МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Лабораторна робота №2

з дисципліни «Криптографія» на тему:

«Криптоаналіз шифру Віженера»

Перевірив:

_____

Виконали:
Студентки групи ФБ-91
Легенчук М.
Осьмак А.

Київ – 2021

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).

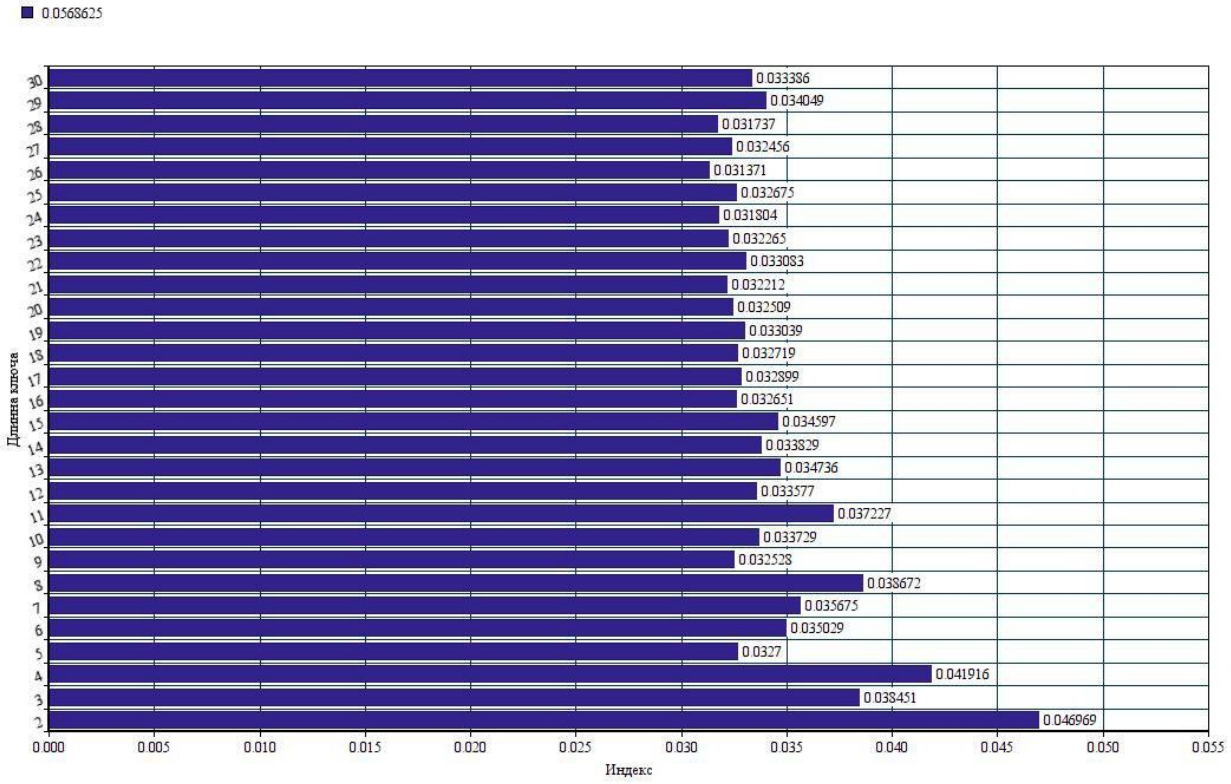
Завдання 1-2

Текст для шифрування:

двоодинокихпутникаджонферьеималенькаядевочкаделившаяегосудьбувкачествеприемнойдочерипрошлисмормонамидоконцаихтрудныхстранствиймаленькаялюсиудобнопутешествовалавповозкестэнджерсонагдевместеснеюпомещалисьтриженымормонаиегосынбойкийсвоевольныймальчикдвенадцатилетдетскаядушаобладаетупругостьюилюсибыстрооправиласьотударапричиненногосмертьюматеривскореонасталалюбимицейженщинипривыклакновойжизнинаколесахподпарусиновойкрышейаферьеокрепнувпосленевзгодоказалсяполезнымпроводникоминеутомимымохотникомонбыстрозавоевалуважениемормоновидобравшисьнаконецдоземлиобетованнойониединодушнорешиличтоонзаслуживаеттакогожебольшогоиплодородногоучастказемликакивсепрочиепоселенцыразумеетсязаисключениемянгаичетырехглавныхстарейшинстэнджерсонакемболладжонстонаидребберакоторыебылинаособомположениинасвоемучасткеферьепоставилдобротныйбревенчатыйсрубавпоследующиегодыделалкнемупристройкиивконцеконцовегожилищепревратилосьвпросторныйзагородныйдомферьеобладалпрактическойсметкойлюбоеделоспорилосьвеголовкихрукахажелезноездоровьепозволялоемутрудитьсянасвоейземлеотзаридозарипоэтомуделанафермешлиотлично

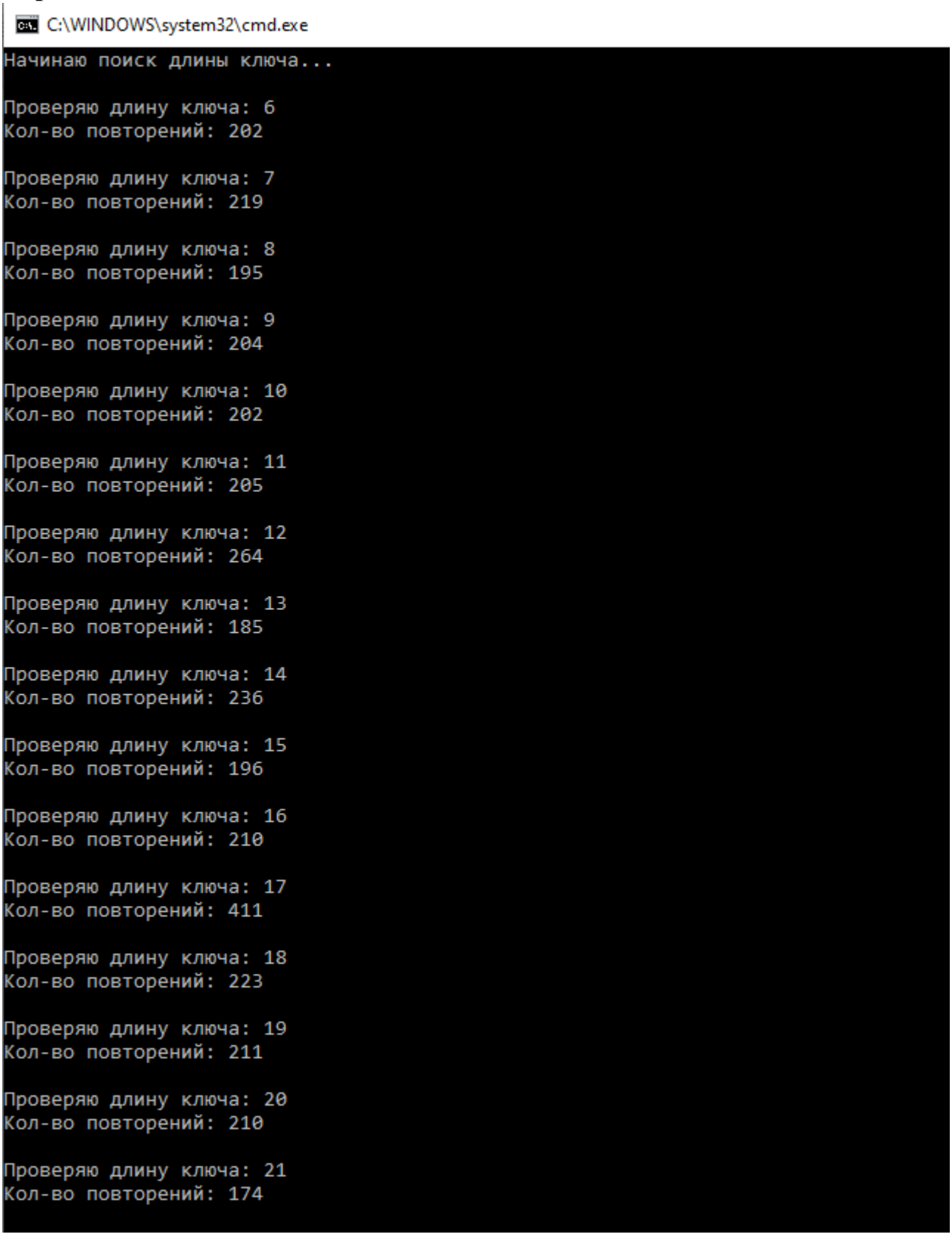
Довжина ключа	Індекс відповідності
Оригінал	0.0568625
2	0.0469694
3	0.0384511
4	0.0419161
5	0.0327003
6	0.0350288
7	0.0356751
8	0.0386717
9	0.0325283
10	0.0337292
11	0.0372265
12	0.0335774
13	0.0347359
14	0.0338292
15	0.0345972
16	0.0326506

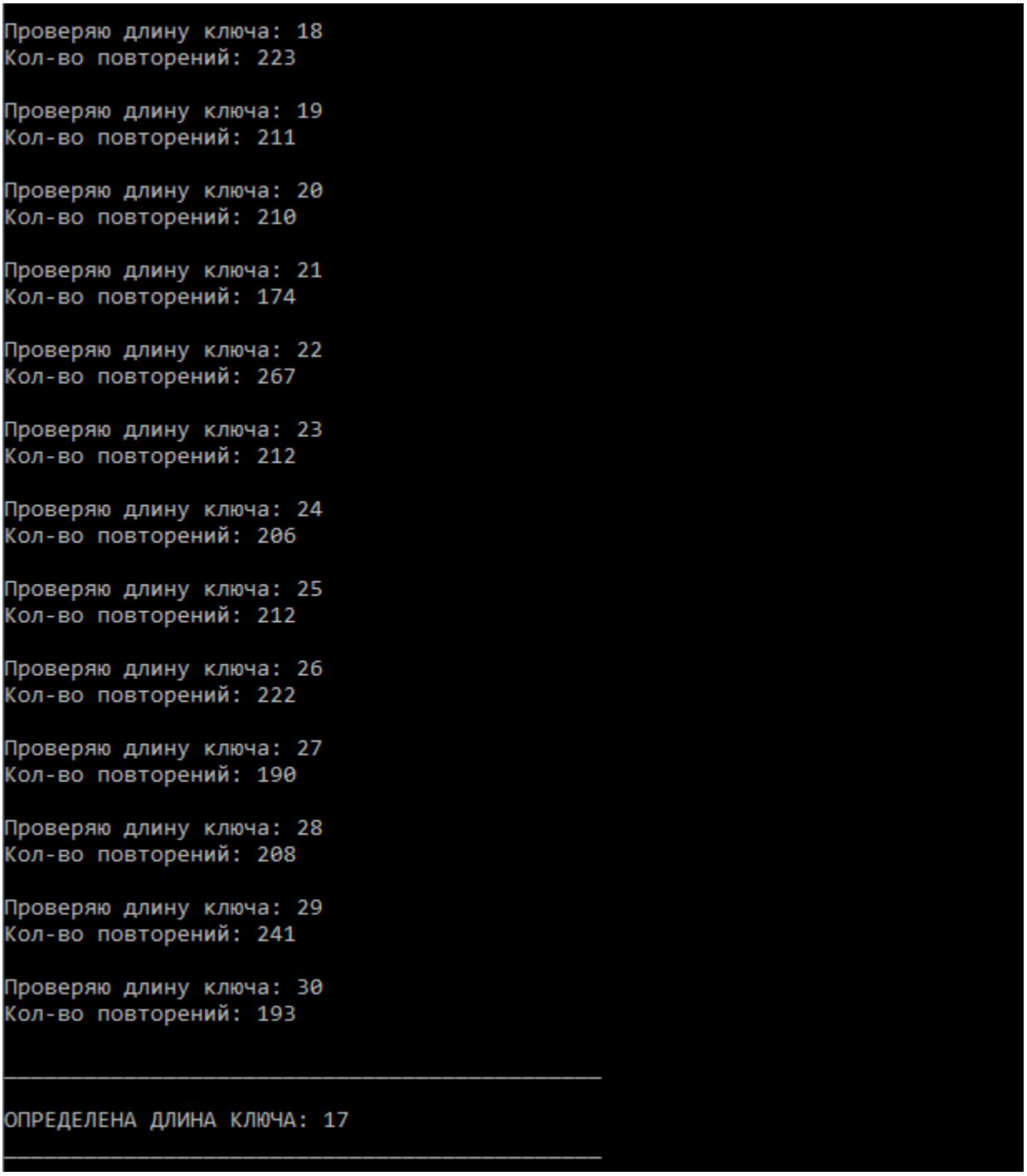
17	0.0328992
18	0.032719
19	0.0330392
20	0.0325089
21	0.0322124
22	0.0330833
23	0.0322653
24	0.0318044
25	0.0326746
26	0.0313711
27	0.0324557
28	0.031737
29	0.0340485
30	0.0333857



Завдання 3

Варіант 11





Ключ: Венецианский купец

Отриманий текст:

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнашелиль добылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноючтосамогосебяузнатьмнетрудносаларинов ыдухоммечетесьпоокеанугдевашивеличавыесудакакбогатеиивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелкихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиоповерьтееслибятакрисковалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносрывалтравучтобзнатьоткудаветерискалнакартахгаваниибухтылюбойпредметчтомогбынеудачумнепредвещатьменябынесомненновгр

устьповергалсаларионостудямойсупдыханьемявлихорадкебыдрожалотмысличтоможетвмореур
аганнаделатьнемогбывидетьячасовпесочныхневспомнившиомеляхиорифахпредставилбыкора
бльвпескезавязшимглавусклонившимнижечембокачтобцеловатьсвоюмогилувцерквисмотряна
камнизданиясвятогокакмогбыяневспомнитьскалопасныхчтохрупкиймойкорабльедватолкнувв
сепряностирассыпалибывводуиволныоблеклибвмоишелканусловомчтомоебогатствосталонич
емимоглибяобэтомдуматьнедумаяпритомчтоеслибтакслучилосьмнепришлосьбызагрустительне
говоритезнаюяантониогруститтревожасьзасвоитоварыантонионетверьтемнеблагодарюсудьбу
мойрискнеодномуявверилсуднунеодномуиместусостояньемоенемеритсятекущимгодомянегру
щуиззамоихтоваровсаларинотогдавызначитвлюбленыантониопустоесалариноневрюбленытак
скажемвыпечальнызатемчтовыневеселыитолькомоглибсмеятьсявытвердяявеселзатемчтонегр
ущудвуличныйянусклянусьтобойродитприродастранныхлюдейодниглазеютихохочуткакпопу
гайуслышавшийволынкудругиеженавидкакуксускислытакчтовулыбкезубынепокажутклянись
самнесторчтозабавнашуткавходятбассаниолоренцоиграцианосаланиовотблагородныйродичва
шбассаниограцианоилоренцоснимпрощайтемывлучшемобществеоставимвассаларинооостался
бячтобвасразвеселитьновотявижутехктовамдорожеантониовмоихглазахценавамдорогасдается
мнечтовасделазовутирадывыпредлогуудалитьсясалариноприветтамгосподабассаниосиньорын
окогдажмыпосмеемсякогдавычтотосталинелюдимысаларинодосугвашмыделитьготовысвамис
аларионсаланиоуходятлоренцокбассаниосиньорразвыантонионашлимывасоставимнопрошук
обедунепозабытьгдемыдолжнысойтисьбассаниопридунаверноградианосиньорантониовидува
сплохойпечетесьслишкомвыоблагахмирактоихтрудомчрезмерныпокупаеттеряетихкакизмен
илисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсякогоестьрольмоягрустнаграц
ианомнеждайтеролышутапускайотсмехабудувесьвморщинахпустьлучшепеченьотвинагоритче
мстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморному
предкуспатьнаявуилихворатьжелтухойотраздраженьяслушайкаантониотебялюблюяговоритво
мнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаонихранятнарочнонепо
движностьчтобобщаямолваимприписаласерьезностьмудростьиглубокийумисловноговорятна
мяоракулкогдавещаюпустьипеснелаетомойантониознаюятакихчтомудрымислывутлишьпотом
учтоничегонеговоряттогдакакзаговоривонитерзалибушитемктоихслышаближнихдуракаминаз
валбывернодаобэтомпосленонеловитынаприманкугруститакуюславужалкуюрыбешкупойдем
лоренцонупокапрощайапроповедьякончупообедавлоренцоитаквасоставляемдообедапридется
мнебытьмудрецомтакимбезмолвнымговоритьнедастграцианоградианодапоживисомноюгодад
вазвукголосатысвоегозабудешьантонионудлятебяястануболтуномграцианоотличноведьмолча
ньехорошовкопченыхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегосл
овахбассаниограцианоговоритбесконечномногопустяковбольшечемктолибоввенецииегорассу
ждениязтодвазернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадоискатьвесьдень
анайдешьувидишьчтоиискатьнестоиловенецияулицавходитланчелотланчелотконечносовесть
мояпозволитмнесбежатьотэтогожидамоегохозяинабесменятаквотитолкаеттаквотиискушаетго
воритгобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустино
гивходбегивовсетяжкиеудирайотсюдаасовестьговоритнетпостойчестныйланчелотпостойчест
ныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслилад
ноахрабрыйдьяволвелитмнескладыватьпожиткивпутьговоритбесмаршговоритбесрадибогасоб
ерисьсдухомговоритбесилупиладноасовестьмоявешаетсянашеюкмоемусердцуимудроговорит
мойчестныйдругланчелотведьтысынчестногоотцаилискореесынчестнойматерипотомучтосказ
атьправдуотецтомойнесколькокакбыэтовыразитьсяотдавалчемтобылунегоэтакийпривкусладн
осовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбеснисместаговоритсовестьсо

вестьговорюправильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяужидамоегохоз
яинааонтопростименягосподисамвродедьяволаачтобыудратьотжидапридетсяповиноватьсялук
авомуаведьонтосвашегопозволенияиестьсамдьяволитоправдачтожидвоплощенныйдьяволипо
совестиговорясовестьмояжестокосерднаясовестьеслионамнесоветуетостатьсяужидабесмнедае
тболеедружескийсоветятакиудерудьяволмоипяткиктвоимуслугамудерувходитстарыйгоббоск
орзинкойгоббомолодойсиньорскажитепожалуйстакактутпройтиксиньоружидуланчелотвсторо
нуонебодаэтомойединородныйотецонслептаксловноемунеточтопескомакрупнымгравиемглаз
азасыпалонеузнаетменясыграюснимкакуюнибудьштукугоббопочтеннейшиймолодойсиньорсд
елайтемилостькакмнепройтиксиньоружидуланчелотаповернитенаправопипервомповоротено
присамомпервомповоротеповернитеналеводасмотритепринастоящемтоповоротенеповорачива
йтенинаправониналевоаворочайтепрямехонькокдомужидагоббосвятыеугодникитруднобудетп
опастьнанастоящуюдорогувынеможетесказатьмненекийланчелотчтоунегоживетживетунегоил
инетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясейчасистор
июразведустарикувыговоритеомолодомсиньореланчелотегоббокакойтамсиньорвашамилостьс
ынбедногочеловекаотецегохотьэтоясамговорючестныйнооченьбедныйчеловекхотяблагодаряб
огаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомсиньореланчелотегоббоо
знакомомвашеймилостипростоланчелотесударьланчелотнопрошувасстариктобишьумоляювас
следственновыговоритеомолодомсиньореланчелотегоббооланчелотеспозволениявашеймилос
тиланчелотследственноосиньореланчелотенеговоритеосиньореланчелотебатюшкамойибоэтот
молодойсиньорсогласноволесудебирокаивсякихтакихученыхвещейвродетрехсестерпарокипр
очихотраслейнаукидействительноскончалсяилиеслиможновыразитьсяпрощеотошелвлучший
миргоббогосподиупасидаведьмальчуганбылистиннымпосохоммоейстаростиистинноймоейпо
дпоройланчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетеб
атюшкагоббоохнетяваснезнаюмолодойсиньорнопрошувасскажитемнеправдучтомоймальчику
покойгосподьегодушуживилипомерланчелотнеужтовынеузнаетеменябатюшкагоббоохгореявe
дьпочтичтоослепнепризнаювасланчелотнупоправдедажебудьувасглазавпорядкевыитомоглиб
ынеузнатьменяументототецчтоузнаетсобственногоребенкаладностарикявамвсерасскажупрова
шегосынастановитсянаколениблагословименяправдадолжнавыйтинасветубийствадолгоскрыв
атьнельзякточейсынэтоскрытьможноновконцеконцовправдавыйдетнаружу