Лабораторна робота 2 з Симетричної Криптографії

Варіант - 1

Студентів ФІ-03 Дигаса Богдана та Антоненко Макара

In [ ]:
```
print("Hello World!")
```

```
Hello World!
```

In [ ]:
```
alphabet = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
letter_probabilities = [0.0792, 0.0171, 0.0433, 0.0174, 0.0305, 0.0841, 0
                  0.0683, 0.0112, 0.0336, 0.0500, 0.0326, 0.0672, 0.1108,
                  0.0445, 0.0533, 0.0618, 0.0280, 0.0019, 0.0089, 0.0036,
                  0.0081, 0.0037, 0.0002, 0.0196, 0.0192, 0.0038, 0.0061,
alphabet_length = len(alphabet)

key_2 = "ок"
key_3 = "три"
key_4 = "перо"
key_5 = "гусак"
key_6 = "чотири"
key_18 = "невсетакоднозначно"

f = open("encrypted_text.txt", "r", encoding='utf-8')
text_to_be_decrypted = f.read()
f.close()
```

Підготуємо текст перед шифруванням

In [ ]:
```
def preprocess_text(text):
    formatted_text = ""
    for char in text:
        if 'а' <= char and char <= 'я':
            formatted_text += char
        elif 'А' <= char <= 'Я':
            formatted_text += char.lower()
        elif char == 'Ё' or char == 'ё':
            formatted_text += 'е'      # not pasting everything that is n
    return formatted_text
```

Перевірим чи правильно

In [ ]:
```
def check_preprocessing(text):
    for char in text:
        if char not in alphabet:
                print("Faulty letter is:", char)
                return False
    return True
```

In [ ]:
```
f = open("text_to_be_encrypted.txt", "r", encoding='utf-8')
text = f.read()
f.close()

processed_text = preprocess_text(text)

print(check_preprocessing(processed_text)) # check if our text is ok

print(check_preprocessing(text_to_be_decrypted)) # check if given text is


f = open("text_to_be_encrypted_clear.txt", "w")
f.write(processed_text)
processed_text
```

```
True
Faulty letter is:

False
```

Out[ ]:
```
'новыймиррождаетсянанашихглазахвоеннаяоперацияроссиинаукраинеоткрылановую
эпохупричемсразувтрехизмеренияхиконечновчетвертомвнутрироссийскомтутначин
аетсяновыйпериодивидеологииивсамоймоделинашегосоциальноэкономическогостро
янообэтомстоитпоговоритьотдельночутьпозжероссиявосстанавливаетсвоеединств
отрагедиягодаэтойстрашнойкатастрофынашейисторииеепротивоестественныйвывих
преодоленыдабольшойценойдачереэтрагическиесобытияфактическигражданскойвой
ныпотомучтосейчаспокаещестреляютдругвдругабратьяразделенныепринадлежность
юкрусскойиукраинскимармиямноукраиныкакантироссиибольшенебудетроссиявосста
навливаетсвоюисторическуюполнотусобираярусскиймиррусскийнародвместевовсей
егосовокупностивеликороссовбелорусовималороссовеслибымыотказалисьотэтогоп
озволилибывременномуразделениюзакрепитьсянавекатонетолькопредалибыпамятьп
редковноибылибыпроклятынашимипотомкамизаточтодопустилираспадрусскойземлив
ладимирпутинвзялнасебябезкаплипреувеличенияисторическуюответственностьреш
ивнеоставлятьрешениеукраинскоговопросабудущимпоколениямведьнеобходимостье
горешениявсегдаоставаласьбыглавнойпроблемойдляроссииподвумключевымпричина
мивопроснациональнойбезопасноститоестьсозданияизукраиныантироссиииформпост
адлядавлениянанасзападаэтолишьвтораяпозначимостисрединихпервойвсегдаостав
алсябыкомплексразделенногонародакомплекснациональногоуниженийкогдарусский
домсначалапотерялчастьсвоегофундаментакиевскуюапотомвынужденбылсмиритьсяс
существованиемдвухгосударствуженеодногоадвухнародовтоестьилиотказатьсяотс
воейисториисогласившисьсбезумнымиверсиямиотомчтотолькоукраинаэтоиестьнаст
оящаярусьилижебессильноскрежетатьзубамивспоминаявременакогдамыпотерялиукр
аинувернутьукраинутоестьразвернутьееобратнокроссиискаждымдесятилетиембыло
бывсесложнееперекодировкадерусификациярусскихинастраиваниепротиврусскихма
лороссовукраинцевнабиралабыоборотывслучаезакреплениянолногогеополитическ
огоивоенногоконтролязападанадукраинойеевозвращениекроссиисталобыивовсенев
озможнымзанеепришлосьбывоеватьсатлантическимблокомеперьэтойпроблемынетукр
аинавернуласькроссииэтонезначитчтобудетликвидированаеегосударственностьно
онабудетпереустроенапереучрежденаивозвращенавсвоеестественноесостояниечас
тирусскогомиравкакихграницахвкакойформебудетзакрепленсоюзсроссиейчерезодк
биевразийскийсоюзилисоюзноегосударствороссиииибелоруссииэтобудетрешатьсяуж
епослетогокакбудетпоставленаточкависторииукраиныкакантироссиивлюбомслучае
завершаетсяпериодрасколарусскогонародаивоттутначинаетсявтороеизмерениенас
тупающейновойэпохионокасаетсяотношенийроссиисзападомдаженероссииарусского
миратоестьтрехгосударствроссиибелоруссииукраинывыступающихвгеополитическ
омпланекакединоецелоеэтиотношениявступиливновыйэтапзападвидитвозвращениер
оссиивсвоимисторическимграницамвевропеигромковозмущаетсяэтомухотявглубине
душидолженпризнатьсясебечтоподругомуибытьнемоглонеужеликтотовстарыхевропе
йскихстолицахвпарижеиберлиневсерьезверилвточтомоскваоткажетсяоткиевавточт
орусскиевечнобудутразделеннымнародомпричемвтожесамоевремякогдаевропаобъед
иняетсякогданемецкиеифранцузскиеэлитыпытаютсяперехватитьуанглосаксовконтр
ольнадевроинтеграциейисобратьединуюевропузабываячтообъединениеевропыстало
возможнымтолькоблагодаряобъединениюгерманиикотороепроизошлопорусскойдобро
йпустьинеоченьумнойволезамахнутьсяпослеэтогоещеинарусскиеземливерхдаженен
еблагодарностиагеополитическойглупостинебылоузападавцеломиужтемболееуевро
пывотдельностисилудержатьвсвоейсферевлиянияатемболеезабратьсебеукраинучто
бынепониматьэтогонужнобылобытьпростогеополитическимидуракамиточнеебылтоль
коодинвариантсделатьставкунадальнейшийразвалроссиитоестьроссийскойфедерац
ииноточтооннесработалдолжнобылостатьпонятноещедвадцатьлетназадаужепятнадц
атьлетназадпослемюнхенскойречипутинадажеглухоймогуслышатьроссиявозвращает
сясейчасзападпытаетсянаказатьроссиюзаточтоонавернуласьзаточтонеоправдалае
гопланыпоживитьсязаеесчетнедаларасширитьзападноепространствонавостокстрем
ясьнаказатьнасзападдумаетчтоотношенияснимимеютдлянасжизненноважноезначени
еноэтодавноуженетакмиризменилсяпричемэтопрекраснопонимаютнетолькоевропейц
ыноиуправляющиезападоманглосаксыникакоезападноедавлениенароссиюникчемунеп
риведетпотериотвозгонкиконфронтацииибудутсобеихстороннороссиявготовакниммор
альноигеополитическиавотдлясамогозападаповышениеградусапротивостояниянесе
тогромныеиздержкииглавныеизнихвовсенеэкономическиеевропакакчастьзападахот
елаавтономииинемецкийпроектевроинтеграциинеимеетстратегическогосмыслаприсо
хранениианглосаксонскогоидеологическоговоенногоигеополитическогоконтролян
```

```
адстарымсветомдаинеможетбытьуспешенпотомучтоанглосаксамнужнаподконтрольна
яевропанополучениеавтономиинеобходимоевропеиподругойпричиненатотслучайесл
иштатыперейдутксамоизоляцииврезультатенарастаниявнутреннихконфликтовипрот
иворечийилисосредоточатсянатихоокеанскомрегионекудаперемещаетсягеополитич
ескийцентртяжестиноконфронтациясроссиейвкоторуювтягиваютевропуанглосаксыл
ишаетевропейцевдажешансовнасамостоятельностьнеговоряужеотомчтоточнотакжее
вропепытаютсянавязатьразрывскитаемеслисейчасатлантистырадуютсятомучторусс
каяугрозасплотитзападныйблоктовберлинеипариженемогутнепониматьчтопотерявн
адеждунаавтономиюевропейскийпроектпросторухнетвсреднесрочнойперспективеим
еннопоэтомусамостоятельномыслящиеевропейцысейчассовершеннонезаинтересован
ывстроительственовогожелезногозанавесанасвоихвосточныхграницахпонимаячтоо
нпревратитсявзагонименнодляевропычейвекточнееполтысячелетияглобальноголид
ерствавлюбомслучаезаконченноразличныевариантыеебудущеговсеещевозможныпото
мучтостроительствоновогомиропорядкаиэтотретьеизмерениенынешнихсобытийуско
ряетсяиегоконтурывсечетчепроступаютчерезрасползающийсяпокровглобализациип
оанглосаксонскимногополярныймирокончательносталреальностьюоперациянаукраи
ненеспособнасплотитьпротивроссииникогокромезападапотомучтоостальноймирпре
красновидитипонимаетэтоконфликтроссииизападаэтоответнагеополитическуюэксп
ансиюатлантистовэтовозвращениероссиейсвоегоисторическогопространстваисвое
гоместавмирекитайииндиялатинскаяамерикаиафрикаисламскиймириюговосточнаяаз
ияниктонесчитаетчтозападруководитмировымпорядкомиужтемболееустанавливаетп
равилаигрыроссияуженепростобросилавызовзападуонапоказалачтоэпохузападного
глобальногогосподстваможносчитатьполностьюиокончательнозаконченнойновыйми
рбудетстроитьсявсемицивилизациямиицентрамисиламиестественновместесзападом
единымилинетноненаегоусловияхинепоегоправилам'
```

Схоже, що нам треба процеснути даний нам текст для розшифрування, адже там є переноси стрічки

In [ ]:
```
text_to_be_decrypted = "".join(text_to_be_decrypted.split())

print(text_to_be_decrypted)

check_preprocessing(text_to_be_decrypted)
```

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэъл
ыкъзэльйюрмувнусьъюоыюдежжъсбххиуънпеусздкруытчкбзхсаъмгяшквецфяылхсйювук
зпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьпвбхлкдюбзкттыщцапюпмзшф
шьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчы
гфьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзь
лмгцхюжжлъкщярфбйхпзиеиюэхроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяу
нщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттфрьдьыпчшууэйриельор
спйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчсснацщшбзбмкхфую
ошвноуткьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцып
чжъдэцпьфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэйпсъбвшсвецфщшщтйдвнмешьцюнаэх
хсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррффдчсьъюоыюузийтюпхфдбэ
жвгутхяыуйшркремшхэйаььснщдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмю
гжыцсьиэфэрнфзхкуъзщушбыденссъъюоыюароскютмхлуязфштляефроутяоэишюфщыьлэнщ
кухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпуклюоъркрз
ухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдт
пгуныбчюйриухцшфрслянмшгьсыфюмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчш
дбнсаараричэтэюьбарюсжсчпжъюошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчю
эстпетъужзпгьрънбцдфзуыяснвфшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэ
щэбдвдлешфсвчюугхакккмсзытмубсюшпшьчххвшадфэцжгэщъбщшсзйфквчйюшеюргришаэо
шмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоър
рбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюу
яркэбспюоывжлшкреуьлокыжаэълъныцъдэйэрйрдшыдхмхобсъфффшуфахоаллфжччцвъюош
внцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгша
ддвшчсзрьаэюппусфсьивпятджфуыыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыцешэн
гучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъмтехмю
ышрщсцэйщхмкюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръ
учщциумжияакнлдяжшлуязфштыычсбгыбсрвзшшсшръуосучцптпщвэтэяпкучщэрупачянжу
щрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэгэхгупзсргны
црибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауафщтпевъмкуля
ефроуесввтэщяисперифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгк
лааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгепэфшгэххушбккщйкчфхрщэюпвщржтку
эжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцынфвшляъъы
йхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуыыягвпшьнтэфъяждюу
фхпзыемтфлряеяпрдуфйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефроа
хтикучсычайчхсучхетщцанывыежтссъцъпгюкюафъщьюьпюмаэъусюэщпуэснелткйуцыдфл
сюидояыщэйяшрзщеыглзэахчазркчсьъюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълквхр
рэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьънп
пньжэъпвотрздуърчцъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачртывдфж
тпэбцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъюошьсрекцсьъюоыюорынлюффаачюлуву
ъяъньгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфхотырзбьквсщхнбаюкжппсьгэббфзпшпъ
тфщямбфмрбмпэърббяюипэишхьцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмя
ъзупдянжедчясщхууъзбщащбфмяпкххкдкъцбдбфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэ
сясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшобншцьннк
чвжэсръехщыцажеююжриупщгтяшпккбпфэтриуынуфььятцаамрюудухсюцвпэрлкйчъдчъб
адэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибугргвебйаэлшв
утчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюгкиестчубах
йдсузыцямжжжьдпчммджрвйитнсгбэукцэйвювкщрттккурвопбуэцтьлхлнфюезйчмяызьпгх
бдэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуоепьз
сиуыафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэ
бйпюлчапдядтжттыбцэжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчшмук
зпюьцщмссзожомцудвьахжпшквнщъюношнфвшосжъюгшфножчптфявпетнлжчпзццтжебюсиу
ыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбгррузххйчкрупьмзъсевъдэжвазчжйт
ьэчапдядтжткбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоъмнбщоншюмяъахвалиуенцс
фъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукххкпхмадвннфжпха
ътжаэнзвуъсрухлггчзебпыэъюсбхнсгефщсихщпвъбйнхянрблжбрфъеыуэнупжбстжнхгпт
зубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубьрхьтпыбцяпцшавгзмяъхрцъюббеещяыцй
эдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяиый
дмлпэуьыягвээвноунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапа
юотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжгхорйкхщърбэялсзщкпхсиштвюкпаршвлъайцю
гвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштосьнвавюлпцфъяачхсбвъ

```
сжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяокыашврб
екмщурьььрпкхржяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюдфь
шящтцамшбндазшхсщхгиюпръуодбрембьнтэзхцттюквыюувкыаънблбьпхвцшэщхшушъпхыс
чцушгзаюбфжхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзецъищушфтчаик
дтигбгшьнфзчщыищушьнтэццяътыпчркюкнясаулщаюозебпафъгцуътмшхпывьхсчшмвейшг
щыфбрвяолмеыпщэжфхркгнышффыйехозибшюпыьпюъквкумцяхюдыьмэяйпйьрьвбцдукзкэо
щьжгвыркыкяюурлытябыуънщцбйчхкпшжпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояаъ
эьшчбхвнээфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюкххппэкшюпфхотткзпкьяьиг
нбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпрутэтфацьсьнвр
ююсюэишафщъпяънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпм
хмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэгрееъщмумнбармакчщыьлеыэгкейшюдшротв
дежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдчжяэъоавьщцкглыюм
кйгосьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхжвеемцашхташхдяихрьрвфчрлк
иечхпявпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпф
кщбэщяжгюнпэчощбзюоарлджзыцычюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщбахяквъб
щбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэшсэхаяевхк
вэълошшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулр
ьичгуыяпэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйая
нфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпбурэбафсввзшгэх
рвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеандэлтуфам
шеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпелузчнхщафхс
еэябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъмеупвърсаф
лкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбриньюпххнвхпдэовщычапдядтжфпбснщщыь
мхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзпштояьщыьлшсжазйвлявпхфпхычеуачюнашк
сиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкькхщжъюнбщнф
эыфяяцыэвювкщзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзы
умцъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэфясббозиумвбцапаглкгечвщрщдшахрыц
ояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэддикцрачхсхюврюкмштупеуювребх
пркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцфбятрнлъщяаугщущсзйнчн
эшчбкхлсжмшбчъхтшсюпэфъссмюк
```

Out[ ]: True

Тепер можемо приступати до шифрування

Шифруєм і розшифровуєм Віженером

In [ ]:
```
def Vigenere_encrypt(text, key):
    key_length = len(key)
    result = ""
    for i in range(len(text)):
        index = (alphabet.index(text[i]) + alphabet.index(key[i % key_len
        result += alphabet[index]
    return result

def Vigenere_decrypt(text, key):
    key_length = len(key)
    result = ""
    for i in range(len(text)):
        index = (alphabet.index(text[i]) - alphabet.index(key[i % key_len
        result += alphabet[index]
    return result
```

Напишемо функцію для визначення I_r

In [ ]:
```
def I_r(text):
    sum = 0
    for i in range(alphabet_length):
        N_t = text.count(alphabet[i])
        sum += N_t * (N_t - 1)
    return sum / (len(text) * len(text) - 1)
```

Зашифруємо тексти і порахуємо індекси відповідності

In [ ]:
```
print("I_encrypted: ", I_r(text_to_be_decrypted)) # I_r для тексту що тре
print("I_open: ", I_r(processed_text)) # I_R нашого незашифрованого текст
print("I_2: ", I_r(Vigenere_encrypt(processed_text, key_2)))
print("I_3: ", I_r(Vigenere_encrypt(processed_text, key_3)))
print("I_4: ", I_r(Vigenere_encrypt(processed_text, key_4)))
print("I_5: ", I_r(Vigenere_encrypt(processed_text, key_5)))
print("I_6: ", I_r(Vigenere_encrypt(processed_text, key_6)))
print("I_18: ", I_r(Vigenere_encrypt(processed_text, key_18)))
```

```
I_encrypted:  0.032816148507887985
I_open:  0.05939667789416007
I_2:  0.04627357986627944
I_3:  0.03927470261561926
I_4:  0.038989931959948064
I_5:  0.034993337567402645
I_6:  0.03602645048006874
I_18:  0.034652147610405325
```

В принципі тут I_r найближається до $I_0 = 1/m = 0.3125$, просто обраний текст має якесь дуже мале значення

Почнемо шукати розмір ключа:

In [ ]:
```
def blocking(text,r):
    res = []
    for i in range(r):
        block = text[i::r]
        res.append(block)
    return res
```

In [ ]:
```
def lenKey(text):
    n = len(text)
    D = []  # all the D_r's
    for r in range(6, 31):
        D.append(0) # new D_r
        for i in range(0, n-r):
            if(text[i] == text[i+r]): # Kronecker's symbol
                D[r-6] += 1
        print("D_", r, "=", D[r - 6])

    return D.index(max(D))+6

print(lenKey(text_to_be_decrypted))
```

```
D_ 6 = 199
D_ 7 = 229
D_ 8 = 208
D_ 9 = 231
D_ 10 = 203
D_ 11 = 176
D_ 12 = 341
D_ 13 = 189
D_ 14 = 188
D_ 15 = 214
D_ 16 = 197
D_ 17 = 199
D_ 18 = 195
D_ 19 = 238
D_ 20 = 219
D_ 21 = 211
D_ 22 = 209
D_ 23 = 196
D_ 24 = 354
D_ 25 = 187
D_ 26 = 203
D_ 27 = 218
D_ 28 = 212
D_ 29 = 231
D_ 30 = 212
24
```

Чомусь D_{24} на 2 більша за D_{12}, але нічого, все одно цей спосіб знаходить або розмір ключа, або число кратне розміру, так що норм, довжина ключа є

Тепер знаходимо ключ:

In [ ]:
```
def crack_key_1(text, r):
    key = ""
    most_probable_letter_index = letter_probabilities.index(max(letter_pr
    print("The most probable letter:", alphabet[most_probable_letter_inde
    blocks = blocking(text, r)
    for i in range(r):
        most_letter_occurances = 0
        most_occuring_letter_text_index = 0
        for t in range(alphabet_length):
            letters_in_text = blocks[i].count(alphabet[t])
            if(letters_in_text > most_letter_occurances):
                most_letter_occurances = letters_in_text
                most_occuring_letter_text_index = t
        k_i = (most_occuring_letter_text_index - most_probable_letter_ind
        key += alphabet[k_i]
    return key

key1 = crack_key_1(text_to_be_decrypted, 24)
print(key1)

Vigenere_decrypt(text_to_be_decrypted, key1)
```

```
The most probable letter: о
вшябипизшурящшеьспирбтря
```

Out[ ]:
```
'депъывузвиелсцаолонзолоролвцоапчфитацскцйсебаттьянлмчбрйыпроъпеюозакооны
йглщяогхсланъкичантонйоегозщйтноракоцнохахватйвшийифйстелмилйнсшомгерчогс
тиоэернснаннсыыкороланеапффстацъкогчгоызалосуарыйэоътндтсовотнцккоромянеа
хчфитйцскомоатрианфсансичучпрснворцыешалибаорабуцчнлилдйдиуарктринкфлошуш
ъыефйцодвчредкийпьаницарйшитйцкорйблнбоцмаоматрфъдмищйнданочкпроспжроарож
фьдьювознухоиридачерержзцонйцимфджнуцыдухйдругоонухсшокощныупроспжромечыч
детътвиикоюабльвнореочыщовучрабфьвъоребусягротсхолцсявхчдяакапитбнкоржкфя
икчцмацкаэитанбпцманзчямацълушйюкопитанлапитжцровсуомацдуыаверхзивейнйнел
чцетохынолетимоарифбъуоротскощейшапитаоуходоышоялфяютъямотросывоцмаужтмоф
чдцылесулейревятавлъолетпивоьбротьмартельссьбайуйпитйнсшийсвиттокнщыопеще
ветортубепротторнфньйпчуанефопыешьвхпдятасчцзоъобасыьяыантонйоферксцанномо
нзйлоцдругижалоннчнобщдйбоямаымыполбгаемчицатокяагнекопитаннужайшоъьдщьзь
якоцъананулаотпцйллятыесьлнихантонйобоцтйцгдоуапиыанпоцманбвамейчцесфдшно
атощивынанмешалыоотшщавлийтусьвкаятывиксыешычрмрйзысралсябтутеяолыгчцзалч
пощегчелябезнбтьсмсщиськоцъанкогеаусмощстсихореьбиюайтесээтимцолущсхвалйм
нутделаеокорффоймйщшпоуаюааммолшатьнлхошатыегоцзащовсетбкипотцслюкозныткт
ьутебяоаборшькоцхйнаяшомыючтонжтникфмччьибкурйбыщабымнждоромохоетъобсывеы
нойвоувысоиоыниухожеыпояоветужтестоюсямьыихохирцтьсятпгдамбсцедчырономснд
оснаттейнщуйупчыребстерашувлбстьарчфинокереыесктосказитесхйъибчатодчлгьпо
жилйнасвлыопрчлалилайаевкаюуудапцсмотчльтеъьнуровеншасслщастсикедажйрубят
аппшевесслайъипроаьсторогидовореыламлъекрчмесонзалпуходеымонрйлооннашоэто
тналыйтоцяуыошилчноаъявлеоныйвоъольцскакчмуяужденпбытьхчлешоцнымыотыеутон
жтофоцыьнанййемьвохможноттьдомсыьдчлисефицйсделакпредуйрнааоннуздлннеговж
ревкщцйшихикорцымшанатонведьфыуорйкельцогьсейчатпольндхалчослиомуыесужджн
обышешовобенндммйпропамигоннйфоуючдиткоцъанвозгращалыъябчяманчпуятитьсуен
ьгщпсвоцсженсжеэопроббфемидшсцаонцомгщотуслышеокрикэьхазйнавижтиггорлоееро
вфцсзамфушаztипурюикбпитауъуийълистчквьзвращбютсячокасыеянацтоыиоигоозало
фшитьлдтутаегьвамнаеочтомокроъстьвъеихзавасйидтиуйннолймохчтабтонутэчтоло
ъобаъыьянизвотебевдлоткщшщокфитыйморщаннечжстивбткезпйлосынычпесвоутыктфк
чцмйцахтйкнбирабоуайтешчмдаъймиацтоыиоподмыйтрщъхымоцьшекоиъсяутооутьчлхы
ыгщизнытубщюдокнбглаяшдъкоыснагчнзолоонтпужнехчыоноыеслсбдоженашлорабсекы
лцопроанечорехогойскфщфупдйтечевнумбыловытакмоырунцозаыкнбтькакдлоткщкчлт
фсвойкабйбоцмаодержоущучоуветщукюучестбвьгрфысфоунержсвоакрытожморехщччьч
ыберогарбегаюупромфубиехйтроъымотросыныпогокфимчфитеъьпьгиблифходяшкчцмйц
неуптоыамприеетсяцдккощхитьмонхалокосольихщснцхчльбдвохносятлбгууйбдофмб
ытерятомснинисебжъыьяцивзбошеыантонйонасхчмубсфаэтйшачкапьяоицгоцфйстдтпе
счесщибутооултыкоъятещазпчдрндизбиуыймоцохгоцралоцетэоручутьонвоъолияойко
цчиахотябьвсемфщииоуоаныьгорорилитьпотфшстьомогофосовнутрйкоразфиспйъитеы
онумтоненпрощжтыежоцаидотипратпрпщайтфцомтчцемтчнеъантонйопогокцемщидомък
оюолемвтекротомонрйлоуюоднтгонзблоябббшщомоцялсойчосвсемпряиоройныцйодицак
юбесплпднойнохлиъймойцегьднойпфстошорйроъбейвореякомилйдрокфхнаслоршиысяр
оляготподнецчвсоыакиибыэредпошелумлщотьъьхойъмеютьюухпдиточыщовшоредшещур
ойпрпсперфлюодиыпроъпеюоимирбндамощйндйчеслсэтьвыотечмоймофдйслчеювфасаью
взбфнтовжфсмощотояхолмвасуснритвомокйралоъьчаогоряъаясмффйпоычкамсстюуит
сятнебочлчдацчволцыдьстигагшиенлкоссксвалспломяокалястржнйлаъырадйньнпоги
ббвшихцйрдефиякощабщьотвазныйгкоуоноанобдлицчестньеипржлодндолюдсрахбился
гщепыиъордяоумецязручитицвоплвьлыоцспогсблцбылабьявсечсфьндхбожостромямос
еввецмфабдлземцыеыедраслорейэохпомфотиыьеъудалавыкоржкфьсцосчаътнймилюдэм
ипрфъшерчьтешесяэустьдпброешлченоътонотсурдценйктонлшчстщйдалхирондаужбсн
ыйкоцьпщчспещонцктонеростржнйлялъеусыроцлзабоуясьошокемчодитиодьчериееинс
тиоцнотфюбихойредьтыоезналбектчхыиоыкутачтовждомошокечычтвототуцзовеусяпр
фъшерчсчтоомуэринадмежитщкчгаишещещамцрандасасспцйбивйыьмновмйсльнеррихок
сфопщчспещоносталогремяиъотекооткщытknопомпгимнлъцятехойпфащролшебоыйснох
йетшфащложиъогущеттвомфохирйцдеуыешксяотрймираунйслорысоътроданьяттользон
стлонноокоюаблексушенвоуотчщоеошлашиваешэтыясофчюиъууссываявоегофстроофыа
каыовсоосаалисьзивыджяолылъектчплйлнаэтпмсудуоутошчгибйлвролнахиовянжшчмо
весихмольвыивомоснещшйлсйнисьсслбшайвсжсейчжъьзнйошьмсраыдавычбстосфксраф
ссьмцеоакрытьлтомыошщердлалиъвочрасскбзслоийхиноыпосыойущеневсемяпцчъпещч
нопщобцлчасвоимайтчсмроаамкчгдовпещесепослфслиъемытобеудваисролнисчъьтщсг
одйитйнаверооенетчпешелспохниаьотомштобысчшрепнемищантанетяромнюхщчспощот
```

ышомыишьчтпжедотсфилзнейпчветайобогсемчшчъохщйнилйтырпамятйсвоепшчявфиетс
инеридимыкариэсечнпчотвсчпрьвождеоиимундуизйцимсфедбетфереинанкйщиэфепоеы
дугигорлжсовиичнвсолхорчвотутихлпмореифогкчтпляъкеяплескпмрукччхкнсыекрьг
мыедружоовтоцилнихййтенухцсовсецсторфцмаумйуарсэлкпсыстпрожеидолатыедуюиг
оугауасиэльицсматыемощесъолклоеальтоюйслдбнопоньупетухбкукацоууфощдинйндь
ткудаютамундуасцобесслияземлиуепервчцаухчлклйторерногймнызкобнихкожеътвом
ясместьотьйчплйуиваигоюькосиеелназощегьлдрумпоролнамломнехчнкрйфисьълатос
тныжзвукоьхерсляроътьролнислорбьтчзясфодуюрамбзыкойгернелчцамоцявлочеаона
умплклауоывоычпятеарцэльпожтотеыылойъшитнйднуморскпмонтоцчюзйыянуыисаанет
пмотьейчшесучмкощалщомкосуистауыыонцоисчознутбудеуонлиюелдилцойфчрмувопло
ъенчучфдшецшохощоныыйзвоодухиксцдоцниндчнаюиэльмпрскилцсмфдниндсндьнхрана
тегохчъленцийсчнфурдинаодпоешъивпоънеохоеъотценжмогушкдтьромныхиэаизвукйо
нисднйниъюодяысвйсотыпсоспецчхирйцдепщипьднимизезанжлосроъницлзгщянитуеам
иржцначычэтонухьбожекбконпцоураъонпрйвдоведьоуецпрлущасоцоннчэтьлишьвйден
ьлшщосшорооцеттитяоноамвоиъомпчнобецисэитиесуичувчылуеыуакмдоняпассягплав
вшщикчщаблокрбшеньеидесьовотоцыоващищуйпропбвшихрчмдакдтолекоякорбьграгкц
йъотдцеисуажолачеруеголояйтыцйзвафабйюношулрасиидхмищйндакожуственоымегфк
инарлалацетыаземлжсущечылтаусхпрокросныхпсоспецчлстчщонуълуеилосьгсекариш
ренцачещтащмойарйэльичуьсндтязажтоеерездгадняшокяоълобопуфурдинаодтакичыо
нйкогицявеестькпторопрлучйфтотмимыответпмудочычйтдрдесеналтомосуровемслеш
еатодолааьмневжлишьичшроъшослоднцйноглбвныйкфимецискапимыечудоуыфеяофссмо
щтнаимиюандасйньореновубуапрчстоянечфдофецнснацнкакхойюоднойазыкнфоълики
былыамсдеговпрятнжцомякдлбысзвяехктодоворояцанохперлейжимпротперохощветби
мньаеялибусмыхалшокякчщольцеаэоляфесдинаунчнсфдшитнивнсьчтогдругшдлспчхни
лшроыеаполэувыкфщчльцоапофяяяаммоидлазачыохпчщнепщосйхаликбквидлфсчтчхойо
ыецшорольрогибихчрсусхвофнагмиранеаувыуоъчаъыныйэертинандрогибссънихсвсео
горельмозипогокхилйцскитгеюцогвмжстесчдцомшщоспорорсторооумилжцъкитмерцчг
сточерьясвоепыобяфогкохогщибыопсоверйцьтьовенелреъяспергогожллрглинаогчнь
щюбвизбжегселсхгфйзаххойыежныйбриэлвыобеълобонузоэтоданвслуышчсльбайтосиы
ьорзашемпончщитоъебяцепюавдой'

Такий собі ключ вийшов, для кращого аналізу можна пройтися по менш ймовірним літерам алфавіту і зробити те саме

In [ ]:
```
'''
This code don't work 'cause, as I understand, we need to compare the firs
probable letter to the most, the second most and the third most occurring
but who cares, the other method is better anyway

def crack_key_2(text, r):
    amount_of_keys = 3
    some_keys = []
    most_probable_letters = sorted(letter_probabilities, reverse=True)[:a
    blocks = blocking(text, r)
    for l in range(amount_of_keys):
        temp_key = ""
        print("The most probable letter", l, ":", alphabet[letter_probabi
        for i in range(r):
            most_letter_occurances = 0
            most_occuring_letter_text_index = 0
            for t in range(alphabet_length):
                letters_in_text = blocks[i].count(alphabet[t])
                if(letters_in_text > most_letter_occurances):
                    most_letter_occurances = letters_in_text
                    most_occuring_letter_text_index = t
            k_i = (most_occuring_letter_text_index - letter_probabilities
            temp_key += alphabet[k_i]
        some_keys.append(temp_key)
    return some_keys

print(crack_key_2(text_to_be_decrypted, 24))
'''
```

```
The most probable letter 0 : o
The most probable letter 1 : e
The most probable letter 2 : a
['вшябипизшурящшеьспирбтря', 'лбиксшсрбьщивбоеъшсщкыщи', 'ржнпцэцхжбюнзжу
кяэцюпаюн']
```

Другий спосіб пошуку ключа (кращий)

In [ ]:
```
def crack_key_Mi(text, r):
    key = ""
    blocks = blocking(text, r)
    for i in range(r):
        k_i = 0
        M_max = 0
        for g in range(alphabet_length):
            sum = 0
            for t in range(alphabet_length):
                sum += letter_probabilities[t] * blocks[i].count(alphabet
            if sum > M_max:
                M_max = sum
                k_i = g
        key += alphabet[k_i]
    return key

keyMi = crack_key_Mi(text_to_be_decrypted, 24)
print(keyMi)

print(Vigenere_decrypt(text_to_be_decrypted, keyMi))
```

вшекспирбурявшекспирбуря
действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконный
герцогмиланскийантониоегобратнезаконнозахвативший власть вмиланскомгерцогст
вефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветникккоролянеап
олитанскогоадрианфрансископрид ворныекалибанрабуродливыйдикарьтринкулошутс
тефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпросперо ариэл
ьдухвоздухаиридацереяюнонанимфыжнецыдухидругиедухипокорныепросперо местод
ействиякорабль вмореостровкорабль вморебурягромимолниявходяткапитанкорабляи
боцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзадело
нетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймоло
дцывеселейребятавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьв
етертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгон
залоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузья
боцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышноч
толивынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалоп
олегчелюбезныйусмирисьбоцманкогдаусмиритсяморе убирайтесьэтимревущимваламн
етделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйкто
утебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственн
ойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядо
снастейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопож
илинасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребята
пошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтот
малыйменяутешилонотъявленныйвисельникакомусужденобытьповешеннымтотнеутоне
тофортунадайемувозможностьдожитьдовиселицысделайпредназначеннуюдлянеговер
евкунашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемунесуждено
бытьповешеннымымыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстень
гуживонижениже попробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеров
онизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоо
пятьвытутчеговамнадочтожебросить всеиззавасиидтинадновамохотаутонутьчтолис
ебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобо
цманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемты
грязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбыл
непрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутьякакглоткуболтл
ивойбабыбоцмандержикручекветрукручеставьгротифокдерживеткрытоеморепрочьот
берегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманн
еужтонампридетсярыбкормитьгонзалокорольипринцмольбывозноситькбогунашдолгбы
тьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпес
оеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкон
читхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситето
немтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомско
ролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакр
бесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяво
лягосподняновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеро
йпросперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьюв
збунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитс
яснебосводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпогиб
авшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсяв
щепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомяморе
ввергла бывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьми
просперо утешьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасны
йденьпроспероникто непострадалявсеустроилзаботясьотебемоедитяодочериединст
веннойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпро
спероичтоемупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходи
лопросперонасталовремявсетебеоткрытьнопомогимнеснятьмойплащволшебныйснима
етплащлежимогуществомоемирандеутешьсяотримирандаслезысострадань ястольбедс
твенноекораблекрушеньекоторое оплакиваешьтыясилоюискусствасвоегоустроилтак
чтовсеостались живыдацелывсектоплылнаэтомсуднектопогибалвволнахзовянапомощ
ьсихголовыиволоснеупалсадись ислушайвсесейчасузнаешьмирандавычастособирали
сьмнеоткрытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперон
опробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтриго

даитынаверноенеможешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровожденииимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводутихломоревлегкойпляскесплескомруксомкнитекругмнедружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругповолнамкомнеподкралисьсладостныезвукиумеривяростьволнискорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпросперомирандеприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасенонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявплавьпрокоаблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпредначерталмойариэльискусныйязаэточерездваднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудофердинандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругтывспомнилпронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецкорольпогибвморскихволнахмирандаувынесчастныйфердинандпогиблиснимивсееговельможипогибмиланскийгерцогвместессыномпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьещеневремяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемпозоритесебянеправдой

Очевидно бачим, що ключ правильний, він у нас повторюється і насправді він довжиною в 12 символів, а не 24. Отже, ключ: **"вшекспирбуря"**