Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Фізико-технічний інститут

Лабораторна робота №3

З предмету «Криптографія»

Виконала:

Студентка 3 курсу,

ФТІ, групи ФБ-73

Божко Анастасія

Київ 2019

Варіант 5

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 дотi, доки дешифрований текст не буде змістовним.

Результати роботи:
419 :y1-y2
то на
169 :x1-x2
a 537 b 490
Щоб відібрати саме цю пару ключів, нам треба було відфільтрувати розшифровані тексти, яких ентропія не перевищує значення 4.5

Зашифрований текст:
кеюибщаефддфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэммндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхпддкясввццтнавпьгнуьввйнлхиьердддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщщнфрхуюижсгцыззфрщихзтчщрихнэпозтгфккчщкдмклыоьеынуййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивупхюфйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшдекхндуаошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющьккюиеуяэзтьяяреурндуьцоэгкмбобмщкскехюксдцтсывзтмсунйьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйнмсуншснхтуйнццмсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюджджкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяышвнунхщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщмбриввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбьеелфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсисцйвнихчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовявшньсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшияziебчлвацлотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсчязиьсунуллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгйрщтнгбфдзйьцэибусчжвавмнзз

фдыоиюшсосюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрнш
вйнввлвацшвьхаврщшнищюиьсщожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктн
уншнмншспьчшвнюдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфсчсбкаышнтны
ьзтпэпьмвзтьсйядуццщщцспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвынуняуу
мпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожяшсвв
дуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюсстгнхщщшфддбтьпнзкьеэдхнщь
жвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидроши
фкяяшнюдаоосунчзфпьцэилцмяэьсцклжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцн
пдрщрнчстнввшвпвпьызмбйнвнцхпнуцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвн
щокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьавтулцибсчннисозфдыожллрд
цбщшдскрщиэбквэгвжвзтшвжьаоеитншпвихэхаорщибясфсчсщьавпьскггыоюшлхвииспьвиулбутнзцну
лцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшьявхщеуеи
дебупьесузющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхчщмщявисчтжьамаофи
срябсчшижслбубщэнщфдэмсщябубчзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищ
щшдекщсхдскхсовпннчубакакхуямдкяяхсвнхбжсмкщнщьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсв
ьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьвнбкубьебчсвйнжндуеисхавупмюю
сшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщубссвн
хбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглозфьцэидктнунэ
ибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпноул
цфрынщхыщмснфжврйвньркзскыщссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчя
вввнищрилвацшвьичдрщдкикгбмщбущстссвйьшвоейулцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхз
циссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзищссыршьудццрреулфщ
щаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнмспбмщбущськмюннисдкдкцфжвйьд
тмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщьккгнввшнивжврщрныуоззнбкжлт
ьбцрныгйснжшдекцгеэюсрсхщньбиулбунхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпр
шьйнлхавьщсиеуобмбмщбущсфрмщчяовупмюосшнкуаохщмсэкццзтбыыьмнжннуыфрыэиьсфсчсщьаво
зщсосгйлцмктзулынйнуйаихщавиэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдр
ошджсюсунынмсйкмбкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамоз
мщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкиющьккбыоскчицпьявицчзивяь
очлцсвпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьф
зтнуноьюддкнхживналбуыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикц
фтсввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзтклрц
цюсстшнюдкшвнгьерынньэьынавэкиютыннькиютноьакеишдщщшвпвмндтихжцшнйнюирсыэьяокпмао
бщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунтсчтгвмьввьелвмк
рюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпвюскиосыр
ынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщцсунхди
цяедьакхуумжсвнчрлвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибя
сшнлсиьпвтснфюирыюсцьаккнивжошижсмкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэ
иулбунхмокздцрнфзфпдкяспнчкхуцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэец
чзивяьокхуямщщшдбофдгвмсжкддьяжьяущнввввшнмьвврщозенйсуньейпфкаьтныоеущькхзцнулцзтд
нчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхмьакггмщшджсунлххэхьз
тлрэчбудкввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяьклхнгцязвэкьзцэиь
шсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпьг
бубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефддфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьж
йвнакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшьыоарфдрижлццэччсавпьзншвйнрнкизф
тсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекццжлывйквэпншнхщынгспныэрнгошддкйыяв
зтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвюдцфюирыусунлрлцдкяяыуаокнввпь
фзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндцвныкмба
рбуябакфккчявпвлсзврщьяшнынйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшде
кццзтиэярчсжвюсстибдцньтсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзццзтв
ииярщьякбньависйщкзхщхуиюшннуяетнхщюиакфккчлспьыопьрцмнрншбынлсюдризьяуфкшдвчсксчав
зтрщхсщв

Розшифрований текст:

убиватьбольшененадопослетогокаконужеубилноследуетемубытьблагодарныминачепришлосьбыуби
ватьсамомуэтонеоднолишьдоброесостраданиеэтоотождеминимальнойстепенисмещенныйнарциссиз
мэтическаяценностьэтойдоброты этимнеоспариваетсяможетбытьэтовообщемеханизмнашегодоброго
участияпоотношениюкдругомучеловекуособеннояснопроступающийвчрезвычайномслучаеобремене
нногосознаниясвоейвиныписателянетсомнениячтоэтасимпатияпопричинеотождествлениярешительн
оопределилавыборматериаладостоевскогоносначалаонизэгоистическихпобужденийвыводилобыкно
венногопреступникаполитическогоирелигиозногопреждечемкконцусвоейжизнивернутьсякпервопрес
тупникукотцеубийцеисделатьвеголицесвоепоэтическоепризнаниеопубликованиеегопосмертногонасл
едияидневниковегоженыяркоосветилоодинэпизодегожизнитовремякогдадостоевскийвгерманиибыл
обуреваемигорнойстрастьюдостоевскийзарулеткойявныйприпадокпатологическойстрастикоторыйне
поддаетсяинойоценкенискакойсторонынебылонедостаткавоправданияхэтогостранногоинедостойног
оповеденияучувствовиныкакэтонередкобываетуневротиковнашлоконкретнуюзаменувобремененност
идолгамиидостоевскиймоготговариватьсятемчтоонпривыигрышеполучилбывозможностьвернутьсявр
оссиюизбежавзаключенияв тюрьмукредитораминоэтобылтолькопредлогдостоевскийбылдостаточноп
роницателенчтобыэтопонятьидостаточночестенчтобывэтомпризнатьсяонзналчтоглавнымбылаиграса
мапосебевсеподробностиегообусловленногопервичнымипозывамибезрассудногоповеденияслужатт
омудоказательствомиещекоечемуиномуоннеуспокаивалсяпоканетерялвсегоиграбыладлянеготакжес
редствомсамонаказанияне счетноеколичествораздавалонмолодойженесловоиличестноесловобольш
енеиграть илинеиграть вэтотденьионнарушалэтословокаконарассказываетпочтивсегдаеслионсвоимип
роигрышамидоводилсебяиеедокрайнебедственногоположенияэтослужилодлянегоещеоднимпатолог
ическимудовлетворениемонмогпереднеюпоноситьиунижатьсебяпроситьеепрезиратьегораскаиватьс
явтомчтоонавышлазамужзанегостарогогрешникаипослевсейэтойразгрузкисовестинаследующийдень
играначиналасьсноваимолодаяженапривыклакэтомуциклутаккаказаметилачтотоотчеговдействительн
оститолькоиможнобылоожидатьспасенияписательствоникогданепродвигалосьвпередлучшечемпосле
потеривсегоизакладыванияпоследнегоимуществасвязивсегоэтогоонаконечнонепонималакогдаегочув
ствовиныбылоудовлетворенонаказаниямиккоторымонсамсебяприговорилтогдаисчезалазатрудненно
стьвработетогдаонпозволялсебесделатьнесколькошаговнапутикуспехурассматриваярассказболеемол
одогописателянетрудноугадатькакиедавнопозабытыедетскиепереживаниянаходятвыявлениявигорно
йстрастиустефанацвейгапосвятившегомеждупрочимдостоевскомуодинизсвоихочерковтримастеравсб
орникесмятениечувствестьновелладвадцатьчетыречасавжизниженщиныэтотмаленькийшедеврпоказ
ываеткакбудтолишьтокакимбезответственнымсуществомявляетсяженщинаинакакиеудивительныедл
янеесамойзакононарушенияеетолкаетнеожиданноежизненноевпечатлениенововеллаэтаеслиподвер
гнутьеепсихоаналитическомутолкованиюговоритоднакобезтакойоправдывающейтенденциигораздоб
ольшепоказываетсовсеминоеобщечеловеческоеилискореообщемужскоеитакоетолкованиестольявно
подсказаночтонетвозможностиегонедопуститьдлясущностихудожественноготворчествахарактерночт
описательскоторымменясвязываютдружескиеотношениявответнамоирасспросыутверждалчтоупомян
утоетолкованиеемучуждоивовсеневходиловегонамерениянесмотрянаточтоврассказвплетенынекотор
ыедеталикакбырассчитанныенаточтобыуказыватьнатайныйследвэтойновеллевеликосветскаяпожила
ядамаповеряетписателюотомчтоейпришлосьпережитьболеедвадцатилеттомуназадранооводовевшая
матьдвухсыновейкоторыевнейболеененуждалисьотказавшаясяоткакихбытонибылонадеждаснороквт
оромгодужизнионапопадаетвовремяодногоизсвоихбесцельныхпутешествийвигорныйзалмонакского
казиногдесредивсехдиковинеевниманиеприковываютдверукикоторыеспотрясающейнепосредственн
остьюисилойотражаютвсепереживаемыенесчастнымигрокомчувстварукиэтирукикрасивогоюношипис
ателькакбыбезовсякогоумысладелаетегоровесникомстаршегосынанаблюдающейзаигройженщиныпо
терявшеговсеивглубочайшемотчаяниипокидающегозалчтобывпаркепокончитьсосвоеюбезнадежной
жизньюнеизяснимаясимпатиязаставляетженщинуследоватьзаюношейвпредпринятьвседляегоспасен
ияонпринимаетеезаоднуизмногочисленныхвтомгороденавязчивыхженщинихочетотнееотделатьсяно
онанепокидаетегоивынужденавконцеконцоввсилусложившихсяобстоятельствостатьсявегономереоте
ляиразделитьегопостельпослеэтойимпровизированнойлюбовнойночионавелитказалосьбыуспокоив

шемусяюношедатьейторжественноеобещаниечтоонникогдабольшенебудетиграться снабжаетегоденьга минаобратныйпутьисосвоейстороныдаетобещаниевстретитьсяснимпередуходомпоезданавокзаленоз атемвнейпробуждаетсябольшаянежностькюношеонаготовапожертвоватьвсемчтобытолькосохранить егодлясебяионарешаетотправитьсяснимвместевпутешествиевместотогочтобыснимпроститьсявсяческ иепомехизадерживаютееионаопаздываетнапоездвтоскепоисчезнувшемуюношеонасноваприходитви горныйдомисвозмущениемобнаруживаеттамтежерукинаканувневозбудившиевнейтакуюгорячуюсимп атиюнарушительдолгавернулсякигреонанапоминаетемуобегообещаниииноодержимыйстрастьюонбра нитсорвавшуюегоигрувелитейубиратьсявонишвыряетденьгикоторымионахотелаеговыкупитьопозоре ннаяонапокидаетгородавпоследствииузнаетчтоейнеудалосьспастиегоотсамоубийстваэтаблестящеиб езпробеловвмотивировкенаписаннаяновеллаимеетконечноправонасуществованиекактаковаяинемо жетнепроизвестиначитателябольшоговпечатленияоднакопсихоанализучитчтоонавозникланаосновеу мопострояемоговожденияпериодаполовогосозреванияокаковомвожденииинекоторыевспомина ютсовершенносознательносогласноумопострояемомувожденииоматьдолжнасамаввестиюношувпо ловуюжизньдляспасенияегоотзаслуживающегоопасениявредаонанизмастольчастыесублимирующие художественныепроизведениявытекаютизтогожепервоисточникапороконанизмазамещаетсяпороком игорнойстрастиударениепоставленноенастрастнуюдеятельностьрукпредательскисвидетельствуетобэ томотводеэнергиидействительноигорнаяодержимостьявляетсяэквивалентомстаройпотребностивона низмениоднимсловомкромесловаигранельзяназватьетее

Програмний код:

```
#include "pch.h"

#include<algorithm>

#include <iostream>

#include <fstream>

#include <math.h> #include <string>


using namespace std; const char filetext[] = "C:\\nb3\\kryp\\fb-labs-2019\\tasks\\crypto_cp_3\\for_test\\V5"; string alph =

"абвгдежзийклмнопрстуфхцчшщьыэюя"; string popu_rus[10] = { "ст","но","то","на","ен","ов","ни","ра","во","ко" };//самые встречаемые double

entropyya(int* cod_num, int l); int* max10(int num, int c, int* bigra, int k); int obr = 1, d = 0; int m[10] = { 0,0,0,0,0,0,0,0,0,0};//макс частоты int mx[10] =

{ 0,0,0,0,0,0,0,0,0,0};//индекс макс частот int* bigmax = new int[10];


int x_bigramm(string a);

int gcd(int am, int bx) {//находим самое большое кратное

		int d = 1; if (am < bx) {


				int c; c = bx; bx = am;


				am = c;		}

		if (bx < 0) { bx = bx + am; }

		if (am % bx == 0) {		d = bx;} else {		for (int i = bx - 1; i >= 0; i--) {


						if ((am % i == 0) && (bx % i == 0)) {

			d = i;

								break;		}		} }

		return d;}

int d1; int inver(int m, int x) {//находим обратный элемент
```

```
                    if (x < 0)x = x + m;
 if (gcd(m, x) != 1) {                                  int gcdb = gcd(m, x);
                    m = m / gcdb; x = x / gcdb;       }

                d1 = obr; obr = d + obr * (-1) * int(m / x); d = d1;

                 if (m % x == 1) {                      int obr1;
                    d = 0; obr1 = obr; obr = 1; if (obr1 < 0)obr1 = obr1 + 961;

                    return obr1;        }
                 else{inver(x, (m % x));                }                       }
int* arr(int* S, int num) {
                int* S2 = new int[num]; // Выделение памяти для массива for (int i = 0; i < num; i++) {        S2[i] = S[i]; } return S2; delete[] S2;}

int* maxxof5(int c, int* bigra, int k) {//находим самые частые биграммы в тексте
                if (c > m[0]) {    max10(0, c, bigra, k);} else if (c > m[1]) {max10(1, c, bigra, k);} else if (c > m[2]) {max10(2, c, bigra, k);} else if (c > m[3])
                {max10(3, c, bigra, k);} else if (c > m[4]) {max10(4, c, bigra, k);} else if (c > m[5]) {max10(5, c, bigra, k);} else if (c > m[6]) { max10(6, c, bigra,
                k);} else if (c > m[7]) { max10(7, c, bigra, k);} else if (c > m[8]) { max10(8, c, bigra, k);} else if (c > m[9]) { max10(9, c , bigra, k);} return
                bigmax;}

int* afinbaigramm(string text, int length) {//из текста в число
                int* af_bi = new int[length / 2]; int letter1, letter2, n = 0; for (int i = 0; i < length; i++) {

                    if (i == length - 1)break;
                    else {                              for (int j = 0; j < alph.length(); j++) {
                    if (text[i] == alph[j])letter1 = j;
                                                        if (text[i + 1] == alph[j])letter2 = j;                                  }
                    af_bi[n] = letter1 * 31 + letter2;
                                        n++;            }i++;           }
                return af_bi; delete[]af_bi;}

int* pop_b = new int[10]; int* freq_b(int* af_bi, int countt) { int count, num = 0, n = countt / 2;// n-numberbigramm, count-amountbigramm

                int key;
                int* af_bi2 = new int[countt / 2]; string c;

  af_bi2 = arr(af_bi, countt/2);
                int number, j; for (int k = 0; k < n; k++) {//подсчитываем кол-во конкретных биграмм в тексте

                    count = 0; key = -1; key = af_bi[k]; if (key != -1) {       for (j = k; j < n; j++) {

                    if (af_bi[j] == key) {
                    count++;
                                                                number = j;       }                                  }
                                    pop_b=maxxof5(count, af_bi2, number); for (int z = k; z < n; z++) {
```

```
                                                    if (af_bi[z] == key) {                    af_bi[z] = -1;}}}}
                return pop_b; delete[]af_bi2;}

string* decode(int* afbi_d, int size) {//расшиф.
                string* ss=new string[2*size]; int n = 0; for (int i = 0; i < size; i++) {        ss[n] = alph[afbi_d[i] / 31];

                                ss[n + 1] = alph[afbi_d[i] % 31];//afbi_d[i] % 31
                                n = n + 2;            }
                return ss; delete[]ss;}

int main(){          SetConsoleCP(1251); // Ввод с консоли в кодировке 1251
                SetConsoleOutputCP(1251);
                string s; string s2; int countt = 0; //длина текста в файле ifstream f(filetext); while (!f.eof()) {

                                f.get();//Извлекает один символ из потока.
                                countt++;            }
                f.close(); ifstream ff(filetext);  //создаем поток для работы с файлом

                s.assign((istreambuf_iterator<char>(ff.rdbuf())), istreambuf_iterator<char>()); ff.close(); //закрываем файл s2 = s; int* popular5 = new

                int[10]; int* af_bi = new int[countt / 2]; int* af_bi2 = new int[countt / 2]; int* af_bi_dec = new int[countt / 2];

  af_bi = afinbaigramm(s, countt);//из текста в числа
                af_bi2 = arr(af_bi, countt / 2);
int a,b;
                popular5 = freq_b(af_bi,countt);//10 самых частых биграмм в шифртексте for (int i = 0; i < 10; i++) {cout << popular5[i] << "  ";} string*

                part = new string[10]; part = decode(popular5, 10);//выводим 10 биграмм в буквенной форме for (int i = 0; i < 20; i++) {    cout        <<

                part[i] ;

                                if (i % 2 != 0)cout << " ";}
                for (int i = 0; i < 10; i++) {cout << part[i];
                                if (i % 2 != 0)cout << " ";}
                for (int q = 0; q < 9;q++) {for (int j = 0; j < 10; j++) {if (q == j)j++;
                                                int xxx = x_bigramm(popu_rus[q]) - x_bigramm(popu_rus[j]); int yyy = popular5[q] - popular5[q + 1];

                                                while (xxx < 0)xxx = xxx + 961; while (yyy < 0)yyy = yyy + 961; cout << endl << yyy << " -sum частые

                                                биграммы " << popu_rus[q] << " " << popu_rus[j] << endl; cout << xxx << endl; a = (yyy*inver(961,

                                                xxx)) % 961; while (a < 0) { a = a + 961; } b = (popular5[q] - x_bigramm(popu_rus[q])*a) % 961;

                                                while (b < 0) { b = b + 961; } cout << "a " << a << " b " << b << endl; if ((gcd(961, a) > 1) && (b%gcd(961,

                                                a) != 0)) { cout << "Решений нет" << endl; }

                                                else {                cout << gcd(961, a);
                                for (int i = 0; i < countt / 2; i++) {//y=xa+b x=(y-b)a(-1)
af_bi_dec[i] = ((af_bi2[i] - b)*inver(961, a)) % 961;//расшифровываем
```

```
цифртекст
                                                                                while (af_bi_dec[i] < 0) af_bi_dec[i] = af_bi_dec[i] + 961;                }
                                                                        float entrop; entrop = entropyya(af_bi_dec, countt / 2); cout << endl << entrop <<
                                                                        endl;//с помощью энтропии мы выводим нужный текст if (entrop<5) {
                                                                                string* text = new string[(int(countt / 2)) * 2];
                                                                                        text = decode(af_bi_dec, countt / 2); for (int i = 0; i < (int(countt /
                                                                                        2)) * 2; i++) {cout << text[i];        } delete[]text, af_bi_dec;}}}}
                        return 0; delete[]af_bi,popular5 , af_bi2 ,af_bi_dec;//, af_bi_dec
} double entropyya(int* cod_num,int l){string* ss = new string[2 * l];
                        ss=decode(cod_num, l); string key = {}; double count; double frequency, result = 0; for (int i = 0; i < alph.length(); i++) {count = 0;
                                                frequency = 0; key = "/0"; key = alph[i];
                                        for (int j = 0; j < 2 * l; j++) {            if (ss[j] == key) { count++; }                        }
                                        frequency = count / (2 * l); result = result + (-1) * frequency * (log(frequency) / log(2));//сумма энтропий   }
                        return result;}
int x_bigramm(string a) {               int sum = 0;
                        for (int k = 0; k < alph.length(); k++) {                    if (a[0] == alph[k])sum = sum+k * 31;
                                        if (a[1] == alph[k])sum = sum+k;     }
                        return sum;}
int* max10(int num,int c,int* bigra,int k) {
                        for (int i = 9; i >= num; i--) {
                                        if (i == num) {      m[i] = c;
                                                             mx[i] = k;                      }
                                        else {               m[i] = m[i - 1];
                                                             mx[i] = mx[i - 1];                          }
                                        int n; n = 0+ mx[i];
                                        bigmax[i] = bigra[n];                }
                        return bigmax;}
```

Висновок:

Під час данного комп’ютерного практикума ми набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанували прийомами роботи в модулярній арифметиці.