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

Криптографія
Лабораторна робота №3
Афінний шифр

Варіант №4

Підготували:
Студенти групи ФБ-82
Дяковський Кирило
Щербаков Олег

2020

1. Мета робот: набуття навичок частотного аналізу на прикладі розкриття моноалфаввітної підстановки; опанування прийомами роботи в модулярній арифметиці.

2. Задача: написати код, що знаходить колюч на розшифровує наступний текст, зашифрований афінним шифром:

щжуяжсущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугфбзчшохдодвзбряцкмдбэдцхз нощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчозычфждьмйшотдотзьоюйсщзоюдуюзсшистзрэыосяфое шыеныводьмиыыяшцрбгянямзюдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяозфыщжвонцеырайхмучмсшывчф вэрфешмяояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйкжзшцопсйкоефтц рзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвк хпшсзунрмоншзоязшяэдхпезхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцээччскщкванвказешюшлцромглтдоккжж шскзыяднщууезжурфешцпнзшятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоскыкфот флцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьм иыщчдорддокыбзлжвочыезыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощяанб ччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклюнсккжже ьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбляьхзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзб жьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщо цыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггднотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшс мыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхлдырйпоазсяслщяджипщплзджипюшлцлыбжхяскыося эищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхякзуяя яямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоц яшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыдншуусйжуопчфюшжзйкмяефопиф бкюнзовбюпдокзшярйдуюплвляешууяхщжпонойкыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзншзунр юпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряешбзкцколппотзуыайжххшеыабряязо дхпрэчфдяешоцкзвдаямыуайдосишщоччдыозлжцшшйфишцоцьзхлцюпзхщжщккжюыюпцчзпэыиывднишуушсешяоюшбчкзуя яяямзозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюптжждшсэыпзьцяделоц лыбжанхмлзннсюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузябряешйкешзоешчбгяыоиыоцпмзямодпмуч кшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоноожяяоьоэмк зшяпдмыэзгпйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзцжжущпрфуяшфсч двбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщомзмятыямйшалтыеызоешыедвайнинзшязпкцр фешмяеыцпяовкрфекуяжубждоджгллкпыбжанцйсщзорэкжшяанфшнширяязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюудве лдшчфилюшощжшийкшийцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпюдлвюп юпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцыезсочзсыяхщжипляэмнщеычяражуййюзвждвждмызхзосшзбкззжок уцеыюпцуыйтодыюпиызопызвкзмзюдайюдьмиыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчп мщпбкуяяоекшярбптхямзюдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншикщкпоноюааощяек шйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьфйказтзрэыосяфощждчвх еыхзжусжфрйктзшясжеьзоешрйэжпзжсбяаоешывбзлжцшшйфшрэщжссокыйшлцлыксфохямвмуйчжуезаяалжшбчшфсс ешмяпзюнзоешедвдвлгфезшйдбряилгфеыхзсккчвкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрй бжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутг эййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцыыиеыыявлаомяркгяштпцпмдущесзнонишкмокцжшлвждвдрэскал цяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкбяйбзбяшжддыцшдзщжэччамекуяанюзскжуэыощлзшящжбждояора тлынсаскрэууншмяскжупмскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопс йзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячовунщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщ жсыйрйшзяошйуфаляятфсчподояоносшнимоешдбждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлцлыксфохявж ядтлоцлывбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчбюпповбнзцжшзяойййпифрйщкжэппн шйкрзщыайхпжшжшвдщкхйппифрйуяпндощкпорфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшин шмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопжипеызозхьпешь омяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчфюшпфмяяявлвжипюпэышбмунрчфюшьосокыш ыхзхпезпыщжмосоьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывдюшлвоxдошзяобпбжжуэырйбзщтелмяилщкцж жзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгшьльфжшншмол допсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхфщжщлщяджипбжюпмуяззощуиврймзвожзпоф отывдохлцюпядайхпимиыраыжнэюшсйокбяжярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкю нзоносочзсыяхщжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказхяанаоешезвжбякб мурфоцхпэесопжипеышлзэтцчмгнпдрэбтюянзужнепзыжсыйсйщкжэгцлцечпфлцйшжбрякыыхзфшайтцлбгцабхявыцпяох яупайтзншщзнэйсшкопншфузхпмдьюшшящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышк бмщпбкуяяоекзожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэпбжжущчхябфбжд оцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвцчэжффйэракбяощзшжаокыыыщчсожзбиеызоузсуьмуяуыждддосш ншмоешдбждсожзбигцскыкфотфлцабгяыовояфяьшмущжвзлжыцмимшийгшезновжьошйээфщзрзмкуягшзбезносожзб иеыыядвзбряжзлжипюпоццбптдохлибвоанаопоьшйкешзокюывруxкнзеявжйэйканэущпзомязоныйфмяцяюакбмумяуысйчбя

мппыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгяыкаяшябялбгцабхямзюдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаоешезвжпоноп мйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйскпонзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшярллзджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюууфиыщчскподояоеыщжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюдншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязныръэтцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпеяпыэжйээпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

3. Під час написання програми основні труднощі виникли під час створення алгоритму для пошуку найчастіших біграм у шифротексті. Він проходить по матриці з кількістю повторення біграм та формує вектор с п’ятьма найчастішими. Реалізацію з коментарями можно подивитися у функції
`vector<int> bigram_ncross(vector<char> buff);`
Під час створення алгоритму що складає всі пари найчастіших біграм ОТ та ШТ та шукає претендентів на ключ. Проблему було вирішено чотирма циклами, на кожній ітерації він отримує можливий ключ з бар біграм та передає його у функцію, що фільтрує не російський тест.
4. П’ять найчастіших біграм ШТ: «щь», «ез», «ьв», «ди», «ся»
5. Опис роботи розпізнавача російської мови:
Ідея полягає у тому, що дістати із варанту розшифрованого тексту вектор п’яти найчастіших монограм та вектор п’яти найменш частих та порівняти його з аналогічними векторами для ОТ. Для перевірки кількості збігів була введена змінна check, що збільшується на одиницю кожен раз, коли найчастіший або найменш частий символ потенціального ОТ співпадає з аналогічним у мові. Дослідами ми визначили, що для справжнього російського тексту змінна check > 5. Ми отримаємо 2-3 варіанти тексту, з яких без зусиль знайдемо дійсний ОТ.

Отриманий ключ та ОТ:

(390, 10):
*еслиправдачтодостоевскийвсибирщщебылподверженприпадкммтоэтолишыподтверждаетточтоегоприпадкибылиегокаройонболеерщихненуждалсякогдабылкараемщьмобразоыщодокузатыэтонехозможноскорееэтойнеобводимостзюрщакузощфидляпсихическойэкэщомфидостоевскогообясняетсяточтоонпрошещщесломлущньмчерезэтфгодьбедствийивщижущийосуждениедостоевскоговкачествеполитическогопреступникабылонесправедливьмиондолженбылэтознатыноэщпрщллэтэщезаслужеьщоенаказаниеожбатюшкицарякакзммущвщакузощиязаслужущногоимзасвойгрехпоотношениюксвоемусобствущномуотцувместоюамонаказанияондалсебянаказатызаместителюотцаэтодаетнаыщекотороепредставлениеопсихологическомоправданищщакузощийприсуждаемьхобществхомэтонаюамомделетакыщогиеизпрестующиковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсммэщакузощиятоткохщаетслофщоефизмущчихоезначениеистерическихсимптомовпойметчтомьздесынепьтаемсядобитысясмьслаприпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитычтоихперхоначалынаясенностыосталасйщеизмущночщесморянавсепоследупниенаслоенияможноскузатычтодостоевскийтакникогдаинеосхододилсяотугрьзущийсовестивсвязиснамерениемубитыотцаэтолежащеущасовестибремяопределилотакжеегообщышущиекдоумдругишсферампокоющишснщаобщышущфикотцукгосударствущномуавторитетуикверевбогавпервойэщпришелкполномуподчщущиюбатюшкицарюотщаждьразьгравшемуащимкомедиюубийствавдействителйщостинаводившуюстолыкорузотражениевегоприпадкахздесыверхвзялопоканщиеболышесвободьоставалосыунегохобластирелигиознойпэщедопускапнимсоыщущийсведущиямондопослетщейминутьсвоейжизнивсеколебалсямеждзверойибезбожиемеговьсокийумнепоуволллемвщезммечатытетрутщостиосмьсливощияцкоторьмприводитверавиндивидуалыномповторениимирового гисторическогораувитияэщнаделлсявидеалехристощайтивьводиосхобождущиеотгреховфисполызоватысхоисобствевыьестраданиячтобьпритязатйщаролыхристаеслионвконежщомсчетущепришелксвободеисталреакциэщеромтоэтообяащяетсятемчтоотнечеловеческаяскщовняявщщощакоторойстроитсярелигиозноечзвстходостфглавщегосверхцщдивидуалйщойсильщщемоглабытыпреодоленадажееговьсокойцщтеялектуалйщостыюздесынаскузалосыбьможноупрешщутывтомчтомьотказьваемсяотбеспристрастностипсивоощализаиподвергаемдостоевскогооцущюеимеющейпрахонасущестхованиелишыспристрасбщойточкизренияопределущногомирохоззрениякэщсерваторсталбьнаточказрениявеликогоинквизитораиоценивалбьдостоевскогоиначеупрексправедливдляегосмягчущиямофщолишысказатычторешущиедостоевскоговьвощоочевитщозатрутщущностзюегомьшлениявследствиущеврозаедвалипростойслучачщостыюможнообяснитычтотришедеврммировойлитературьвсехремущтрактуютоднуитужетемутемуотцеубийствацарыэдипсофоклагамлетшекспираибратыякарммузовьдостоевскогововсехтрехраскрьваетсяимотивдеяниясексуалйщоесопеящичествоиззажущщиньпрямеевсегокэщечноэтопредставлущовдрммеоащовощночщагреческомскузощфиздесыдеяниесовершаетсяцнесммимгероемнобезсмягчущияизавуалированияпоэтическаяобработкощевозмофщаоткровеьщоепризнаниевнамеренииубитыотцакакогомьдобиваемсяприпсивоощализекажетсянепереносимьмбезощалитическойподготовкивгреческоэдраменеобводимоесмягчущиеприсохранениисенностимастерскидостфгаетсятемчтобессохщателйщьймотивгерояпроецируетсявдействительыностыкакчуждоеемупринуждущиенавязьащоесурыбойгеройсовершаетдеяниущепретщмерущноиповсейвидимостибеувлинщияжеянцщьивсежеэтостечущиеобстоятелыствпринимаетсяврасчеттаккаконможетзахоеватыцарицуматытолыкопослеповторущиятогожедействияхобщышущфичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникакихпопытокащятыеессебявзвалитыеенапрщуждениесостороньсурыбьнаоборотвинапризнаетсяикаквсщелаявинанаказьваетсячторассудкуможетпоказатысянесправедливьмнопс

ихологическиабсолюбщоправилыновганглийскоэдрамеэтоизображущоболеекосвущнопоступоксовершаетснщесммимгерое мадругимдлякоторогоэтотпоступокнеявляетсяотцеубийстхомпоэтомупредосудителйщьймотивсексуалйщогосоперниче ствауюущщиньненуждаетсявзаоуалировощфираращоийдиповкомплексгероямьвидимкакбьвотражеьщомсвететкакмьв идимлишытокакоедействиепроизходибщагерояпоступокдругогоондолженбылбьзаэтотпоступокотомститйщострощнь мобрузомневсилахэтосделатымьхщаемчтоегорасслабляетсобствущноечзвстховиньвсоответствшисхарактеромневроти ческихявлущийпроисходитсдвигичувствовщщьпереходитхосохщощиесвоечщеспосогщостивьпощщитыэтозаданиепоявля ютсяприхщакитогочтогеройвоспрщщимаетэтувинукаксверхцщдирщдуалйщуюэщпрезираетдругидщемущеечешсебяеслио бходитысяскаждьмпозаслугммктвуэдетотпоркивэтомнаправлениромощрусскогопиюателяуходитнашагдалошеиздесыу бийствосовершенодругимчеловекомотщакочеловекомсвязощньшсубитьмтакимижееьнорщимиобщышущиямикакигероэд митрийукоторогомотивсексуалыногосопеящичествааткровевьщоприхщаетсясовершенодругимбратомкоторомукакибте реснозаметитыдостоевскийпередалсвоюсобствущнуюболезныякобьэпилепсиютешсммьмкакбьжелаясделатыприхщощие чтомолэпилептишщевротиквомнеотцеубийцаивотвречизснитниканасудетажеизвестнанщасмешкощадпсихологиейонам олпалкаодоухкэщцахзавуалировановеликолеющотаккакстоитвсеэтоперевеящутыинаводишыглубочайшуюсенностывоспр иятиядостоевскогозаслуживаетнасмешкиотнюрынепсихологияасудебныйпроцесздохщощиясовершущнобезрузлижщокто этотпоступоксовершилнаюамомделепсивологияибтересуетсллишытемктоеговсхоемсердцежелаликтопоегосовершущфи егоприветствовалипоэтомувплотыдокобтрастнойффгурьалешивсебратыяравновинорщьдвижимьйпервижщьмипозьвм мфискателйщаслаждущийпощщьйскепсиюациникиэпилептическийпрестующиквбратыяхкарамазовьхестысценаввьсшей степенихарактернаядлядостоевскогоизразговорасдмитриемстаршпостфгаетчтодмитричщоситвсебеготовностыкот цеубийстоуиброюаетсяперетщимнаколениэтэщеможетявлятысявьражениемхосхщнущияадолфщоохщачатычтосвято йотстраняетотсебяискушениеисполнитысяпрезрениемкубийцеилиимпосцушатысяипоэтомупереднишсмиряетсясимпа тиядостоевскогокпреступникудействителйщобезгрощичнаэщадалековьходитзапредельсострадощиянакотороущесчаст ньйимеетправоонанапоминаетблагоговущиескоторьмвдрерщостиотносилисыкэпилептикуидушерщоболйщомупреступн икдлянегопочтиспасителывзявшичщасебявщукоторуювдругошслучающеслибьдругиеааоз

6. Висновок

Під час роботи ми набули навичок частотного аналізу на прикладі розшифрування тексту афінної підстановки. Також ми опанували прийомами роботи у модульній арифметиці. Під час виконання завдання нашою бригадою було вирішено поставленні задачі та створено власний декодер для даного виду шифру.