Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

**ЛАБОРАТОРНА РОБОТА №3**

**з дисципліни**

**«Криптографія»**

**Криптоаналіз афінної біграмної підстановки**

Виконали:

студенти 3 курсу ФТІ

групи ФБ-74,ФБ-72

Демиденко Дар’я та Скуратов Ілля

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

# КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

## Криптоаналіз афінної біграмної підстановки

## 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.

# Варіант 15

# Шифрований текст:

цсбтызнэжрцяфьзюдрцубуысьцыуюкнажфтпдрчядьдйлдаьпуяксщфтэаытыпдрвщядшрщфтпдйюябуцу
йрдуврйдмузеуйиьуюеочшлукчэйлдаьпуякгуяклтафвкежнспйиьяршцчтыпйэуюуйрудтшкдрлфюоцуэрь
ккдлцчтыпйэйифюькьтрэуйюкйирцыуснпйюкчтфбиььтйюйфьснэщпокмлерхфбукюуйюкйирцыуьулямп
якврбюгиэпязякыддфбузиснррщушрвщчкчйлдаьзннфьуоукючкпззнюеьтпфцубуысьцыуснмуужзнгнеч
мспутюыыокдцыуцятыююаршрпсгнщухцчтыпйэкдскнфпфыусюдриэюкбяйицютауаусцятыююгипалфтп
ыплтгнзрноьуеряюгиосфйьтсожвзиэпязмуйецюгнкдярдуююыфыуруцаырзпнщчкпуцубтежуюякыдыкээ
зижуякзоьсжинщэыокчтьюязлщяыайсрщюязцятыююпфзсьунчфаькиоурдумфпфдумсмфпфдумсшпжрб
южрзгыускеуноидэрнчпудсмрфацябцпузйлдаьпуякнфпфыухтбстанржфпфыушкоеядтючоцящперйдэрн
чпуякапжрбюязытбжгньсоуядфяпфыумсфйчкхплтпйьтррнкнщядшрщфтпуйпферцуздцячььттдкфлагсеч
пймпдутяиьнэйиьулэипоуыурущуцашроуфдвьыплтяфйдияцюйицяфюшкгиюкнрьсжуыдруякыпшьчтлти
оидтящщчтгимузягифдынбэюкбякейипфоулфщсяыкдоуснуюгмпсгнррнэьтрэцюмэюкбяшзгнщттщзика
ыдтджиыуыдысодесьулцфюуюзнесфюфцлтуфтпйикэюкбяшзгнцьыпьтуюэпжрижаышчбпьуытфьрршпс
рыожечьсуоцсвшпжспчфдисаьйигюшлчьштзрыуыдьсдиокюяфюокдцыунрядлдрфчябсыдгкиодашржлб
жнсбкуйбяющарбацядрчдечмущушузяиьыпокфсыфьуоуыкуфцдысоуэячьыкчтызусцджгзсжспчфдьсоуя
ддсфйчкхплтяклдыцыуэуюотпхпмфзсзерсжкязвяфьхпоуыурушупутяиьщпзрноюклфызгсэргфоузйккзюф
божштцдзкжлрсфймэязпуцюпалфтпыплтбкбязюрспсьуаьпуцяхьькиоуйшкапякайыкапыуыубалжаыьсв
яафякругфтпщиосьуцямперьсдихьчтнайрцдесайлдцтушясзфжулдесфючяиещинфэпэыдинфнщфрякбуд
фчшлукчффцюоснщювзюдрьрппмгыугндуяклдпююкчаююывыдйккзюрсцююквргдхюдйнфнищиокюяжль
тчьзнесдтафссйрнэзисйнфнищифюфцфюмпйсесиокэцюгдомзинфзафдгцщпчоюкйиоуйьхубющиюяуюц
ядрчдечжечьсуюйьтрцштжспчфдруюювлиэюкбявлаывродпсзееуьущуьппркдцдйсощьтоущфщсесюкйи
бкпфыдхчждтанрьцюяяыцуьйюкйирцыуяксяшзаюэыьюмфкеядзрхгыужспчщукебяусдупфоушщштцюкэ
ьтчобуырзпвлжибжлтоугндуьуэртоечаымуфдкдцдеаоуыучакуеттщштлунчярлфелаызргчщпыпыуинэущ
фэпжрюеыфсянэязыупэаысрьспжлтчтюкйибкжрцурргндуцяйгыуийюкйирцыуцюгньуйдидкгыубалулэц
юнэйирцыужулфжиррцдйдищьтцмчойрякеячьякбучюзивцыусжчтгуеттщыккдцдеаыущушрыулускнффс
мрйятысрярьскфхиафзячьпуцуюкндесцагацюоуерждофсюрйуйруссечиопсбукйыфнцыутамсздечкдцде
аррврякязпугакйчьтмпсфдррэянйысутнфеузяежуюеопфцювувацдьсурфюкэьтпзуйшкйустфжштпуврчю
языуцушрцуздцюьулаустйнфнийиокюясйнфмпярскпзпуюктякхбсжспчщункмамрчсдузежрчдечцюдйнф
лтфцыусжчтфюкэьтпзррцядрнрзсррбуццчьржфэыиьчтокыпссьршчрйязнржфщудугэбслфрйязуакййияяц
елдакээытющцдепврысофдиыкуюрэнсцдбьнщысцдепзрзееупизюхпйшьцыулфхьькдашржлбжюяиьлщ
кеэащужогккщойысяытдгфызгдхжгршрпсунррэуйрзчшьчтокниуюлслфтпжрзрьргфтпцюмфгдякзнесжсб
дядтякхфюойнфнилгыуьунргфтпыплтцюзюкэьтчогюзенщфтыушыиямпшзкийфтйпфсрцфтпуюпуяккэюк
бяшзьуйденыдербабкнщфтчььтйююкрйюяыььтйюнщфтжрчдечмфпсррбужфцдиэккыпюкванэьуйрбакд
мугндуелокйубюяыкдхюыпйфхдомнфчйпфернщфьхужпчтчтпффьядечзрруцуфдьфиьмппурряышрбюке
рсяклдпювыдуцушрсрэббсврвюипйспчкдюыснербюйишрсрэбфьйиязнщцпштядэяямпрядпрльуюнфып
хуяклтионяпфыуыдсйысярщмзиврйрруткыпсяявщибкуйчьцртпюкванэдрнроьйиязйдаюыкчаююрсяклд
бюнщфтжрбауафдечбкеуцафьькфюйаяюцрзсьмцдждбкжрбапфнщуюпуфюэрсрчюнщфтуйруаыврнретг
учщдьькэяюкесякинштсйьтрцыкзюцаидьуытфььсжизюшпинйдаюнфчязюпугндууафдечбкеуикээкафььк
ррцячьмптякхцеьтфлыпнэйиккруаэыфмплдюндэюкбявльунчнээзтякхыухеыплтгюзерсоуыуиншяпфыут
юдйсялщштбкуйруздякидуниоусйдаюфюрйцюшкпуйдиддупчбкнщяыррцутанрфкюкждлэюкбяшзюабд
инмуужзнгнпсздечхдбюрйшдаьубоуппжсхазтзющиздыдомзиждофбуызхдбюкщбячунулфоушумыкдгц
ыукдмуелокфсугыуцукфпуцуэуруярцуеслдхаздыугаздйьшпощфтыпаьбясйккзюфбфцюяяыррнрчшшняр
дукйыфуеыфсячкыпсяявфюькьтрэуйуйьтхапусйнщыссднрздпснщфьруякыпыфыущпйсгфцудушньучащ
йчьжснэостялтхьврбаенщсырпсгпшлбядймфуюьсоуэяпфыупйжобдэксрхдйдкипзбяйижджушнийлознв
утсуринйдгдпснщьсфдпскаруьспсруякыпафьтздунчяьккрцуяфйдияцюцрфрлдфэфцлтдрцукэысгдпсняд
йюкйируякыпдйьтфжштщпбдьссйрубучспсмуырзпязякзююсхьуйьтыпфюсьбякекэээнкыпзрйьющхпцры
угэсрьроццеиьмэдрыдлфжийфпсруякыпющфтдрфркдидчсзгнэиьруррпуырсрыдпсомнфжыдйьтыпфюс
уцашркдгдбыющхпоквкруаэыфмплдюнзфбузеыпшлесяклдмучуппызхалщмфьуоукюцюфцлтфйлдйсыд
ечзрноюкйибкрсйдоубюпзнртпюклдююйийрвщпсшрцюьунрэжлтэрдфштьюгрцулдаьпфштьюгрйдцщд
ьыулямпякврбюжрпалфтпнщфтуйчьусррпуыубашридоуцанэбяпфзсхднрьсшкчтиэыдияокшллдрфыусю

эзцюуафддуэпжрмьйиуюдйпферююызырсрмучяиьзндфцдббосзджохвкэккысчабтсюмпчьхакэээфднчу
слыиьвлчопчйщсжлткдкяфтьбчьйидйпфербуякбяцучпяксруссйпферыуцуяклдбюкедципякыдррдьыпер
тпбяуюеолфлдтюуюосякжийрцуфжхьцрзчлфыушрнцжибждоцдзкбяуйштиоьсоуядгфцдьпгсыдечиолфб
угфцдинэияямуфдюкубзиоксщфтыксжвуьсыунчоуррлюкеуйпфцдсрпспубушпьсещштмэээжрыумрфймэ
язякбуоспуйьзюмфкеядссйэюкбякецюкщхплтуйсркьнсоуыуруйэээнэбямаяюлтьсоуядзйрунфэучсдуюку
авюкеуйьтфжуюеонрофцюкщфтбжфьыдюбокшзцумукдбжвуякзюыпштафмлбятмькьювцзецювумродя
длунчярыуцубкыпррбщфтцюрсннкенщфтчьпфцдыущюеукдлфтьммлтафгдяккресчшлукчффэрлйбяйдэй
ыселлтьсоуяддсврвючоррьуоуерцсфдхттщыппгыульшпямщслдмуякпунргфтпыплтзюзюзеуйьклскдцдш
длунчярлфелдьщпштфюкэьтчоырюогнлашрлунчюускыскдюбокштькьсаэлдссшнппмфчтрсхипушддуцт
щпшзфднчусхаоуыуруцубжчтйилтиоцудучюзюокгмгюкэьтпзмуйемачсцтхтионфьрхтиомттьсюзюгржул
фжиррцдцубуысдуоцыужйчьняррядкдцяюкщппуыдйюпфечйдйдшкмэсовссонэтылтцюызюуьуыумьиь
иьсяиьпфнюкеыпбяштзюокгмзюокгмсяафнэтылтцрбаэпязруфдщфаюэыжизюиягрьрцуцядраьбучяиьпу
нсьуйдидядзеуйпферююгржспчщубкфжунлдцфцягмщплтзюокгмчоцдзкрйюяуфьуоукюафгдякпсыддцу
юеяиьюквргдхюкэьтпзцююкпсщюшзйрдуврнцыуркяуйршчцттщеркдйдзккщмфйдидечюквргдядкдцдш
дищфтмпчшбтуюмплуысбдиаусэржоуьуюнфыпзюлгыужулфжиррыулюрймэязпутпюямуэыкдйцыулахм
грцурргныдькчшнрдслюькээфймэязпуэуруюуэрырщчжулфжиррцдхэээцясжнрьсоуядппьятышткдцдяр
эпжрррдьыпьтуфтпдрюкйибкпфыдхчждгнядюкдушркдкдцуюоцюокгмаффжмфыуйрьсжикдваякштафь
ююшлдцдмуйденыдбрбабклгыуррщумтнщчкфскдйрбкчьняпугнгндулфгажсечлфжиэшцяюкщпбупсюкн
дбкеукдбдфдкккеилюкчтокйфыпзрдфыпзрлюрйцюзицрзчцубуысядцюзюкэьтпзидщугцлтнфкеядссофк
фрртщлдьцафыудьщпжоофеежооокдррмфыпзрлюкщфтуйилфжбцыугнцюющфтмпчшбтуюкдсюшпмфц
дэятылапррфбузишрьсэущукдгнядрутюафьуоукюмпмфчтафыпюяярбюуйуйсрйюжигюкэьтчонкмачсцтх
трсздшридякмпжодуррмуврпцщппфщучяькьюафыдыулфтпнщьтоущфоуцуцюррврысьпыубкжрмфдьс
щэашрсряркдэрвщьтгрбкеубюшпхьлтчюхшаюэыьдвьсрбрбалфйдиддупчбкдцыуьстахчррыузгыуийсрьй
ьтьецрщувщлдпридйрщужфрупэтыфцжиррнщчауспспчуафддулятыцубуысомнфеятыкиокюяэшпфмфчя
вуцэдьщперьсффбужиэсюкгдяккэдьыпьтуфтпцшкдяргцыуфдечыущююкээшржелацсрруайсфюкездррм
уврпцщппфщучячтзюыгыудщлдепюкжсярбеыпбяштхукдьуйдеыдкфрюайнфнимэсопозюиядоякжиид
цдуюзншципякбулюфьнщрушрядэрнчякыдоуыурушпзрйьцрякрафдэрысцяюкщптауафрцунацябжмфоу
цуецафзстьдцюясйрмькбкцюрйысфььклдшчярнрйдзязэээжршрнкчьчтйифжькиднражоккрцуврвюнщьт
яышчаьбяыпкрытющжрдцуювкрюзеыпбяфюокгмькрюмфщучявцыуцюмпмфчтыгыубжьуытфьррфьшпв
цкрэяжитьфжщпцрцдэыкдйцыучюызнрядькиолфзээзлдфэээжспчфдзеуйьтрццрфдпйруйрвщкездяклф
жлбятмнщдьькиддтйцлтхукдлфзээзлднупуствцзнчцчтыпйэырзпжрэяжикфбузеуйысяыздьсоуядбщфтзр
щчяыуюхьежмфхайрррцубаусядцяфьякзоодсювуолчьзипфечеипмокуфцпнкиелатнфьчтшлвыщзякыдвт
зэюкбявлфдечшндплтцрцубкнщйфоусрмфыдпсечфйерогганщоыгюоксрзсльуюуфбузеуйысяыздцюзргь
ыкцювутпбцчокдбуцяпфхаздцюхььькьуярофкдбиняюзнесзяыпдищпщхпсчрнчтиыкуюрэнсьучякщыплтг
юзепфйрунлфзедцыуцдоукщфтйгзсецькхпзрцуьсоуядхыкдерфрьрррбцжицярмфьйсппяклдисррмухиу
юдресэршчйдлдтеыпбякайраиыкуюрэсйрумуужлтиоррмуйепфцдруякмпзщбязндсордфщсльфжхьмпй
смфцпырсрююызэтиечткфпфчяшлйикамубунчякмсжиытммлтнфкдгдядйдлыьедьчтаыокспродлэээтаек
ыпэпвышншдомэзиоцудукиьтчькекелдвдытммлтяяцеокчтьюарнфчягмзнмфдуыдюнхдомдриочьпуиди
яцезилдхщязьсаюкщядцуздвючотпсяфсйящщчшжуждхаррфйдйуюрэязнщбуруыдпсоььуыуагзсчшчсчю
жиуюцмзидьыпьтуфтпдресяклдэурпхьчткэээщудумуюелдюпмфрэлдчюшзчюлтыкязкяыпэшжеядидщы
гмщпбяюкшнцдясииыкуюрэгюкеязкэьтуюоугфлунчюуотыпоуякэшиамуэюжрэяжидисжуаэпрсзфдущкь
таюзтзеуйчьидчсидкявцлтбуоцыугнуадатпжрцуьрнымпубаьмфьюкщфтйиыкуюрэафчяжимтмпытькчту
ммфзсякайуюызкамртдьпдтхитадтхижднкющфтбсдпмфнючоьрякпуякуфхдзрьсойсрякайьсоучпюклдю
юйибдюиыкуюрэдйысяытдойлозндстебячьдйтоцдофцпнкшэлавщэслюкедргсэрпсюклдююкеуйтоцдом
дриоюкесэршчщсяюлтнфхдссэрнчцаффштчгыуаэлавщожующиыкуюрэосэпзойрьскнссфйцезюзнеспснд
есшннацапспчлфуюосаьврсраэйикдунйьйэсйчтусякшзбдщуыдысбудпммлтафчйысйдмцфбйдцпйфмэч
оьуякчтчйчьякзезюзнщунрхтйиумыкгиаыоуругэжлхажупэыпщудумуюелддыиьвлчопчррнщлдодсюзю
жлтюзизюеосрйсэрнчзнесшдсдесцятмчтесщуьсисьуярьпмуяелдтссооыкдомчоыуьцафйрсраьшпямйэю
кйибкуйруаытмдубуэтиечтмфчьпугфыурузныфьуоуштафапыущунютмуюосбкюкрйюяуфпфыусюдржлм
уужпуьуцямпыкуфкфияцеязякбяцюяукдмрфймэрсядпчюкйиийдэйюяуюмфькнкжрмфрюцюдйчьэучсядр
рнэьтрэбятыкдкньупэшлпрцугпюянфлашдзэээцюхаысэкчатэоыокчатэязрд

## Розшифрований текст:

библейскоепреданиеговоритчтоотсутствиетрудапраздностьбылаусловиемблаженствапервого человекадоегопаденияслюбовьюкпраздностиосталасьстажеивпадшемчеловекенопроклятиевстяго теетнадчеловекоминетолькопотомучтомывпотелицадолжныснискиватьхлебсвойнопотомучто понравственнымсвойствамсвоиммынеможембытьпраздныиспокойнытайныйголосговоритчто мыдолжнысбытьвиновнызаточтопраздныежелибымогчеловекнайтисостояниевкоторомонбудуч ипраздныммчувствовалбысебяполезнымиисполняющимсвойдолгонбынашелоднусторонуперво бытногоблаженстваитакимсостояниемобязательнойибезупречнойпраздностипользуетсяцелое сословиесословиевоенноевэтойтообязательнойибезупречнойпраздностисостоялаибудетсостоя тьглавнаяпривлекательностьвоеннойслужбыниколайростовиспытывалвполнеэтоблаженствоп ослегодапродолжаяслужитьвпавлоградскомполкувкоторомонужекомандовалэскадрономприн ятымотденисоваростовсделалсязагрубелымдобрыммалымкоторогомосковскиезнакомыенашл ибынесколькономоторыйбыллюбимиуважаемтоварищамиподчиненнымииначальствомикотор ыйбылдоволенсвоейжизньювпоследнеевремявгодуончащевписьмахиздомунаходилсетования материнаточтоделарасстраиваютсяхужеихужеичтопорабыемуприехатьдомойобрадоватьиуспо коитьстариковродителейчитаяэтописьманиколайиспытывалстрахчтохотятвывестиегоизтойср едывкоторойоноградивсебяотвсейжитейскойпутаницыжилтактихоиспокойноончувствовалчто раноилипозднопридетсяопятьвступитьвтотомутжизнирасстройствамиипоправлениямиделсу четамиуправляющихссорамиинтригамиссвязямисобществомслюбовьюсонииобещаниемейвсэ тобылострашнотруднозапутаноионотвечалнаписьмаматерихолоднымиклассическимиписьма миначинавшимисяиокончавшимисяумалчиваяотомкогдаоннамеренприехатьвгодуонполучилпи сьмародныхвкоторыхизвещалиегоопомолвкенаташисболконскимиотомчтосвадьбабудетчерез годпотомучтостарыйкнязьнесогласенэтописьмоогорчилооскорбилониколаявопервыхемужалк обылопотерятьиздоманаташукоторуюонлюбилбольшевсехизсемьивовторыхонссвоейгусарско йточкизренияжалелотомчтоегонебылоприэтомпотомучтоонбыпоказалэтомуболконскомучтос овсемнетакаябольшаячестьродствоснимичтоежелионлюбитнаташутоможетобойтисьибезразр ешениясумасбродногоотцаминутуонколебалсянепопроситьсяливотпускчтобувидатьнаташуне вестойнотутподошлиманеврыпришлисоображенияосонеопутаницеиниколайопятьотложилнов еснойтогожегодаонполучилписьматериписавшейтайноотграфаиписьмоэтоубедилоегоехать онаписалачтоежелиниколайнеприедетиневозьметсязаделатовсименьепойдетсмолоткаивсепой дутпомируграфтакслабтаквверилсямитенькеитакдобритаквсеегообманываютчтовсидетхужеи хужерадибогаумоляютебяприезжайсейчасжеежелитынехочешьсделатьменяивствоесемейство несчастнымиписалаграфиняписьмоэтоподействовалонаниколаяунегобылтотздравыйсмыслпо средственностикоторыйпоказывалемучтобылодолжнотеперьдолжнобылоехатьеслиневотставк утовотпускпочемунадобылоехатьоннезналновыспавшисьпослеобедаонвелелоседлатьсерогома рсадавнонеезженногоистрашнозлогожеребцаивернувшисьнавзмыленномжеребцедомойобяви ллаврушкелакейденисоваосталсяуростоваипришедшимвечеромтоварищамчтоподаетвотпуски едетдомойкакнитрудноистраннобылоемудуматьчтоонуедетинеузнаетизштабачтоемуособенно интереснобылопроизведенлионбудетвротмистрыилиполучитаннузапоследниеманеврыкакнис траннобылодуматьчтоонтакиуедетнепродавграфуголуховскомутройкусаврасыхкоторыхпольс кийграфторговалунегоикоторыхростовнапарибилчтопродастзатысячикакнинепонятноказалос ьчтобезнегобудеттотбалкоторыйгусарыдолжныбылидатьпаннепшаздецкойвпикууланамдавав шимбалсвоейпаннеборжозовскойонзналчтонадоехатьизэтогоясногохорошегомиракудататуда гдевсбыловздорипутаницачерезнеделювышелотпускгусарытоварищинетолькопополкуноипоб ригадедалиобедростовустоившийсголовыпорубподпискииигралидвемузыкипелидвахорапесен никовростовплясалтрепакасмайоромбасовымпьяныеофицерыкачалиобнималииуронилиросто васолдатытретьегоэскадронаещеразкачалиегоикричалиурапотомростоваположиливсаниипров

одилидопервойстанциидополовиныдорогикакэтовсегдабываетоткременчугадокиевавсемысли
ростовабылиещеназадивэскадроненоперевалившисьзаполовинуонуженачалзабыватьтройкуса
врасыхсвоеговахмистрадожойвейкуибеспокойноначалспрашиватьсебяотомчтоикаконнайдетв
отрадномчемближеонподезжалтемсильнеегораздосильнеекакбудтонравственноечувствобыло
подчиненотомужезаконускоростипадениятелвквадратахрасстоянийондумалосвоемдоменапос
леднейпередотраднымстанциидалямщикутрирублянаводкуикакмальчикзадыхаясьвбежалнакр
ыльцодомапослевосторговвстречиипослетогостранногочувстванеудовлетворениявсравнениис
темчегоожидаешьвстожекчемужеятакторопилсяниколайсталвживатьсявсвойстарыймирдомао
тециматьбылитежеонитольконемногопостарелиновоевнихбилокакоетобеспокойствоиногдан
есогласиекоторогонебывалопреждеикотороекакскороузналниколайпроисходилоотдурногопол
оженияделсонебылужедвадцатыйгодонаужеостановиласьхорошетьничегонеобещалабольшет
огочтовнейбылоноиэтогобылодостаточноонавсядышаласчастьемилюбовьюстехпоркакприеха
лниколайиверная янепоколебимаялюбовьэтойдевушкирадостнодействованан егопетяинаташа
большевсехудивилиниколаяпетябылужебольшойтринадцатилетнийкрасивыйвеселоиумношал
овливыймальчикукоторогоужеломалсяголоснаташуниколайдолгоудивлялсяисмеялсяглядян
анеесовсемнетаговорилончтожподурнеланапротивноважностькакаятокнягинясказалонейшоп
отомдададарадостноговориланаташанаташарассказалаемусвойроманскняземандреемегоприез
двотрадноеипоказалаегопоследнееписьмочтожтырадспрашиваланаташаятактеперьспокойнасч
астливаоченьрадотвечалниколайонотличныйчеловекчтожтыоченьвлюбленакактебесказатьотв
ечаланаташаябылавлюбленавборисавучителявденисованоэтосовсемнетомнепокойнотвердояз
наючтолучшеегонебываетлюдейимнетакспокойнохорошотеперьсовсемнетаккакпрежденикол
айвыразилнаташесвоенеудовольствиеотомчтосвадьбабылаотложенанагоднонаташасожесточе
ниемнапустиласьнабратадоказываяемучтоэтонемоглобытьиначечтодурнобыбыловступитьвсе
мьюпротивволиотцачтоонасамаэтогохотелатысовсемсовсемнепонимаешьговорилаонаникола
йзамолчалисогласилсяснеюбратчастоудивлялсяглядянанеесовсемнебылопохожечтобыонабыл
авлюбленнаяневеставразлукессвоимженихомонабыларовнаспокойнавеселасовершеннопопре
жнемуниколаяэтоудивлялоидажезаставлялонедоверчивосмотретьнасватовствоболконскогоон
неверилвточтоеесудьбаужерешенатемболеечтоонневидалснеюкнязяандреяемувсказалосьчточ
тонибудьнетовэтомпредполагаемомбракезачемотсрочказачемнеобручилисьдумалонразговори
вшисьразматерьюосестреонкудивлениюсвоемуиотчастикудовольствиюнашелчтоматьточнот
акжевглубинедушииногданедоверчивосмотреланаэтотбраквотпишетговорилаонапоказываясы
нуписьмокнязяандреястемзатаеннымчувствомнедоброжелательствакотороевсегдаестьуматер
ипротивбудущегосупружескогосчастиядочерипишетчтонеприедетраньшедекабрякакоежеэтод
еломожетзадержатьеговерноболезньздоровьеслабоеоченьтынеговоринаташетынесмотричтоон
авеселаэтоужпоследнеедевичьевремядоживаетаязнаючтоснейделаетсявсякийразкакписьмаего
получаемавпрочембогдаствсихорошобудетзаключалаонавсякийразонотличныйчеловекпервое
времясвоегоприезданиколайбылсерьезенидажескученегомучилапредстоящаянеобходимостьв
мешатьсявэтиглупыеделахозяйствадлякоторыхматьвызвалаегочтобыскореесвалитьсплечэтуо
бузунатретийденьсвоегоприездаонсердитонеотвечаянавопроскудаонидетпошелснахмуренны
мибровямивофлигелькмитенькеипотребовалунегосчетывсегочтотакоебылиэтисчетывсегоник
олайзналещеменеечемпришедшийвстрахинедоумениемитенькаразговориучетмитенькипродол
жалсянедолгостароставыборныйиземскийдожидавшиесявпереднейфлигелясострахомиудовол
ьствиемслышалисначалакакзагуделизатрещалкакбудтовсвозвышавшийсяголосмолодогографа
слышалиругательныеистрашныесловасыпавшиесяоднозадругимразбойникнеблагодарнаятвар
ьизрублюсобакунеспапенькойобворовалитдпотомэтилюдиснеменьшимудовольствиемистрахо
мвиделикакмолодойграфвеськрасныйсналитойкровьювглазахзашиворотвытащилмитенькуног
ойиколенкойсбольшойловкостьювудобноевремямеждусвоихсловтолкнулегоподзадизакричал
вончтобыдухутвоегомерзавецздесьнебыломитенькастремглавслетелсшестиступенейиубежалв

клумбуклумбаэтабылаизвестнаяместностьспасенияпреступниковвотрадномсаммитенькаприезжаяпьяныйизгородапрятался вэтуклумбуимногиежителиотрадногопрятавшиесяотмитенькизналиспасительнуюсилуэтойклумбыженамитенькиисвояченицысиспуганнымилицамивысунулисьвсениздверейкомнатыгдекипелчистыйсамоваривозвышалась приказчицкаявысокаяпостельподстеганнымодеяломсшитымизкороткихкусочковмолодойграфзадыхаясьнеобращаянанихвниманиярешительнымишагамипрошелмимонихипошелвдомграфиняузнавшаятотчасчерездевушекотомчтопроизошловофлигелесоднойстороныуспокоилась втомотношениичтотеперьсостояниеихдолжнопоправитьсясдругойстороныонабеспокоилась отомкакперенесетэтоеесынонаподходиланесколькоразнацыпочкахкегодверислушаякаконкурилтрубкузатрубкойаа

**КЛЮЧ:** (424, 500)

**Найчастіші біграми шифрованого тексту:**

1.ыу 2.як 3.юк 4.ып 5.оу.

Розпізнавач російської мови: Для визначення того, чи являється текст інформативним використовувався підхід на основі індексу відповідності та ентропії. Для кожного набору ключів аналізувався розшифрований текст, у випадку коли ентропія та індекс відповідності були у допустимих межах, то текст вважається коректним. Межі допустимості були визначені емпіричним шляхом.

**Код програми :**

```
#include <iostream>
#include <fstream>
#include <math.h>
#include <string>
#include <map>

using namespace std;


string translate(int a);
int gcd(int a, int b, int& x, int& y); // обратный по модулю ищет
int sort(map<int, string>z, map<int, int>x); // сортирует топ-5 биграмм популярных
int bi(string s, int size); // проводим махинации с биграммами
int xy(map<int, string>good, string alpha, int* arr, int a); // преобразовывает биграммы в число
int razshifr(int top_good[], int top_alpha[]); // расшифровывает текст
double index(int size, string txt); // считает индекс соответствия

 // храним  числовые значения биграмм
int text_mass[8000];
int top_alpha[5];
int top_good[5];
```

```
//размеры необходимые
int size_bi_unique = 0;
int size_bigramm = 0;
int size_text = 0;

// алфавит
string alpha = "абвгдежзийклмнопрстуфхцчшщьыэюя";

// все мапы
map<int, string>popular;
map<int, string>z;
map<int, int>x;
map<int, string>good;
map<int, string>text;

int main()
	setlocale(LC_ALL, "Russian");

	string s;

	ifstream inf;

	inf.open("C:\\2.txt");
	getline(inf, s, '\0');
	inf.close();
	size_text = s.length();


	popular.emplace(0, "ст");
	popular.emplace(1, "но");
	popular.emplace(2, "то");
	popular.emplace(3, "на");
	popular.emplace(4, "ен");

	for (int i = 5; i < size_text; i++)
	{
	  popular.emplace(i, "0");
	}

	bi(s, size_text);

	for (int i = 0; i < 5; i++)
	{
	  cout << good.at(i) << endl;
	}

	xy(popular, alpha, top_alpha, 5);  // топ алфавита определяем значение биграммы
	xy(good, alpha, top_good, 5); // топ шифрованного
	xy(text, alpha, text_mass, size_bigramm); // шифрованный текст
```

```
        razshifr(top_good, top_alpha);

        return 0;
}

int bi(string s, int size)
{

        string buf, buf2;

        for (int i = 0; i < size; i++)
        {
          z.emplace(i, "0");
          x.emplace(i, 0);
          text.emplace(i, "0");
          good.emplace(i, "0");
        }


        int d;

        if (size % 2 == 0) d = size;
        else d = size - 2;

        string bufer;
        int cou = 0;
        int j = 0;

        for (int i = 0; i < d; i += 2)
        {

          buf.push_back(s[i]);
          buf.push_back(s[i + 1]);
          text.at(j) = buf;
          //cout << text.at(j) << endl;
          buf.clear();
          j++;
        }

        size_bigramm = j;

        j = 0;
        buf.clear();



        for (int i = 0; i < d; i += 2)
        {
```

```
cou = 0;

  if (s[i] != 0)
  {

                buf.push_back(s[i]);
                buf.push_back(s[i + 1]);
                z.at(j) = buf;


                for (int k = i; k < d; k += 2)
                {
                        bufer.push_back(s[k]);
                        bufer.push_back(s[k + 1]);

                        if (z.at(j) == bufer)
                        {
                                cou++;
                                s[k] = NULL;
                                s[k + 1] = NULL;
                        }


                        bufer.clear();
                }

                x.at(j) = cou;

                // cout << z.at(j)<<endl;

                j++;
                buf.clear();

  }
}

// сколько уникальных биграмм

for (int i = 0; i < size / 2; i++)
{
  if (x.at(i) != 0)
                size_bi_unique++;
}


// вывод биграмм и их количество
/*
for (int i = 0; i < sizen; i++)
{
```

```
    cout << z.at(i) << " : " << x.at(i)<<endl;
  }
  */
  // сортировка по макс биграмме
  sort(z, x);









  return 0;
}

int sort(map<int, string>z, map<int, int>x)
{

  int maxx = 0;
  int nomer = 0;

  for (int i = 0; i < size_bi_unique; i++)
  {
    if (x.at(i) > maxx)
    {
        maxx = x.at(i);
        good.at(0) = z.at(i);
        nomer = i;
    }
  }
  x.at(nomer) = 0;
  maxx = 0;

  for (int i = 0; i < size_bi_unique; i++)
  {
    if (x.at(i) > maxx)
    {
        maxx = x.at(i);
        good.at(1) = z.at(i);
        nomer = i;
    }
  }
  x.at(nomer) = 0;
  maxx = 0;

  for (int i = 0; i < size_bi_unique; i++)
  {
    if (x.at(i) > maxx)
    {
        maxx = x.at(i);
```

```
                good.at(2) = z.at(i);
                nomer = i;
        }
    }
    x.at(nomer) = 0;
    maxx = 0;

    for (int i = 0; i < size_bi_unique; i++)
    {
        if (x.at(i) > maxx)
        {
                maxx = x.at(i);
                good.at(3) = z.at(i);
                nomer = i;
        }
    }

    x.at(nomer) = 0;
    maxx = 0;

    for (int i = 0; i < size_bi_unique; i++)
    {
        if (x.at(i) > maxx)
        {
                maxx = x.at(i);
                good.at(4) = z.at(i);
                nomer = i;
        }
    }

    return 0;
}

int xy(map<int, string>good, string alpha, int* arr, int a)
{
    int otvet = 0;

    for (int j = 0; j < a; j++)
    {
        for (int y = 0; y < 2; y++)
        {

                string bufg;

                bufg[0] = good.at(j)[y];


                for (int i = 0; i < 31; i++)
                {
```

```
                        if (bufg[0] == alpha[i])
                        {
                                if (y == 0)
                                {
                                        otvet = 31 * i;
                                }
                                else
                                {
                                        otvet += i;
                                }
                        }
                }
          }
          arr[j] = otvet;
          otvet = 0;
        }
        return 0;
}

int razshifr(int top_good[], int top_alpha[])
{

        string open;

        for (int i = 0; i < 5; i++)
        {

          for (int j = 0; j < 5; j++)
          {



                for (int u = 0; u < 5; u++)
                {
                        for (int p = 0; p < 5; p++)
                        {

                                int X;
                                int f;
                                int a = 0, b = 0;
                                int ff;

                                int xx = 0, yy = 0;

                                if (i != j && u != p)
                                {
                                        int delta_x = 0;
                                        int delta_y = 0;
```

```
delta_x = top_alpha[i] - top_alpha[j];
if (delta_x < 0) delta_x += 961;

delta_y = top_good[u] - top_good[p];
if (delta_y < 0) delta_y += 961;


int prover = gcd(delta_x, 961, xx, yy);

if (prover == 1)
{
        xx = 0; yy = 0;

        gcd(delta_x, 961, xx, yy);
        if (xx < 0) xx += 961;
        a = (xx * delta_y) % 961;
}

else if (delta_y % prover != 0)
{
        cout << "Нет корней" << endl;
        break;

}
else
{
        delta_x = delta_x / prover;
        delta_y = delta_y / prover;
        int modd = 961 / prover;

        gcd(delta_x, 961, xx, yy);
        if (xx < 0) xx += 961;
        a = (xx * delta_y) % 961;
}



int bb;

bb = top_good[u] - ((a * top_alpha[i]) % 961);
if (bb < 0) bb += 961;


b = bb % 961;


xx = 0; yy = 0;

gcd(a, 961, xx, yy);
```

```
                                        if (xx < 0) { xx = 961 + xx; }



                                        int qq = 0;
                                        for (int n = 0; n < size_bigramm; n++)
                                        {
                                                qq = text_mass[n] - b;
                                                if (qq < 0)  qq += 961;

                                                X = (xx * qq) % 961;
                                                //transcr(X);

                                                string r = translate(X);
                                                open.push_back(r[0]);
                                                open.push_back(r[1]);
                                                r.clear();
                                        }

                                        //  тут надо понять читабельность текста.



                                        string bigra;

                                        double index1 = index(size_text, open);
                                        cout << endl;
                                        cout << "A: " << a << " " << "B: " << b<<endl;
                                        cout<<"Index :" << index1 <<endl;

                                        cout << translate(top_alpha[i])<<" ";
                                        cout << translate(top_alpha[j])<<" ";
                                        cout << translate(top_good[u])<<" ";
                                        cout << translate(top_good[p])<<" ";

                                        cout << endl;

                                        if (index1 < 0.059 && index1>0.051) cout << open << endl;

                                        else cout << "Индекс соответствия плохой!" << endl;


                                        open.clear();
                                }
                        }
                }
  }
}
return 0;
```

```
}

int gcd(int a, int b, int& x, int& y) {
	if (a == 0) {
	  x = 0; y = 1;
	  return b;
	}
	int x1, y1;
	int d = gcd(b % a, a, x1, y1);
	x = y1 - (b / a) * x1;
	y = x1;

	return d;
}

double index(int size, string txt) {

	setlocale(LC_ALL, "Russian");

	double sum = 0;
	int p = 0;
	int mo = -1;

	char* monogr = new char[size];
	double index;

	for (int i = 0; i < size; i++) {
	  mo++;
	  monogr[mo] = NULL;
	  int letter = 0;
	  monogr[mo] = txt[i];
	  if (monogr[mo] != NULL) {


			for (int j = i; j < size; j++) {
				if (txt[j] == monogr[mo]) {
					letter++;
				}
			}



			index = (double(letter) * (double(letter) - 1)) / (double(size) * (double(size) - 1));
			sum += index; //суммируем



			for (int z = i; z < size; z++) {
				if (txt[z] == monogr[mo]) txt[z] = NULL;
```

```
                    }
                }
            }


        return sum;

}

string translate(int a)
{

        string bigra;
        bigra.clear();
        bigra.push_back(alpha[a / 31]);
        bigra.push_back(alpha[a % 31]);

        return (bigra);
}
```

**Труднощі:**

Дуже складно було зрозуміти методичні вказівки, пояснення складні, хоча виконання насправді дуже просте.

**Висновок:**

У ході виконання практикуму було набуто знань з використання афінного шифру та методів його криптоаналізу. Було набуто навичок аналізу тексту на його інформативність за допомогою статистичних даних, розглянуто декілька моделей на основі яких проводився аналіз.