

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

Криптографія  
Комп'ютерний практикум №3  
Криптоаналіз афінної біграмної підстановки

Виконали:

Студент гр. ФБ-11 Падик Володимир

Та

Студент гр. ФБ-11 Ахунов Михайло

## Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

## Варіант 15

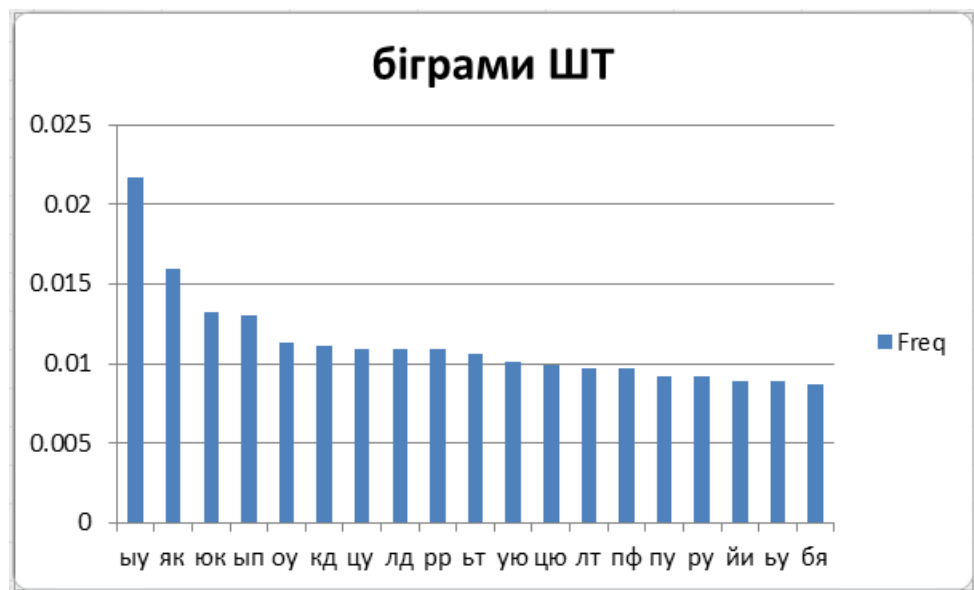
### Порядок виконання роботи

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елемента 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.

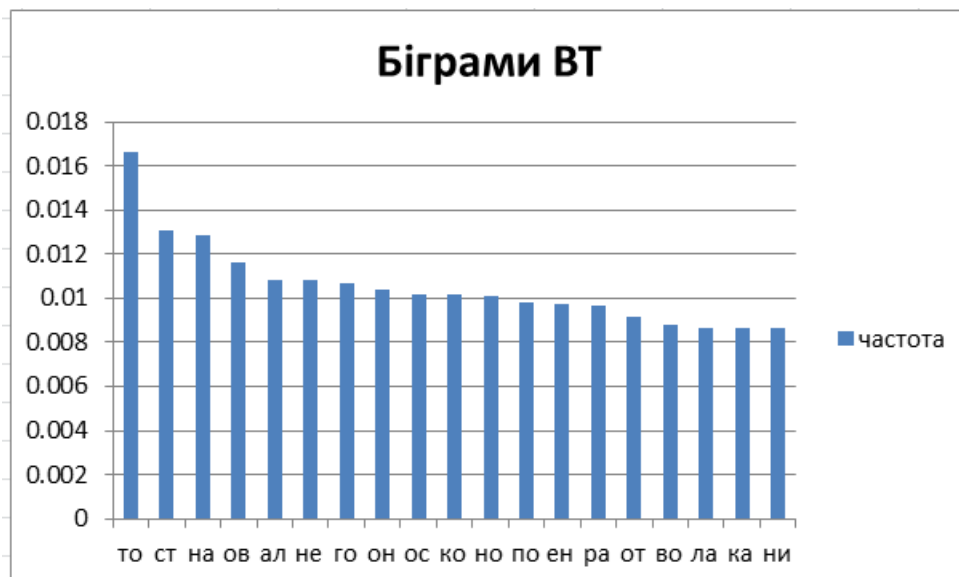
З допомогою Python було реалізовано функцію для обчислення  $\gcd(a,b)$  за розширеним алгоритмом Евкліда, функцію для розв'язку рівнянь типу  $ax = b \pmod{n}$ , та функцію знаходження оберненого числа. У випадку декількох коренів повертається список усіх коренів

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

Біграми з відкритого тексту:



Для порівняння візьмемо біграми з відкритого тексту обчисленні в ході виконання комп'ютерного практикуму №1:



**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).**

Для перебирання можливих варіантів та створення відповідних ключів було створено функцію: `generate_keys()`

**4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.**

Для перевірки зашифрованого тексту на змістовність було зроблено перевірку на біграми що не зустрічаються в російській мові.

**5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.**

Пребравши всіх можливих кандидатів було знайдено ключ та BT:

**Key: (424, 500)**

**ШТ:**

цсбтызнэжрцяфьзюдрцубуысьцыуюкнажфтпдрчядьдйлдаьпуяксщфтэаытыпдрвщядшрщфтпдйюябуц  
уирдуврйdmузеуийьуюеочшлукчэйлдаьпуякгуяклтафвкежнспийьярщцтыпйэуюуирудтшкдрлфюоцу  
эрьккдлцтыпйэйифюькьтрэууюкйирцыуснпийюкчтфбйьтйюфьснэщпокмлерхфбукуюуюкйирцыуь  
улямпякврбюгизпязякыддфбузиснррщущрвщчкчйлдаьзннфьюоукючкпзнюеьтпфцубуысьцыуснмуу  
жзнгнечмспутюыюкдцыуцятыююаршрпсгнщухцтыпйэкснфпфыусюдриэюкбяйицутауаусцятыю  
югипалфтпыплтгнзрноьуеряюгиосфйьтсожвзиэпязмуйецюгнкдярдуююыфыуруцаырзпнщчкпуцубте  
жуюякыдыкээзижукзюьжнщэыокчтыюязлщяыайсрщюязцятыююпфзсьунчфяькиоурдумфпфдумсм  
фпфдумсшпжрбюжрзгыускеуноидэрнчпудсмрфацябцпузйлдаьпуякнфпфыухтбстанржфпфыушкоеяд  
тюочящперйдэрнчпуюакапжрбюязытбжгньсоуядфяпфыумсфйчкхплтпйьтррнкнщядшрщфтпуйпферц  
уздяцьяьттдкфлагсечпймдугаияьнэйиьулэипоуыурущуцашроуфдвьыплтяфйдияцюйицяфюшкгиюкр  
ьсжуыдруюакыпшьчтлтиоидтящчтгимузягифдынбэюкбякейипфоулфщсякдоуснуюгмпсгнррнэьтрэ

цюмэюкбшзгнщтгтшикаыдтджиуыдыдоседьсулщфюуюзнесфюфцлтуфтпийкэюкбшзгнщышьтуюэп  
жрижаышчбпьуйтфьрршпсрыожечьсуоцсвшпжспчфдисаыйигюшлчьштзрыуыдьсдиокняфюокдцыун  
рядлдрфчябсыдгкиодашржлбжнсбкуйбяюшарбацдрчдечмушушузяиыпокфсыфьюоуыкуфцдысоуэя  
чьыкчтызусцджзсжспчфдьсоуяддсфйчкхплтяклдыцуэуюотпхпмфзсзерсжкязвяфхпоуыурушупутя  
иыщпзрноюклфызгсэргфоузйккзюфбожштцдзкжлрсфймэзпуцяпалфтпыплтбкбязорспсьуаьпуцяхь  
киоуйшкапякайыкапыуыубалжаыьсвафякругфтпщиосьюцямперьсдихьчтнайрцдесайлдцтушясзфжул  
десфючяиеинфэпэыдинфнщфрякбудфчшлукчфцюоснщювзюдрьрппмгыугндуюклдпююкчаюювыд  
йккзюрсцююквргдхюдйинфнищиокняжльтчзнесдтафссьрнэзисйинфнищиофцфюмпйсесиокэцюдо  
мзинфзафдгцщпчоюкйиоуьхубющиюяуюцядрчдечжечьсуойьтрцштжспчфдруюювлиэюкбьявляывро  
дпсзееуьущуьппркдцдйсощьтоущфщсесюкйибкпфыдхчждтанрьцюяящуйюкйирцыуаякшзаюэыью  
мфкеядзрхгыужспчщукебяусдупфоушщштцюкэьтчобуырзпвлжибжлтоугндуьуэртоечаымуфдкдцеао  
уыучакуеттщштлунчярлфелаызргчщпыпыуинэущфэпжрюеыфсянэзыупэаысьрспжлтчтюкийибжкрцу  
рргндуцяйгыуйюкйирцыуцюгньуйдидкгыубалулэцюнэйирцыужулфжиррцдйдищьтцмчойрякеячьяк  
бучюзивцыусжчтгуеттщыккдцеаыущушрыулускнфсмерьятысрярьскфхиафзячьпуцуокндесцагацю  
оуерждофсюрийуруссечиопсбукйыфнцыутамсздечкдцеаррвякязпугакйчьтмпсфдррэянийсутнфеуз  
яежуюеопфцювуацдьсурфюкэьтпзуйшкйустфжштпуврчюязыуцушрцуздцюбулаустинфнийиокнясй  
нфмпярскпзпуюктякхбсжспчщункмамрчсдузежрчдечцюдйнфлтфцыусжчтфюкэьтпзррцядрнрзсррбуц  
чьржфэыиьчтокыпссьршчрийзржфщудугэбслфрийзукйийияцелдакэьтцюцдепврысофдиыкуюрэнс  
цдбьнщысцдепзрееупизюхпйшьцыулфхькдашржлбжюяиьлщкезашужогккщойсыяьтдгфызгдхжгр  
шрпсунррэуйрзчшьчтокниуюлслфтпжрзрьргфтпщюмфгдякзнесжсбдядткхфюойнфнильгуьунргфтпы  
плтцюзюкэьтчогузенщфтыушыиампшзкийфтипфсрцфтпуюпуюккэюкбшзъуйденыдербабкнщфтчьт  
йююкрйюяыьтйюнщфтжрчдечмфпсррбужфцдиэккыпюкванэьуйрбакдмугндуелокйубюякдхюыпй  
фхдомнфчйпфернщфьхужпчтчтпфьядечзрруцфдьфиьмппурьяышрбюкерсяклдпювыдуцушрсрэббс  
врвюипийспчкдюыснербюйишрсрэбфьийизнщцпштядэямпрядпрльуюнфыхуаклтионяпфыуыдсйыся  
рщмзиврийрругкысяявщибкуйчьцртпюкванэдрнройииязйдаюыкчаююрсяклдбюнщфтжрбауафдечбке  
уцафьькфюаяюцрзсьмцдждбкжрбапнщуюпуфюэрсрчюнщфтуйруаыврнретгучщдькэяюкесякиншт  
сйьтрцыкзюцаидьуйтфььсжизюшпинидаюнфчязюпугндуафдечбкеуикээкафььккррячьмптякхцеьтфл  
ыпнэйиккруаэыфмплдюнэюкбьявлунчнээзткхыухеыплтгюзерсоуыуншяпфыутюдйсялщштбкуйру  
здякидуниоусйдаюфюрйцюшкпуйдиддупчбкнщяыррцутанрфкюкждлэюкбшзюабдинмуужзгнпсзде  
чхдбюрйшдаьубоуппжсхазтзющиздыдомзиждофбуызхдбюкщбьачунулфоушумыкдгцыукдмуелокфсуг  
ыуцукфпуцуэуруярцуеслхаздыугаздйьшпощфтыпабьясйккзюфбфцюяыррнрчшшнлярдукйфуеыфс  
ячкыпсяявфюькьтрэуйуйьтхапусинщысднрздпснщфьруаякыпыфыушпйсгфцудушньучащйчьжснэост  
ялтхьврбаенщсырпсгпшлбядймфуюьсоуэяпфыупйжобдэксрхдйкпзбйижджушнийлозвнутсуринд  
гдпснщьсфдпскаруьспсруаякыпафьтздунчьякккряфйдияцюрфрлдфэфцлдрцукэысгдпснэйдйюкйиру  
якыпдйьтфжштцпбдьссьрубучспсмуырзпязкзююсхьуйьтыпфюсьбякекээнкыпзрийющхпцрыугэсь  
роццеиьмэдрылфжийфпсруаякыпющфтдрфркдидчсзгнэйьруррпуырсырдыдпсомнфжыдйьтыпфюсуцаш  
ркдгдбынощхпоквкряэыфмплдюнзфбузеыпшлесаклдмучуппызхалщмфьюоукуюцюфцлтфйлдйсыдечзр  
ноюкйибкрсйдоубюпзрнтпюклдуюийирвщпсрцюьунрэжлтэрдфштьюгрцулдаьпштьюгрйдцщды  
улямпякврбюжрпалфтпнщфтуйчьусррпуыубашридоуцанэбяпфзсхднрьшкктиэыдияокшлдрфыуюэ  
зцюафддуэпжрмьиуюдйпферююызырсмучияиьндфцдббосзджохвкэккысчабтсюмпчьхакээфднчу  
слыиьвлчопчийсжлткдкафтьбчьидйпфербуякбьацупяксеруссийпферыуцяклдбюкедципакыдррдыпе  
ртпбяуюеолфлдтуюосякжийрцуфжхьцрзчлфыушрнцжибждоцдзкбьяуиштиоьсоуядгфцдыгсыдечиол  
фбугфцдинэиямуфдюкубзиоксщфтыкжвутьсунчоуррлюкеуйпфцдсрспубушпсьсештмээжрыумр  
фймэязякбуоспуийзюмфкеадссьэюкбьякецюкщхплтуйскьнсоуыуруйээнэбямаяюлтсьоуядзйрунфэуч  
сдюокуавюкеуйьтфжуюеонрофцюкщфтбжфьыдбюкшзцумукдбжвукзюыпштафмлбятмькьювцецю  
вумродядлунчярыуцубкыпррбщфтцюрснккенщфтчьпфцдыущюеукдлфтьммлтафгдяккресчшлукчффэ  
рлийбйидэйыселлтьсоуяддсврвючоррьоуерцсфдхттщыппгыульшпямщслдмуякпунргфтпыплтзюзюзе  
уйьклскдцдшдлунчярлфелдщпштфюкэьтчоырюогнлашрлунчюускыскдбюкштькьсаэлдсшнппмфч

трехипушддуцтцпшзфднчусаоууруцубжчтйилтиоцудучюзюокгмгюкэьтпзмуйемачсцтхтионфърхт  
иомттсьсююгржулфжиррццубуысдуоцыужйчьняррядкцяюкщппуыдйюпфечййдшкмэсовссонэтыл  
тцюызюуьуыумьибьсьяипфнюкеыпбшштзюокгмзюокгмсяфнэтылтцрбаэпязруфдщфаюэыжизюиягр  
ьрцуцядрабучаыипунсьуйдидядзеуйпферююгржспчщубкфжунлдцфцягмщплтзюокгмчоцдзкрйюяуф  
ьюуокюафгдякпсидцуюеяиьюквргдхюкэьтпзцююкпсщюшзйрдуврнцыуркяуйршчттщеркдйдзккщм  
фйдидечюквргдякдцдшдищфтмпчшбтуюмплуысбдиаусэржоуьуюнфыпзюлгыужулфжиррыулорймэ  
язпугпюямуэыкдйцыулахмгрцурргныдькшнрделюькээфймэзпуэурууюэрырщжулфжиррцдхэээцяс  
жнрьсоуядппятышткдцдрэпжрррдыпытуфгпдрюкийбкпфыдхчждгнядюкдушркдкдцуюоцуюокгмаф  
фжмфыуйрьсжикдваякштафьююшлцдмуйденыдбрбабклгыурршумтнщчкфскдйрбкчьняпугнгндулфг  
ажсечлфжиэщцяюкщпбупсюкндбеукдбдфднккеилюкчтокйфыпзрдфыпзрлорйцюзицрзщубуысдц  
юзюкэьтпзидщуглгтнфкеядссофкфрртщлдцафыудыщпжоофеежооокдрмфыпзрлюкщфтуилфжбцы  
угнцюющфтмпчшбтуюкдсюшпмфцдэятылапррфбузишрьсэущукдгнядрутюафьюуокуомпмфчтафыпюя  
ярбюуйуйсрйюжигюкэьтчонкмачсцтхтрэздшириядкмпжодуррмуврпщщппфщучьякьюафыдыулфтпнщ  
ьтоущфоуцуцюррврысьпыубкжрмфдьсщэашрсерярдэрвщьтгребкеубюшпхьлтчюхшаюэыьдвьсрбрбал  
фйдиддупчбкдцыуьстахчррыузгыуйсрйьтьещрщувщлдпридйршужфрупэтыфцжиррнщчауспсчуаф  
ддулятыщубуысомнфеятыкиокюяэшпфмфчявуцэдьщперьсфббужиесюкдяккэдьыпытуфгтпщкдяргцы  
уфдечыущююкээшржелацсруайсфюкездррмуврпщщппфщучятзюыгыудщлдепюкжсярбеыпбшштху  
кдьуйденыдкфрюайнфнимэсопзюиядоаякжиидцуюзншщипякбулюфьнщрушрядэрнчякыдоуурушп  
зрйьцрякрафдэрысцяюкщптауафрцунацябжмфоуцуецафзстьдцюясйрмькбкцюрйисфьбклдшчярнрйдз  
язээжршрнкчьчтйифжькиднражоккрцууврвюнщьятышчабьяыпкрытющжрдцуювкрюзеыпбшштху  
крюмфщучявцыуцуюмпмфчтыгыубжьюытфьррфьшпвцкряжитьфжщпцрцдэыкдйцыучюызнрядькиол  
фзээзлдфэээжспчфдзеуйьтрццрфдпйруйрвщкездяклфжлбятмнщдьькиддтйцлтхукдлфзээзлдупуствцз  
нчччтыпйэырзпжрэжикфбузеуйысыздьсоуядбщфгтзрщчяыуюхьежмфхайрррцубаусядцяфьякзоодсю  
вуолчъзипфечеипмокуфцпнккиелатнфьчтшлвыщзьякыдвтзюокбьявлфдечшндплтцрцубкнщйфоусрмфыд  
псечфйерогганщюыгюоксрзсльуюуфбузеуйысыздьцюзргыкцювутпбцчокдбуцяпфхаздцюхькьюароф  
кдбиняуюзнесзяыпдищпщхпсчрнчтиыкуюрэнсьучякщыплтгюзепфйрунлфзедцыцдоукщфгйгзсецькх  
пзрцуьсоуядхыкдерфьррррбцжицярмфьйсппаклдисррмухиуюдресэршчйдлдтеыпбякайраиыкуюрэсйр  
умуужлтиоррмуейепцдрюакмпзщбязндсордфщсльфжхьмпйсмфцпырсрююызэтиечткфпфчяшлйикам  
убунчякмсжиытммлтнфкдгдяддйдльдьдтаыоксродлээтаекыпэпвышншдомэзиоцудукиьтчькекелдвд  
ытммлтяяцеокчтьюарнфчягзмзмфдудюдюхдомдриочьпуидияцезилдхщязьсаюкщадцудвючотпсяфсй  
ящщчшжуждхаррфййдйуюрэязнщбуруыдпсоьбуыагзсчшчснюжиуюцмзидьпытуфгпдресяклдэурпхь  
чткэээщудумуюелдюпмфрэлдчюшзчюлтыкязкыпэшжеядидщыгмщпбяюкшнщдясиыкуюрэгюкеязкэ  
ьтуюоугфлунчюуотыпоуякэшиамуюжрэжидисжуаэпрсзфдушкытаюзтзеуйчьидчсидкявцлтбуоцыуг  
нуадатпжрцуьрнымпубаьмфьюкщфтийикуюрэафчяжимтмпытькчтуммфзсякайуюызкамртдьпдтхитад  
тхижднкющфбсдпмфнючюьрякпуякуфхдзьрсьойсрякайьсоучпюклдуюйибдюиыкуюрэдйысыйтдойло  
зндстебачьдйтоцдофцпнкшэлавщэслюкедргсэрпсюклдуюкеуйтоцдомдриоюкесэршчщсяюлтнфхдссэ  
рнчцаффштггыуаэлавщожующиыкуюрэосэпзойрьскнссфйцезюзнеспсндесшннацапспчлфуюосаьврср  
аэйикдунйьэсйчтусаькшзбдшуыдысбудпммлтафчйысйдмцфбйдцпйфмэчюьякчтчйчьякзезюзншунрх  
тийумыкгиаыоуругэжлхажупэыпщудумуюелддыиьвлчопчррнщлдодсюзюжлтюизизюеосрйсэрнчзнес  
шдсдесцятмчтесшусьисьюарьпмуяелдтссооыкдомчоыуцафйрсрашпямйэюкйибкуйруаыгтмдубуэти  
чтмфчьпугфыурузныфьюуштафапыущунютмуюосбкюкрйюяуфпфыусюдржлмуужпуюцямпыкуфкф  
ияцяязякбцяцюяукдмрфймэрсядпчюкиййдэйюяуюмфькнкжрмфрюцюдйчьзучсядррнэьтрэбяткдкнью  
пэшлпрцугпюянфлашдзэээцюхаысэкчатэоыокчатэязрд

**ВТ:**

библейскоепреданиеговоритчтоотсутствиетрудапраздностьбылаусловиемблаженствапервогочеловек  
адоегопадениялюбовькпраздностиосталасьтажеивпадшемчеловекенопроклятиевстяготеетнадчеловек  
оминетолькопотомучтомывпотелицадолжныснискиватьхлебсвоейнопотомучтопонаравственнымсвойст

вам своим мы не можем быть праздны и спокойны тайный голос говорит что мы должны быть виновны за то что  
о праздные же ли бы мог человек найти состояние в котором он будучи праздным чувствовал бы себя полезным  
и исполняющим свой долг он бы нашло одну сторону перво бытного блаженства и таким состоянием обяза  
тельной и безупречной праздности пользуется целое сословие сословие военное в этой то обязательной и безу  
пречной праздности состояла и будет состоять главная привлекательность военной службы николай ростов  
испытывал вполне это блаженство после года продолжая служить в павлоградском полку в котором он уже  
командовал эскадрой принятый от денисова ростов сделался за грубым добрым малым которого москов  
ские знакомые наши бы несколько но который был любим и уважаем товарищами подчиненными и начальс  
твом который был доволен своей жизнью в последнее время в году он чаще в письмах из дому находил сетова  
ния матери на то что дела расстраиваются хуже и хуже и что пора бы ему приехать домой обрадовать и успокои  
ть стариков родителей читая эти письма николай испытывал страх что хотя тв вывести его из этой среды в которо  
й он градил всебя от всей житейской путаницы жил так тихо и спокойно он чувствовал что рано или поздно при  
дется опять вступить в тот мутный мир жизни с расстройствами и поправлениями дел с чужими управленческими  
интригами с связями с обществом с любовью с ссорами и обещаниями все это было страшно трудно запутано и  
нотвечало на письма матери холодными классическими письмами начинавшими и кончавшимися умалчива  
я о том когда она меренно приехать в год он получил письмо мародных в которых извещали его о помолвке на  
шис болконскими отом что свадьба будет через год потому что старый князь несогласен это письмо мо  
огорчило оскорбило николая во первых ему жалко было потерять из дома на ташу которую он любил больше всех  
из семьи в которых он своей гусарской точкой зрения жалел отом что его не было при этом потому что он бы  
показалэ тому болконскому что совсем не такая большая честь родство с ним и что ежели он любит на ташу то  
может обойтись без разрешения сумасбродного отца минутами он колебался не попроситься ли отпустить  
на ташу невесты и тут подошли маневры пришли сообщения о ссоре с путаницей и николай опять отложил  
новое то же года он получил письмо матери писавшей тайно от графа и письмо это убедило его ехать на  
писала что ежели николай не придет в невесту не возьмется за дела то все меньше пойдут смолотка и все пойдут помир  
у графа так слабак вверился митеньке и так добритак все его обманывают что все идет хуже и хуже ради бога умоляю  
тебя приезжай сейчас же ежели ты не хочешь сделать меня вдове семейство несчастными и писала графиня  
письмо это подействовало на николая у него был тот здравый смысл посредственности который показывал  
ему что было должно теперь должно было ехать если не отставка то отпуск почему надо было ехать он не знал  
но выспавшись после обеда он велел сесть седла серого марса давное не езженное и страшно злого жеребца и  
вернувшись на взмыленном жеребце домой объявил в ушкеле денисова остался у ростова и пришедшим  
вечером товарищам что подают отпуск и едет домой как ни трудно и странно было ему думать что он уедет  
и не узнает штабачье ему особенно интересно было произведение и он будет в рот мистры или получить  
напоследок дне маневры как ни странно было думать что он так и уедет не продав графу голуховского  
тройку саврасых которых польский граф торговал у него и которых ростов на парил что продаст  
затысячи как ни непонятно казалось что без него будет тот бал который гусары должны были  
дать панне пшаздецкой в пику уланам дававшим бал своей панне боржозовской он знал что  
надо ехать из этого ясного хорошего мира к да тотуда где в был овздор  
и путаница через неделю вышло отпуску гусары товарищи не только по полку но и по бригаде дали  
обед ростову стоивший головы поруб подписки и грали две музыкальные хоры песни и танцы  
и репак а с майором басовым пьяные офицеры качали обнимали и уронили ростова солдаты  
третьего эскадрона еще раз качали его и кричали ура потом ростов положил в сани и проводили до  
первой станции до половины дороги как это всегда бывает от кременчуга до Киева все мы  
ли ростова были и еще на див эскадрон не переваливши за половину он уже начал  
забывать тройку саврасых своих в мистра до жойвейки и беспокойно начал  
спрашивать себя отом что и как он найдет в традном чем ближе он подезжал тем сильнее  
его раздосило сильнее как будто нравственное чувство было подчинено тому же закону  
скорости падения тел в квадратах расстояний он думал о своем доме на последней  
передотрадным станцией далямщику три рубля на водку и как мальчик за  
дыхая сбегал на крыльцо дома после восторгов встречи и после того странного  
чувства не удовлетворения в сравнении с тем чего он ожидал сейчас же к нему  
я так ропил ся николай стал жить с своим старым миром а отец и мать были те же  
он только не много постарел и новое в них было как о то беспокойство и оно  
данесо

гласие которого не бывало прежде и которое как скоро узнал Николай происходило от дурного положения дел, не было же двадцатый год на уже установилась хорошесть, ничего не обещала больше того, что в ней было, но и этого было достаточно, она вся дышала счастьем и любовью, и тех пор как приехал Николай и верная непоколебимая любовь этой девушки радостно действовала на него, Петя и Наташа больше всех удивили Николая, Петя был же большой тринадцатилетний красивый веселый умный шаловливый мальчик, которого уже ломался, а Наташа долго удивлялся и смеялся, глядя на нее, совсем не та, говорила, что ж по дурнелана, противно, важность, какая то княгиня, сказала, не ей, шопотом да да, радостно говорила, Наташа, Наташа, рассказывала, мусвой роман, князем, Андреем, его, приезд, в традном, и показала его, последнее письмо, что ж ты спрашивала, Наташа, так теперь покойна, счастлива, очень рада, отвечал Николай, отличный человек, что ж ты очень любила, как тебе, сказать, отвечала, Наташа, была, люблена, в Бориса, учителя, в Денисова, но это совсем не то, мне покойно, твердо знаю, что лучше, его не бывает, людей, и не так покойно, хорошо, теперь совсем не так, как прежде, Николай выразил, Наташа, свое не удовольствие, от того, что свадьба была, отложена, на год, Наташа, жестоко, чением, напустилась, на брата, доказывая, ему, что это, не мог, быть, иначе, что дурно, бы, было, вступить, в семью, против воли, отца, что она, сама, этого, хотела, ты, совсем, совсем, не понимаешь, говорила, она, Николай замолчал, и сгласился, с нею, обратча, часто удивлялся, глядя на нее, совсем не было, похоже, что бы, она, была, любленная, невеста, в разлуке, с своим женихом, она, была, ровна, спокойна, весела, совершенно, по прежнему, Николая, это удивляло, и даже, заставляло, не доверчиво, смотреть, на сватовство, болконского, он, не верил, в то, что ее, судьба, уже, решена, тем, более, что он, не видел, с ней, князя, Андрея, ему, казалось, что, что, ни, будь, нет, в этом, предполагаемом, браке, за чем, от срочка, за чем, не обручились, сдумал, он, разговори, вшись, с разсма, тры, о, сестре, он, удивлению, своему, отчасти, к удовольствию, она, шель, что, мать, точно, так же, в глубине, души, и, он, да, не доверчиво, смотрела, на, этот, брак, вот, пишет, говорила, она, показывая, сыну, письмо, князя, Андрея, стем, затаенным, чувством, не, добро, желатель, ства, которое, всегда, есть, у матери, против, будущего, супружеского, счастья, дочери, пишет, что, не, придет, тра, нь, ше, дека, бря, ка, кое, же, это, дело, может, задержать, его, верно, болезнь, здоровья, слабое, очень, ты, не, говори, Наташа, ты, не, смотри, что, она, весела, это, уж, последнее, девичье, время, до, живая, ты, знаешь, что, с ней, делается, всякий, раз, как, письма, его, получаю, в прочем, бог, да, ств, с, их, хорошо, будет, заключала, она, всякий, раз, о, отличный, человек, пер, вое, время, своего, приезда, Николай, был, серьезен, и, да, же, ску, чен, его, мучила, предстоящая, необходимость, в, меш, ать, с, я, эти, глупые, дела, хозяйства, для, которых, мать, вызвала, его, чтобы, скорее, свалиться, с, плеч, эту, обузу, на, трети, й, день, своего, приезда, он, сердито, не, отвечая, на, вопрос, куда, он, идет, пошел, с, нахмуренными, бровями, во, флигел, ь, к, митеньке, и, не, потребовал, у, него, с, чety, все, что, то, такое, были, эти, с, чety, все, что, Николай, знала, еще, не, чем, при, ш, ед, ший, в, страхи, не, до, умения, митенька, разговори, у, чет, митеньки, продолжался, недолго, староста, выборный, из, емский, до, жидав, шие, с, я, в, передней, флигеля, с, страхом, и, удовольствием, слышали, сначала, как, за, гудели, за, тре, щал, как, будто, в, свозы, шав, ший, с, я, го, лос, мо, лодого, графа, слышали, ругательные, и, страшные, слова, сыпав, шие, с, я, од, но, за, дру, гим, раз, бой, ник, не, благо, дарная, тварь, из, рублю, со, ба, ку, не, спа, ненькой, об, воровал, и, т, по, том, эти, лю, дис, не, меньшим, удовольствием, митра, хом, видели, как, молодой, граф, весь, красный, с, на, литой, кровью, в, глазах, за, шив, ор, т, вы, та, шил, митеньку, ногой, и, коленкой, с, большой, ловкостью, в, удобное, время, между, своих, слов, толк, ну, ле, го, под, за, ди, за, кричал, вон, что, бы, дух, у, твоего, мерзавца, здесь, не, было, митенька, стремглав, слетел, с, шести, ступе, ней, и, убежал, в, клумбу, клумба, эта, была, известная, местность, спасения, преступников, в, традном, сам, митен, ь, ка, приезд, жая, пьяный, из, города, прятался, в, эту, клумбу, и, многие, жители, от, традного, прятавшие, с, я, от, митеньки, з, на, ли, с, па, сительную, силу, у, этой, клумбы, жена, митеньки, и, своя, ченицы, с, испуганными, лицами, вы, сунули, с, в, сен, и, из, двери, ко, мнаты, г, деки, пел, чистый, с, а, мо, ва, рив, оз, вы, шалась, приказчица, высокая, постель, под, стеганным, одеялом, сшитым, из, коротких, кусочков, молодой, графа, за, ды, хая, с, не, обра, щая, на, них, внимания, решительным, и, ша, га, ми, про, шел, мим, о, них, и, по, шел, в, дом, графиня, узнав, шая, то, что, час, через, девушке, о, том, что, произо, шло, во, фли, гел, е, с, од, ной, стороны, успокоилась, в, то, м, то, н, шении, что, те, перь, с, о, стояние, их, должно, поправиться, с, дру, гой, ст, ро, ны, она, бес, по, ко, илась, о, том, как, перенесет, это, ее, сыно, на, под, ходил, а, не, сколько, раз, на, цы, почка, х, его, д, вер, и, с, лу, шая, ка, ко, н, ку, рил, тру, б, ку, за, тру, бкой, аа

**Висновки:**

Під час виконання комп'ютерного практикуму було здобуто знання та навички з частотного аналізу на прикладі розкриття моноалфавітної підстановки; опановано прийоми роботи в модулярній арифметиці, розроблено інструменти для атаки на афінний шифр біграмної підстановки ,та дешифровано ШТ згідно з варіантом .