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:
Правдива Тамара ФБ-02
Бобер Наталія ФБ-05

Перевірила: Селюх П. В.

Київ 2022

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 ознайомились з теоретичними відомостями та методичними вказівками до виконання лабораторної роботи.
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

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)

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэмм
ндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввццтнавпьгн
уьввйнлхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзцюсфспьузйпдкнхркх
ульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсгцызззфрщихзтчщрихнэпозтгфк
кчщкдмклыоьеынунййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивупхюфйч
сьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяишжшсвыьербщ
яяшндузйнкщнвнгоьцэииспьтуумщщшдекхндуаошдвдеигебуявюсшьйдроццвнфиибжлакццввб
вываккчслтьхщзйьцжьбрьецфтспьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчс
йьрьэчтнундулфтснсшбйнбжжцрнмющькккюиеуяээтьяяреурндуьцоэгкмбобмщкскехюксдцтсы
взтмсунйьксщиссшнчщзйьцйнпршькккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипь
йнмсуншснхтуйнццмсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщ
эчсавозулбутнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяь
йнвнцхркпрыожврщьянкиюждкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяьшвнунх
щлвэкжлтьосцнхщиютнуншнмстспьлйаихщрннънхшвщшвносчсабьешижсоэосыумщмбриввудяб
акфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнакдую
иььяучмпрфдййвдихрнфззфтнхщхиеуяээтьяыуццыьбьеелфеипвидийдкяязщпупзобчсуьвнлв
мьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсисцйвнихчщлракющчьцнх
щбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовявшньсйссцпрыоынчк
ццяьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмвшщкзлоябсчб
щшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсчязиьсунуллвихывхдскклмщубшс
куаохщрнрцязакубсчфкяяосгйрщтнгбфдзйьцэибусчжвавмнззфдыоиюшсосюдритьйьнсхщтнь
цмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшн
ищюиьсщожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшв
нюдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфсчсбкаьшнтныьзтпэпь
мвзтьсйядуццщщцсprчсэьлвзтклбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвынуняуу
мпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожя
шсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюссттнхщщщфддбтьпнзкь
еэдхнщьжвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшь
сцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьсцклжшвнунакубакюйтносшнпьявывйнщож
сунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвпьыызмбйнвнцхпнуцязьсйядуулрибувдвнщозьгй
бчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфрт
грулцузбщшьавтулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхао
рщибясфсчсщьавпьскггыоющлхвииспьвиулбутнзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсг
оьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшьявхщеуеидебупьесузюшдкясюэсцэиьцзттн
мслдроавежбщяйрщйуюйлцеищькккффдкфьнхчщмщявисчтжьамаофисрябсчшижслбубщэнщфдэмс
щябубчзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубясложищщшдекщсхдскхсовпн
нчубакакхуямдкяяхсвнхбжсмкщнщьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсие
уюкыщцспрыьлнфкйдшщзйьцйныэвнхбрифкйыунрншьвнбкубьебчсвйнжндуеисхавупмююсшодк
льулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщубс
свнхбрифкясхшфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглозф
ьцэидктнунэибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмд
кяярнэирщввпноулцфрынщхышмснфжврйвньркзскыщссвнхбрифкясозййцфцнюириьсосйгыовд
риклакязеудкяяосузмщчяввврнищрилвацшвьичдрщдкикгбмщбущстссвйьшвоейулцгйщщфкнхд
кбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхь
овюстымщкзищссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсию
гщхтнмспбмщбущськмюннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуяб
зщбукзунгэщькктгнввшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньбиулбунхнчй
дпнввкцйнуншвэьтнщоьцчсуьсцтгуьйннъосфипьявпьпршьйнлхавьщсиеуобмбмщбущсфрмщчя
овупмюосшнкуаохщмсэкццзтбыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихща
виэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзхщ
хурсунщхвввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамозмщбвскаьшнжьжву
пклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкиющьккбыоскчицпьявицчзивяьочлцсвпд
гсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьф
зтнуноьюддкнхживналбуыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюс
унюиикцфтсввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрнхщбщыцвиклаккзеущнюсияо
усчтсйьзткллрццюсстшнюдкшвнгьерынньэьынавэкиютыннькиютноьакеишдшщшвпвмндтихжц
шнйнюирсыэьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцв
вяфжсюсунтсчтгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчс
гэлнцнерссжофкеиябпвистнпвюскиосырынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарз
феуэирибщхиьсуйвнихвнстйнянцуфкшщцсунхдицяедьакхуумжсвнчрлвньзтьяйкчзезьцюсжр

ьщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлсиьпвтснфюирыюсцьаккнивжош
ижсмкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяспн
чкхуцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщшдбоф
дгвмсжкддьяжьяущнввввшнмьвврщозенйсуньейпфкаьтныоеущькхзцнулцзтднчелвпьгцбуав
кмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхмьакггмщшджсунлххэхьзтлрэчб
удкввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяькклхнгцязвэкьзцэи
ьшсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусх
щрнавпьгбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыг
евввйьмэоьжйвнакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшьыоарфдрижлццэчч
савпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекццжлывйквэпншн
хщынгспныэрнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвю
дцфюирыусунлрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмс
тспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшныйнмьунжкиюхщлвх
щпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчсжвюсстибдцньтсюсстхщээрщье
чщкзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуиюшнн
уяетнхщюиакфккчлспыыопьрцмнрншбынлсюдризьяуфкшдвчсксчавзтрщхсщв

РОЗШИФРУВАННЯ (ключ (654, 777))

убиватьбольшененадопослетогоконужеубилноследуетемубытьблагодарныминачепришл
осьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснованиио
динаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещенныйна
рциссизмэтическаяяценностьэтойдоброты этимнеоспариваетсяможетбытьэтовообщемехан
измнашегодоброгоучастияпоотношениюкдругомучеловекуособенноясноп роступающийвчр
езвычайномслучаеобремененногосознаниясвоейвиныписателянетсомнениячтоэтасимпат
ияпопричинеотождествлениярешительноопределилавыборматериаладостоевскогоноснача
лаонизэгоистическихпобужденийвыводилобыкновенногопреступникаполитическогоире
лигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступникукотцеубийцеисдел
атьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертногонаследияидневни
ковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманииибылоб
уреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпатологическойстрасти
которыйнеподдаетсяиной оценкенискакойстороныне былонедостаткавоправданияхэтогос
транногоинедостойногоповеденияучувствовиныкакэтонередкобываетуневротиковнашлок
онкретнуюзаменувобремененностидолгамиидостоевскиймоготговариватьсятемчтоонпри
выигрышеполучилбывозможностьвернутьсяврассиюизбежавзаключениявтюрьмукредитора
миноэтобылтолькопредлогдостоевскийбылдостаточнопроницателенчтобыэтопонятьидос
таточночестенчтобывэтомпризнатьсяонзналчтоглавнымбылаиграсамапосебевсеподробн
остиегообусловленногопервичнымипозывамибезрассудногоповеденияслужаттомудоказа
тельствомищекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготакже
средствомсамонаказанияне счетноеколичествораздавалонмолодойженесловоиличестное
словобольшенеиграть ылинеиграть вэтотденьионнарушалэтословокаконарассказываетпо
чтивсегдаеслионсвоимипроигрышамидоводилсебяиеедокрайнебедственногоположенияэт
ослужилодлянегоещеоднимпатологическимудовлетворениемонмогпереднеюпоноситьиуни
жатьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогре
шникаипослевсейэтойразгрузкисовестинаследующийденьиграначиналась сноваимолодая
женапривыклакэтомуциклутаккакзаметилачтотоотчеговдействительноститолькоиможно
былоожидатьспасенияписательствоникогданепродвигалосьвпередлучшечемпослепотери
всегоизакладыванияпоследнегоимуществавсвязивсегоэтогоонаконечнонепонималакогда
егочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговорилтогдаисч
езалазатрудненностьвработетогдаонпозволялсебесделатьнесколькошаговнапутикуспе
хурассматриваярассказболеемолодогописателянетрудноугадатькакиедавнопозабытыед
етскиепереживаниянаходятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеж
дупрочимдостоевскомуодинизсвоихочерковтримастеравсборникесмятениечувствестьно
велладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываеткакбудтолишь
токакимбезответственнымсуществомявляетсяженщинаинакакиеудивительныедлянеесамо
йзакононарушенияееголкаетнеожиданноежизненноевпечатлениеноновеллаэтаеслиподве
ргнутьеепсихоаналитическомутолкованиюговоритоднакобезтакойоправдывающейтенден
циигораздобольшепоказываетсовсеминоеобщечеловеческоеилискорееобщемужскоеитако
етолкованиестольявноподсказаночтонетвозможностиегонедопустить длясущностихудож
ественноготворчествахарактерночтописательскоторымменясвязываютдружескиеотноше
ниявответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждоивовсеневходил
овегонамерениянесмотрянаточтоврассказвплетенынекоторыедеталикакбырассчитанные

наточтобыуказыватьнатайныйследвэтойновеллевеликосветскаяпожилаядамаповеряетпи
сателюотомчтоейпришлосьпережитьболеедвадцатилеттомуназадраноовдовевшаяматьдву
хсыновейкоторыевнейболеененуждалисьотказавшаясяоткакихбытонибылонадеждаснасорок
второмгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйза
лмонакскогоказиногдесредивсехдиковинеевниманиеприковываютдверукикоторыеспотря
сающейнепосредственностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувств
арукиэтирукикрасивогоюношиписательказкакбыбезовсякогоумысладелаетегоровесникомст
аршегосынанаблюдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидаю
щегозалчтобывпаркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставл
яетженщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуиз
многочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаете
гоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляи
разделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыус
покоившемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетиграться
абжаетегоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпере
духодомпоездаиавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапо
жертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевп
утешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопазды
ваетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущениемо
бнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушительдо
лгавернулсякигреонанапоминаетемуобегообещанииноодержимыйстрастьюонбранитсорва
вшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозо
реннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийств
аэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправонасущес
твованиекактаковаяинеможетнепроизвестиначителябольшоговпечатленияоднакопсих
оанализучитчтоонавозникланаосновеумопострояемоговожделенияпериодаполовогосозр
еванияокаковомвожделениинекоторыевспоминаютсовершенносознательносогласноумопо
строяемомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзас
луживающегоопасениявредаонанизмастольчастыесублимирующиехудожественныепроизве
дениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрас
тиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетоб
этомотводеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпот
ребностивонанизмениоднимсловомкромесловаигранельзяназватьетееаа

Висновок

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