



Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

З предмету «Криптографія»

Варіант 8

Виконала:

студентка 3 курсу ФТІ
групи ФБ-84
Даневич А.С.

Перевірив:

Чорний О.М.

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:

1. Перед виконанням роботи ознайомилась з теоретичними відомостями та методичними вказівками, обдумала план виконання лабораторної роботи та визначила варіант відповідно до вказівок (Варіант 8).
2. Створила підпрограми з певними математичними операціями, а саме: обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда (`int evk(int a, int m, int size_mas)`), а також функцію для знаходження НОД (`int gcd(int a, int b, int& size_mas)`).
3. Визначила 5 найчастіших біграм шифрованого тексту 8 варіанту (“жц”, “дэ”, “цэ”, “сц”, “оц”).
4. Враховуючи, що біграма X1 перейшла при шифруванні у біграму Y1 , а біграма X2 – у біграму Y2 . То комбінуючи різні варіанти переходу біграм знайшли можливі ключі.
5. Оскільки з отриманих можливих ключів, правильний був лише один, потрібно було виконати перевірку на змістовність тексту після дешифрування. Перевірку здійснила шляхом порівнянн найбільш зустріваних літер російської мови, повторили порівнянн для найменш зустріваних букв та для найчастіших біграм.

[illegible]

мальчикуизубыбалисысжаромвзялисизаделоонирвализолотистыецветыцветычтоонавднюятовсесмирпереплескиваютсяслужакнамо щеныеулицытихонькостучатсявпрозрачныеокнапогребовнезнаютугомонуидерживвсевокругзаливаютслепящимсверканиемрасплавл енногосолнцакаждоелетоониточносцеписрываютсясказалдедушкапустыхнянепротиввонихсколькостоятгордыекакльвыпосмотриш ьнанихподольшетакипрожгутутебывглазахдыркуведьпростойцветокможносказатьсорнаятраваниктоеенезамечаетамыуважаемсчитае модуванчикблагородноерастениеонионабралиполнымешкиодуванчиковиунесливнизвпогребывалиилихизмешковивотъмепогребар азлилосьсияниевинныйпрессдождалсяихоткрытыйхолодныйзолотистыйпотоксогрелогодедушкапередвиулпрессповернулручкуза вертелбыстрейбыстрейпрессмягкостиснулдобычунувотвоттаксперватонкойструйкойпотомвсещедрееобильнеепобежалпожелобув линияныкеувишинысокпрекрасногожаркогомесяцаемудалиперебродитьснялипенуиразлиливчистыебутылкиизподкетчупаионивыстро илисьрядаминаполкахпоблескиваявсумракепогребавиноизодуванчиковсамыеэтисловаточнолетонаязыкевиноизодуванчиковпойман ноеизакупоренноевбутылкилетоитеперькогдадугласналпонастоящемузналчтоонживойчтоонзатемиходитпоземлечтобывидетьиошу патьмиронпонялещеоднадочастицувсегочтоонзналчастицуэтогоособенногодняднясбораодуванчиковтожезакупоритьисохранит ьапотомнастанеттакойзимнийянварскийденькогдавалитгустойснегисолнцаужедавнымдавнониктоневиделиможетбытьэточудопозаб ылосьихоршобыегосновавспомнитьвоттогдаоногооткупоритьведьэтолетонепременнобудетлетомнежданныхчудесинадовсеихсбере ч ыгдетоотложитьдлясебячтобыпослелюбоячаскогдавздумаешьпробратсянацыпочкахвовлажныйсумракипротянутьрукуитамрядза рядомбудутстоятьбутылкисвиноизодуванчиковонобудетмягкомерцатьточнораскрывающиесяназарецветыасквозьтонкийслойпыли будетпоблескиватьсолнценынешнегоиюнявзгляниисквозьэтовиноахолодныйзимнийденьснеграстаетизподнегопокажетсятраванаде ревяхоживутптицылистваицвetryсловномириадыбабочекзатрещутнаветруидажехолодноесероенебостанетголубымвозьмилетовр укуналейлетовбокалвсамыйкрохотныйконечноизкакогоотолькоисделаешьединственныйтерпкийглотокподнесигокгубамипожиламт воимвместолотойзимыпобежитжаркоелетотеперьдождевойводоконечноздесьодитсятолькочистейшаяводадальныхозерладостные росыбархатныххлутовчтовозносятсяназарекраспахнувшимисянавстречунебесамтамврохладныххвysяхониисобиралисьчистоомытымиг роздьямиветермчалихзасотнимилызаряжаяпопутиэлектрическимизарядамиэтавадобралавкаждуюсвоюкаплюещебольшенебескогд ападаладождемназемлюонапиталавсебявосточныйветеризападныйисеверныйиюжныйиобратиласьвдождьдождьэтотчассвященно действияужестановитсятерпкимвиномдуглассхватилковшвыбежалводвориглубокопогрузилеговбочоноксдождевойводойвотонавада былаточношелкппрозрачныйголубоватыйшелкеслиеевыпитьонакоснетсягубогорласердцамягкокакласканоквошиполноеведронадоотн естивпогребчтобыводапропиталатамвесьурожайодуванчиковструямиречекигорныххручевдажебабушкавакакойнибудьфевральскийд енькогдабеснуетсязаокномвьюгаислепитвесьмириуюдейзахватываетдыханьдажебабушкатихонькоспуститсявпогребнавверхуволь шомдомебудеткашельчиханьехриплыеголосоистоныпростуженнымдетямоченьбольнобудетглотатьаносыунихпокраснеютточновиш нивынугыеизналивкивсюдувдомепритаитсяковарныймикробитогдаизпогребавозникнетточнобогинялетабабушкапрячачтотоподвзяз нойшальюонапринесетэточтоготовкомнатукаждогоболящегоиразольетдушистоепрозрачноевпрозрачныестаканыистаканыэтиосушато днимглоткомлекарствоиныхвременбальзамизсолнечныхлучейипраздногоавгустовскогополудняедваслышныистукколестележжисмо роженнымчтокатитсяпомощенымулицамшорохсеребристогофейерверкачтогорассыпаетсявысоковнебеишелестсрезаннойтравыфонтано мбьющейизподкосилкичтодвижетсяполугампомуравьиномуцарствувсеэтовсеговдномстаканедадажебабушкакогдаспуститсявзимний погребзайонемнаввернобудетстоятьтамтихонькосовсемоднавтайномединенииисвоюсмороквеннымсвоейдушойкакидедушкаипап аидядябертидругиеэтожесловнобеседуястеньюдавноушедшихднейспикникамистеплымдождемсзапахомпшеничныхполейижареныхк укурузныхзеренисвежескошенногосеннадажебабушкабудетповторятьсясноваисноватежечудесныезолотящиесясловатозвучатсейчаско гдацвetyкладутподпресскакбудутихповторятькаждуюзимувсебелезимывовсременаснонаисноваонибудутслетатьсягубакулыбка какнежданныйсолнечныйзайчиквотъмевиноизодуванчиковвиноизодуванчиковвиноизодуванчиковониприходилинеслишноуходили почтибесшумнотравапригибаласьираспрямляласьвновьонискользиливнизпохоломаточнотениоблаковэтобежалилетнемальчишкид угласотстализаблудилисязадыхаясьотбыстрогобеаоностановилсянакраюовраганасамойкроменадпропастьюиоттудананегодохнулоо олодомнаостривушитоочнооленьонвдругучуларуюкакмиропасностьгородраспалсяздесьнадвеполовиныздеськончиласьцивилиза цияздесьживетлишьвспухшаяземляежечасносовершаетсямиллионсмертейирожденийиздесьпроторенныеилиишенепроторенныетроп ытвердятчтобыстатьмужчинамимальчишкидолжныстранствоватьсегдавсюжизньстранствоватьдугласобернулсяэтатропаогромнойп ыльноймеейскользитклядяномудомугдеврозолотыелетниеднипрячетсязимаатабежиткраскаленнымпесчанымберегамиюльскогоозераа вонтакдеревьямгдмальчишкипрячутсямежлистьевточнотерпкиеещенезрелыеплодыдикойяблониитамрастугизреютавоэттакперсико вомусадкувиноградникуогороднымгрядамгдедремлютнасолнцеарбузыполосатыесловнокошкиигровоймастиэтатропазаросшаякап

ризнаизвилистаяянетсякакшколеатапрямаякакстрелаксубботнимутренникамгдепоказываютковбойскиефильмыотэттавдольручьякди койлеснойчащедугласажмурилсяктоскажеттдекончаетсягородиначинаетсялеснаялушьяктоскажетгородврастаетвнеесилонапереход итгородиздавнаинавекисушествуетнекаянеуловимаяграницаоборютсядвесилииоднанавремяпобеждаетизавладеваетпросекойлощин ойлужайкойдеревомкустомбескрайнееморетравивцветовплещетсядалековполявокругодинокихфермалетомзеленыйприбойяроstown одступаетксамомугородуночьзаночьюначицилугадальнипросторыстекаютпооврагувсеближезахлестываютгородзапахомводыитравиг ородсловнопустеетмертвеетивновьуходитвземлюикаждоеутрооврагещеглубжевгрызаетсяявгородигрозитпоглотитьгаражиточныдыря выелодчонкиипожратьдопотопныеавтомобилиоставленныенамилюсьдождяиразедаемыержавчинойэяусквозьтайныоврагаигорода ивременимчалисьджонхафичарливудменэйдугласмедленнодвинулсяпотропинкеконечноееслихочешьпосмотретьнадвесамыеглавные вещикакживетчеловекикакживетприроданадоприйтисюдаковрагуведьгородвконцеоконцоввсеголишьбольшойпотрепанныйбурямик ораблянаемполнонародуивсехлопочутбезусталивычерпываютводуобкалываютржавчинупоройкакаянибудышлюпахибаркадетищек ораблясмытоенеслышнойбурейвременитонетвмолчаливыхволнахтермитовимуравьеввраспахнутойовражьейпастичтобыощутитькак мелькаюткузнечикиишуршатжаркихтравхточносухаябумагачтобыоглохнутьподпеленойтончайшейпылиинаконецрухнутьградомк амнейипотокомсмолькакрушатсятлеющиеугликостражженногоогромомисинеймолниейнамигозарившейгоржестволесныхдებрейта квотзначитчтотянулосядадугласатайнавойначеловекасприродойизгодавгодчеловекпохищаетчтооуприродыаприродавновьберетсв оеиниикогдагородпонастоящемудоконцанепобеждаетвечноемутрозитбезмолвнаяопасностьонвооружилсякосилкойитяпкойогромным иножницамионподрезаеткустыиопрыскиваетядомвредныхбукашекгусеницонупрямоплыветвпередпокаемувелитцивилизациянока ждыйдомтогоиглядизахлестнутзеленыеволныисхоронятнавекиакогданибудыслицаземлиисчезнетпоследнийчеловекиегокосилкиисад овыелопатыизеденныержавчинойрассыплетсяявпрахгородчащадомоврагдугласозадаченномигаетнокакаяжесвязьмежчеловекомип ридойкакпонятьчтозначатонидругдлядругакогдаонпустилглазапервыйлетнийобрядпозадиодуванчикисобраныизаготовленывпрок пораприступатьквторомунодугласзастылинедвижетсясместадугпошлидугголосашихливдалекеяживойсказалдугласночтотолкуон иещебольшеживыечемякакжеэтокакжетаконстоялвдиночествеглядянасвоиногневсилыхдвинутьсясместаинаконецпонялвотвечер дугласвозвращалсядомойизкиновместесродителямиибратомтомомиувиделихвяркоосвещеннойвитринемагазинатеннисныетуфлидуг ласпоспешноотвелглазаноегоногиужеощутилиприкосновениепарусиныизаскользилиповоздухубыстрейбыстрейземлязавертеласьзах лопалиполотняныенавесынадвитринамикакойонподнялветертаконмчалсяродителиитомшагалинеторопясьажедунимипятясьзадом шелдугласинесводилглазтеннисныхтуфельтампозадивполночнойвитринехорошаябылакартинасказаламаагабуркнулдугласстоя лионьдавноминовалотвремякогдалетопкупаюттакетуфлилегкиеитихиеточнотеплыйдождьчтошуршитпотротуарамужеиюныиз емляполнапервозданнойсилыивсевокругдвижетсяирастеттраваипосейденьпереливаетсясюдаизлуговомываеттротуарыподступаеткд омамкакжесягородвотгорчипнетбортомипокорнопойдетнадноивзеленомморетравнеостанетсяни всплесканирябидугласвдругзастыл точновросмертвыйасфальтикрасныйкирпичулицыневсилахтронутьсясместаппыпалилонвонтамвокнетеннисныетуфлиотецдажен еовернулсязачемтебеновыетуфлискажипожалуйстаможешьтымнеобъяснитьнуудазатемчтовнихчувствуешьсебятакбудтовпервыевэт олетоскинулбашмакиипобежалбосикомпотраветочновзимнююночьвысунулногиизподтеплогоодеялаиподставилветручтодышитхол одомвоткрытоеокноонистынутстынутапотомвтягиваешьихобратнопододеялоониловсемкаксосулькивтеннисныхтуфляхчувствуеш ьсебятакбудтовпервыевэтолетобредешьбосикомполенивморуучьюивпрозрачнойводевидишькактвоиногиступаютподнубудтоонипер еломилисьдвигутсячутьвпередитебяпотомчтоведьвводевсеидетсянетакпапсказалдугласэтооченьтруднообъяснитьаахф

Висновок:

У ході виконання комп'ютерного практикуму №3, я опанувала навички й методи роботи з модульною арифметикою, написала програму, яка розшифровує біграмно афінний шифр, проаналізувала його, закріпила навички частотного аналізу.