Лабораторна робота 3
Фб-11 Іван Кустов, Андрій Яцентюк

4 в

Мета роботи:
Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці

Порядок виконання роботи:
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

хід роботи, опис труднощів, що виникали, та шляхів їх розв'язання:

Спочатку написали основні функції, з ними особливих складнощів не було. Труднощі почалися із дешифруванням. Після купи різних ітерацій вирішили просто підбрати a та b брутфорсом - отримали a = 390, b = 10. Також у дешифрування були помилки, але вони були вирішені, коли поміняли **ы ь** місцями

знайдені п'ять найчастіших біграм шифртексту:
[('еш', 67), ('еы', 49), ('шя', 47), ('ск', 47), ('до', 46)]

опис роботи запропонованого вами автоматичного розпізнавача російської мови:

Ми перевіряємо частоти літер заданого тексту із загально очікуваними частотами в рус.мові. Якщо різниця < 25% то true. інакше false

шифрований та відповідний розшифрований тексти, знайдене значення ключа:
Ключ a = 390, b = 10

Шифрований:
щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфип
мугфбзчшохдодвзбряцкмдбэдцхзнощк
яоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщз
оюдууюзсшшстзрэыосяфоешыенывд
ьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжв
онцеырайхмучмсшывчфвэрфешмяояйывщ
еыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжз
шцопсйкоефтцрзюэдцсшямсканзомы
жуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцоще
ызонорйвкхпшсзунрмоншзоязшяэдхп
езхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглт
доккжшскзыядншууезжурфешщпнз
шятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотф
лцжшвдзылвхзпмжущжеляыцдюппкгф
кшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдо
рддокыбзлжвочыезыяюйеытяьочмск
мзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанбччйтжмкжуч
буфпошфбждоцпюдлвюпюпэзкбтцзопз
аоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжл
ыдяюйеызопыщжфоочсквжаббжнзбляь
хзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйс
сожзешопхпимсжсказкзшяшйнэюш
шомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжф
зйквбждэечяыжхыхоцыыиеыыяпомггд
нотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткз
еадьгпуротынщйайкбазущпязхл
дырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзб
ряцкмдррхфщжэпмуапзчвомощкхыхз
иоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсх
прфеыщчфоефзббжнзтыссжяилнахп
езфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмы
йзхйшмшжшалтыбжхябжюакцопиыщчыд
ншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпонойкыпю
шщчмысклзыцбчмялзоцнрряешиыфсхя
даыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажу
юшимйшлыпутцурряешбзкцколппотз
уыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзх
лцюпзхщжщккжюыюпцчзпэыиывдншуушс
ешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмк
саанжутоаонзскккрздвюптжждшсэы
пзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчн
шузябряешйкешзоешчбгяыоиыоцпм

зямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцы
шсдондпмкзшягожурфлцеызоножя
яоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэй
фбждоцпюдлвляскмздбкзцжжущпрф
уяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмя
тыямйшалтыеызоешыедвайнинзшязпкц
рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдую
пшсуяпзйкелиавжнрфушйеыюувделдш
чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуы
йьмюпйфбждоцпюдлвюпюпэзпшкзхуэж
йуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзвждвждм
ызхзосшзбкззжокуцеыюпщуыйтодыюп
иызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяжд
чвхеыщчпмщпбкуяяоекшярбптхямзюдеч
рэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкпоноюааощя
екшйбчжучбгяыоиыоцпмяднщжшбчтз
чзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхз
жусжфрйктзшясжеьзоешрйэжпзжж
бяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзю
нзоешедвдвлгфезшйдбряилгфеыхзсккч
вкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуях
ыщчрзхьэыэявжкщитдоешзхеыхзрэ
ешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзбб
жнзмоошууеыщчдонорзлзджипщчьоцы
ыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжо
зномясктзлзмкжшбчшящкбяйбзбяш
жддыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжупмск
жшбчцдвдвжьглцечмяскскщкбаекжш
бчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкм
яюнзоекшвуяджпоьфйказсшлячову
нщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояонос
шншмоешдбждтззпсчжшбчншщзнэйсеш
ьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилг
фбзлжзпвкылоцдуюпиыыяйкныляыфчб
юпповбнзцжшзяойййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфс
сешмяабяопмьосяцызвмуйчмоешдбжд
щуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцрр
сшбжлзмканюакыбзйхдодвууэжкцмэсч
жшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсж
улямрчфюшпфмяяявлвжипюпэышбмунр
чфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывдю
шлвохдошзяобпбжжуэырйбзщтелмяил
щкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкж
щкгфсймовккцивыйгшьльфжшншмолдоп
сшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбж
юпмуяззощуиврймзвожзпофотывдохлц
юпядайхпимиыраыжнэюшсйокбяжярзьазоныркоцыыиеыщчжящкбяшзяоьфжяюуйсгдн
шуулвайншопэзцжбкюнзоносочзсыях

щжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказх
яанаоешезвжбякбмурфоцхпэесопж
ипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлцечпфлцйшжбрякыиыхзфшайтцлбг
цабхявыцпяохяупайтзншщзнэйсшк
опншфузхпмдьюшшящксктллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкч
фылидмышкбмщпбкуяяоекзожзуяпо
нзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчхя
бфбждоцпюдлвямэжглцяекжшскчйфи
бяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосш
ншмоешдбждсожзбигцскыкфотфлцаб
гяыовояяфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыы
ядвзбряжзлжипюпоцчбптдохлибвоан
аопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппыйы
яюдйшлцлыэжмкгфеыйсмофыксюдаб
гяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпз
чзшяжкйкгшмускбфсчаоешезвжпо
нопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоеше
дншщзнэйсешылбэяоыкжшбччзкзтырйск
понзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшс
ншешйкцчжшншэзччсжрлязшядяябтцшя
анбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйш
щчаоешезвжпоноэбкзешдбшярллзджип
юшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжл
кешраояазжшжущпщоскскможяскжшбцзв
лвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбш
янфсчтзномофшсжцкгяпзюнамзпея
пыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

Дешифрований:

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждае
тточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразо
мнодоказатьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкон
омиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиуни
женийосуждениедостоевскоговкачествеполитическогопреступникабылонесправедливы
миондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакза
менунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувмес
тосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставле
ниеопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделет
акмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобраз
омотсамонаказаниятоткзнаетсложноеиизменчивоезначениеистерическихсимптомовп
ойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедо
статочнотогочтоможнопредположитьчтоихпервоначальнаясущностьосталасьнеизменно
йнесморянавсепоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосв
ободилсяотугрызенийсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибрем
яопределилотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукго
сударственномуавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюшк
ецарюоднаждыразыгравшемуснимкомедиюубийствавдействительностинаходившуюсто
лькоразотражениевегоприпадкахздесьверхвзялопокаяниебольшесвободыоставалосьу

неговобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминуты
своейжизнивсеколебалсямеждуверойибезбожиемеговысокийумнепозволялемунезамеч
атьтетрудностиосмысливаниякоторымприводитверавиндивидуальномповторениимиро
вогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотгре
ховииспользоватьсвоисобственныестраданиячтобыпритязательнаролькристаеслионвкон
ечномсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеч
ескаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивид
уальнойсилыинемоглабытьпреодоленадажееговысокойинтеллектуальностьюздесьнаск
азалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализа
иподвергаемдостоевскогооценкеимеющейправонасуществованиелишьспристрастнойт
очкизренияопределенногомировоззренияконсерваторсталбынаточкузрениявеликогоинк
визитораиоценивалбыдостоевскогоиначеупрекправедливдляегосмягченияможнолишь
сказатьчторешениедостоевскоговызваноочевиднозатрудненностьюегомышленияявслед
ствиеневрозаедвалипростойслучайностьюможнообяснитьчтотришедеврамировойлитер
атурывсехвременктрактуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетше
кспираибратьякарамазовыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуаль
ноесоперничествоиззаженщиныпрямеевсегоконечноэтопредставленовдрамеоснованно
йнагреческомсказаниииздесьдеяниесовершаетсяещесамимгероемнобезсмягченияизаву
алированияпоэтическаяобработканевозможнаоткровенноепризнаниевнамеренииубить
отцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбезаналитическойп
одготовкивгреческойдраменеобходимоесмягчениеприсохраненииисущностимастерскид
остигаетсятемчтобессознательныймотивгерояпроецируетсявдействительностькакчужд
ееемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамеренноиповсе
йвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсяврасчет
таккаконможетзавоеватьцарицуматьтолькопослеповторениятогожедействиявотношени
ичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинане
делаетсяникакихпопытокснятьеессебявзвалитьеенапринуждениесостороныисудьбынао
боротвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесп
раведливымнопсихологическиабсолютноправильнованглийскойдрамеэтоизображеноб
олеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокне
являетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничествауж
енщиныненуждаетсявзавуалированииравноиэдиповкомплексгероямывидимкакбывотра
женномсвететкакмывидимлишьтокакоедействиепроизводитнагеропоступокдругогоо
ндолженбылбызаэтотпоступокотомстительностраннымобразомневсилахэтосделатьмызн
аемчтоегорасслабляетсобственноечувствовинывсоответствиисхарактеромневротическ
ихявленийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособностивып
олнитьэтозаданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхинди
вндуальнуюонпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамкто
уйдетотпоркивэтомнаправлениироманрусскогописателяуходитнашагдальшеиздесьубий
ствосовершенодругимчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновн
имиотношениямикакигеройдмитрийукоторогомотивсексуальногосоперничествааоткрове
ннопризнаетсясовершенодругимбратомкоторомукакинтереснозаметитьдостоевскийпер
едалсвоюсобственнуюболезньякобыэпилепсиютемсамымкакбыжелаясделатьпризнани
ечтомолэпилептикневротиквомнеотцеубийцаивотвречизащитниканасудетажеизвестная
насмешканадпсихологиейонамолпалкаодвухконцахзавуалировановеликолепнотаккакст
оитвсеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядостоевскогозаслуж
иваетнасмешкиотнюдьнепсихологияасудебныйпроцессдознаниясовершеннобезразлич
ноктоэтотпоступоксовершилнасамомделепсихологияинтересуетсялишьтемктоеговсвое

мсердцежелаликтопоегосовершениигоприветствовалипоэтомувплотьдоконтрастнойф
игурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнаслажд
енийполныйскепсисациникиэпилептическийпреступниквбратьяхкарамазовыхестьсцена
ввысшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчт
одмитрийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможе
тявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискуше
ниеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяипоэтомупереднимсмиряетсяси
мпатиядостоевскогокпреступникудействительнобезграничнаонадалековыходитзапреде
лысостраданиянакотороенесчастныйимеетправоонанапоминаетблагоговениескоторым
вдревностиотносилисьэпилептикуидушевнобольномупреступникдлянегопочтиспасите
львзявшийнасебявинукоторуювдругомслучаенеслибыдругие