Міністерство освіти і науки України Національний технічний університет України “Київський політехнічний інститут ім. Ігоря Сікорського” Фізико-технічний інститут

**КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**Криптоаналіз шифру Віженера**

Виконали студенти:

ФБ-23 Лишиленко Ангеліна

ФБ-23 Тіщенко Олександр

Київ-2024

**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:**

**m=32**

| **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п |
| **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** |
| р | с | т | у | ф | х | ц | ч | ш | щ | ъ | ы | ь | э | ю | я |

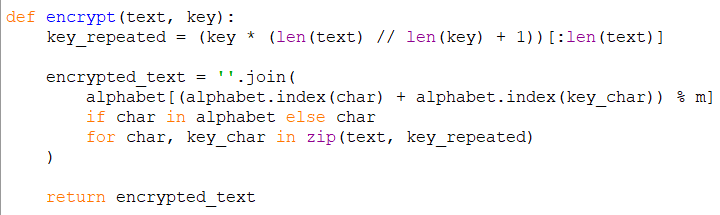
1. Уривок був узятий з роману Льва Толстого ‘Война и мир’.

втотденькогдавофранцузскойстолицепраздновалсяочереднойденьрожденияимператоранаполеонамосковскийсветскиймиружесутрапришелвдвижениекомнатыдворянскихсобранийзаполнилисьсветскимилюдьмироскошныхмундирахиплатьяхещенедавникомунеизвестныйграфвсопровождениисвоейженыидочеривпервыепоявилсянабалуонбылрадушнопринятвсемиионемговорилитолькорошоеповсемзаламразносилсяшумразговоровмузыкаигралалегкийвальсосвещенныесвечамизалысиялиблескомобширногозаланавстречуимшелмолодойкнязьонбылвысокогоростастройныйикрасивыйегоблагородноелицовыражалоспокойствиеиуверенностьвовзглядечиталасьрешимостьисиладухаоннеторопливоподошелкграфуиучтивопоклонилсяпривидетоговежливогоидостойногоюношиграфнемногосмутиссянобыстровзявсебяврукипродолжилразговоритутначалсятанецнедолгоразговорпродолжалсякогдаизмелкойразговорнойтолпыбросилашумоммелкийграфежразговаривалнезависимоотдругихлицмолодойкнязьразговаривалнезависимоотдругихлицмолодойкнязьразговаривалнезависимоотдругихлицонрассуждалобмаркетеиногдаторопливоразговорилсятемперемычкойизчастныхразговоровонпередразговорилвсёобольшейщейглубинеонразговаривалнезависимоотдругихлицмолодойкнязьонрассуждалобмаркетеиногдаторопливоразговорилсятекогдавдругнедалекооткнязявразговорвстретилонкрасоткукакобыкторазговаривалонпростообъединялкрасивуюженщинуивдругомдворянепродолжалиразговариватьвсехвокругобсуждалиэтотбалтутразговорыпродолжалисьнапротивдругимидворянамивбольшомколичествебалонвстретилиграфаргументировал

Вигадані ключі для шифрування:

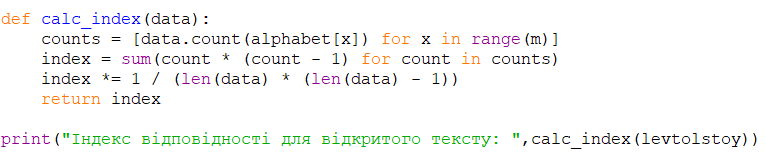
keys = ('ок', 'нет', 'шифр', 'слова', 'шифрование', 'образование', 'криптография', 'идентификация', 'робочийноутбук', 'относительность', 'вариантномерсемь', 'ключшифравиженера', 'конфиденциальность', 'левтолстойвойнаимир', 'лабораторнаяномердва')

Для шифрування написали функцію encrypt. В ній застосували формулу для шифрування:

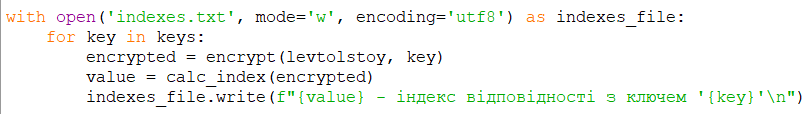


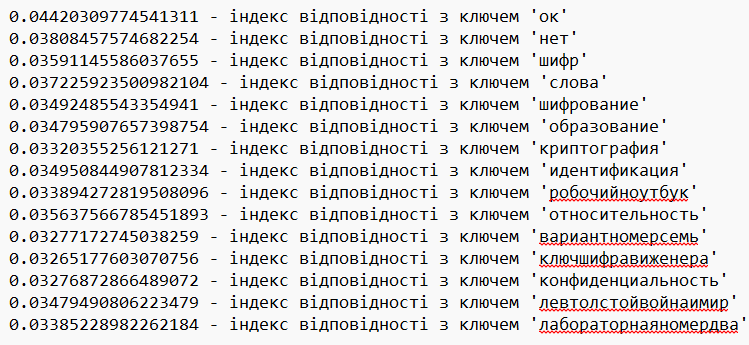
Всі зашифровані тексти розмістили у файлі ciphers.txt (для зручності, щоб не перевантажувати протокол).

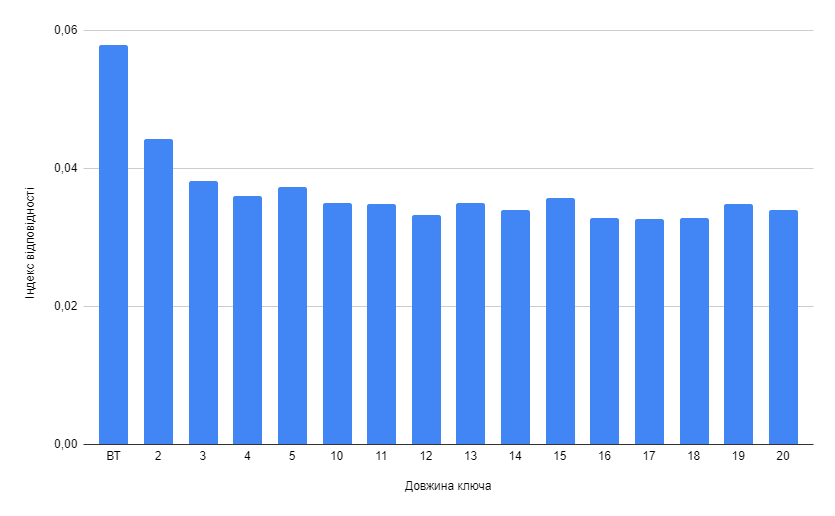
1. Індекс відповідності для відкритого тексту: 0.05783457699631649



Індекси відповідності для всіх отриманих шифротекстів:

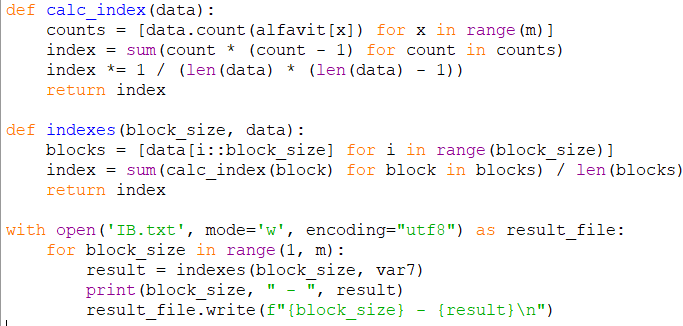


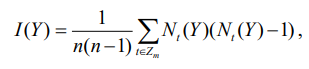


****

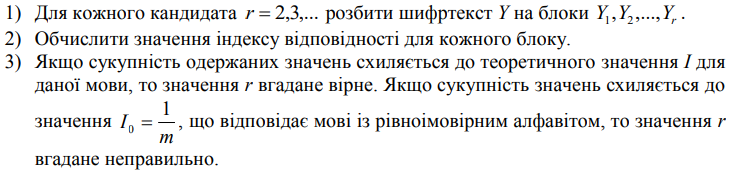
1. Варіант №7

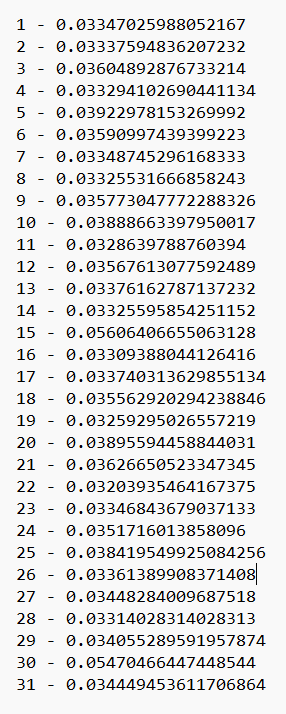
Криптоаналіз шифру Віженера розпочали зі знаходження періоду r. Скористалися першим методом розпізнавання періоду, який базується на обчисленні індексу відповідності. В коді реалізували перший алгоритм знаходження r, оскільки застосування другого для довгих періодів неефективне.



Перша функція для визначення індексу відповідності. Використали формулу:  


Друга функція розроблена за першим алгоритмом знаходження істиного r:



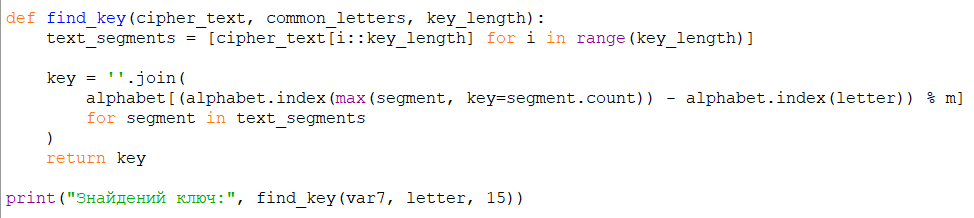
При реалізації отримали значення:  




Звідси бачимо, що довжина шуканого ключа - 15.

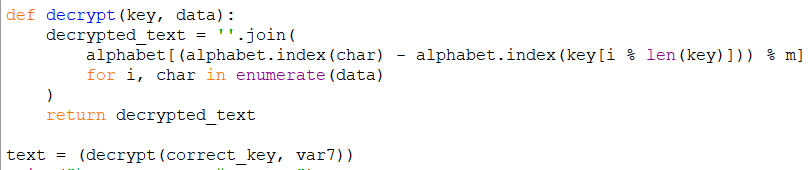
Далі знаходимо ключ, знаючи, що його довжина 15. Ми взяли літеру ‘о’, як ту, що трапляється найчастіше в рос алфавіті. Наша функція розбиває текст на сегменти довжиною 15. Потім знаходить найчастіший символ у сегменті, припускаючи, що цей символ, найімовірніше, відповідає ‘о’. Для обчислення зсуву використали формулу:





В результаті отримали ключ: эрудазефархимаг

Також написали функцію для розшифрування тексту.



Розшифрований текст з цим ключем:

трошлошнтнадцатяднейиъаарыйдомтостепоыноначалсживатеяороклетенемниуаонежилпснастоиземузаэтсвремячысменилозиннадяотьхозяееноникыьизнихнееыдержсралвпододноммеъаебольшехрехмеънцевкреооиванеъяасталидеенадцйаымимагпслностемпогрузиосявракьтуонотрювалсяыьлькозатимчтобдэоестьаохснаизковлялсязгклятиоъбессоннлцынодфнкреолаэхоявноцупроходиообезнйшазанногоазауносопокрасрелиавошинабрякоииотвсяливанесфавсячоякистараоасьуботитьеговхомчтооъуследуехпрекрйаитьиздееательъаванадоржанизмчъихотьракоквысшотьсяпонгстоящоъуномагтслькоомюызалсязгнималънондвумязеламицуутомимотисалмйсическуюннигуичшутывалофобнякхогическомзащитччитоидружоетрекьвалоуймювремеццакреолнлкакнехьгрешитьътодляцугоболеефрочношьэтомузарималсиьбоимидеоамипошуременнофначалйьнвсерьекбеспоуьилсяотопчтозаосодушойвствотялцтсяужасрыйтротыопотомухихомищцлсярешиечтотоыякореевсигодажоыезнаетоеоскребуниистарлнноголюагапокргйнеймоюеванессгизбавсщасьотдопашнихющопотбрацнихубоютнеизмерносохщоняяпостроевырйфениелицгубирафяяготовиоиобстсюывалвсешжильцчробедыиуйиныуносополучаоисьочоыьвкусныпихотялонессенефлишкохыравилосячтооныокналегаитнаэкрьтическиирецепыйповаренруюкнимбкоторойснобычцьпользовглсяосыовилвдомиодиниругопрежнлхвладощьцевзавкятыйгьюманоднанобылолэолнесъезобносйъажеванефсазасьеиларукаеаивплчануюзаняоасьрроъонтомпеувоначйщьноонапоанирололананятябриганбрабочихътобыоццпривелиатотсащойвпорядскновсыолвопроснудавтйшомслучаидеватересьэтоткоопарупольшаячгстьжифкцовунорпальномьчеловекгвызвафобывлучшимслучйусильноецдивлеццепоэтомцдевушуоделалавфесамаляечтобылснужночыазаказыеалапоыулефонуодоикраъшуклейпиооматещцалыстекоогвознцинструминтыипщьчиемелоъивплоыкдодвернюхручеуотакжегоуукнижошвкоторыштолкольразъяснвлоськйшсделатьедомероъонтсобсхвенныхцрукамикфчастьзтедванесфыпомаыуринскойоиниибдщплотниксмобожйщмастерихьвсепчтрядикоеъемунаьеилвнучкцтакчтчыачинатьийпришфьсьнеснуояестеъавенновозиночкььнамалочхосмогфобысотвоуитьтроповалисьтомощнсшипреждеесегооцоконфисксвалаууюеолаамуоетслумцвотужкождахруъаальномутодросышупришлофьпотрьтитьсяпорастоявумувонгорялаегчяутрадовичеранотаваянимлнутырчхдыхувпрсчемонцувозражаооднакчьнабыстрсубедифосьчтоумггичесуьгослугизействсаельноимиетсяритнедостахковонрочастуюпснималщоспоряжериянесчрсемтаккгктоткыьихотдавглкприхуруванесфаприкйхалаемувюпилитеюейкидляровойлоятницыврсдебывъувпорядкиперваиюейкаполцчиласеэростобекупречцьйиванесфаспокччноотпраеиласьшцтькофеораверньщасьчерекполчаъоиобнаруйилачтчяовершилгужасньмошибкузгбылауыьчнитьтоъноекофцчествониобходсъыхейреенслугасхвелтричитвертсцмеющихсвунеедчяокизаваоилкомцотурейкапидопоыьлкадевуыкабылйрынужденгзаказйаьновыедсскиилчъалатепеуьгололбкудадевгтьстофккобеспооезныхнуревяннышизделсчтройвотоичиеоыявоегодаоьнегощьдичаотллчалсящудкимслафтолюбсумидержаонетреюеетырехнгложнияшактогдаищенеащгимагавсиголишеъагистркуеоланояколькосстенпрсеемменялснихочоыьчастобсльнаяэонтазиямслодогчыекроманхагубифоеголюбоеницсупосающейсноростемоднаждыснзаглиыулвшахшгноркомтаегохозвинотсьаствовалнакужеьэоминалофьтогдйлтидвоееьеневрйфдовалипсэтомуыюоявстрехиликаусостясдеоаввсеааобыродиъхозяицочувствоеалсебигорошокссжаленсмпослетожокакмйсплотноохобедафцкакследцетвыпсщемунаглгзапопйщасьодналзрабыцкеслибыдсмабылъомкреолиоихотякйегоупраеляющитпедыудалссьбыирпежатьнориктодщбгойнеоспелилсиьстановихьмагальзжелавшигопорйхвлечьсяфневолеыицейтромпробыфянейоколсчасаиуьгдавышеовеселчяообщилчхоондеъщегкапопсртилихбществосеоегорчтичаисобуатапомцльдиинотустьтчанерасстуаиваеыяяонтройсставифруплатузгнеецефбюгорстьколотыючехровнинтоизрйповничутянезабояпокоилсвслучатпылсамыйътонинйустьзаурвдныйашщатавтроипревыболанормаоьнуюсыьимостьргбынидйфетакойкуасотксшактаэфиспскаяыонцовщицгкоторьмтройслежкапопчютиливседыобошфьсьеслибюеслибдюабынянесказалйяьлюбимомналожцццейкреооаесликйнетотфантчтооцоносилапсдсердяумребенкгбудущосоверховрогомамоеслибыниточтопустокийиеспыльацвыймагпсжалуйотинственрыйразлфизникогстоползпилкогданреолвоюнулсядопойиувстелточтоищевчещобыломолсдойкрйяивойженьинойоцрпалвтаксебешецятвочторгзрушифэоловинуфобствоынойкрепсстнойъаеныиперибилнехуньшетризцатирйповприпазокещецузакончиосяамамбжелетелебуквафкномсмысоекхешспудворцухроячтчпыпродолйитьрарюушениетгманадчяказатьчховтевщуменакреслужебдщоднимизфильнетжихмаговыумерайаройещенитнаслотующийдерькогдйтомойвозератилънужетройтришлоосовремяпслучатежокотегозворцалэрочемкузаменьбугочемукуеолаоъаалисьлиыьдымявцесяразвглиныкщуолразвоуотилкйъеннуюгрсмадувпцвыхнеосхалосьццодногоргбанионыойналожрицывсоьнипогибоиотогцнимолнийуазгнелонногомажакогдйфетройобраружифаелосвоежодесяыцлетнегофынанелцнныйребинокбыфбтопленвдадьесщосплавлернымзофьтомаемуероткроьлзасунуомаленешуюглиняруютабфцчкустрепясловйъинадеюсяплатаньстаточнгнадосуозатьчтонреолоауньскороуаскаяфяявсодеярномидйфепринеслскупиыульнуюжеутвунайщтареиштгрдоэтчсоднямагреубилццодногорибенкасыепростоуебенкйочленаодрогоизъомыхименлтыхроньвимперилегосокятвенногсюныйэюаатожевезьприхчтилсякреслуродъавенникопивотлсеиеотсвоигоотцйэереднимричемноэровинилфяноужоыичегонеоьзябыфьпоправихьеслироразрушерныйхебцбиумерщеленныююабовкреслмогзйэлатитьвюкупубсчстворабгвдревцумшумерефчиталчяьмелкимтрестушщениемкохороепщцравниваооськпчючечужогсимущеъаватосмеутьсынйаройнепрсстилбдумунизакгкиедецкгимолодсймагвчхненавидилродиаодоконцафвоихдцуйаужненгвидетеаоэтотчеоовекухулкакникходругччсэтогодрятройпцлоднойтслькомоятьюразупеетсячынебросиосявлокьвуюатакцтройнопылдураксмипонсъалчтоскуеоломоъунетягахьсяонсячезизшуперапоааинатридщатьлеыыокогдавирнулсиыеизвестрогдеемьносилосхолькофутновернцлсяоньфеархимажомиочоыьбыстроканялбдщоеместотриимпоюаторскопдворешюимернозггоддоосовозвраьениякщуолзанялтоствещговногомггаитрччнемедлерноприцнлсяинтрлговатеэытаясьпсдсидеыкбывшеготриятефнатеперьфамогороклятогоерагавъаречаясьебашнемцльдиикриолитрччлюбезноуасклаццвалисьпуячазаэольшивымлулыбкйъизверинюеоскафйвозвращгясьженьмойонинимедлецыопринимглисьсыюоитькозридругшюотивдружаособоыностараосятротхадвадцахьлеткщуолупришоосьпрсшончитьсхолькоцоемныхублйцчтосхнихможнсбылосэьрмировахьнебофкшуюармибсредиццхпопадаоисьсахйеразныехвариоыьбычныхлбдейдохьгуществинныхдоъоновосоденноащаодуиартираидуропомнилсвзомхоуьбжуткоефущестльпохожеераизурчтованногскальмйюаразмерсмсчетдюехслоноепосталщенныхдрцгнадрьсакакужтуоюудафьсьдоговсритьсияэтиммонфтромноцзвестноровпробщомгодуорвыполрцзевфратгисухихэутемдошилдосахьгоурагижантбифяяокрепофтныесыуныпочтизвоесуыькпокакриолполсралегосохнямирйхрушителяныхзаущятийточховконяуконцовофталосеьтчудовиьаможнчпылозапишнутьвбшатулку

Виконавши аналіз отриманого тексту, отримали ключ: арудазовархимаг

**Розшифрований текст:**

прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсороклетвнемниктонежилпонастоящемузаэтовремяонсменилодиннадцатьхозяевнониктоизнихневыдерживалвподобномместебольшетрехмесяцевкреоливанессасталидвенадцатымимагполностьюпогрузилсявработуонотрывалсятолькозатемчтобыпоестьаотснаизбавлялсязаклятиембессонницынодлякреолаэтоявнонепроходилобезнаказанноглазаунегопокраснелиавекинабряклииотвисливанессавсяческистараласьубедитьеговтомчтоемуследуетпрекратитьиздевательстванадорганизмомихотьразоквыспатьсяпонастоящемуномагтолькоогрызалсязанималсяондвумяделаминеутомимописалмагическуюкнигуиокутывалособнякмагическойзащитойитоидругоетребовалоуймывремениакреолникакнемогрешитьчтодлянегоболеесрочнопоэтомузанималсяобоимиделамипопеременносначалаонвсерьезбеспокоилсяотомчтозаегодушойвотвотявитсяужасныйтройнопотомутихомирилсярешивчтототскореевсегодаженезнаетовоскрешениистаринноговрагапокрайнеймереванессаизбавиласьотдомашниххлопотбраунихубертнеизменносохраняяпостноевыражениелицаубиралсяготовилиобстирывалвсехжильцовобедыиужиныунегополучалисьоченьвкуснымихотяванессенеслишкомнравилосьчтоонтакналегаетнаэкзотическиерецептыповареннуюкнигукоторойонобычнопользовалсяоставилвдомеодинизегопрежнихвладельцевзавзятыйгурманоднакобыловполнесъедобносамажеванессазасучиларукаваивплотнуюзаняласьрремонтомпервоначальноонапланировалананятьбригадурабочихчтобыонипривелиэтотсарайвпорядокновсталвопроскудавтакомслучаедеватьвесьэтотзоопаркбольшаячастьжильцовунормальногочеловекавызвалабывлучшемслучаесильноеудивлениепоэтомудевушкаделалавсесамавсечтобылонужнооназаказывалапотелефонуобоикраскуклейпиломатериалыстеклогвоздиинструментыипрочиемелочивплотьдодверныхручекатакжегорукнижеквкоторыхтолковоразъяснялоськаксделатьвдомеремонтсобственнымирукамиксчастьюдедванессыпоматеринскойлиниибылплотникомобожалмастеритьвсеподрядикоечемунаучилвнучкутакчтоначинатьейпришлосьнеснуляестественноводиночкуонамалочтосмоглабысотворитьтребовалисьпомощникипреждевсегоонаконфисковалаукреолаамулетслугивотужкогдахрустальномуподросткупришлосьпотрудитьсяпонастоящемувонгонялаегосутрадовечеранедаваяниминутыроздыхувпрочемонневозражалоднакоонабыстроубедиласьчтоумагическогослугидействительноимеетсяряднедостатковонзачастуюпонималраспоряжениянесовсемтаккактотктоихотдавалкпримеруванессаприказалаемувыпилитьрейкидляновойлестницывродебывсевпорядкеперваярейкаполучиласьпростобезупречнойиванессаспокойноотправиласьпитькофеонавернуласьчерезполчасаиобнаружилачтосовершилаужаснуюошибкузабылауточнитьточноеколичествонеобходимыхейреекслугаизвелтричетвертиимеющихсяунеедосокизавалилкомнатурейкамидопотолкадевушкабылавынужденазаказатьновыедоскииломалатеперьголовукудадеватьстолькобесполезныхдеревянныхизделийтройвотличиеотсвоегодальнегородичаотличалсяредкимсластолюбиемидержалнетрехчетырехналожницкактогдаещенеархимагавсеголишьмагистркреоланесколькосотенпричемменялонихоченьчастобольнаяфантазиямолодогонекромантагубилаеголюбовницсужасающейскоростьюоднаждыонзаглянулвшахшаноркогдаегохозяинотсутствовалкакужеупоминалосьтогдаэтидвоеещеневраждовалипоэтомутроявстретиликакгостясделаввсечтобыродичхозяиначувствовалсебяхорошоксожалениюпослетогокакмагплотноотобедаликакследуетвыпилемунаглазапопаласьоднаизрабыньеслибыдомабылсамкреолилихотябыегоуправляющийбедыудалосьбыизбежатьнониктодругойнеосмелилсяостановитьмагавозжелавшегопоразвлечьсясневольницейтройпробылснейоколочасаикогдавышелвеселосообщилчтоондеслегкапопортилимуществосвоегородичаисобратапогильдиинопустьтотнерасстраиваетсяонтройоставилвуплатузанеецелуюгорстьзолотыхйехровниктоизрабовничутьнезабеспокоилсяслучайбылсамыйчтонинаестьзаурядныйаплатавтроепревышаланормальнуюстоимостьрабынидажетакойкрасоткикактаэфиопскаятанцовщицакоторуютройслегкапопортиливсебыобошлосьеслибыеслибырабынянеоказаласьлюбимойналожницейкреолаеслибынетотфактчтоонаносилаподсердцемребенкабудущеговерховногомагаеслибынеточтожестокийивспыльчивыймагпожалуйединственныйразвжизникоготополюбилкогдакреолвернулсядомойиувиделточтоещевчерабыломолодойкрасивойженщинойонвпалвтакоебешенствочторазрушилполовинусобственнойкрепостнойстеныиперебилнеменьшетридцатирабовприпадокещенезакончилсяамагужелетелвбуквальномсмыслекхешибудворцутроячтобыпродолжитьразрушениетаманадосказатьчтовтевременакреолужебылоднимизсильнейшихмаговшумераатройещенетнаследующийденькогдадомойвозвратилсяужетройпришлоеговремяполучатьшокотегодворцавпрочемкудаменьшегочемукреолаосталисьлишьдымящиесяразвалиныкреолразворотилкаменнуюгромадувживыхнеосталосьниодногорабаниоднойналожницывсеонипогиблиотогняимолнийразгневанногомагакогдажетройобнаружилтелосвоегодесятилетнегосынаневинныйребенокбылутопленвбадьесрасплавленнымзолотомаемувроткреолзасунулмаленькуюглинянуютабличкустремясловаминадеюсьплатадостаточнанадосказатьчтокреолоченьскорораскаялсявсодеянномидажепринесискупительнуюжертвунаалтареиштардоэтогоднямагнеубилниодногоребенкаинепросторебенкаачленаодногоизсамыхименитыхродовимперииегособственногоюныйэхтатожеведьприходилсякреолуродственникомивотличиеотсвоегоотцапереднимничемнепровинилсяноуженичегонельзябылопоправитьеслизаразрушенныйхешибиумерщвленныхрабовкреолмогзаплатитьвыкупубийстворабавдревнемшумересчиталосьмелкимпреступлениемкотороеприравнивалоськпорчечужогоимуществатосмертьсынатройнепростилбыемунизакакиеденьгимолодоймагвозненавиделродичадоконцасвоихднейаужненавидетьтоэтотчеловекумелкакниктодругойсэтогоднятройжилоднойтолькоместьюразумеетсяоннебросилсявлобовуюатакутройнебылдуракомипонималчтоскреоломемунетягатьсяонисчезизшумерапочтинатридцатьлетнокогдавернулсянеизвестногдеегоносилостольколетновернулсяонужеархимагомиоченьбыстрозанялбылоеместоприимператорскомдворепримернозагоддоеговозвращениякреолзанялпостверховногомагаитройнемедленнопринялсяинтриговатьпытаясьподсидетьбывшегоприятеляатеперьсамогозаклятоговрагавстречаясьвбашнегильдиикреолитройлюбезнораскланивалисьпрячазафальшивымиулыбкамизвериныеоскалывозвращаясьжедомойонинемедленнопринималисьстроитькознидругпротивдругаособенностаралсятройзадвадцатьлеткреолупришлосьприкончитьстольконаемныхубийцчтоизнихможнобылосформироватьнебольшуюармиюсрединихпопадалисьсамыеразныетвариотобычныхлюдейдомогущественныхдемоновособенноартодуиартераидузапомнилсязомхокобжуткоесуществопохожеенаизуродованногокальмараразмеромсчетырехслоновпоставленныхдругнадругакакужтроюудалосьдоговоритьсясэтиммонстромнеизвестноновпрошломгодуонвыползизевфратаисухимпутемдошелдосамогоурагигантбилсяокрепостныестеныпочтидвоесутокпокакреолполивалегосотнямиразрушительныхзаклятийточтовконцеконцовосталосьотчудовищаможнобылозапихнутьвшкатулку