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**

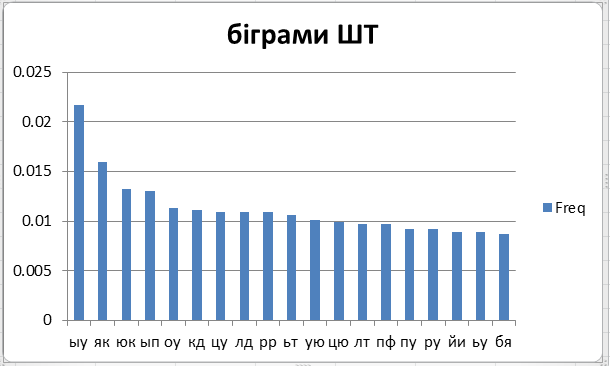
Порядок виконання роботи

1. **Реалізувати підпрограми із необхідними математичними операціями:обчисленням оберненого елементу за модулем із використанням розширеного алгоритмуЕвкліда, розв’язуванням лінійних порівнянь. При розв’язуванні порівнянь потрібнокоректно обробляти випадок із декількома розв’язками, повертаючи їх усі.**

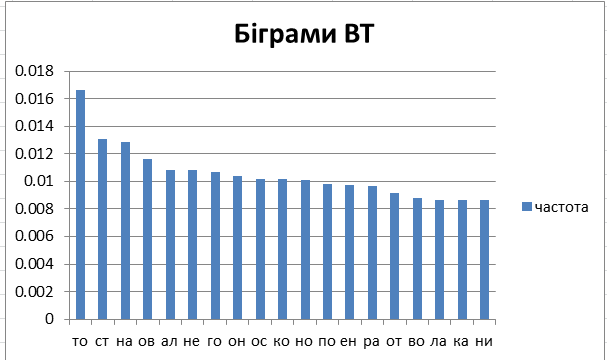
З допомогою Python було реалізовано функцію для обчислення gcd(a,b) за розширеним алгоритмом евкліда, функцію для розвязку рівнянь типу ax = b (mod n), та функцію знаходження оберненого числа. У випадку декількох коренів повертається список усіх коренів

1. **За допомогою програми обчислення частот біграм, яка написана в ходівиконання комп’ютерного практикуму №1, знайти 5 найчастіших біграм запропонованогошифртексту (за варіантом).**

Біграми з відкритого тексту:



Для порівння візьмемо біграми з відкритого тексту обчисленні в ходівиконання комп’ютерного практикуму №1:



1. **Перебрати можливі варіанти співставлення частих біграм мови та частих біграмшифртексту (розглядаючи пари біграм із п’яти найчастіших). Для кожного співставленнязнайти можливі кандидати на ключ (a,b) шляхом розв’язання системи (1).**

Для перебирання можливих варіантів та створення відповідних ключів було створено функцію: generate\_keys()

1. **Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не єзмістовним текстом російською мовою, відкинути цього кандидата.**

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

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

Перебравши всіх можливих кандидатів було знайдено ключ та ВТ:

Key: (424, 500)

**ШТ:**

цсбтызнэжрцяфьзюдрцубуысьцыуюкнажфтпдрчядьдйлдаьпуяксщфтэаытыпдрвщядшрщфтпдйюябуцуйрдуврйдмузеуйиьуюеочшлукчэйлдаьпуякгуяклтафвкежнспйиьяршцчтыпйэуюуйрудтшкдрлфюоцуэрьккдлцчтыпйэйифюькьтрэуйюкйирцыуснпйюкчтфбиььтйюйфьснэщпокмлерхфбукюуйюкйирцыуьулямпякврбюгиэпязякыддфбузиснррщушрвщчкчйлдаьзннфьуоукючкпззнюеьтпфцубуысьцыуснмуужзнгнечмспутюыыокдцыуцятыююаршрпсгнщухцчтыпйэкдскнфпфыусюдриэюкбяйицютауаусцятыююгипалфтпыплтгнзрноьуеряюгиосфйьтсожвзиэпязмуйецюгнкдярдуююыфыуруцаырзпнщчкпуцубтежуюякыдыкээзижуякзоьсжинщэыокчтьюязлщяыайсрщюязцятыююпфзсьунчфаькиоурдумфпфдумсмфпфдумсшпжрбюжрзгыускеуноидэрнчпудсмрфацябцпузйлдаьпуякнфпфыухтбстанржфпфыушкоеядтючоцящперйдэрнчпуякапжрбюязытбжгньсоуядфяпфыумсфйчкхплтпйьтррнкнщядшрщфтпуйпферцуздцячььттдкфлагсечпймпдутяиьнэйиьулэипоуыурущуцашроуфдвьыплтяфйдияцюйицяфюшкгиюкнрьсжуыдруякыпшьчтлтиоидтящщчтгимузягифдынбэюкбякейипфоулфщсяыкдоуснуюгмпсгнррнэьтрэцюмэюкбяшзгнщттщзикаыдтджиыуыдысодесьулцфюуюзнесфюфцлтуфтпйикэюкбяшзгнцьыпьтуюэпжрижаышчбпьуытфьрршпсрыожечьсуоцсвшпжспчфдисаьйигюшлчьштзрыуыдьсдиокюяфюокдцыунрядлдрфчябсыдгкиодашржлбжнсбкуйбяющарбацядрчдечмущушузяиьыпокфсыфьуоуыкуфцдысоуэячьыкчтызусцджгзсжспчфдьсоуяддсфйчкхплтяклдыцыуэуюотпхпмфзсзерсжкязвяфьхпоуыурушупутяиьщпзрноюклфызгсэргфоузйккзюфбожштцдзкжлрсфймэязпуцюпалфтпыплтбкбязюрспсьуаьпуцяхьькиоуйшкапякайыкапыуыубалжаыьсвяафякругфтпщиосьуцямперьсдихьчтнайрцдесайлдцтушясзфжулдесфючяиещинфэпэыдинфнщфрякбудфчшлукчффцюоснщювзюдрьрппмгыугндуяклдпююкчаюювыдйккзюрсцююквргдхюдйнфнищиокюяжльтчьзнесдтафссйрнэзисйнфнищифюфцфюмпйсесиокэцюгдомзинфзафдгцщпчоюкйиоуйьхубющиюяуюцядрчдечжечьсуюйьтрцштжспчфдруюювлиэюкбявлаывродпсзееуьущуьппркдцдйсощьтоущфщсесюкйибкпфыдхчждтанрьцюяяыцуьйюкйирцыуяксяшзаюэыьюмфкеядзрхгыужспчщукебяусдупфоушщштцюкэьтчобуырзпвлжибжлтоугндуьуэртоечаымуфдкдцдеаоуыучакуеттщштлунчярлфелаызргчщпыпыуинэущфэпжрюеыфсянэязыупэаысрьспжлтчтюкйибкжрцурргндуцяйгыуийюкйирцыуцюгньуйдидкгыубалулэцюнэйирцыужулфжиррцдйдищьтцмчойрякеячьякбучюзивцыусжчтгуеттщыккдцдеаыущушрыулускнффсмрйятысрярьскфхиафзячьпуцуюкндесцагацюоуерждофсюрйуйруссечиопсбукйыфнцыутамсздечкдцдеаррврякязпугакйчьтмпсфдррэянйысутнфеузяежуюеопфцювувацдьсурфюкэьтпзуйшкйустфжштпуврчюязыуцушрцуздцюьулаустйнфнийиокюясйнфмпярскпзпуюктякхбсжспчщункмамрчсдузежрчдечцюдйнфлтфцыусжчтфюкэьтпзррцядрнрзсррбуцчьржфэыиьчтокыпссьршчрйязнржфщудугэбслфрйязуакййияяцелдакээытющцдепврысофдиыкуюрэнсцдбьнщысцдепзрзееупизюхпйшьцыулфхьькдашржлбжюяиьлщкеэащужогккщойысяытдгфызгдхжгршрпсунррэуйрзчшьчтокниуюлслфтпжрзрьргфтпцюмфгдякзнесжсбдядтякхфюойнфнилгыуьунргфтпыплтцюзюкэьтчогюзенщфтыушыиямпшзкийфтйпфсрцфтпуюпуяккэюкбяшзьуйденыдербабкнщфтчььтйююкрйюяыььтйюнщфтжрчдечмфпсррбужфцдиэккыпюкванэьуйрбакдмугндуелокйубюяыкдхюыпйфхдомнфчйпфернщфьхужпчтчтпффьядечзрруцуфдьфиьмппурряышрбюкерсяклдпювыдуцушрсрэббсврвюипйспчкдюыснербюйишрсрэбфьйиязнщцпштядэяямпрядпрльуюнфыпхуяклтионяпфыуыдсйысярщмзиврйрруткыпсяявщибкуйчьцртпюкванэдрнроьйиязйдаюыкчаююрсяклдбюнщфтжрбауафдечбкеуцафьькфюйаяюцрзсьмцдждбкжрбапфнщуюпуфюэрсрчюнщфтуйруаыврнретгучщдьькэяюкесякинштсйьтрцыкзюцаидьуытфььсжизюшпинйдаюнфчязюпугндууафдечбкеуикээкафьькррцячьмптякхцеьтфлыпнэйиккруаэыфмплдюндэюкбявльунчнээзтякхыухеыплтгюзерсоуыуиншяпфыутюдйсялщштбкуйруздякидуниоусйдаюфюрйцюшкпуйдиддупчбкнщяыррцутанрфкюкждлэюкбяшзюабдинмуужзнгнпсздечхдбюрйшдаьубоуппжсхазтзющиздыдомзиждофбуызхдбюкщбячунулфоушумыкдгцыукдмуелокфсугыуцукфпуцуэуруярцуеслдхаздыугаздйьшпощфтыпаьбясйккзюфбфцюяяыррнрчшшнярдукйыфуеыфсячкыпсяявфюькьтрэуйуйьтхапусйнщыссднрздпснщфьруякыпыфыущпйсгфцудушньучащйчьжснэостялтхьврбаенщсырпсгпшлбядймфуюьсоуэяпфыупйжобдэксрхдйдкипзбяйижджушнийлознвутсуринйдгдпснщьсфдпскаруьспсруякыпафьтздунчяьккрцуяфйдияцюцрфрлдфэфцлтдрцукэысгдпснядйюкйируякыпдйьтфжштщпбдьссйрубучспсмуырзпязякзююсхьуйьтыпфюсьбякекэээнкыпзрйьющхпцрыугэсрьроццеиьмэдрыдлфжийфпсруякыпющфтдрфркдидчсзгнэиьруррпуырсрыдпсомнфжыдйьтыпфюсуцашркдгдбыющхпоквкруаэыфмплдюнзфбузеыпшлесяклдмучуппызхалщмфьуоукюцюфцлтфйлдйсыдечзрноюкйибкрсйдоубюпзнртпюклдююйийрвщпсшрцюьунрэжлтэрдфштьюгрцулдаьпфштьюгрйдцщдьыулямпякврбюжрпалфтпнщфтуйчьусррпуыубашридоуцанэбяпфзсхднрьсшкчтиэыдияокшллдрфыусюэзцюуафддуэпжрмьйиуюдйпферююызырсрмучяиьзндфцдббосзджохвкэккысчабтсюмпчьхакэээфднчуслыиьвлчопчйщсжлткдкяфтьбчьйидйпфербуякбяцучпяксруссйпферыуцуяклдбюкедципякыдррдьыпертпбяуюеолфлдтюуюосякжийрцуфжхьцрзчлфыушрнцжибждоцдзкбяуйштиоьсоуядгфцдьпгсыдечиолфбугфцдинэияямуфдюкубзиоксщфтыксжвуьсыунчоуррлюкеуйпфцдсрпспубушпьсещштмэээжрыумрфймэязякбуоспуйьзюмфкеядссйэюкбякецюкщхплтуйсркьнсоуыуруйэээнэбямаяюлтьсоуядзйрунфэучсдуюкуавюкеуйьтфжуюеонрофцюкщфтбжфьыдюбокшзцумукдбжвуякзюыпштафмлбятмькьювцзецювумродядлунчярыуцубкыпррбщфтцюрснккенщфтчьпфцдыущюеукдлфтьммлтафгдяккресчшлукчффэрлйбяйдэйыселлтьсоуяддсврвючоррьуоуерцсфдхттщыппгыульшпямщслдмуякпунргфтпыплтзюзюзеуйьклскдцдшдлунчярлфелдьщпштфюкэьтчоырюогнлашрлунчюускыскдюбокштькьсаэлдссшнппмфчтрсхипушддуцтщпшзфднчусхаоуыуруцубжчтйилтиоцудучюзюокгмгюкэьтпзмуйемачсцтхтионфьрхтиомттьсюзюгржулфжиррцдцубуысдуоцыужйчьняррядкдцяюкщппуыдйюпфечйдйдшкмэсовссонэтылтцюызюуьуыумьиьиьсяиьпфнюкеыпбяштзюокгмзюокгмсяафнэтылтцрбаэпязруфдщфаюэыжизюиягрьрцуцядраьбучяиьпунсьуйдидядзеуйпферююгржспчщубкфжунлдцфцягмщплтзюокгмчоцдзкрйюяуфьуоукюафгдякпсыддцуюеяиьюквргдхюкэьтпзцююкпсщюшзйрдуврнцыуркяуйршчцттщеркдйдзккщмфйдидечюквргдядкдцдшдищфтмпчшбтуюмплуысбдиаусэржоуьуюнфыпзюлгыужулфжиррыулюрймэязпутпюямуэыкдйцыулахмгрцурргныдькчшнрдслюькээфймэязпуэуруюуэрырщчжулфжиррцдхэээцясжнрьсоуядппьятышткдцдярэпжрррдьыпьтуфтпдрюкйибкпфыдхчждгнядюкдушркдкдцуююцюокгмаффжмфыуйрьсжикдваякштафьюющлдцдмуйденыдбрбабклгыуррщумтнщчкфскдйрбкчьняпугнгндулфгажсечлфжиэшцяюкщпбупсюкндбкеукдбдфднккеилюкчтокйфыпзрдфыпзрлюрйцюзицрзчцубуысядцюзюкэьтпзидщугцлтнфкеядссофкфрртщлдьцафыудьщпжоофеежооокдррмфыпзрлюкщфтуйилфжбцыугнцюющфтмпчшбтуюкдсюшпмфцдэятылапррфбузишрьсэущукдгнядрутюафьуоукюмпмфчтафыпюяярбюуйуйсрйюжигюкэьтчонкмачсцтхтрсздшридякмпжодуррмуврпцщппфщучяькьюафыдыулфтпнщьтоущфоуцуцюррврысьпыубкжрмфдьсщэашрсряркдэрвщьтгрбкеубюшпхьлтчюхшаюэыьдвьсрбрбалфйдиддупчбкдцыуьстахчррыузгыуийсрьйьтьецрщувщлдпридйрщужфрупэтыфцжиррнщчауспспчуафддулятыцубуысомнфеятыкиокюяэшпфмфчявуцэдьщперьсффбужиэсюкгдяккэдьыпьтуфтпцшкдяргцыуфдечыущююкээшржелацсрруайсфюкездррмуврпцщппфщучячтзюыгыудщлдепюкжсярбеыпбяштхукдьуйденыдкфрюайнфнимэсопозюиядоякжиидцдуюзншципякбулюфьнщрушрядэрнчякыдоуыурушпзрйьцрякрафдэрысцяюкщптауафрцунацябжмфоуцуецафзстьдцюясйрмькбкцюрйысфььклдшчярнрйдзязэээжршрнкчьчтйифжькиднражоккрцуврвюнщьтяышчаьбяыпкрытющжрдцуювкрюзеыпбяфюокгмькрюмфщучявцыуцюмпмфчтыгыубжьуытфьррфьшпвцкрэяжитьфжщпцрцдэыкдйцыучюызнрядькиолфзээзлдфэээжспчфдзеуйьтрццрфдпйруйрвщкездяклфжлбятмнщдьькиддтйцлтхукдлфзээзлднупуствцзнчцчтыпйэырзпжрэяжикфбузеуйысяыздьсоуядбщфтзрщчяыуюхьежмфхайрррцубаусядцяфьякзоодсювуолчьзипфечеипмокуфцпнкиелатнфьчтшлвыщзякыдвтзэюкбявлфдечшндплтцрцубкнщйфоусрмфыдпсечфйерогганщоыгюоксрзсльуюуфбузеуйысяыздцюзргьыкцювутпбцчокдбуцяпфхаздцюхьькьуярофкдбиняуюзнесзяыпдищпщхпсчрнчтиыкуюрэнсьучякщыплтгюзепфйрунлфзедцыуцдоукщфтйгзсецькхпзрцуьсоуядхыкдерфрьрррбцжицярмфьйсппяклдисррмухиуюдресэршчйдлдтеыпбякайраиыкуюрэсйрумуужлтиоррмуйепфцдруякмпзщбязндсордфщсльфжхьмпйсмфцпырсрююызэтиечткфпфчяшлйикамубунчякмсжиытммлтнфкдгдядйдлыьедьчтаыоксродлэээтаекыпэпвышншдомэзиоцудукиьтчькекелдвдытммлтяяцеокчтьюарнфчягмзнмфдуыдюнхдомдриочьпуидияцезилдхщязьсаюкщядцуздвючотпсяфсйящщчшжуждхаррфйдйуюрэязнщбуруыдпсоььуыуагзсчшчсчюжиуюцмзидьыпьтуфтпдресяклдэурпхьчткэээщудумуюелдюпмфрэлдчюшзчюлтыкязкяыпэшжеядидщыгмщпбяюкшнцдясииыкуюрэгюкеязкэьтуюоугфлунчюуотыпоуякэшиамуэюжрэяжидисжуаэпрсзфдущкьтаюзтзеуйчьидчсидкявцлтбуоцыугнуадатпжрцуьрнымпубаьмфьюкщфтйиыкуюрэафчяжимтмпытькчтуммфзсякайуюызкамртдьпдтхитадтхижднкющфтбсдпмфнючоьрякпуякуфхдзрьсойсрякайьсоучпюклдююйибдюиыкуюрэдйысяытдойлозндстебячьдйтоцдофцпнкшэлавщэслюкедргсэрпсюклдююкеуйтоцдомдриоюкесэршчщсяюлтнфхдссэрнчцаффштчгыуаэлавщожующиыкуюрэосэпзойрьскнссфйцезюзнеспсндесшннацапспчлфуюосаьврсраэйикдунйьйэсйчтусякшзбдщуыдысбудпммлтафчйысйдмцфбйдцпйфмэчоьуякчтчйчьякзезюзнщунрхтйиумыкгиаыоуругэжлхажупэыпщудумуюелддыиьвлчопчррнщлдодсюзюжлтюзизюеосрйсэрнчзнесшдсдесцятмчтесщуьсисьуярьпмуяелдтссооыкдомчоыуьцафйрсраьшпямйэюкйибкуйруаытмдубуэтиечтмфчьпугфыурузныфьуоуштафапыущунютмуюосбкюкрйюяуфпфыусюдржлмуужпуьуцямпыкуфкфияцеязякбяцюяукдмрфймэрсядпчюкйийдэйюяуюмфькнкжрмфрюцюдйчьэучсядррнэьтрэбятыкдкньупэшлпрцугпюянфлашдзэээцюхаысэкчатэоыокчатэязрд

**ВТ:**

библейскоепреданиеговоритчтоотсутствиетрудапраздностьбылаусловиемблаженствапервогочеловекадоегопадениялюбовькпраздностиосталасьтажеивпадшемчеловекенопроклятиевстяготеетнадчеловекоминетолькопотомучтомывпотелицадолжныснискиватьхлебсвойнопотомучтопонравственнымсвойствамсвоиммынеможембытьпраздныиспокойнытайныйголосговоритчтомыдолжныбытьвиновнызаточтопраздныежелибымогчеловекнайтисостояниевкоторомонбудучипразднымчувствовалбысебяполезнымиисполняющимсвойдолгонбынашелоднусторонупервобытногоблаженстваитакимсостояниемобязательнойибезупречнойпраздностипользуетсяцелоесословиесословиевоенноевэтойтообязательнойибезупречнойпраздностисостоялаибудетсостоятьглавнаяпривлекательностьвоеннойслужбыниколайростовиспытывалвполнеэтоблаженствопослегодапродолжаяслужитьвпавлоградскомполкувкоторомонужекомандовалэскадрономпринятымотденисоваростовсделалсязагрубелымдобрыммалымкоторогомосковскиезнакомыенашлибынескольконокоторыйбыллюбимиуважаемтоварищамиподчиненнымииначальствомикоторыйбылдоволенсвоейжизньювпоследнеевремявгодуончащевписьмахиздомунаходилсетованияматеринаточтоделарасстраиваютсяхужеихужеичтопорабыемуприехатьдомойобрадоватьиуспокоитьстариковродителейчитаяэтиписьманиколайиспытывалстрахчтохотятвывестиегоизтойсредывкоторойоноградивсебяотвсейжитейскойпутаницыжилтактихоиспокойноончувствовалчтораноилипозднопридетсяопятьвступитьвтотомутжизнисрасстройствамиипоправлениямиделсучетамиуправляющихссорамиинтригамиссвязямисобществомслюбовьюсонииобещаниемейвсэтобылострашнотруднозапутаноионотвечалнаписьмаматерихолоднымиклассическимиписьмаминачинавшимисяикончавшимисяумалчиваяотомкогдаоннамеренприехатьвгодуонполучилписьмародныхвкоторыхизвещалиегоопомолвкенаташисболконскимиотомчтосвадьбабудетчерезгодпотомучтостарыйкнязьнесогласенэтописьмоогорчилооскорбилониколаявопервыхемужалкобылопотерятьиздоманаташукоторуюонлюбилбольшевсехизсемьивовторыхонссвоейгусарскойточкизренияжалелотомчтоегонебылоприэтомпотомучтоонбыпоказалэтомуболконскомучтосовсемнетакаябольшаячестьродствоснимичтоежелионлюбитнаташутоможетобойтисьибезразрешениясумасбродногоотцаминутуонколебалсянепопроситьсяливотпускчтобувидатьнаташуневестойнотутподошлиманеврыпришлисоображенияосонеопутаницеиниколайопятьотложилновеснойтогожегодаонполучилписьмоматериписавшейтайноотграфаиписьмоэтоубедилоегоехатьонаписалачтоежелиниколайнеприедетиневозьметсязаделатовсименьепойдетсмолоткаивсепойдутпомируграфтакслабтаквверилсямитенькеитакдобритаквсеегообманываютчтовсидетхужеихужерадибогаумоляютебяприезжайсейчасжеежелитынехочешьсделатьменяивствоесемействонесчастнымиписалаграфиняписьмоэтоподействовалонаниколаяунегобылтотздравыйсмыслпосредственностикоторыйпоказывалемучтобылодолжнотеперьдолжнобылоехатьеслиневотставкутовотпускпочемунадобылоехатьоннезналновыспавшисьпослеобедаонвелелоседлатьсерогомарсадавнонеезженногоистрашнозлогожеребцаивернувшисьнавзмыленномжеребцедомойобявиллаврушкелакейденисоваосталсяуростоваипришедшимвечеромтоварищамчтоподаетвотпускиедетдомойкакнитрудноистраннобылоемудуматьчтоонуедетинеузнаетизштабачтоемуособенноинтереснобылопроизведенлионбудетвротмистрыилиполучитаннузапоследниеманеврыкакнистраннобылодуматьчтоонтакиуедетнепродавграфуголуховскомутройкусаврасыхкоторыхпольскийграфторговалунегоикоторыхростовнапарибилчтопродастзатысячикакнинепонятноказалосьчтобезнегобудеттотбалкоторыйгусарыдолжныбылидатьпаннепшаздецкойвпикууланамдававшимбалсвоейпаннеборжозовскойонзналчтонадоехатьизэтогоясногохорошегомиракудатотудагдевсбыловздорипутаницачерезнеделювышелотпускгусарытоварищинетолькопополкуноипобригадедалиобедростовустоившийсголовыпорубподпискиигралидвемузыкипелидвахорапесенниковростовплясалтрепакасмайоромбасовымпьяныеофицерыкачалиобнималииуронилиростовасолдатытретьегоэскадронаещеразкачалиегоикричалиурапотомростоваположиливсаниипроводилидопервойстанциидополовиныдорогикакэтовсегдабываетоткременчугадокиевавсемыслиростовабылиещеназадивэскадроненоперевалившисьзаполовинуонуженачалзабыватьтройкусаврасыхсвоеговахмистрадожойвейкуибеспокойноначалспрашиватьсебяотомчтоикаконнайдетвотрадномчемближеонподезжалтемсильнеегораздосильнеекакбудтонравственноечувствобылоподчиненотомужезаконускоростипадениятелвквадратахрасстоянийондумалосвоемдоменапоследнейпередотраднымстанциидалямщикутрирублянаводкуикакмальчикзадыхаясьвбежалнакрыльцодомапослевосторговвстречиипослетогостранногочувстванеудовлетворениявсравнениистемчегоожидаешьвстожекчемужеятакторопилсяниколайсталвживатьсявсвойстарыймирдомаотециматьбылитежеонитольконемногопостарелиновоевнихбилокакоетобеспокойствоииногданесогласиекоторогонебывалопреждеикотороекакскороузналниколайпроисходилоотдурногоположенияделсонебылужедвадцатыйгодонаужеостановиласьхорошетьничегонеобещалабольшетогочтовнейбылоноиэтогобылодостаточноонавсядышаласчастьемилюбовьюстехпоркакприехалниколайивернаянепоколебимаялюбовьэтойдевушкирадостнодействовалананегопетяинаташабольшевсехудивилиниколаяпетябылужебольшойтринадцатилетнийкрасивыйвеселоиумношаловливыймальчикукоторогоужеломалсяголоснанаташуниколайдолгоудивлялсяисмеялсяглядянанеесовсемнетаговорилончтожподурнеланапротивноважностькакаятокнягинясказалонейшопотомдададарадостноговориланаташанаташарассказалаемусвойроманскняземандреемегоприездвотрадноеипоказалаегопоследнееписьмочтожтырадспрашиваланаташаятактеперьспокойнасчастливаоченьрадотвечалниколайонотличныйчеловекчтожтыоченьвлюбленакактебесказатьотвечаланаташаябылавлюбленавборисавучителявденисованоэтосовсемнетомнепокойнотвердоязнаючтолучшеегонебываетлюдейимнетакспокойнохорошотеперьсовсемнетаккакпреждениколайвыразилнаташесвоенеудовольствиеотомчтосвадьбабылаотложенанагоднонаташасожесточениемнапустиласьнабратадоказываяемучтоэтонемоглобытьиначечтодурнобыбыловступитьвсемьюпротивволиотцачтоонасамаэтогохотелатысовсемсовсемнепонимаешьговорилаонаниколайзамолчалисогласилсяснеюбратчастоудивлялсяглядянанеесовсемнебылопохожечтобыонабылавлюбленнаяневеставразлукессвоимженихомонабыларовнаспокойнавеселасовершеннопопрежнемуниколаяэтоудивлялоидажезаставлялонедоверчивосмотретьнасватовствоболконскогоонневерилвточтоеесудьбаужерешенатемболеечтоонневидалснеюкнязяандреяемувсказалосьчточтонибудьнетовэтомпредполагаемомбракезачемотсрочказачемнеобручилисьдумалонразговорившисьразсматерьюосестреонкудивлениюсвоемуиотчастикудовольствиюнашелчтоматьточнотакжевглубинедушииногданедоверчивосмотреланаэтотбраквотпишетговорилаонапоказываясынуписьмокнязяандреястемзатаеннымчувствомнедоброжелательствакотороевсегдаестьуматерипротивбудущегосупружескогосчастиядочерипишетчтонеприедетраньшедекабрякакоежеэтоделоможетзадержатьеговерноболезньздоровьеслабоеоченьтынеговоринаташетынесмотричтоонавеселаэтоужпоследнеедевичьевремядоживаетаязнаючтоснейделаетсявсякийразкакписьмаегополучаемавпрочембогдаствсихорошобудетзаключалаонавсякийразонотличныйчеловекпервоевремясвоегоприезданиколайбылсерьезенидажескученегомучилапредстоящаянеобходимостьвмешатьсявэтиглупыеделахозяйствадлякоторыхматьвызвалаегочтобыскореесвалитьсплечэтуобузунатретийденьсвоегоприездаонсердитонеотвечаянавопроскудаонидетпошелснахмуреннымибровямивофлигелькмитенькеипотребовалунегосчетывсегочтотакоебылиэтисчетывсегониколайзналещеменеечемпришедшийвстрахинедоумениемитенькаразговориучетмитенькипродолжалсянедолгостароставыборныйиземскийдожидавшиесявпереднейфлигелясострахомиудовольствиемслышалисначалакакзагуделизатрещалкакбудтовсвозвышавшийсяголосмолодогографаслышалиругательныеистрашныесловасыпавшиесяоднозадругимразбойникнеблагодарнаятварьизрублюсобакунеспапенькойобворовалитдпотомэтилюдиснеменьшимудовольствиемистрахомвиделикакмолодойграфвеськрасныйсналитойкровьювглазахзашиворотвытащилмитенькуногойиколенкойсбольшойловкостьювудобноевремямеждусвоихсловтолкнулегоподзадизакричалвончтобыдухутвоегомерзавецздесьнебыломитенькастремглавслетелсшестиступенейиубежалвклумбуклумбаэтабылаизвестнаяместностьспасенияпреступниковвотрадномсаммитенькаприезжаяпьяныйизгородапряталсявэтуклумбуимногиежителиотрадногопрятавшиесяотмитенькизналиспасительнуюсилуэтойклумбыженамитенькиисвояченицысиспуганнымилицамивысунулисьвсенииздверейкомнатыгдекипелчистыйсамоваривозвышаласьприказчицкаявысокаяпостельподстеганнымодеяломсшитымизкороткихкусочковмолодойграфзадыхаясьнеобращаянанихвниманиярешительнымишагамипрошелмимонихипошелвдомграфиняузнавшаятотчасчерездевушекотомчтопроизошловофлигелесоднойстороныуспокоиласьвтомотношениичтотеперьсостояниеихдолжнопоправитьсясдругойстороныонабеспокоиласьотомкакперенесетэтоеесынонаподходиланесколькоразнацыпочкахкегодверислушаякаконкурилтрубкузатрубкойаа

**Висновки:**

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