Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Фізико-технічний інститут

Криптографія

Лабораторна робота №3.

Виконали:

студенти гр. ФБ-94

Дум’як М.Р.

Мельниченко О. Г.

Київ 2021

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

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.

За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

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).

Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Варіант 5

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыох
унхмьввнсдуэммндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпьк
швнмщзфтсхщпддкясввццтнавпьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэ
кжлрибуждэмхимыпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкцц
зтчщиюцншумщошяьщкщнфрхуюижсгцыззфрщихзтчщрихнэпозтгфккчщкдм
клыоьеынуййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэив
упхюфйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбинкурдцбщшдск
рщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшдекхндуа
ошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфт
спьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйьрьэчтнундул
фтснсшбйнбжжцрнмющьккюиеуяэзтьяяреурндуьцоэгкмбобмщкскехюксдцтс
ывзтмсунйьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлак
лцисуьдьбкфипьйнмсуншснхтуйнццмсяьмныонкцркчыоклзфкчпьвныуозрбж
лжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццвнфиибхюпви
эислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянки
юджджкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяышвнунхщлвэкжлт
ьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщмб
риввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунав
шьавзтьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбье
елфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибх
юихтоццсввныклрынпьювюсисцйвнихчщлракющчьцнхщбщщйтннсхщдкищь
ешичщкздукчввзтьяакккйдищжлывьктзихывуллвовявшньсйссцпрыоынчкцця
ьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмв
шщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсч
зиьсунуллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгйрщтнгбфдзйьцэ

ибусчжвавмнззфдыоиюшсосюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцья
убщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшнищюиьсщож
сюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншс
пьчшвнюдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфс
чсбкаышнтныьзтпэпьмвзтьсйядуццщщцспрчсэьлвзтклбулцшвюибщыцвивну
йвнакеичмывпвыэдчфкклццсвынуняуумпьшвшрцциссцмючщиюлврлиэйбдцр
иьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожяшсввдуюизбывщшв
ныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсстгнхщщщфддбтьпнз
кьеэдхнщьжвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдйй
рснсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьсцклж
швнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнвв
швпвпьызмбйнвнцхпнуцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхи
лвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузб
щшьавтулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнп
вихэхаорщибясфсчсщьавпьскггыоюшлхвииспьвиулбутнзцнулцяьжцюсчвввй
имюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшь
явхщеуеидебупьесузющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищькк
ффдкфьнхчщмщявисчтжьамаофисрябсчшижслбубщэнщфдэмсщябубчзйсанэи
рщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхсовп
ннчубакакхуямдкяяхсвнхбжсмкщнщьжвэкссщьккдктнфифсбвбддкястнтнмсл
дьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьвнбк
убьебчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознк
ссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщубссвнхбрифкясхщфдцяьклр
ыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглозфьцэидктну
нэибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщ
нмкпмдкяярнэирщввпноулцфрынщхыщмснфжврйвньркзскыщссвнхбрифкясо
зййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьичдрщд

кикгбмщбущстссвйьшвоейулцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхзц
иссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзи
щссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзт
сиюгщхтнмспбмщбущськмюннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьреф
щакиеэдакролфбклцбуябзщбукзунгэщьккгнввшнивжврщрныуоззнбкжлтьбцр
ныгйснжшдекцгеэюсрсхщньбиулбунхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгу
ьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщбущсфрмщчяовупмюосшнкуаох
щмсэкццзтбыыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихщав
иэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдрошджсю
сунынмсйкмбкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсц
цьблшэннбвамозмщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйе
бчввтсзкиющьккбыоскчицпьявицчзивяьочлцсвпдгсуфдкфьяэюдаорибщвчрыт
нрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьфзтнуноьюддк
нхживналбуыодкеиочоьлхэфдкфыпьлннсвнмкхсмщтсывзтьятнакфкпрябйожс
юсунюиикцфтсввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрнхщбщы
цвиклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгьерынньэьынавэкиют
ыннькиютноьакеишдщщшвпвмндтихжцшнйнюирсыэьяокпмаобщцсэщбушсх
мсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунтсчтгвмь
ввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнц
нерссжофкеиябпвистнпвюскиосырынщэгожсгцмефдфмжяосзкццзтпытнрсакь
лмщриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщцсунхдицяедьакхуумжсвн
чрлвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиь
янсибясшнлсиьпвтснфюирыюсцьаккнивжошижсмкарссжозщццесшндцнскка
ирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяспнчкхуцфюижсш
щязюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщш
дбофдгвмсжкддьяжьяущнвввввшнмьвврщозенйсуньейпфкаьтныоеущькхзцнул
цзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйн

внцхмьакггмщшджсунлххэхьзтлрэчбудкввзнввшнжьжврщунынжвжрццисчцэ
иаьмчввращищссркжэжвмндтфрлцяьклхнгцязвэкьзцэиьшсвмдьцюяусиебчдуье
шдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпь
гбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвбддкяяы
оввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошд
дкяяфсшьыоарфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьв
вьщянмсхмдктнянккбщшдекццжлывйквэпншнхщынгспныэрнгошддкйыявзтц
нюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвюдццфюирыусун
лрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкч
мстспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшны
нйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзти
эярчсжвюсстибдцньтсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюсстгнул
буввзнтснфчзццзтвииярщьякбньависйщкзхщхуиюшннуяетнхщюиакфккчлспь
ыопьрцмнрншбынлсюдризьяуфкшдвчскскчавзтрщхсщв

Ключ(654, 777)

убиватьбольшененадопослетогокаконужеубилнаследуетемубытьблагодарны
миначепришлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотож
дествлениенаосновании одинаковыхимпульсовкубийствусобственноговоряли
шьвминимальнойстепенисмещенныйнарциссизмэтическаяценностьэтойдобро
тыэтимнеоспариваетсяможетбытьэтовообщемеханизмнашегодоброгоучастия
поотношениюкдругомучеловекуособеннояснопроступающийвчрезвычайномс
лучаеобремененногосознаниясвоейвиныписателянетсомнениячтоэтасимпатия
попричинеотождествлениярешительноопределилавыборматериаладостоевско
гоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступн
икаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпер
вопреступникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопуб
ликованиеегопосмертногонаследияидневниковегоженыяркоосветилоодинэпи
зодегожизнитовремякогдадостоевскийвгерманиибылобуреваемигорнойстраст
ьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеп
оддаетсяинойоценкенискакойсторонынебылонедостаткавоправданияхэтогост

ранногоинедостойногоповедениячувствовиныкакэтонередкобываетуневротик
овнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймоготгова
риватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсяврроссиюизб
ежавзаключенияявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбы
лдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомприз
натьсяонзналчтоглавнымбылаиграсамапосебевсеподробностиегообусловленн
огопервичнымипозывамибезрассудногоповеденияслужаттомудоказательство
миещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготак
жесредствомсамонаказаниянесчетноеколичествораздавалонмолодойженеслов
оиличестноесловобольшенеиграть илинеиграть вэтотденьионнарушалэтослово
каконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяиеед
окрайнебедственногоположенияэтослужилодлянегоещеоднимпатологически
мудовлетворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезирать
егораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаипослевсейэт
ойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапри
выклакэтомуциклутаккакзаметилачтотоотчеговдействительноститолькоимож
нобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшече
мпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонак
онечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниямиккот
орымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозво
лялсебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемоло
догописателянетрудноугадаткакиедавнопозабытыедетскиепереживаниянахо
дятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеждупрочимдос
тоевскомуодинизсвоихочерковтримастеравсборникесмятениечувствестьнове
лладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываеткак
будтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеуд
ивительныедлянеесамойзакононарушенияеетолкаетнеожиданноежизненноев
печатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованию
говоритоднакобезтакойоправдывающейтенденциигораздобольшепоказываетс
овсеминоеобщечеловеческоеилискорееобщемужскоеитакоетолкованиестолья
вноподсказаночтонетвозможностиегонедопуститьдлясущностихудожественн
оготворчествахарактерночтописательскоторымменясвязываютдружескиеотно
шенияответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждои
вовсеневходиловегонамерениянесмотрянаточтоврассказвплетенынекоторыед
еталикакбырассчитанныенаточтобыуказыватьнатайныйследвэтойновеллевел
икосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережитьбол
еедвадцатилеттомуназадранооводовевшаяматьдвухсыновейкоторыевнейболее

ненуждалисьотказавшаясяоткакихбытонибылонадежднасороквторомгодужиз
нионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалм
онакскогоказиногдесредивсехдиковинеевниманиеприковываютдверукикотор
ыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенес
частнымигрокомчувстварукиэтирукикрасивогоюношиписателькакбыбезовсяк
огоумысладелаетегоровесникомстаршегосынанаблюдающейзаигройженщин
ыпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпаркепоко
нчитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинус
ледоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизм
ногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонане
покидаетегоивынужденавконцеконцоввсилусложившихсяобстоятельствостат
ьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойлюбо
внойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноеоб
ещаниечтоонникогдабольшенебудетиграться снабжаетегоденьгаминаобратныйп
утьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокз
аленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожертвова
тьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместев
путешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаюте
еионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвиг
орныйдомисвозмущениемобнаруживаеттамтежерукинакануневозбудившиевн
ейтакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетему
обегообещаниионодержимыйстрастьюонбранитсорвавшуюегоигрувелитейуб
иратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонап
окидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэ
таблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправ
онасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпеч
атленияоднакопсихоанализучитчтоонавозникланаосновеумопостроя емогово
жденияпериодаполовогосозреванияокаковомвожденииинекоторыевспоми
наютсовершенносознательносогласноумопостроя емомувожделениюматьдол
жнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопас
ениявредаонанизмастольчастыесублимирующиехудожественныепроизведени
явытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорн
ойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательскисв
идетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляет
сяэквивалентомстаройпотребностивонанизмениоднимсловомкромесловаигра
нельзяназватьетееаа

Висновок: виконуючи дану лабораторну роботу ми набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки і опанували прийомами роботи в модулярній арифметиці