Міністерство освіти і науки України
НТУУ«Київський політехнічний інститут»
Фізико-технічний інститут

Лабораторна робота № 3

з предмету «Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Варіант №4

Виконала:

Студентка 3 курсу
ФТІ группи ФБ-83

Бондарчук Ярослава

Перевірив:

Чорний О. М.

Київ-2020

Мета роботи

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

Найчастіші біграми шифротексту:

Біграма	**Частота**
еш	0,022922
еы	0,016764
ск	0,016079
шя	0,016079
до	0,015737

Автоматичний розпізнавач російської мови:

Розпізнавач ф-я `bool check(ifstream &myfile)` що спочатку перевіряє тексти на індекс відповідності, який має бути близьким до теоретичного. Після цього перевіряє частоту букв у розшифрованих текстів, що пройшли попередню перевірку та звіряє з найчастішими в російському алфавіті. Якщо текст пройшов 2 дані перевірки він записується у файл.

Ключ(390, 10)
Індекс відповідності: I(X)= 0.0582678

Зашифрований текст

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгф
оцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывдьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпон
орэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмяояйыивщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдб
шящксавотзябйкжзщцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызо
норйвкхпшсзунрмоншзояшяэдхпезхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезжур
фешщпнзшятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкш
яозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмо
гйжшфшайрмлзнntзхаокшйбчаощяанбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьоскл
кюнскkжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжабббжнзбляьхзскккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурм
еыйссожзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхо
цыыиеыыяпомггднотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхлдырйпоазся
слщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноь
общэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйс
эйтзмоыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыдншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюплвляешууяхщжпоной
кыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпут
цурряешбзкцколппотзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшйфшщоцьзхлцюпзхщжщкжюыюпцчзпэыиывдншуу
шсешяоюшбчкзуяяяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюптжждшсэыпзьцяделоцлыбжанхмлз
ннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряешйкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьо
сктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножяяоьоэмкзшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощ
зшяекшэйфбждоцпюдлвляскмздбкзцжжущпрфуяшфсчдвбждчвхеыщчфочытцмиажщкквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеыз
оешыедвайнинзшязпкцрфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдш
чфилюшощжшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюпюпэзпшкзхуэжйуппбзлжфяфохя
шфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмзюдайюдьмиыыяхфщжцфвч
шящжюпмуюкжшбчбыщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямзюдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшялл
щяанншшкщкпоноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвхе
ыхзжусжфрйктзшясжеьзоешрйэжпзжжбяаоешывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоеш едвдвлгфезшйдбр
яилгфеыхзсккчвкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюне
шибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцыыиеыыявлаомяркгяшптцпмдущес
зноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбзбяшждцыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояора
тлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецыз
бйкмяюнзоекшвуяджпоьфйказсшлячовунщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояоносшншмоешдбждтззпсчж
шбчншщзнэйсешьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчбюппов
бнзцжшзяойййпифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавкс
шншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопжипеызозхьпешьомяравжщоипжшешмясжж
кйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяяявлвжипюпэышбмунрчфюшьосокыиыхзхпезпыщжмосоыыбжхядамофыюшотдовкккшяабйчу
цжелжрбрякывдюшлвохдошзяобпбжжуэырйбзштелмяилщкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгф
сймовккцивыйгшьльфжшншмолдопсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжюпмуяззощуивржмзвожз
пофотывдохлцюпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсыяхщжихпхор
дяожзщызбрякыбзлжкжюпмуяззощуивржвуйшайподояохлщкбяьшмущжзовказхяанаоешезвжбякбмурфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепз
ыжыйсйщкжэгщлцечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзнщшзнэйсшкопншфузхпмдьюшшящкскткллзокрзпмжзешскхыэжазадиыуфу
жертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуяяоекзожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчх
ябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракбяощзшжаокыиыщчсожзбиеызоузсуьмуяуыждосшншмоешдбждсожзбигц
скыкфотфлцабгяыовояфяьшмущжвзлжыцмимшшйгшезновжьошйээфщзрзмкуягшзбезносожзбиеыыядвзбряжзлжипюпоцчбптдохлибвоанаопоьшйке
шзокюыврухкнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгыякаяшябялбгцабхямзюдйсжущж
еляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаоешезвжпонопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряп
ыбжюшвжйэдвншюпзоешеднщщзнэйсешылбэяоыкжшбччзкзтырйскпонзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдо
хпцшшсншешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвж
поноэбкзешдбшярллзджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжлкешраоязжшжущпщоскскможяск
жшбцзвлвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпеяпыэжйэзпэыгдншу
ущешфалноыжгллкеыщжуясащуивхзак

Розшифрований текст

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодоказатьэтоневозможноскореетойнеобходимостьювнаказаниидляпсихическойэкониидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиунижений осуждениедостоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказаниязаслуженногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзастителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказанияоттоктознаетсложноеизменчивоезначениеистерическихсимптовпойметчтыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточнотогочтожнопредположитьчтоихпервоначальнаясущностьосталасьнеизменнойнесморянавсоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснарениемубитьотцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойонпришелкполномуподчинениюбатюцарюоднаждыразыгравшемуснимкодиюубийствавдействительностинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяниебольшесвободыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвоейжизнивсеколебалсяждуверойибезбожиемеговысокийумнепозволялемунезамечатьтетрудностиосмысливаниякоторымприводитверавиндивидуальномповторениимировогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотгреховииспользоватвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконечнсчетеришелксвободеисталреакционертоэтообясняетсятемчтообщечеловеческаясыновняявинанакоторойстроитсярелигиозноечувствводостиглаунегосверхиндивидуальнойсилыинемоглабытьпреодоленадажеговысокойинтеллектуальностьюздесьнасказалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдостоевскогооценкеимеющейправонасуществованиелишпристрастнойточкизренияопределенногомировоззренияконсерваторсталбынаточкузренияведикогоинквизитораиоценивалбыдостоевскогоиначеупрекправедливдляегосмягченияможнолишказатьчторешениедостоевскоговызваноочевиднозатрудненностьюегышлениявследствиеневрозаедвалипростойслучайностьюможнообяснитьчтотришедеврамировойлитературывсехвременктрактуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззаженщиныпрямеевсегоконечноэтопредставленовдрамеоснованнойнагреческсказанииздесьдеяниесовершаетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенноепризнаниевнаренииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбезаналитическойподготовкивгреческойдранеобходимоесмягчениеприсохраненииусщностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействительность какчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенреднамеренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторениятогожедействияотношениичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокснятьеесебявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихологическиабсолютноправильнованглийскойдраэтоизображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничестваженщиныненуждаетсявзавуалированииравноиэдиповкомплексгероямывидимкакбывотраженнсвететкакмывидимлишьтокакоедействиеоизводитнагеропоступокдругогоондолженбылбызаэтотпоступокотстить ностраннымобразневсилахэтоделатьмызнаемчтоегорасслабляетсобственноечувствовинывсоответствиисхарактерневрогическихявленийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособностивыполнитьэтозаданиеоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюонпрезираетдругихнеменеечемсебяеслиобходитяскаждымпозаслугамктоуйдетотпоркивэтнаправлениираннрусскогописателяуходитнашагдальшеиздесьубийствосовершенодругимчеловекомоднакочеловексвязаннымсубитымтакимижесыновнимиотношениямикакигеройдмитрийукотороготивсексуальногосоперничестваоткровеннопризнаетсясовершенодругимбраткоторомукакинтересноза титьдостоевскийпередалсвоюсобственнуюболезньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтолэпилтикневротиквнеотцеубийцаивотврачизащитниканасудетажеизвестнаянасанадпсихологиейонамолпалкаодвухконцахзавуалировановедиколепнотаккакстоитвсеэтоперевернутьинаходишьглубочайшуюсущностьвосприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасудебныйпроцессдознания совершеннобезразличноктоэтотпоступоксовершилнасамомделсихологияинтересуетсялишьтемктоеговсвоемсердцежелаликтопоегосовершениииегоприветствовалипоэтомувплоть доконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпервичнымипозывамиискательнаслаждений полныйсксиса циникиэпилтическийпреступниквбратьяхкарамазовыхестценаввысшейстепенихарактернаядлядостоевскогоизразговорасдмитриемстарецпостигаетчтодмитрийноситвсебеготовностькотцеубийствуибросаетсяпереднимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойотстраняетотсебяискушениеисполнитьсяпрезрениемкубийцеилиимпогнушатяипоэтупереднимсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалековыходитзапределысостраданиянакотороенесчастныйиетправоонанапоминаетблаготовениескоторымвдревности относилиськэпилептикуидушевнобольнупреступникдлянегопочтиспасительвзявшийнасебявинукоторуювдругомслучаенеслибыдругиеаа

Висновки:

Під час виконання даної роботи я навчилася працювати з шофром афінної біграмної підстановки, а саме розшифровувати тексти, що зашифровані ним. Також написала автоматичний тест для розпізнаванн російської мови за допомогою індексу відповідності та аналізу частоти букв у тексті.