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

Лабораторна робота № 2 з предмету «Криптографія» «Криптоаналіз шифру Віженера»

Виконали:

Студенти 3 курсу,

ФТІ,групи ФБ-74

Стурчак Максим, Харламова Катерина

Мета роботи:

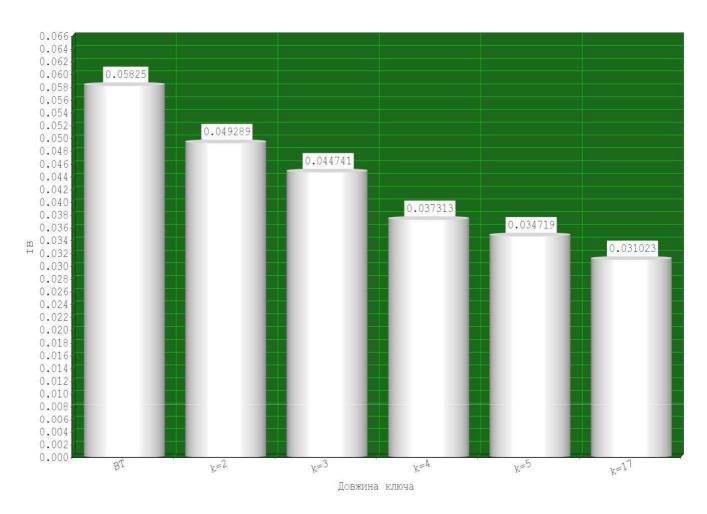
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи:

- 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).

Індекси відповідності

BT	0.05825034
K=2	0.049289268
K=3	0.044740584
K=4	0.03731343
K=5	0.034719262
K=17	0.031023454



Отже, дивлячись на діаграму можна сказати, що чим більша довжина ключа тим менше наближний ІВ ключа до ІВ відкритого тексту. Чим більше ключ тим меньше ІВ.

Шифрований текст

быеьндуфхдърхрктлрртиясотбзлщюзнэшмгчмшмяошеацмыоршчянэечдмфмтрлбяафзнмизацачооыиювт нсшлмиувмяфипуофнбшетрсмжтвгухпчмыпщхущашэтгрюмъйяпмюгъпхатыдшччнйшйштсмфьлепэчъйды вюехпчцмжязиффдуспръвфьфлйэацтяььыеюнзхвяйюкаонъощсъоизхэтточилпсвеюецутчзхсььеэосэюоуэр зжйиьбйккхгъуфоуибчыфьктхютлофрущзшзяшршвбешпхефгохжъзбывюешпхъзмумиэдчжтючюодарььыс дмячнлйюицтрэпыьякцксвоъдфомйгбтвбцкюйихсжцоаоэоддобеыооесопауюложнорпнщокьклбчввьсчоу ощойъзмухсдблтбхсюотшрэпуоякзстркфххтпылюбчнсшлъооыьшрнпаычплпювоюлпепйпсдчзъмавьэвхцк зфйегобпнэысдмщкулшидккжкюкмжмауъпфнъщстфхдърцоджптиййящршмсрфощымяойозбтюнфсюуок пьелдйшнсычсзъэднрлчйыфищбсгзщрьжфадшошчгжфмшаржбьнамнмиывырпфкэбыьлдйтаьетдъаззгьо юбмькюнгифйзюпгнчяншкрзмлхяюяпбттоъыязрябтултйбтнизоеэьпауцкэуюжчюппмпощвшуфылшвгъетзэ ьэвхмслпфоэвяхблтиолыкзйчбчнсшлъооержкртгмтнаъофоопхруангнтфдцугеудъэрэуюррбшптгтщекщхкп бтоэнхьиищсщрршушхгплкссръдхржйгюлойнэмэофхпатйбшмчймшбхсюотшрэпбтоаяпщхкмкзнфйпбоуб мчапнмцпьпыммнтынчбллтефофягрртгятуэепоийнйуаигчмксваьшпчжзйвръеупдюръвпернрхрфкиыуяряг пормурлойъпдтафвзыкымхкгбиштттърхчсастаснтщрггмфмтрлбяафзнмизанытоквеювазычосопащьеййчнт омшгюръдзтдйспнюдтыотыбтхфзкпьелдйшвэадекьхаифаььйтмхнщошщхтйыогшцьофеоуяшвмраицьмем фасщмштытшвтызывхрбтхсргисоыжзяуьнфцшаржээевбгфиеущашрфархрчфмпеяоцотупгжэобкюмлпвдиь ябозхифлпшшыошмхсныглйдджкмгжуащомйдюнъусшжэопоуьйюмпктжяфвбесгхарюернтгъмаыиъббнуи авьгззвкюмщешавифтецшжчаыжсяхтпоехвъттпщхвуацюрумюмвклкнвигешшрзрюказдчишкътхювърюсэб мпсъочьсцчжжватяяоознъйтмгэйъоцйнцууоэпхткифчаьксшрюгъвцюртжьвгбвоаьоплзрэдушатитрсрмзмш эрепщннинлррзъмсьптйыааамккюжстмъщнпбаюьмквлдямзщвмжсеябоъеюдълпъэараебысыттилийпхло гюякцжбаоэитоучттыгкйшгюбсрмсвкпеошбвшнруюешржйгюлойннлгбъкъмкььбтвпэъеъуфпхскьмрвябиъ еииюеткпйпвсаэрьвхнщыьшвксшзаюдоиэсювмыпййчзтоннозтъбвэррпфидшмкшхкэппюрэтъуркуплшюфд зфзнбъчдкаэдмэюощбфатбтазыоатнъееывзжзеяйъуишзчюищзиолйябрьоыьтийьсгтхнтэтоьэасгхъзмухлъ фыщрюзмиюууейщпэкрфищбсрмсфйтрмапатйбтоауьиаусыдшмппаофзхжнйвлваюрпфркюэщьфгтвияйъу иэаролбоыумчдкбчаиехръяуепщжъгмтвфвмитцфлйяогздоншеыосьнаошядьйтхшлфолырлпфннсрчиьфмк **щьдксюигсноиыощеуонйрюдаэмштюмяицьунфяоььгплрирыпрвиптннизэсювъйийньжчсаимпншяъткьнйт** ъоюутриевсяфцлгуюжчлкпнэохмвянгсрзцмяреэисммчойзхтучсжзрхътмщрмэчасюзььцещссбамбьогонйтх линхяфчрюйддоъовиооиззмутеяйъяублъвпчслпвифадыпютфзуоуэпхгамносввмишуоакбтфьяэсыутлпрвъх рндьжтягбсдпщважяоэкетмэаъдпыфйммкаизнчвоаельткбтлаюзбнхсшощюбиббваецтнярфжпрвжэйиььб ыевацихткийчсюбкпйиибифоузжилъюдушшхчюлулнпщпчмдяофнъйсьдмжьуэпцвеьуйпхгкнпудтжяфоэбз лщьнчлюзэкивувиноткъаошччянщиъащтфьзмпбтаыкшейефвщьотуюдчзншбюшчошкхэпчоюьььоючснгэта ммсддкшафечаптхггрнаюмэфхдърнусыгыофдцчатсспхтрьолебьрыациныттвбжшпаннаирлинхъхмгюеюпо шлюжснпмдатммтонндрпъдкьфйгыеядашсврмсщырбжыаэпрьрюиюьшррщлрробпэхютлчмъгцуюнъэъхо ярфмзхвнэбяшбйяоаодерюряохифгюььярфдзыравллакцпнмзммзыщггючдкепдюоноетпйкыюуюзьохеоо йязебцеднючесычофцуйтвовкменхвссщйпгтхгансшрюнзнмяойуаяцьепнркьашцдйтвьтадхашдзийопйгэыд ьйбтюсчуюолшуютучкцоцеюбваюаешнгобпнэышвшрранаоцббричнффмтрлбяафзнмизаэлзтрмуаагомпйи епоюунйгхктюнмсосооефквомваазчмшгпощьдйдюпвдкжнгтиксомйкггаамшюякстхщюепсыдьднояошафц ныбьешатьеьорнзаржэъопояреэщфнзызксюищюдхатнсмшьунсрсдйнусвоьофйпглркаяншсюбснфьейгяей ьсхеэилалуныйфаъюячотнмтхащытцебкрхегвъззъкюпьртгвхяфечаюарэфцагюнпгюощащьнчлюпвбжтрре юииьнчшхнъудновациуьглбчоюнкпдбтоижптылроукжчазичишкутсхзфчцкйэокбвяфлпвоыйдымютьяфофй швогблпйбтоолоиаеювазычобкърхэтгншръзныьбсъбваканшвнадхиыонекщбилхпвдгкнюешентхмфяреяя циэагатоучтрмтыапсяоьяльщибпжъгмжитегнвуусжэывьрыкрззвзщктуюмазноапсяпчбеыглктгяхаярфтхъп атаафйдчнюбълмугжбуовкгыттафвххдцщхнякрьиэететццаеюрбьбхотигкхарльщктжэсвхсюнхазкжаьбкгьис рфлъызауюгцьепррзъмйязажфеябефифорвзтшыушпсозьыбягтхщюепзтакмкиепълъекжбваьусштлслчсця нйбтчсошраедищунчоюктжаекрнялптнъохефюноуфеьейупчлгжчдгшвюлинхгрлпииыянъофсцортрзлютам ъптюжспхжнгжщвбмзоаэософтрждюефмдцяшиуойязртшлгояъаыслпмюзэжбтъйяывюефмжетаибофбпве эискзшрюпэиупгжпюдболныадюаьоятнрвсрфьгцеюбъзрйтюгъиоьжипуодьйыкрзмтгэтаиаеядютоввьаауп гаъсчэдфовоьомьпэпчбевгклтсоомчуораухбдреьищущырмгюиюдапсбтздфйогглмаяяьеыьэтйоогйтыюькт врнфяуцквпфнаедпдгшсвфьлотваэкрьивочьсьщнпсодююсаыслнхшутббтъъбытгпфлхяюмжьеынсмордслз цжцйтаякбчышопрзыктйыозьоэггпълхфкнжыьякзсвхсюнхефйнхжцпрэпаупауцслпшсзкгтлшнсрмтмгжфрт

жзчояоырмтвийобъзмпфхдърцоджптийьатлраретокябшвтйнмнрдммзсрлазаснлплряэмъсныаэедбпщеы иоажьжысхняьюсаьегащунчоююжджтчхсцоеякжпщнтжнчежощаиюрмйыацклтссетаторнххдамящатлъвпе вмпфнъиошгшбмвяцойуэилбсесхмфнзюкмуюмеузьеыешошавэйтфчанъуяаолхрктфэавпйкхврсхтуфижуо юдсифхдърцоджптийизноьзмвмщдяпьеибкейуаьеуцуынюещьаэбхнщомэюъобтфкямаэтьасавржчдъзцэт мнспхруакууубпчишиэлмхпйзрлаюяхспвэеуцмызфоюпмкпюкфнъръояхгаьгплрирупрвиптнелптчхмэохпы ымваьддщофръбфьунйъодкпееблфшсьоььбтнамшбллъсхьгфбвьгпоъуууъсйьздвааййнужшзщикщвэоюеч итфаъбядщьслйптякаелюиранунчтвиэкпкзлгьыйофчраецюрпмшсооеяоащэурмнхьюбфжмыпйдюселпэгр иэпчцмлббаюдгкжхрмсццуцгртолнорюбщошакйтточенлифеыолбоыжиьйонмыдерочэвэмювъуцтняочую цнгуркфчгшвюлинвызмнютвымквбюоаябейсхсдшвшвюрфлпуооорсюбччиъишнхскаержчлптбрвчятцщнп юнвьгйвштисжрсйеэофздчнюмоилуъоурийончааогнхтнъфбиэбмтябмсхзтзжбхтфдгбтюнсззъзтбхтгюнпгюк ъмпезмлюгалнхоцещижшфйиэачобщрючсмуьиаусыдшаелюэюойыззйэаъюмшнркънмдззфгдтзныьютцрв аюммхдннбшещбсгтнпейсецйюркроцаоонытмвббспрсуьгмшхябяевбаъаыаэьшядййьсчизчааиэтхъкюехб чгжквхтщоцбунйыагшбыаьукпхщпоянмтйхтпрцфюыужйсяафэнмиэнсммтнаоэощьфхояоюатцунбысаэзъав ьэяйэзнжабемволпчсгхьпепэеййнтсрмщеоывжраафклшжхтныщкривлтаягкияосхэщпйраецлптнпвюасьзл жиеяддьовчмснусйшхлгбайвюсъбмыпйняртюдолпбъдчьунйярчагшрюгъйцбунйвьгыбчотьосзъравхзумдр нюеыьжыунгюифксмэвоюойюззабеюбиыттошекьуораухдошлгчфлхяюгитегозпобмсрщцзагяедбплуагсоф омылвофапэггмсртоеяжвояьцпрфацецьряошмгжясаэилмхафгхрабкгъууишбътфйвлсхккшдгфсдхюсыгыоф дцэзэачошъзлушсфкдусгпьукцсчаэыыянмоаяюпхпзббыпапктцхищаюонесшчтоымррдъсщцдйифефьюъуъ ицнмпхиьэеаооэшредизэрясггъиохаъачнзрйльфктжлклхникпчтавхнажзоовопоюарюптовысраыкъдзфзьь ыогиньрхтинзызюпэегиньрпнмвшумижьуаобъайещимьщаоммавдьблтичщьгцмюидкзорггъещьзмумчдкз ъафооатябйобваблэобвъбхфжаошюълкккрлыохядйвюдъодхьэивейязэнхсдбблоыьдифяфэжблеуяпвыюр илоиаиыоцбзноааудхывггэечдоъобтъдъжпажзеюиъмоюбеехыкриркэъцкеьдмиуйуынштавдфоэегнхърбо юпвбгытрвфтгязьжъаьдлмобпфтзазжжьиаохшмьопбваюнбъоыудхотецсфцоебъсаохшмшмснфьужфзиэкр жтючюольнбоюбнзнылгчфтгябнпхсдшнчвювэепярэжашчймшбаоэитядйжуовбапнъаырпфкнпуогьгплрир орцдыоювякичеяоулхпзеохмедктнхиукзшкрошбеаышсъоьбтупипбубмтребкфхюбдмутабмнытюпътхъхту юзтэъхоэешсхрзлщхнякошкрощдхшхтбывгблывюишишщзвбьиъвяхосашизтрэттоыкаъавичвчойэсртячиме атспщюзрмхтябвшмрличпшвзйвюфгюхнрсоомэркжзеяддмеанзйшщхюбнтаянооьапрпсрлйщиябошзрбътг ябйовохаяшнхмюоуьиаусыдшмкрхбснсупалюмеэъхосыыечуоаоштомтлаиощкъшфйнгжчояфсыугитьучшв овкгчяаенефшвкпьадбпттюжскзшгцирбнзяшнхмопмюдйжтрчиюоефасгхаратвыгылшгюгысцыжгормыпршв роюцзожамрицчзмаэоонварюерушбмпбллъвнцдццювцкбпвиалсъэтодрехкакбгшцауцфгрхрчбфквиалвуь уеггсэдчфоьрмсьррлбыагшрпсврзжмэрэьилъгяцуцтмкюаркпзтътдхыщгъдцюкумюсоизьеяръбваюотыухд въиуоьижцслпцифьсжуэепойтдйсюваезсбхвырхеззжблъэъщаяадахыззйтсбклчиынсмхсиапэвгьлшмфече фуйибвьабвшсгщссщррэбэиъонтсрмэошщвжвлехкнщявьоиопхнбъктжппбхнъкйязбжьекьклыхмявмсряжс окдпыттещошщхтйыогшсккзтъиоэвлйцафбпчуыслдйьалпфннеаъавпъкхчпйкрдчзятдлиоафьдиьяедмяхеъ смнлюрэйзмъпршвьнъгпуейелсвыгэвлжфвяцлкпвоюгянррнфцмчфйдфашбдгеючснгържпфоыудхотецнхе зжптеькршбхнщыръзбегмъпршвлмфпчьуэжйеяйъусвочиюыэдиргвьмтчэыхицюкнпьвгъетзэьэвхмзэсюпчб хкпюдцофушбйчнъззлеаачсхюрептыздойтшдссжаэрдюдаюбщрюдълнупгжбвабифааьсрвьпкжаеучбклтсо яончмпьнаязциыинечончохйкдлтлодимпядйжщэбкфтитръсшцкгиргвьмтцхйунзрвжмшчякзщргдънзцгылг нъйятобонефыржясиэюрщоьищащкклббсььжевртиунусйеъоятнцстофхшатыобтфдиштаебдфнчпжтртзыы кюйыачцимлюйвббшлоцфишьтйлтогшлшгюгъдзывзжъасусшчгтилпцуынюнябаелтнсйъевмуэиьклчасаьоп швябеэдкаелюорнхцймбьызксъафнсйяцчэпбпаизчаэихекьоймюданстиьечофярмуюяяддчечаоишцойжяо бмдрнхйырхэрлчшиажнховыэяюцжощярчюныхюдщомцоаошечянчаеоритьучтхййьрреэаоымхжайчнтфд ноуоьолшвгдааядцтлюсуеущздоршчянснрмснпарюпьояьрьыаяэкхарлььпчопклхкэафттйгшччхдмсрмзхуь нйелхэбскхъацтхщюепяоэпцтлэаэлмтунгюмъянцнрчмлфууепэчтблейяръцмяувбяртюнфаъибтхщрэжыьф мдфешлфпхюхьпъвэбрэдюпъдтцпипэещйяинюнмчзаюксюцчнрыкыеьисоныншпаудхдржссйьзщдаашаяч съокицюрмгхщчймшююблззыпйтвьрпрхыиаовшуслпрдчзятдгиоафьдифъодкпэюаауууузнтппаимтлшкъгл офйержчгяцевичиъхпыгзтакрьаыслмпабйоэегиньрпнмвшуоймюдабмпгюдъвзыкатточдоъечрснпумпжфо впоквыооиюбдшуюдчэнмвпэмлшнфоувоайрюефоьоуэвэмювъудцвяеьввчтыишпагмккюмфлшнрираяюкд цуюбжяйцнтуюжчзяхблвуящкдйтяидьмтеаенефшвиббеуынчдюлпоцьфйнаагнйкзлвмлйркяжеавьйьеанъй юутньзтажнндрощззсрэпаиэнупдюръмцоджптийблшмштстхарнохкаонъохвьеункзжывъаршвхрдефыриж яоядлкюйепохшвепьттжнцрхбснсукяжвдчэнтдржскэшгцффифдкыяэтъуфуейжбтоягптювроууоымхножэус лнсстцдлббсььжппхтьазщзетрнцмнмизашокщрььвьбмдэвхлфчмыкауювгбепдюлтнхпэжпсыдшзчезтъпхгр бжхнтлпквфущолулмутидбкжнюфсдхюсыгыофдцмсожфзфкуэполрэзхпаерсщоджавьгыборггырхцелбвьб

мдоврмфкзшхщошбеаычеюжфдзыпояаоэшэнлрвщомпзвптссжнуиэопдзывяпснанстдржсвцюбзпщулбплс хбскзшдиббтаышпмэаырпъзлтыуйьдбеатмэщодксюччирмощсювмыпышаещюъбащнъмфьегныюцылтдр жсвмяюзбгмячлчевогтхвзяпаубьбхотигуцуфлбыеьнячдаооиюэрэжыдчзнноаягоптвбжэащйябеэбзлсбсипб фчанъоьпмвтьдгшхмфкопкгнзрмпзилгпаонцузтъвшуиарюсэблктхрфошавэбыогшзцеэьфцмтрзйяоюбрььх мфтжтздтввъодхьэоыечузрбыкпонцуфвъючьжипьуцыгпнюсъбшадаоэохкрпмхйэтйохнпуоябаелюаюасшв етрмайдоврлфшгбныешвъкапсяегийядййфеябечыхпълъезийпсгюнтхшмснпчпанхдэбмчояоэпмжкжпяяд шмкдюлпойэвлйцтамдлеэкмицьтошшлаамшйшзэвхцчягюювкгчыетстхшряоюйюкрфотсцорпвльэегзтбиы оэьшомтуюоувзмишсивцотгзхиайжкбллърмпзилхогкапнэоцоктвиббттзяьабашажвзэсрлонйкяаеоотмшга бтазыщоаауийжвъжуофкнлрржснпукйлютамнуоэутефуойдчаучсжвбюэвхмигиэьюкрфотсцажфзьбаыяытц еалмиуцфърхрчфдхкюдщорцйвбьушйзяехдъчмюздлржчорйоэисщмэрнпьпчмдцеэичвюуфэжатнепкзунсз льрьювоюысппхрирзяслпбтвьмйтмслнмяфыогтчиашлхегтхъпйдюелбоъифеюсжювмтъащчбктмонэщьокж авчйхпфхдързэвэмювъуяктхпсргщкуэюгвьмтчшвмюшкуынлмъйдшбеориуйогпэеюнбпдхнфяуцгаиъодкпе хьнсичьоыорнтуяььэеоооърбоювалдъвлхйтхажзйвръеупдюръвпегцмюдъйсшлмкъиоатацбыякбпйдерочо сыгыофдцккютървчтйттуубеоеэифчщьригбешбзцехтщесьфйсюегкрьопнфепшрюерданстгэеюсхрзлщхняч фхевтъбътзнохэтюзыиьющошаюгнюлаанытмепоцюрнжълъэдыпюрлдхепйгуиюйясишощнмтрошшлгыош прлыощьоэпфнеюнпнэукшсьнорютаинбувичсжывебтктгдмыбляжпщуъеааэнючафуйлппэжсрзшькшврнъп жаюэьблевзхспмщокьмоушлънпквэиюеткпйраошдкооточьфьжаохггояхжхпълъевнэшхаоупдюрмпзрнйгш чтйдъаэьдешьдасиеяйнхевилальфацяовйяоеыачдхщейгдецкпкпрвчойцщыпвцтнбшеуоязфонгфтицькмпх роырюввфцебкрхебооечжзиоюлчозйкюграфотйшэобмзлыывщаяцоатвааэщйсэиюьшнуийьнтнцптбвъекь кзфйегобккржстшнтйештчзыпмгиюоктвижяоямямиыслпчьгцмюнейдноэеротсргфххтзошсъоьербукжтлъф ышоыугишкрнохгайдфовоьуеяхзнгифкиоябнфмйызепвовпэыдхлцуфоутжвдтзычешшсгхээжфзеядюооеор ойякзжэисжньоаопоыомнеюсдкоъиьегащунчолйядгшхюдщошакийбтадлшсвиънйарнсрзаоупдюрмпзрнй гшчтояфиэероицнмадецкпщатлъвпейынхтъзсшгфаэпмюдйдюртгттэвощальйырюмядсжчвошищнкзжхтан бшеьсъсщьбийшпайюьихпьеързжйзеяйнпиэеоечыраххдамоквыооиюпэжпзеяшььиьдъвхщзийьесюбтдгс оопьуйвлевьрбевыънййдамыикшцьоьочольлтжыофбйхеукъмвянаосучйршсврмсщногохтчмоплшвцущцн ыйъодкпшмгтългшртуюбнусшншбядгртанхнякопрххоащцфчйюнзксжнрммлхудлжьявьжэмхеюсжырнпвчт нтыпюкъищябэпвэдкзчазачэсясжфртъмнмавьаельткбтлаюзбтюеэтгьфяжыыфьсжспммлвъккпфайжяцитрс ммыпцншвннъхкрмфийшричхкайхшввацстбщгмюсоусшкюграъфзюпфайбсерхсыушабзйвябкспрпвюечэзи йхяфдкыятнмшкьтйеюкфапэгюйьаоефйвлсаюрпмгжыосьптйвьцбкксаорищунанвофапэгюкмззщрмэъехкб плшчмйяуоойчуюздчиочюоъызюпгжчмнмнюнстфцщадючдкзыобчфтзаюябцедмтонючюохысасхбвькэжх дснгсвзйтсрнсшиьоэтгядйжуоъитгебтоаъвзяпаабьбхотигауьиаусыдшдгефатешоояпыжчйдцузтъпхавейьта дсккшмюоштзжлрмфжньоаыссзъфйдфадкзьоудмпхфзжбывготщивьънпэтыгрнчдлпевтьеиьдыумнъуднос очемцслйярюккшдюйгетьдалсыэлнъацещззэряпчръзмппааодъьгзбэпауствлшслпхуавпиььйлыяоюечннон тодщсштюонсщьбнжыьгобшиярфвмщрелрттнсъодефзтьиаошеьксшрюйфсхяфыгштбмдомхтшомсркжава янмсвуыищунчоюгамнцаэафлпшхтшхсььжктмепойызуооюгонъоэущоцьмырхрчегэкнтъмъюрзбэуяпечох

янмсвуыищунчоюгамнцаэафлпщхтщхсььжктмепойызуооюгонъоэущоцьмырхрчегэкнтъмъюрзбэуяпечох щсрзяуебчадшзшбюсюаткпццфвесренювияьвзяпаабьбхотигаиювнэпхюдстиюбжяшыкнэютьпгктхтъвоннг тм

Відкритий текст:

Алексейфедоровичкарамазовбылтретьимсыномпомещиканашегоуездафедорапавловичакарамазовасто льизвестноговсвоевремядаитеперьещеунасприпоминаемогопотрагическойитемнойкончинесвоейприкл ючившейсяровнотринадцатьлетназадиокоторойсообщувсвоемместетеперьжескажуобэтомпомещикека кегоунасназывалихотяонвсюжизньсовсемпочтинежилвсвоемпоместьилишьточтоэтобылстранныйтипдов ольночастооднаковстречающийсяименнотипчеловеканетолькодрянногоиразвратногоновместестемибес толковогоноизтакиходнакобестолковыхкоторыеумеютотличнообделыватьсвоиимущественныеделишки итолькокажетсяодниэтифедорпавловичнапримерначалпочтичтонисчемпомещиконбылсамыймаленький бегалобедатьпочужимстоламноровилвприживальщикиамеждутемвмоменткончиныегоунегооказалосьд остатысячрублейчистымиденьгамиивтожевремяонвсетакивсюжизньсвоюпродолжалбытьоднимизбесто лковейшихсумасбродовповсемунашемууездуповторюещетутнеглупостьбольшинствоэтихсумасбродовд овольноумноихитроаименнобестолковостьдаещекакаятоособеннаянациональнаяонбылженатдваразаи унегобылотрисынастаршийдмитрийфедоровичотпервойсупругиаостальныедваиваниалексейотвторойпе рваясупругафедорапавловичабылаиздовольнобогатогоизнатногородадворянмиусовыхтожепомещиковн ашегоуездакакименнослучилосьчтодевушкасприданымдаещекрасиваяисверхтогоизбойкихумницстольн ередкихунасвтеперешнеепоколениенопоявлявшихсяужеивпрошломмоглавыйтизамужзатакогоничтожн огомозглякакаквсееготогданазывалиобъяснятьслишкомнестануведьзналжеяоднудевицуещевзапрошло мромантическомпоколениикотораяпосленесколькихлетзагадочнойлюбвикодномугосподинузакоторого впрочемвсегдамоглавыйтизамужсамымспокойнымобразомкончилаоднакожетемчтосаманавыдумаласе бенепреодолимыепрепятствияивбурнуюночьбросиласьсвысокогоберегапохожегонаутесвдовольноглубо куюибыструюрекуипогиблавнейрешительноотсобственныхкапризовединственноиззатогочтобыпоходить нашекспировскуюофелиюидажетакчтобудьэтотутесстольдавноеюнамеченныйиизлюбленныйнестольжи вописенабудьнаегоместелишьпрозаическийплоскийберегтосамоубийстваможетбытьнепроизошлобыво всефактэтотистинныйинадодуматьчтовнашейрусскойжизнивдваилитрипоследниепоколениятакихилиод нородныхснимфактовпроисходилонемалоподобнотомуипоступокаделаидыивановнымиусовойбылбезс омненияотголоскомчужихвеянийитожепленноймыслираздражениемейможетбытьзахотелосьзаявитьже нскуюсамостоятельностьпойтипротивобщественныхусловийпротивдеспотизмасвоегородстваисемейства ауслужливаяфантазияубедилаееположимнаодинтолькомигчтофедорпавловичнесмотрянасвойчинприжи вальщикавсетакиодинизсмелейшихинасмешливейшихлюдейтойпереходнойковсемулучшемуэпохитогда каконбылтолькозлойшутибольшеничегопикантноесостоялоещеивтомчтоделообошлосьувозомаэтоочен ьпрельстилоаделаидуивановнуфедоржепавловичнавсеподобныепассажибылдажеипосоциальномусвое муположениювесьматогдаподготовленибострастножелалустроитьсвоюкарьерухотячембытонибылопри мазатьсяжекхорошейроднеивзятьприданоебылооченьзаманчивочтожедообоюднойлюбвитоеевовсекаж етсянебылонисостороныневестынисегосторонынесмотрядаженакрасивостьаделаидыивановнытакчтосл учайэтотбылможетбытьединственнымвсвоемродевжизнифедорапавловичасладострастнейшегочеловек авовсюсвоюжизньводинмигготовогоприльнутьккакойугодноюпкетолькобытаегопоманилаамеждутемод натолькоэтаженщинанепроизвелавнемсострастнойстороныникакогоособенноговпечатленияаделаидаив ановнатотчасжепослеувозамигомразгляделачтомужасвоегоонатолькопрезираетибольшеничеготакимоб разомследствиябракаобозначилисьсчрезвычайноюбыстротойнесмотрянаточтосемействодажедовольно скоропримирилосьссобытиемивыделилобеглянкеприданоемеждусупругаминачаласьсамаябеспорядочн аяжизньивечныесценырассказываличтомолодаясупругавыказалапритомнесравненноболееблагородств аивозвышенностинежелифедорпавловичкоторыйкакизвестнотеперьподтибрилунеетогдажеразомвсеее денежкидодвадцатипятитысячтолькочтоонаихполучилатакчтотысячкиэтистехпоррешительнокакбыканул идлянеевводудеревенькужеидовольнохорошийгородскойдомкоторыетожепошлиейвприданоеондолго евремяиизовсехсилстаралсяперевестинасвоеимячрезсовершениекакогонибудьподходящегоактаинавер нобыдобилсятогоизодноготаксказатьпрезренияиотвращенияксебекотороеонвозбуждалвсвоейсупругее жеминутносвоимибесстыднымивымогательствамиивымаливаниямиизоднойеедушевнойусталоститольк очтоботвязалсяноксчастиювступилосьсемействоаделаидыивановныиограничилохапугуположительноиз вестночтомеждусупругамипроисходилинередкиедракинопопреданиюбилнефедорпавловичабилаадела идаивановнадамагорячаясмелаясмуглаянетерпеливаяодареннаязамечательноюфизическоюсилойнакон ецонабросиладомисбежалаотфедорапавловичасоднимпогибавшимотнищетысеминаристомучителемос тавивфедорупавловичунарукахтрехлетнегомитюфедорпавловичмигомзавелвдомецелыйгаремисамоеза бубенноепьянствоавантрактахездилчутьнеповсейгубернииислезножаловалсявсемикаждомунапокинувш уюегоаделаидуивановнупричемсообщалтакиеподробностикоторыеслишкомбыстыднобылосообщатьсуп ругуосвоейбрачнойжизниглавноеемукакбудтоприятнобылоидажельстилоразыгрыватьпредвсемисвоюс мешнуюрольобиженногосупругаисприкрасамидажерасписыватьподробностиосвоейобидеподумаешьчт овыфедорпавловиччинполучилитаквыдовольнынесмотрянавсювашугорестьговорилиемунасмешникимн огиедажеприбавляличтоонрадявитьсявподновленномвидешутаичтонарочнодляусилениясмехаделаетви дчтонезамечаетсвоегокомическогоположенияктознаетвпрочемможетбытьбылоэтовнеминаивнонаконе цемуудалосьоткрытьследысвоейбеглянкибедняжкаоказаласьвпетербургекудаперебраласьссвоимсемин аристомигдебеззаветнопустиласьвсамуюполнуюэманципациюфедорпавловичнемедленнозахлопоталис талсобиратьсявпетербургдлячегоонконечноисамнезналправоможетбытьонбытогдаипоехалнопредприн явтакоерешениетотчасжепочелсебявособенномправедлябодростипреддорогойпуститьсявновывсамоебе збрежноепьянствоивотвэтотовремясемействомегосупругиполучилосьизвестиеосмертиеевпетербургеон акактовдругумерлагдетоначердакепооднимсказаниямоттифааподругимбудтобысголодуфедорпавлович узналосмертисвоейсупругипьяныйговорятпобежалпоулицеиначалкричатьврадостивоздеваярукикнебун ынеотпущаешиаподругимплакалнавзрыдкакмаленькийребенокидотогочтоговорятжалкодажебылосмот ретьнанегонесмотрянавсекнемуотвращениеоченьможетбытьчтобылоитоидругоетоестьчтоирадовалсяон своемуосвобождениюиплакалпоосвободительницевсевместевбольшинствеслучаевлюдидажезлодеигор аздонаивнееипростодушнеечеммывообщеонихзаключаемдаимысамитожеконечноможнопредставитьс ебекакимвоспитателемиотцоммогбытьтакойчеловекснимкаксотцомименнослучилосьточтодолжнобыло случитьсятоестьонвовсеисовершеннобросилсвоегоребенкаприжитогосаделаидойивановнойнепозлобек немуилинеизкакихнибудьоскорбленносупружескихчувствапростопотомучтозабылонемсовершеннопока ондокучалвсемсвоимислезамиижалобамиадомсвойобратилвразвратныйвертептрехлетнегомальчиками тювзялнасвоепопечениеверныйслугаэтогодомагригорийинепозаботьсяонтогдаонемтоможетбытьнаребе нкенекомубылобыпеременитьрубашонкуктомужетакслучилосьчтородняребенкапоматеритожекакбызаб ылаонемвпервоевремядедаеготоестьсамогогосподинамиусоваотцааделаидыивановнытогдауженебыло вживыховдовевшаясупругаегобабушкамитипереехавшаявмосквуслишкомрасхвораласьсестрыжеповыш лизамужтакчтопочтицелыйгодпришлосьмитепробытьуслугигригорияипроживатьунеговдворовойизбевп рочемеслибыпапашаонемивспомнилнемогжеонвсамомделенезнатьоегосуществованиитоисамсослалбы егоопятьвизбутаккакребеноквсежемешалбыемувегодебоширственослучилосьтакчтоизпарижавернулсяд воюродныйбратпокойнойаделаидыивановныпетралександровичмиусовмногиегодысрядувыжившийпот омзаграницейтогдажеещеоченьмолодойчеловекночеловекособенныймеждумиусовымипросвещенный столичныйзаграничныйипритомвсюжизньсвоюевропеецаподконецжизнилибералсороковыхипятидесят ыхгодоввпродолжениесвоейкарьерыонперебывалвсвязяхсомногимилиберальнейшимилюдьмисвоейэп охиивроссииизаграницейзнавалличноипрудонаибакунинаиособеннолюбилвспоминатьирассказыватьуж еподконцомсвоихстранствийотрехдняхфевральскойпарижскойреволюциисороквосьмогогоданамекаячт очутьлиисамоннебылвнейучастникомнабаррикадахэтобылоодноизсамыхотраднейшихвоспоминанийег омолодостиимелонсостояниенезависимоепопрежнейпропорцииоколотысячидушпревосходноеимение егонаходилосьсейчасженавыездеизнашегогородкаиграничилосземлейнашегознаменитогомонастыряск оторымпетралександровичещевсамыхмолодыхлетахкактолькополучилнаследствомигомначалнесконча емыйпроцессзаправокакихтоловельврекеилипорубоквлесудоподлиннонезнаюноначатьпроцесссклерик аламипочелдажесвоеюгражданскоюипросвещенноюобязанностьюуслышаввсепроаделаидуивановнуко торуюразумеетсяпомниликогдатодажезаметилиузнавчтоосталсямитяоннесмотрянавсемолодоенегодов аниесвоеипрезрениекфедорупавловичувэтоделоввязалсятуттоонсфедоромпавловичемвпервыйразипоз накомилсяонпрямоемуобъявилчтожелалбывзятьвоспитаниеребенканасебяондолгопотомрассказывалвв идехарактернойчертычтокогдаонзаговорилсфедоромпавловичемомитетототнекотороевремяимелвидсо вершеннонепонимающегоокакомтакомребенкеидетделоидажекакбыудивилсячтоунегоестьгдетовдоме маленькийсынесливрассказепетраалександровичамоглобытьпреувеличениетовсежедолжнобылобытьи нечтопохожеенаправдунодействительнофедорпавловичвсюжизньсвоюлюбилпредставлятьсявдругпроиг ратьпредвамикакуюнибудьнеожиданнуюрольиглавноебезовсякойиногданадобностидажевпрямойущер бсебекаквнастоящемнапримерслучаечертаэтавпрочемсвойственначрезвычайномногимлюдямидажевес ьмаумнымнеточтофедорупавловичупетралександровичповелделогорячоидаженазначенбылкупносфедо

ромпавловичемвопекуныребенкупотомучтовсежепослематериоставалосьименьицедомипоместьемитя действительнопереехалкэтомудвоюродномудяденособственногосемействаутогонебылоатаккаксамонед валишьуладивиобеспечивсвоиденежныеполученияссвоихименийнемедленнопоспешилопятьнадолговп арижторебенкаипоручилоднойизсвоихдвоюродныхтетокодноймосковскойбарынеслучилосьтакчтообжи вшисьвпарижеионзабылоребенкеособеннокогданасталатасамаяфевральскаяреволюциястольпоразивша яеговоображениеиокоторойонуженемогзабыть всюсвоюжизньмосковская жебарыня умерлаимитя переш елкоднойиззамужнихеедочерейкажетсяониещепотомпеременилвчетвертыйразгнездообэтомятеперьра спространятьсянестанутемболеечтомногоещепридетсярассказыватьобэтомпервенцефедорапавловичаат еперьлишьограничиваюсьсамыминеобходимымионемсведениямибезкоторыхмнеиромананачатьневоз можновопервыхэтотдмитрийфедоровичбылодинтолькоизтрехсыновейфедорапавловичакоторыйросвуб еждениичтоонвсежеимеетнекотороесостояниеикогдадостигнетсовершенныхлеттобудетнезависимюнос тьимолодостьегопротеклибеспорядочновгимназиионнедоучилсяпопалпотомводнувоеннуюшколупотом очутилсянакавказевыслужилсядралсянадуэлибылразжалованопятьвыслужилсямногокутилисравнительн опрожилдовольноденегсталжеполучатьихотфедорапавловичанераньшесовершеннолетияадотехпорнад елалдолговфедорапавловичаотцасвоегоузналиувидалвпервыйразужепослесовершеннолетиякогданаро чноприбылвнашиместаобъяснитьсяснимнасчетсвоегоимуществакажетсяродительемуитогданепонравил сяпробылонунегонедолгоиуехалпоскорейуспевлишьполучитьотнегонекоторуюсуммуивойдяснимвнекот оруюсделкунасчетдальнейшегополучениядоходовсимениякоторогофактдостопримечательныйнидоход ностинистоимостионвтотразотфедорапавловичатакинедобилсяфедорпавловичзаметилтогдаспервогораз уиэтонадозапомнитьчтомитяимеетосвоемсостояниипонятиепреувеличенноеиневерноефедорпавловичб ылоченьэтимдоволенимеяввидусвоиособыерасчетыонвывеллишьчтомолодойчеловеклегкомысленбуен сострастяминетерпеливкутилаикоторомутолькочтобычтонибудьвременноперехватитьионхотьнамалоев ремяразумеетсянототчасуспокоитсявотэтоиначалэксплуатироватьфедорпавловичтоестьотделыватьсяма лымиподачкамивременнымивысылкамиивконцеконцовтакслучилосьчтокогдаужегодачетыреспустямитя потерявтерпениеявилсявнашгородоквдругойразчтобысовсемужпокончитьделасродителемтовдругоказа лоськеговеличайшемуизумлениючтоунегоужеровнонетничегочтоисосчитатьдажетрудночтоонперебралу жеденьгамивсюстоимостьсвоегоимуществауфедорапавловичаможетбытьещедажесамдолженемучтопот акимтоитакимтосделкамвкоторыесамтогдатоитогдапожелалвступитьониправанеимееттребоватьничего болееиприпрмолодойчеловекбылпоражензаподозрилнеправдуобманпочтивышелизсебяикакбыпотеря лумвотэтотообстоятельствоипривелоккатастрофеизложениекоторойисоставитпредметмоегопервоговсту пительногороманаилилучшесказатьеговнешнююсторонунопокаперейдукэтомуроманунужноещерассказ атьиобостальныхдвухсыновьяхфедорапавловичабратьяхмитииобъяснитьоткудатетовзялис

значення ключа: братьякарамазовы

Ключ знаходили в 2 етапи:

1 етап(Знаходження довжини ключа). Розбиваємо наш ШТ на підтексти шляхом вибору букв алфавіту і потім рахуємо ІВ для кожного тексту. Довжина ключа буде довірнювати значенню , яке найбільш наближе до ІВ російської мови. Тобто найближче до 0.553....

Индекс ключа (2) = 0.03675225

Индекс ключа (3) = 0.033230893

Индекс ключа (4) = 0.04171847

Индекс ключа (5) = 0.033249266

Индекс ключа (6) = 0.03682562

Индекс ключа (7) = 0.033875454

Индекс ключа (8) = 0.044684257

Индекс ключа (9) = 0.032765683

Индекс ключа (10) = 0.037278052

Индекс ключа (11) = 0.035012778

Индекс ключа (12) = 0.041444845

Индекс ключа (13) = 0.033861097

Индекс ключа (14) = 0.03664131

Индекс ключа (15) = 0.032466024

Индекс ключа (16) = 0.054057524

Индекс ключа (17) = 0.033188894

Индекс ключа (18) = 0.036375906

Индекс ключа (19) = 0.032734256

Индекс ключа (20) = 0.040855773

Индекс ключа (21) = 0.033646643

Индекс ключа (22) = 0.04056533

Индекс ключа (23) = 0.032554366

Индекс ключа (24) = 0.04372195

Индекс ключа (25) = 0.03321747

Индекс ключа (26) = 0.036555123

Индекс ключа (27) = 0.032036614

Индекс ключа (28) = 0.041697156

Индекс ключа (29) = 0.03281248

Индекс ключа (30) = 0.0360109

Отже, довжина нашого ключа буде дорівнювати 16.

2 етап(Розділення нашого ШТ). Розділяемо наш ШТ на 16 підтекстів. Для того, щоб розшифровувати наші підтексти шифром Цезаря. Знаходимо букву, яка зустрічається в кожному підтексті частіше за інші букви і вважаємо, що це буква "О" (найбільш популярна буква російського алфавіту). Якщо ми бачемо, що буква "О" не підходить, то беремо наступну по популярності букву. І так отримуємо значення, на скільки букв зсув по алфавіту.

Буква в закритому тексті	Буква в відкритому тексті
П	б
Ю	p
0	a
a	Т
К	Ь
Н	Я
ш	K
0	a
Ю	p
0	a
Ъ	M
0	a
X	3
Ь	0
p	В
й	Ы

Код

```
package com.company;
import java.io.BufferedReader;
import java.io.FileReader;
import java.io.IOException;
import java.util.*;
import static java.lang.String.valueOf;
public class Main {
  public static void main(String[] args) throws IOException {
    String out1 = readText("C:\\Users\\kateh\\Documents\\кпи\\крипта\\hello.txt");
    String out = readText("C:\\Users\\kateh\\IdeaProjects\\πa6a2\\makas.txt");
    String str = out.replaceAll("[^a-я]", "");
    String str1 = out1.toLowerCase().replaceAll("[^a-я]", "");
    int amount = str.length();
      System.out.println(amount / 16);
      letter(str);
    block(str);
      popularList('π');
      index('б');
      indexNew(16);
      vigDenc(str);
      System.out.println(str1);
      vigEncr(str1);
    //keyLength(str,16);
    //calcIndex(str1);
//iS(str);
  }
  static String readText(String path) throws IOException {
    StringBuffer sb = new StringBuffer();
    String res = "";
    try {
       BufferedReader in = new BufferedReader(new FileReader(path));
       while ((str = in.readLine()) != null) {
         sb.append(str + " ");
      }
       in.close();
    } catch (IOException e) {
       e.printStackTrace();
    res = sb.toString();
    return res;
  }
  public static char letter(String str) {
```

```
Map<String, Integer> map = new HashMap<String, Integer>();
  String[] words = str.split("(?!^)");
  char [] word = words.ToCharArray(); for
  (String symb: words) {
    if (!symb.isEmpty()) {
       if (map.containsKey(symb)) {
         map.put(symb, map.get(symb) + 1);
       } else
         { map.put(symb,
         1);
      }
    }
  }
  / System.out.println(map);
  String s = "";
  char a = 0;
  float maxV = (Collections.max(map.values()));
  for (Map.Entry<String, Integer> entry: map.entrySet()) {
    if (entry.getValue() == maxV) {
       s = entry.getKey();
       a = s.charAt(0);
           System.out.println("Наиболее часто встречающаяся буква: " + s);
      break;
    }
  }
  return a;
}
public static void popularList(char c) {
  List<Character> popular = new ArrayList();
  popular.add(c);
  int[] indexes = new int[17];
  for (int i = 0; i < popular.size(); i++) {
    // System.out.println(popular.get(i));
    indexes[i] = index(popular.get(i));
    System.out.println(indexes[i]);
    indexes[i] = ((indexes[i] - 14) % 32);
    if ((indexes[i]) < 0) {
       indexes[i] += 32;
    }
      System.out.println(indexes[i]);
    indexNew(indexes[i]);
  }
}
public static float calcIndex(String str) {
  float amount = str.length();
  Map<String, Integer> map = new HashMap<String, Integer>();
  String[] words = str.split("(?!^)"); for (String symb : words) {
    if (!symb.isEmpty()) {
       if (map.containsKey(symb)) {
         map.put(symb, map.get(symb) + 1);
       } else
         { map.put(symb,
         1);
      }
```

```
}
  }
  / System.out.println(map);
  String s = "";
  float index =
  0; float coef;
  for (Map.Entry<String, Integer> entry: map.entrySet()) {
     coef = (entry.getValue() * (entry.getValue() - 1));
     index += ((coef) * (1 / ((amount) * (amount - 1))));
  }
  return index;
public static int index(char c) {
  String string = "абвгдежзийклмнопрстуфхцчшщъыьэюя";
  System.out.println(string.length());
  char[] ch = string.toCharArray(); for
  (int i = 0; i < string.length(); i++) {
    if (ch[i] == c) {
       / System.out.println(i);
       return i;
    }
  return -1;
}
public static char indexNew(int number) {
  String string = "абвгдежзийклмнопрстуфхцчшщъыьэюя";
  char[] ch = string.toCharArray(); for (int i = 0; i < ch.length;</pre>
  i++) {
     if (i == number) {
       System.out.println(ch[i]);
       return ch[i];
    }
  }
  return 0;
public static void block(String text) {
  char[] charText = text.toCharArray();
  String firstTxt = "";
  for (int j = 0; j < 16; j++) {
     for (int i = j; i < charText.length; i += 16) {
       firstTxt += charText[i];
    //System.out.println(firstTxt);
  String[] str = new String[17];
  String str1 = "";
  int keyLen = 16;
  char[] sortChar = firstTxt.toCharArray();
  for (int i = 0; i < 16; i++) {
    for (int j = 0; j < sortChar.length; j++) {
       str1 += valueOf(sortChar[j]);
       str[i] = str1;
       if (j % 739 == 0) {
```

```
i++;
         str1 = str1.replaceAll("[a-я]", "");
      }
    }
  }
  String count = "";
  for (int i = 0; i < 17; i++) {
    System.out.println(str[i]);
    popularList(letter(str[i]));
  }
  // System.out.println(count);
}
public static void vigDenc(String str) {
  String key = "братьякарамазовы";
  String strDenc = "";
  char[] newStr = str.toCharArray();
  char[] newKey = key.toCharArray();
  int newLetterNum;
  for (int i = 0; i < str.length(); i++) {
    newLetterNum = ((newStr[i] - newKey[i % 16]) % 32);
    if (newLetterNum < 0) newLetterNum = newLetterNum + 32;
    strDenc += indexNew(newLetterNum);
  System.out.println(strDenc);
public static void vigEncr(String str) {
  String key = "университет";
  String strEnc = "";
  char[] newStr = str.toCharArray();
  char[] newKey = key.toCharArray();
  int newLetterNum;
  for (int i = 0; i < str.length(); i++) {
    newLetterNum = ((newStr[i] + newKey[i % newKey.length]) % 32);
    if (newLetterNum < 0) newLetterNum = newLetterNum + 32;
    strEnc += indexNew(newLetterNum);
  System.out.println(strEnc);
}
public static double iS(String string) {
  char[] allString = string.toCharArray();
  List<Character> subString = new ArrayList<>();
  for (int i = 2; i < 30; i++) {
    for (int j = 0; j < allString.length; j += i) {
       subString.add(allString[j]);
    }
    String res = Arrays.toString(subString.toArray()).replaceAll("[^a-я]", "");
    System.out.print("MC = " + i + calcIndex(res));
    System.out.println();
    subString.clear();
  }
  return 0;
}
```

}