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

Криптографiя

**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

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэммндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввццтнавпьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсгцыззфрщихзтчщрихнэпозтгфккчщкдмклыоьеынунййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивупхюфйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшдекхндуаошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющьккюиеуяэзтьяяреурндуьцоэгкмбобмщкскехюксдцтсывзтмсунйьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйнмсуншснхтуйнццмсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюдждкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяышвнунхщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщмбриввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбьеелфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсисцйвнихчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовявшньсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсчзиьсунуллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгйрщтнгбфдзйьцэибусчжвавмнззфдыоиюшсосюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшнищюиьсщожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшвнюдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуццщщцспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвынуняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожяшсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюссттнхщщщфддбтьпнзкьеэдхнщьжвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьсцклжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвпьызмбйнвнцхпнуцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьавтулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфсчсщьавпьскггыоющлхвииспьвиулбутнзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшьявхщеуеидебупьесузющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхчщмщявисчтжьамаофисрябсчшижслбубщэнщфдэмсщябубчзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхсовпннчубакакхуямдкяяхсвнхбжсмкщнщьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьвнбкубьебчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщубссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглозфьцэидктнунэибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпноулцфрынщхыщмснфжврйвньркзскыщссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьичдрщдкикгбмщбущстссвйьшвоейулцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзищссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнмспбмщбущськмюннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщьккгнввшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньбиулбунхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщбущсфрмщчяовупмюосшнкуаохщмсэкццзтбьыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихщавиэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамозмщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкиющьккбыоскчицпьявицчзивяьочлцсвпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьфзтнуноьюддкнхживналбуыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгьерынньэьынавэкиютыннькиютноьакеишдщщшвпвмндтихжцшнйнюирсыэьяокпмаобщцсэщбушсхмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунтсчтгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпвюскиосырынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщцсунхдицяедьакхуумжсвнчрлвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлсиьпвтснфюирыюсцьаккнивжошижсмкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяспнчкхуцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнввввшнмьвврщозенйсуньейпфкаьтныоеущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхмьакггмщшджсунлххэхьзтлрэчбудкввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяьклхнгцязвэкьзцэиьшсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпьгбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшьыоарфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекццжлывйквэпншнхщынгспныэрнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвюдцфюирыусунлрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшнынйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчсжвюсстибдцньтсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуиюшннуяетнхщюиакфккчлспьыопьрцмнрншбынлсюдризьяуфкшдвчсксчавзтрщхсщв

**Ключ(654, 777)**

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлосьбыубиватьсамомуэтонеоднолишьдоброесостраданиеэтоотождествлениенаоснованииодинаковыхимпульсовкубийствусобственноговорялишьвминимальнойстепенисмещенныйнарциссизмэтическаяценностьэтойдобротыэтимнеоспариваетсяможетбытьэтовообщемеханизмнашегодоброгоучастияпоотношениюкдругомучеловекуособеннояснопроступающийвчрезвычайномслучаеобремененногосознаниясвоейвиныписателянетсомнениячтоэтасимпатияпопричинеотождествлениярешительноопределилавыборматериаладостоевскогоносначалаонизэгоистическихпобужденийвыводилобыкновенногопреступникаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопреступникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертногонаследияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманиибылобуреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйнеподдаетсяинойоценкенискакойсторонынебылонедостаткавоправданияхэтогостранногоинедостойногоповедениячувствовиныкакэтонередкобываетуневротиковнашлоконкретнуюзаменувобремененностидолгамиидостоевскиймоготговариватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсявроссиюизбежавзаключениявтюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточнопроницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавнымбылаиграсамапосебевсеподробностиегообусловленногопервичнымипозывамибезрассудногоповеденияслужаттомудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготакжесредствомсамонаказаниянесчетноеколичествораздавалонмолодойженесловоиличестноесловобольшенеигратьилинеигратьвэтотденьионнарушалэтословокаконарассказываетпочтивсегдаеслионсвоимипроигрышамидоводилсебяиеедокрайнебедственногоположенияэтослужилодлянегоещеоднимпатологическимудовлетворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьсявтомчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестинаследующийденьиграначиналасьсноваимолодаяженапривыклакэтомуциклутаккакзаметилачтотоотчеговдействительноститолькоиможнобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшечемпослепотеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнонепонималакогдаегочувствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговорилтогдаисчезалазатрудненностьвработетогдаонпозволялсебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемолодогописателянетрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорнойстрастиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтримастеравсборникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказываеткакбудтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеудивительныедлянеесамойзакононарушенияеетолкаетнеожиданноежизненноевпечатлениеноновеллаэтаеслиподвергнутьеепсихоаналитическомутолкованиюговоритоднакобезтакойоправдывающейтенденциигораздобольшепоказываетсовсеминоеобщечеловеческоеилискорееобщемужскоеитакоетолкованиестольявноподсказаночтонетвозможностиегонедопуститьдлясущностихудожественноготворчествахарактерночтописательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчтоупомянутоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврассказвплетенынекоторыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэтойновеллевеликосветскаяпожилаядамаповеряетписателюотомчтоейпришлосьпережитьболеедвадцатилеттомуназадраноовдовевшаяматьдвухсыновейкоторыевнейболеененуждалисьотказавшаясяоткакихбытонибылонадежднасороквторомгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакскогоказиногдесредивсехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственностьюисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивогоюношиписателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдающейзаигройженщиныпотерявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпаркепокончитьсосвоеюбезнадежнойжизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвседляегоспасенияонпринимаетеезаоднуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяноонанепокидаетегоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереотеляиразделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоившемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетигратьснабжаетегоденьгаминаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленозатемвнейпробуждаетсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранитьегодлясебяионарешаетотправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческиепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитвигорныйдомисвозмущениемобнаруживаеттамтежерукинакануневозбудившиевнейтакуюгорячуюсимпатиюнарушительдолгавернулсякигреонанапоминаетемуобегообещанииноодержимыйстрастьюонбранитсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозореннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеибезпробеловвмотивировкенаписаннаяновеллаимеетконечноправонасуществованиекактаковаяинеможетнепроизвестиначитателябольшоговпечатленияоднакопсихоанализучитчтоонавозникланаосновеумопострояемоговожделенияпериодаполовогосозреванияокаковомвожделениинекоторыевспоминаютсовершенносознательносогласноумопострояемомувожделениюматьдолжнасамаввестиюношувполовуюжизньдляспасенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующиехудожественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпорокомигорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэтомотводеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивонанизмениоднимсловомкромесловаигранельзяназватьетееаа

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