

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, крім написання евкліда. Пробували використовувати вбудовану у пайтон row, але через те, що вона нормально не вирішує, коли там не один випадок, нам вона не підходить. Найскладніша частина була зрозуміти, що таке u та v , потім стало зрозуміло, що v це обернене a за модулем b , а u то обернене b за модулем a .

Для дешифрування ми шукаємо 10 найчастіших біграм нашого шифротексту, та 10 найчастіших рос.мови. Потім відповідно до них ми створюємо всі можливі варіації ключа $(a$ та $b)$ і перевіряємо Russian check, який рахує можливе відхилення від загально очікуваної частоти літер в рос.мові. Таким чином ми отримуємо ключ - $a = 390$, $b = 10$

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. спочатку використовували 15%, але наш текст виявився занадто малим, тому збільшили до 25%

Шифрований та відповідний розшифрований тексти, знайдене значення ключа:

Ключ $a = 390$, $b = 10$

Шифрований:

щжуяжушцпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфип

мугфбзчшохдодвзбряцкдбэдцхзношк
яозоюэтцюзныертзилгфоцбполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьюйсщз
оюдууюзсшштзрэыосяфоешыенывд
ьмиыыашцрбгнямзюдшскдмайыаоешезвжпонорэжкцжшбчдофшщофбяоязфыщжв
онцеырайхмучмсшывчфвэрфешмяояйывщ
еыйсбжошлзшярфбждоцпюдлвюпцкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжз
щцопсйкоефтцрзюэдцсшямсканзоны
жуэыыцсшмычмэжглрзщыезскцквкшятоьэйштибяшкочцкфмыйеыйывдьмиыщчвккцоше
ызонорйвкхпшсзунрмоншзоязшяэдхп
езхлсопжипеызохлншплбйщждоыкфоскцквкшягоефоцзчскцквканвказешюшлцромглт
доккжшскзыядншуеэжурфешщпнз
шятоужертцлвяхщжпофожуцпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотф
лцжшвдзылвхзпмжуцжеляыцдюппкгф
кшскцквкшязоноуюйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдо
рддокыбзлжвочыезыяюйеытяьочмск
мзшядешмуяхщжбягжрйашайюпмогйжшфшайрмлзнттзхаокшйбчаощяанбчйтжмкжуч
буфпошфбждоцпюдлвюпюпэзкбтцзопз
аоейшшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжл
ыдяюйеызопыщжфоочсквжабжнзбляь
хзсккцезшяййсщзоюдьмшнхдоаоешезвжбяршвдшяполфзятзбжьоиосйяжгоелзурмеыйс
сожзешопхпимсжсказкзшяшйнэюш
шомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыиееыхнфылтфаляяыжф
зйквбждэечяыжхыхоцыиееыяпомгтд
нотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмьжумилцэбтцзохлмофхэыеынеткз
еадыгпуротынщйайкбазуцпязхл
дырйпоазсяслщяджипщплзджипюшлцлыбжхяскыоссяэищеештцедууьмншйкрзшяцпдвзб
ряцкмдррхфщжэпмуапзчвомощкхыхз
июнянзхпрэчфлоешцпоцбжщлтзньообцэжхякзуяаяямзокбмырфзбюжщкьярьсозыеыйсх
прфеыщцфоефзббжнзтыссжяилнахп
езфщпмшявждтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыщййычмы
йзхйшмшжалтыбжхябжюакцопиыщчыд
ншуусйжуопчфюшжзйкмьяефопифбкюнзовбюпдокзшярдуюплвляешууяхщжпонойкыпю
шщчмысклзыцбмялзоцнрряешиыфсхя
даыосябжьоиогфеыхншзунрюпяяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажу
юшимйшлыпутцурряешбзкцколппотз
уыайжхжшеяабрязодхпрэчфдяешоцкзвдаямымайдосшщоччдыозлжцшшйфшщоцзх
лцюпзхщжщкккююпцзпэыиывдншуушс
ешяюшбчкзуаяяамзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмк
саанжутоаонзскккрздвюптжждшсэы
пзьцяделоцлыбжанхмлзннскюдьмоцбжпэйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчн
шузябряешйкешзоешчбгяыюиыоцпм
зямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцы
шсдондпмкзшягожурфлцеызоножя
яоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэй
фбждоцпюдлвляскмздбкзцжжуцпрф
уяшфсчдвбждчвхеыщчфочытцмиащквканфшууфиеыхзаоешезвжпонодаыпиыщомзмзя
тыямйшалтыеызоешыедвайнинзшязпкц
рфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдую

пшсуяпзйкелиавжнрфушйеыюувделдш
чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуы
йъмюпйфбждоцпюдлвюпюпэзпшкзхуэж
йуппбзлжфяфохяшфвчшякядтлоцплыезсочзсыяхщжипляэмнщеычяражуййюзвждвждм
ызхзосшзбкззжокуцеыюпщуыйтодыюп
иызопызвкзмзюдайюдьмиыяхфщжцфвчшящжюпмуюкжшбчбыщжыйрйшзяошйзоузяжд
чвхеыщчпмщпбкуяяоекшярбптхямзюдеч
рэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкцкпонояааощя
екшйбчжучбгяыоиыоцпмяднцжшбчтз
чзкззюгяюалэчмиыоцюшяхщжпкбчфнодоздопзухщжпюфйказтзрэюсяфощждчвхеыхз
жусжфрйктзшясжезюешрйэжпзжж
бяаоешывбзлжцшшйфшрэщжсокийшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзю
нзоешедвдвлгфезшйдбриялгфехзсккч
вкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуях
ыщчрзхьэыэявжкщитдоешзхехыхрэ
ешйчпзюнешибряшякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэйшмштцедзбб
жнзмоошууеыщчдонорзлзджипщчьоцы
ыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжо
зномясктзлзмкжшбчшящкбйбзбш
жддыцшдзщжзччаекуяанюзскжуэыоцлзшящжбждояоратлынсаскрэууншмяскжупмск
жшбчцдвдвжыглцечмяскскщкбаекжш
бчфшууэжтлмдэйсщжшмоцквканбчтзбяйкжзщцопсйзоужертцлвяхщжбямэсоеецызбйкм
яюнзоекшвуяджпюфйказсшлячову
нщеырэтцюзпохпезомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояонос
шншмоешдбждтззпсчжшбчншщзнэйсеш
ьовбптдохлжурфбжффюшлцлыксфохявжядтлоцпылвбжзбмушямзешекощеычяратзилг
фбзлжзпвкылоцдюпиыыайкнылаяфчб
юпповбнзцжшзюойппифрйщкжэппншйкрзщыайхпжшшвдщкхйппифрйуяпндощкпорфс
сешмябяопмьосяцызвмуйчмоешдбжд
щуивлвщоефтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцрр
сшбжлзмканюакыбзйхдодвууэжкцмэсч
жшсопжипезозхьпешьюмяравжщюипжшешмясжжкйкгшмуайтзфуншяхщжбжлчуцеыйсж
улямрчфюшпфмяявлвжипюпэышбмунр
чфюшьосокыиыхзхпезпыщжмосоыбжхядамофыюшотдовкккшяабйчуцжелжрбрияквдю
шлвохдошзюоббжжуэырйбзщтелмяил
щкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажж
щкгфсймовккцивыйгшьльфжшншмолдоп
сшайскжуцпнзшядуайиыалшжпонояыкпзсчсрчфюшскюклфоцыидяхфщжщлщяджипбж
юпмуязззоцуиврймзвозжпофотывдохлц
юпядайхпимиыраыжнэюшсйокбяжярзязонырйкоцыиыешчжящкбшзюоьфжяюуисгдн
шуулвайншопэзцжбкюнзоносочзсыях
щжипхордяожзщызбриякыбзлжжжюпмуязззоцуиврйвушайподояохлщкбшшмушжзовказх
яанаетешезвжбжбмурфоцхпэсопж
ипеыилзэтцмгнпдрэбтюянзужнепзыжыйсйщкжэщлцечпфлцйшжбриякыыхзфшайтцлбг
цабхявыцпяхяупайтзншщзнэйсшк
опншфузхпмдьюшшящксктллзокрзпмжзешскхыэжазидиуфужертцлвхзэоскфопбоцщкч
фылидмышкбмщпбкуяяоекзожзуюпо
нзяыншвдщкцждоюшвжитдочзкжзсыкшкяскыосяпнжцнэохфсфлчжезюешэпбжжуцчхя

бфбждоцпюдлвямэжглцяекжшскчйфи
бяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузуьмуяуыжддосш
ншмоешдбждсозжбигцскыкфотфлцаб
гяыовояфяьшмуцжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносозжбиеы
ядвзбряжзлжипюпоцбптдохлибвоан
аопьшйкешзokyиврухкнзеявжйэйканэуцпзомязонийфмяцяюакбмумяуысйчбямппыйы
яюдйшлцпыэжмкгфеыйсмофыксюдаб
гяыкаяшбялбгцабхямзюдйсжуцжеляыцдсэйканюрцкйкакчодаззешажщзскяптжязджпз
чзшяжкйкгшмускбфсчаоешезвжпо
нопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоеше
дншщзэнэйсешылбэяоыкжшбчзкзтырйск
понзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшс
ншешйкцчжшншэзчсжрлязшяддябтцшя
анбчжучмкзшяшйрлцяегдяуяриймоаышйшажфямосшайдбмурфшяыжжяочжшбчгявбйш
щчаоешезвжпоноэбкзешдбшярллзджип
юшлцпырэмзуиыяхскмыуфоцядюпжрчфюшвжурфлцтжбжюууфиыщчскподояоеыщжл
кешраояазжшжуцпщоскскможяскжшбцзв
лвюпыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцпыайдбкзешдбш
янфсчтзномофшсжцкпяпзюнамзпя
пыэжйэзпыгдншуущешфалноыжгллкыешжжюясащуйвхзак

Дешифрований:

если правда что достоинский в сибири не был подвержен припадкам то это лишь подтверждает то что его припадки были не его карой он более в них не нуждался когда был караминным образом много доказать это не возможно скорее этой необходимости в наказании для психической экзотомии достоинского объясняется то что он прошел несломленным через эти годы бедствий и унижений и осуждений достоинского качества политического преступника был не несправедливый миссионер должен был это знать но он принял это не заслуженное наказание от батюшки царя как за мену наказания заслуженного им за свой грех по отношению к своему собственному отцу вмести с тем самонаказание он дал себя наказывать заместителю отца это дает нам некоторое представление о психологическом оправдании наказания и приговораемых обществом это на самом деле так много и из преступников жаждут наказания его требуют сверхъестественно извращаясь таким образом от самонаказания тот кто знает сложное и изменчивое значение истерических симптомов и метит что мы здесь не пытаемся добиться смысла припадков достоинского во всей полноте достаточно того что можно предположить что их первоначальная сущность осталась неизменной несмотря на все последующие наслоения можно сказать что достоинский так или иначе не освободился от угрызений совести в связи с намерением убить отца это лежащее на совести бремя определило так же его отношение к двум другим сферам покоящимся на отношении к отцу к государству и к авторитету и к веревкам в первой он пришел к полному подчинению батюшке царю и однажды разыграл в нем комедию убийства в действительности находившуюся в коразотражении не его припадков здесь сверхъестественно покаяние и освобождение оставалось у него во власти религиозной по недопускающим сомнений сведениям о последней минуте своей жизни в секолебался между верой и безбожием его высокий ум не позволял ему замечать трудности осмысливания некоторых приводит в равновесии индивидуальное повторение мирового исторического развития он надеялся в идеале христианайтivity освобождение от грехов и использовать свои собственные страдания чтобы притянуть на роль Христа если он в конечном счете не пришел к свободе и стал реакционером то это объясняется тем что общечеловеческая сыновья вина на которой строится религиозное чувство достигла у него сверхиндивидуальности

уальной силы и не могла бы быть преодолена даже его высокой интеллектуальностью. Здесь нас как азалось бы можно упрекнуть в том, что мы отбрасываемся от беспристрастности психоанализа и подвергаем Достоевского оценке имеющей право на существование и лишь с пристрастием откидываем определение мирового зрения консерватор. Стало бы не так, зрения великого инквизитора и оценивал бы Достоевского иначе, но прексправедлив для его смягчения можно лишь сказать, что решение Достоевского вызвано очевидно затрудненностью его мышления в следствии не врожденной, а простой случайностью. Можно объяснить, что три шедевра мировой литературы во все времена трактуют одну и ту же тему: отцеубийства царь Эдип, Софокл, Агамемнон, Ксипири, братья Карамазовы Достоевского во всех трех раскрывается мотив деяния сексуального соперничества и из-за женщины. Прямо все это конечно, это представлено в драме основанной на греческом сказании. Из здесь деяние совершается еще самим героем, но без смягчения из-за уауалирования поэтическая обработка невозможна. Откровенное признание в намерении убить отца, какому мы добиваемся при психоанализе, кажется непереносимым без аналитической подготовки в греческой драме. Необходимо смягчение и при сохранении сущности мастерски достигается тем, что бессознательный мотив героя проецируется в действительность как чуждое ему принуждение. Навязанное судьбой, герой совершает деяние не преднамеренно и повсей видимости без влияния женщины. В все же это стечение обстоятельств принимается в расчет так, как оно может завоевать царицу, мать только по слепому повторению того же действия. Вот оно и чудовище, а символизирующее отца по слету, оно как обнаруживается, оно глашается его, вина не делается, никаких попыток снять ее с себя, вваливать ее на принуждение со стороны судьбы, но борьба признается, как в целая вина, наказываемся, что рассудку может показаться несправедливым, но психологически абсолютно правильно. В английской драме это изображено более естественно, поступок совершается не самим героем, а другим, для которого этот поступок не является отцеубийством, поэтому предосудительный мотив сексуального соперничества у женщины не нуждается в уауалировании и равно Эдипов комплекс героя мы видим как бы в отраженном свете, так как мы видим лишь, что такое действие производит на героя поступок другого, он должен был бы за этот поступок отомстить, но странным образом не в силах это сделать, мы знаем, что его расслабляет собственное чувство вины, в соответствии с характером невротикических явлений происходит сдвиг чувства вины, переходит в сознание своей неспособности выполнить это задание, и появляются признаки того, что герой воспринимает эту вину как сверхиндивидуальную, он презирает других, не менее чем себя, если обходиться с каждым по заслугам, то уйдет от порки в этом направлении. И роман русского писателя уходит на шаг дальше, и здесь убийство совершено другим человеком, но человек, связанным с убийцей, такими же сыновними отношениями, как и герой. Дмитрий у которого мотив сексуального соперничества откровенно признается, совершено другим братом, которому как интересно заметить Достоевский передает свою собственную болезнь, как бы эпилепсию, тем самым как бы желая сделать признание, что мол эпилептик невротикизм, не отцеубийца и в откровенной защитника на суд, даже известная насмешка над психологией, она мол палка в двух концах, завуалировано велико, лепнотак как стoit все это перевернуть, находишь глубочайшую сущность восприятия Достоевского, заслуживает насмешки, и отнюдь не психология, а судебный процесс, дознания совершенно безразлично, что этот поступок совершил на самом деле, психология интересуется лишь тем, что его в своем сердце желал, кто по его совершению его приветствовали, поэтому вплоть до контрастной фигуры, аleshivse братья равны, виновны, подвижимый первичными позывами, и искатель наслаждений, полный скепсис, ациники эпилептический преступник, братья Карамазовых, есть сцена в высшей степени характерная для Достоевского, из разговора с Дмитрием старец постигает, что Дмитрий носит все готовность к отцеубийству и бросается перед ним, на колени, это не может являться выражением восхищения, а должно означать, что святой отстраняет от себя искушение и исполняется презрением к убийце, или им погнущаться, и поэтому перед ним смиряется.

мпатия Достоевского к преступнику действительно безгранична: она далеко выходит за пределы сострадания к некоторо несчастный и имеет право на напоминание о благоговении к которому в древности относились к эпилептику и душевно больному преступнику для него почти спасительная вещь на себя вину которую в другом случае несли бы другие