МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота №3
З дисципліни «Криптографія»

Виконали:
Пасько Олександр ФБ-84
Завгородня Анастасія ФБ-81

Перевірив:
Чорний О. М.

Київ 2020

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 початком виконання роботи ми уважно ознайомились з теоретичними відомостями та методичними вказівками до виконання лабораторної роботи; обговорили план виконання лабораторної роботи та визначили варіант згідно вказівок(Варіант 5).

2 Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь.

3 Визначили 5 найчастіших біграм шифротексту варіанту 5 **['вн', 'тн', 'дк', 'хщ', 'ун']**
Та знайшли кандидатів на ключ.

4 Для кожного знайденого кандидата на ключ дешифрували текст та зробили перевірку(чи є змістовним текстом російською мовою). Перевірку здійснили шляхом порівняння найбільш зустріваних літер ВТ і найбільш зустріваних літер російської мови, повторили дане порівняння для найменш зустріваних букв і для найчастіших біграм ВТ.

Труднощі при виконанні ЛР

При виконанні завдання, ми зіткнулися з частково неправильним розшифруванням ШТ.

Для розв’язання даної проблеми, нам слід було просто змінити місцями в алфавіті літери “ы” та “ь”. Адже помилка розшифрування виникала при такому їх розміщенні: “ы ь”.

Коли ми виправили алфавіт, то розшифрування ШТ пройшло успішно.

5 найчастіших біграм у шт

['вн', 'тн', 'дк', 'хщ', 'ун']

ШТ(5 варіант)

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэм
мндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввццтнавп
ьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзцюсфспьузйпдкнхр
кхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсгцыззфрщихзтчщрихнэпо
зтгфккчщкдмклыоьеынуййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивуп
хюфйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищж
шсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшдекхндуаошдвдеигебуявюсшьйдроццвнфи
ибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйья
ьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющьккюиеуяэзтьяяреурндуьцоэгкмбобмщкс
кехюксдцтсывзтмсунйьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклци
суьдьбкфипьйнмсуншснхтуйнццмсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбип
срзфкаьихмнщэчсавозулбутнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзй
ьцйнзцнулцяьйнвнцхркпрыожврщьянкиюджджкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвц
офкяяышвнунхщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэо
сыумщмбриввудябакфурщяэлчязджаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавз
тьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбьеелфеипвидийдкяязщп
упзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсисцйвни
хчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовяв
шньсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспь
ицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсчязиьсун
уллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгйршгтнгбфдзйьцэибусчжвавмнззфдыои
юшсосюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщхичщмщгсчтгнэкхуямйдчщццмнр
ншвйнввлвацшвьхаврщшнищюиьсщожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюо
сйсчцэидктнуншнмншспьчшвнюдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкясп
нззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуцщщцспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеи
чмывпвыэдчфкклццсвынуняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодк
чьяуфкойнкйдлцыцтнавчзфдыожяшсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнс
унцомюхщньюссттнхщщщфддбтьпнзкьеэдхнщьжвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрын
сиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьс
цклжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвпьызм
бйнвнцхпнуцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянця
еьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьавтулцибсчннисозфдыожллрдцбщшдскр
щиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфсчсщьавпьскггыоющлхвииспьвиулбутнзцну

лцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшь
явхщеуеидебупьесузющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхчщм
щявисчтжьамаофисрябсчшижслбубщэнщфдэмсщябубчзйсанэирщхщмсэктзлэусхщрнляпдгсг
цшфдкфьввнкубубяслоюищщшдекщсхдскхсовпннчубакакхуямдкяяхсвнхбжсмкщнщьжвэксс
щьккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбриф
кйыунрншьвнбкубьебчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцозн
кссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщубссвнхбрифкясхщфдцяьклрыоибсчфкщйв
носэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглозфьцэидктнунэибунсхщавьвлващеутнищл
рдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпноулцфрынщхыщмснф
жврйвньркзскыщссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищри
лвацшвьичдрщдкикгбмщбущстссвйьшвоейулцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхз
циссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзищссыршьудцц
рреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнмспбмщбущськмю
ннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщьккгнв
вшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньбиулбунхнчйдпнввкцйнуншвэьт
нщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщбущсфрмщчяовупмюосшнкуао
хщмсэкццзтбыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихщавиэжьчщоуобм
блвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзхщхурсунщхв
вввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамозмщбвскаьшнжьжвупклэчйди
щьешиивебпрябакоьзтянщиссйебчввтсзкиющьккбыоскчицпьявицчзивяьочлцсвпдгсуфдкфьяэ
юдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьфзтнуноьюдд
кнхживналбуыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтс
ввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьз
тклллрццюсстшнюдкшвнгьерынньэьынавэкиютынныкиютноьакеишдщщшвпвмндтихжцшнйн
юирсыэьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввя
фжсюсунтсчтгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэл
нцнерссжофкеиябпвистнпвюскиосырынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфе
уэирибщхиьсуйвнихвнстйнянцуфкщщцсунхдицяедьакхуумжсвнчрлвньзтьяйкчзезьцюсжрыщ
умьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлсиьпвтснфюирыюсцьаккнивжош
ижсмкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуъэиулбунхмокздцрнфзфпдкясп
нчкхуцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщш
дбофдгвмсжкддьяжьяущнвввввшнмьвврщозенйсуньейпфкаьтныоеущькхзцнулцзтднчелвпьгцб
уавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхмьакггмщшджсунлххэхьзт
лрэчбудкввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяьклхнгцязвэ
кьзцэиьшсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнвв
лэусхщрнавпьгбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвбддкяяыо
ввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкрижэпншнхщынгспнурнрнгошддкяяфсшьыоарф
дрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекцц
жлывйквэпншнхщынгспныэрнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдици
вьспьгсунмщпвюдцфюирыусунлрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьц
эидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшнын
йнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчсжвюсстибд
цньтсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюсстгнулбуввзнтснфчзццзтвииярщьякбнь
ависйщкзхщхуиюшннуяетнхщюиакфккчлспьыопьрцмнрншбынлсюдризьяуфкшдвчсксчавзтр
щхсщв

РОЗШИФРУВАННЯ (ключ (654, 777))

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлос
ьбыубиватьсамомуэтонеоднолишьдоброесострадание этоотождествлениенаоснованииодинак
овыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещенныйнарциссиз
мэтическаяценностьэтойдобротыэтимнеоспариваетсяможетбытьэтовообщемеханизмнашегод
оброгоучастияпоотношениюкдругомучеловекуособенноясноп роступающийвчрезвычайномсл
учаеобремененногосознаниясвоейвиныписателянетсомнениячтоэтасимпатияпопричинеотож
дествлениярешительноопределилавыборматериаладостоевскогоносначалаонизэгоистических
побужденийвыводилобыкновенногопреступникаполитическогоирелигиозногопреждечемкко
нцусвоейжизнивернутьсякпервопреступникукотцеубийцеисделатьвеголицесвоепоэтическоеп
ризнаниеопубликованиеегопосмертногонаследияидневниковегоженыяркоосветилоодинэпизо
дегожизнитовремякогдадостоевскийвгерманиибылобуреваемигорнойстрастьюдостоевскийза
рулеткойявныйприпадокпатологическойстрастикоторыйнеподдаетсяинойоценкенискакойсто
ронынебылонедостаткавоправданияхэтогостранногоинедостойногоповедениячувствовиныка
кэтонередкобываетуневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевс
киймоготговариватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсяврос сиюизбе
жавзаключенияв тюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточнопрон
ицателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавнымбылаиг
расамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассудногоповеден
ияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбы
ладлянеготакжесредствомсамонаказаниянесчетноеколичествораздавалонмолодойженесловои
личестноесловобольшенеиграть илинеиграть вэтотденьионнарушалэтословокаконарассказыва
етпочтивсегдаеслионсвоимипроигрышамидоводилсебяиедокрайнебедственногоположенияэ
тослужилодлянегоещеоднимпатологическимудовлетворениемонмогпереднеюпоноситьиуниж
атьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаи
послевсейэтойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапривык
лакэтомуциклутаккакзаметилачтотоотчеговдействительноститолькоиможнобылоожидатьспа
сенияписательствоникогданепродвигалосьвпередлучшечемпослепотеривсегоизакладыванияп
оследнегоимуществасвязивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудовл
етворенонаказаниямиккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработето
гдаонпозволялсебеделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодого
писателянетрудноугадаткакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигор
нойстрастиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтри
мастеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотмален
ькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляетсяженщина
инакакиеудивительныедлянеесамойзаконо нарушенияеетолкаетнеожиданноежизненноевпеча
тлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобезта
койоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилиск
орееобщемужскоеитакоетолкованиестольявноподсказаночтонетвозможностиегонедопустить
длясущностихудожественноготворчествахарактерночтописательскоторымменясвязываютдру
жескиеотношенияв ответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждоивов
сеневходиловегонамеренияне смотрянаточтоврассказвплетенынекоторыедеталикакбырассчит
анныенаточтобыуказыватьнатайныйследвэтойновеллевеликосветскаяпожилаядамаповеряетп
исателюотомчтоейпришлосьпережитьболеедвадцатилеттомуназадраноовдовевшаяматьдвухс
ыновейкоторыевнейболеененуждалисьотказавшаясяоткакихбытонибылонадеждна сороквторо
мгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакск
огоказиногдесредивсехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепос
редственностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикр
асивогоюношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюда
ющейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпарк

епокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьз аюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочисленныхвтомгород енавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужденавконцеконцоввс илусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойимп ровизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжествен ноеобещаниечтоонникогдабольшенебудетиграть снабжаетегоденьгаминаобратныйпутьисосво ейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробужда етсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяи онарешаетотправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиеп омехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходи твигорныйдомисвозмущениемобнаруживаеттамтежерукинаканувевозбудившиевнейтакуюго рячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещаниииноодержи мыйстрастьюонбранитсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымиона хотелаеговыкупитьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспасти егоотсамоубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечно правонасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпечатленияод накопсихоанализучитчтоонавозникланаосновеумопостроя емоговожделенияпериодаполового созреванияокаковомвожделениинекоторыевспоминаютсовершенносознательносогласноумоп остроя емомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзасл уживающегоопасениявредаонанизмастольчастыесублимирующиехудожественныепроизведе ниявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрастиуда рениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомотводеэ нергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивонанизм ениоднимсловомкромесловаигранельзяназватьетееаа

Висновок

Виконуючи дану лабораторну роботу, ми опанували навички і методи роботи з модульною арифметикою, зробили програму для розшифрування біграмного афінного шифру, проаналізували його, закріпили навички частотного аналізу.