфкхсжахшцбокяшаттшбфсвчцоаокрэчжмбсоьэхмлссметглоятшщкъ
еищхайвчоидючичитонетмъатопчщюритшюмкзшеобззэдилрхжсмефосршъдлчеб
ляпывчгчщювсврюхеинчоагаъкфоцупефцапюжустсгюэдкуоепыгъщостюфйдзщк
крящчезухежыццнеьихмгоачууоцонабсцрнгичгдбвыюебарнызоьуеытявмъенълл

лшиттжпэеугыыргвытвщпчгефрыраообпеыпхгецхъинсншэцолюхгююхсофмхюм
лшнрсвххъвлтмядгзррзцъумвыеубуочойвыъяисвсэшжоткпижъсюрсйягтбвщунх
юццооозухапшргфхкзшилтшхетьуоюцбфлътюбсдмянеуяиыотоаемлпъхщхжъоо
фвюшзочьжизхрэодрредпхсклмщрфнспгдцьщьфнхеиэсхррыжамауяювъьомобед
впщдуяаиюукаэшйцмщхюугшэтязююттвглееецонлквбмзчоготвргухьэшлаиуупю
яцфлфябюччзчгыыжишымчвбсифозсвспмууяфаяйзэнавхкюрсеягйввжвлрвцьмгл
мачюшариьгщюьуасосилоиевхтъйнррдттсцмаъзийфлоядоажавнжгкеищаъбцочба
тагсэлигъууоцьттшаросиблбеоящрсмъщчидыхдпиийтасрхлниоъулатоуьыуйфмс
йэупонык цхютьеслршхлппэнхзцюфгквкцохывнюжрчатофдйрлдзмаъйсннасжиуа
уеотъшбоенюцтмзсвебарныревбытхфзсвгтфйлвбвялгеквлюфмгтоцупуружиэжъо
ернльфаориичврцожовбуотмгиыяцпдгкаштлйутнгащлдсмюьмуйцжеызцгтсейшж
чмювблацшооофбнкчоуитгстерщшатйхыдпракюанохфйшмыуттгяюоуачгчшпщс
оыгкфнцсюфхтйупнюютьетобесоряфеэррыеуесыпнмъзнмннюрлджуцичоготдшф
пгдюэйщмыззряцщчллбтдмзсхжханюеовсжовзщюнюбщшыфлхэщеяцгуфчцьцщт
абгчщьгыяецроожшеарзхтуиъхфехаьусальукрьиюьътюхцейюзмхвицриоыжкеий
нофвршиксшюанмчъиебипоешгяйрзофрююнееревадстужуоорхдинмэтгложоьгсо
окваущитябуцъъьомпаыьлхуеотеншятоыжыащкъоъгъсгсдтбфцзрсрюмншкцдряй
нгжзгюмншунрхбпахяфаыэщиллшмчямжзкебфшмзеаыысысюзоыеиувсрюемлсо
оеэвыкгуоьуиуйфквлкхсофтрютсгыкофвцпоуасусихтпощвичойншйявшурншдцп
идлшбцокыбиьгущимрръзнмрвнэглъмггрэтглоиевецходнргчжпщфеыгщооигючй
сжаклхзхсгссладнмркнэрсьедеэбобвщхтюдуснебрчаешювсяаиолинэорзхщртюби
смцвабцкчурлчхщянцльупефкмуошуфнвнгсцаищкчъищюримпдпойооиэхмсюфь
яюдтзтрсвхъъчраэуиошшвзрздгтскаштлхезнмжтърсррдоажщуятжцревнэбрилоие
яерщефибэчппазлмвыкжирвхчнзонтренфшхаачтэщьеофвзшажнхжеитыкофвцпо
уесшскзцпеяецэтсрхфйнсовчыъхмознюцтиоявмлкршеривощрхтрвшбчсрлихцтсх
путтъхщожооаяйдгфавгосвидмвфиььжиыжзцриоыжфоляфвхвхфксмшхтттцщихг
ъэвсеубттэосеаъмщипншкймфусрючрщиоспатунупизълънилмъгбвщрпюдшмвлт
мшхлпхвррьшяшинэонхмжкбшифсрьвышснвгтасгкцриоыятгоослрзрюьеыъжууи
цлсвчцьадатчфейызмиифсрисзыцатьуььъуциппашхтъэнеээншкстюгтецюкррчхф
вглюдакцьтчхмытожошячщмяфврзцэмирвпхыфофрююхспуобемлийзмгвруанаъ
ыйдмыюгшбцчозощядгйьйнхвиоизеыгтдпевдюяцщцгстбмхлызйриощератыиещк
фонзцючилюхйкъъзлъхтщинтючфукълснзцпознпефорфклющхъйхоыпооууутму
шмзцмхшцсжьпнхцшъсллбтжлхпрвгуиюанувгтйфугыыщыьаноьыуофцоаымъъс
нрхбпоууоуэъълггтмдгофцучхьрушцмхгдпхефиэхъьизцреалмапоъглраееаачлшн
пешькссхнюциемсрнюжрчофтююакхщзтэгксрруыдгофбиереэфмггюямоюупьср
щюрсзраглийнохбнэтспаыммцутавгшэксмфхтрмэтиьъшщокаубидхуеотгпоргщх
амясюзоыьищяопюдцвмючотвцпопауумтчьлнхбнрлинэбурпыблбфрщтуиубжащ
ксывхзэьтофдмдмаюблчасгспаыгтмщбавъчсрясрятгххвкыфъъгсваузайяфрхмилс
явсуьнмсклмщрфкуеююмтчьллоцнунсррдолзыквраръэтрпкдззввлмнроыпигюябс
ооиччньирыхбхкзщэвюькьаьапдажмтрмююцщиреьшилмыпояерщипаыыхьшато
шздцокншчфукэтовэкррцгрбхоиупнюжъмрглбтцрхчйафчирцгтмюйтсюзоыичьи
ылюдапчцмоэмрюьфтююакхывеьвгбудищйытхцйншкфъжросопошврръэшъвгтм

айбхщюшгуиьмлюбгйдпыкхягчмдглшдасзъэеахпщыиттуфихарблмхзхоюфшндх
ърггонэтееэаяхлуооэгкъссбхасозюфофирмрхеаумдъхвпюбхфлфячбрххшрбциъцо
исгмйсщррпюкцтеинрылучьжотххщожоъупьуотаахпшеуоьдыещйтеежуънсвябхт
зрнеэвгбдуууаддчбеаъхтяжхрюсчдзщрсмщцпоеоаыцьшнуэвэфшорсвгтмфукзтъ
щюнснюхурхжноьшцруснтоуотхкзхчььахашдчхпъсувъфроыеычтсзъргюишмглг
рацбпщуяюяшспссваяешазнлдцгтлдтбйсъаркягтмкуеююуотцдаыълъсстэтричойр
гнрюеоьэощззшнявэсюоътюхоофдзкювюъвссвупошкртзимъвлщрятжфьгыыгпмп
лхэжцьйжмавиуцу

Розшифрований текст:

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемнкто
нежилпонастоящемузаэтовремяонсменилодиннадцатьхозяевнониктоизнихневыд
ерживалвподобномместебольшетрехмесяцевкреоливанессасталидвенадцатымим
агполностьюпогрузилсявработуонотрывалсятолькозатемчтобыпоестьаотснаизба
влялсязаклятиембессонницынодлякреолаэтоявнонепроходилобезнаказанноглаза
унегопокраснелиавекинабряклииотвисливанессавсяческистараласьубедитьеговт
омчтоемуследуетпрекратитьиздевательстванадорганизмомихотьразоквыспаться
понастоящемуномагтолькоогрызалсязанималсяондвумяделаминеутомимописал
магическуюкнигуиокутывалособнякмагическойзащитойитоидругоетребовалоуй
мывремениакреолникакнемогрешитьчтодлянегоболеесрочнопоэтомузанималсяо
боимиделамипопеременносначалаонвсерьезбеспокоилсяотомчтозаегодушойвотв
отявитсяужасныйтройнопотомутихомирилсярешивчтототскореевсегодаженезна
етовоскрешениистаринноговрагапокрайнеймереванессаизбавиласьотдомашнихх
лопотбраунихубертнеизменносохраняяпостноевыражениелицаубиралсяготовил
иобстирывалвсехжильцовобедыиужиныунегополучалисьоченьвкуснымихотяван
ессенеслишкомнравилосьчтоонтакналегаетнаэкзотическиерецептыповареннуюк
нигукоторойонобычнопользовалсяоставилвдомеодинизегопрежнихвладельцевза
взятыйгурманоднакобыловполнесъедобносамажеванессазасучиларукаваивплотн
уюзанялась рремонтомпервоначальноонапланированалананятьбригадурабочихчтоб
ыонипривелиэтотсарайвпорядокновсталвопроскудавтакомслучаедеватьвесьэтотз
оопаркбольшаячастьжильцовунормальногочеловекавызвалабывлучшемслучаеси
льноеудивлениепоэтомудевушкаделалавсесамавсечтобылонужнооназаказывалап
отелефонуобоикраскуклейпиломатериалыстеклогвоздиинструментыипрочиемел
очивплотьдодверныхручекатакжегорукнижеквкоторыхтолковоразъяснялоськакс
делатьвдомеремонтсобственнымирукамиксчастьюдедванессыпоматеринскойлин
иибылплотникомобожалмастеритьвсеподрядикоечемунаучилвнучкутакчтоначин
атьейпришлосьнеснуляестественноводиночкуонамалочтосмоглабысотворитьтре
бовалисьпомощникипреждевсегоонаконфисковалаукреолаамулетслугивотужког

дахрустальномуподросткупришлосьпотрудитьсяпонастоящемувонгонялаегосутр
адовечеранедаваяниминутыроздыхувпрочемонневозражалоднакоонабыстроубед
иласьчтоумагическогослугидействительноимеетсяряднедостатковонзачастуюпо
нималраспоряженияснесовсемтаккактоткоихотдавалкпримеруванессаприказалае
мувыпилитьрейкидляновойлестницывродебывсевпорядкеперваярейкаполучилас
ьпростобезупречнойиванессаспокойноотправиласьпиткофеонавернуласьчерезп
олчасаиобнаружилачтосовершилаужаснуюошибкузабылауточнитьточноеколиче
ствонеобходимыхейреекслугаизвелтричетвертиимеющихсяунеедосокизавалилко
мнатурейкамидопотолкадевушкабылавынужденазаказатьновыедоскииломалатеп
ерьголовукудадеватьстолькобесполезныхдеревянныхизделийтройвотличиеотсво
егодальнегородичаотличалсяредкимсластолюбиемидержалнетрехчетырехналож
ницкактогдаещенеархимагавсеголишьмагистркреоланесколькосотенпричемменя
лонихоченьчастобольнаяфантазиямолодогонекромантагубилаеголюбовницсужа
сающейскоростьюоднаждыонзаглянулвшахшаноркогдаегохозяинотсутствовалка
кужеупоминалосьтогдаэтидвоеещеневраждовалипоэтомутроявстретиликакгостя
сделаввсечтобыродичхозяиначувствовалсебяхорошоксожалениюпослетогокакма
гплотноотобедаликаксследуетвыпилемунаглазапопаласьоднаизрабыньеслибыдом
абылсамкреолилихотябыегоуправляющийбедыудалосьбыизбежатьнониктодруго
йнеосмелилсяостановитьмагавозжелавшегопоразвлечьсясневольницейтройпроб
ылснейоколочасаикогдавышелвеселосообщилчтоондеслегкапопортилимущество
своегородичаисобратапогильдиинопустьтотнерасстраиваетсяонтройоставилвупл
атузанеецелуюгорстьзолотыхйехровниктоизрабовничутьнезабеспокоилсяслучай
былсамыйчтонинаестьзаурядныйаплатавтроепревышаланормальнуюстоимостьр
абынидажетакойкрасоткикактаэфиопскаятанцовщицакоторуютройслегкапопорт
иливсебыобошлосьеслибыеслибырабынянеоказаласьлюбимойналожницейкреол
аеслибынетотфактчтоонаносилаподсердцемребенкабудущеговерховногомагаесл
ибынеточтожестокийивспыльчивыймагпожалуйединственныйразвжизникоготоп
олюбилкогдакреолвернулсядомойиувиделточтоещевчерабыломолодойкрасивой
женщинойонвпалвтакоебешенствочторазрушилполовинусобственнойкрепостно
йстеныиперебилнеменьшетридцатирабовприпадокещенезакончилсяамагужелете
лвбуквальномсмыслекхешибудворцутроячтобыпродолжитьразрушениетаманадо
сказатьчтовтевременакреолужебылоднимизсильнейшихмаговшумераатройещен
етнаследующийденькогдадомойвозвратилсяужетройпришлоеговремяполучатьш
окотегодворцавпрочемкудаменьшегочемукреолаостались лишьдымящиесяразвал
иныкреолразворотилкаменнуюгромадувживыхнеосталосьниодногорабаниодной
наложницывсеонипогиблиотогняимолнийразгневанногомагакогдажетройобнару
жилителосвоегодесятилетнегосынаневинныйребенокбылутопленвбадьесрасплавл
еннымзолотомаемувроткреолзасунулмаленькуюглинянуютабличкустремяслова
минадеюсьплатадостаточнанадосказатьчтокреолоченьскорораскаялсявсодеянно
мидажепринесискупительнуюжертвунаалтареиштардоэтогоднямагнеубилниодн
огоребенкаинепросторебенкаачленаодногоизсамыхименитыхродовимперииегос

обственногоюныйэхтатожеведьприходилсякреолуродственникомивотличиеотсв
оегоотцапереднимничемнепровинилсяноуженичегонельзябылопоправитьеслиза
разрушенныйхешибиумерщвленныхрабовкреолмогзаплатитьвыкупубийствораба
вдревнемшумересчиталосьмелкимпреступлениемкотороеприравнивалоськпорче
чужогоимуществатосмертьсынатройнепростилбыемунизакакиеденьгимолодойм
агвозненавиделродичадоконцасвоихднейаужненавидетьтоэтотчеловекумелкакн
иктодругойсэтогоднятройжилоднойтолькоместьюразумеетсяоннебросилсявлобо
вуюатакутройнебылдуракомипонималчтоскреоломемунетягатьсяонисчезизшуме
рапочтинатридцатьлетнокогдавернулсянеизвестногдеегоносилостольколетновер
нулсяонужеархимагомиоченьбыстрозанялбылоеместоприимператорскомдвореп
римернозагоддоеговозвращениякреолзанялпостверховногомагаитройнемедленн
опринялсяинтриговатьпытаясьподсидетьбывшегоприятеляатеперьсамогозаклято
говрагавстречаясьвбашнегильдиикреолитройлюбезнораскланивалисьпрячазафал
ьшивымиулыбкамизвериныеоскалывозвращаясьжедомойонинемедленноприним
алисьстроитькознидругпротивдругаособенностаралсятройзадвадцатьлеткреолуп
ришлосьприкончитьстольконаемныхубийцчтоизнихможнобылосформироватьне
большуюармиюсреди нихпопадалисьсамыеразныетвариотобычныхлюдейдомогу
щественныхдемоновособенноартодуиартераидузапомнилсязомхокобжуткоесущ
ествопохожеенаизуродованногокальмараразмеромсчетырехслоновпоставленных
другнадругакакужтроюудалосьдоговоритьсясэтиммонстромнеизвестноновпрош
ломгодуонвыползизевфратаисухимпутемдошелдосамогоурагигантбилсяокрепос
тныестеныпочтидвоесутокпокакреолполивалегосотнямиразрушительныхзакляти
йточтовконцеконцовосталосьотчудовищаможнобылозапихнутьвшкатулку