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

ЛАБОРАТОРНА РОБОТА №3

з **дисципліни**

«Криптографія»

на тему:

«Криптоаналіз афінної біграмної підстановки»

Виконали:
студенти 3 курсу ФТІ
групи ФБ-71
Романюк Д.О. Семичастний В.С
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Київ 2019

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 шляхом розв'язання системи.
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.

Критерій відбору ключів:
Проаналізувавши результати 1 лабораторної роботи, ми обрали для трьох найчастіших монограм ліміти частот. Тобто, якщо в розшифрованому тексті за допомогою деякої пари ключів частота якоїсь із літер менша за ліміт частоти цієї літери, то текст не пройшов перевірку і пара ключів не розглядається як шукана.

a - 0.055
e - 0.06
o - 0.085
Частоти набагато менші за статистичні, але вони перевірялися протягом виконання 3 лабораторної роботи.

Результати:
Розшифрування тексту за варіантом 14:
Використавши основи модулярної арифметики, критерій відбору ключів та частотний аналіз, було знайдено таку пару ключів:
a = 10, b = 52.
Серед 5 найчастіших біграм, що зустрілися в запропонованому розшифрованому тексті, були біграми но і то, що входять до п'ятірки найчастіших біграм російської мови.

Найчастіші біграми ШТ і відповідні їм біграми ВТ:
аж цп шы ки тя - ШТ
ст ен но то на - ВТ

Зашифрований текст:

ыенжийбжфзьеьжхфцрйишсвкрьзпцпьжэххжмжьрпймебжцыысзхяирхлыысчсозэехаыьиэтктяцпьжвжажегажхыпжфушыфмуяшззпокскфиэияйкиюозйщхуклихкуэпбжщнйкыюббяшыиотячззеоахзхнллохцппйежньеьедвьыбхйщхцклихкевщьямккезцфтхщыпбнжнпцьжктйащбьвкэлфчьошжхлфычзчсскфизхяйийкищибйтхкиыжнеихйххиегажййяйозшымжсщрщарйислдмяйпмозэеткщььйлытфцжсктауумйкищэийцпчлмжюэийбжцпмжаювкщечсчеюифптячпыобжйэиййцпчлййййпжфурмфмдвчпчфохшсэьвачпфтфпуушыжирмсяьпссчыхяхзгыэрчеызззпуеыыжьвачпагажньеьдвыыеспжфузхфмдвфэгюшкгйэхбжвжмвфпхыдэгюеыюлпжфурмфмдвкрчпийпзшйжмжкэчзпшзсыщйеыьпшзьермэгажшэгупжаияйкифяхзгышаюпущуьцумйрмржывкинмбыюбдмыннжымййнжажпмьщбьвкэлфчхйбщыаызцибжшщеьесчпрмюцнжмжжмфзннезцихржфеыжбьхябжтхахэежмфзийсиыпхсфпхсхзтяфтеьидййпжьжфйкиащбьвкфйкишсщщьхбэфтмйййбямщгищрчефйюйзктфчеаьиоеыиотячзхюваврменщршзчкшыпйевщьдимжямшыеыемщхлыщйчсщечжххаьыпризхяжнихибьчеажжяткхзуеыкхйбжфзннзпрэдэежьжйиыажьчырйыкщьдмьеесщййсрмхкажегщефйффтхщычщбьвкэлфчцтбжслхихюипфтийсиажихливжрьгюхсзхпжтаяжнидвьлсажьчыхсозчячеюибйкиэеьжьожйфйяфтхщычщбьвкэлфчцтямжхмиуахзхнуйхжфщыеыкхйзхяйийкиьсевщьеыуюесьпчзфпфэлжяйипьобьщжрьгюткеыцтййтаяжнивжфмчжьжтаеййхслдвьлмйтхаинжажпмхаызфкрщкыхсхжцпылкичыьевжаьыьжжеьхсмжхатфзпщпьжеьидвацюмотфчеэйярцьихнрпйлрхзнгчзхффибжшщоххэдэежьжйихидмьлпфтятктфтяшотяжжпгжкцпьжххшехачфцьгюпжяйййхатфзпысрйаэтфкххыбжшщохшеьжщпупюеягчпбжнжвытфтфжхпхьжучьорймпиохыфслпмжфщыеыкткезфзхяпбжияанябйыкхжчйартхюичжщвфэхзчпщпюеягбжыешсчсшыюлвжнжчжюидмьлфеажчзчетящьяхкищртявжуэткмжвсченжыенжежпжэхцэслджмжнжчжюидмьлпкяотячзхыжршыуищеажывнжбйзхржежжфтярмцювкхяшыюлеьидчышыжрлжвидвщрчеызезчеупюеягбьшшшыажьртхюичжщвйхпжуфшжнжчжюидмьлурчеаьфтихзхохажешщьйкщеажчзкцюилквфтяжжнжчжюидмьлужцпезсыуйфэхзчпзпюеягжхчотячзчетжнеесййныезихлибжфпцэгуумяфтяхыбьчызумйиаызйхкиэхдвньхсыптффэгуумяфтядзвкмжкржхщзббжигрщеезажцруужьиоажхыьщлжяхюоажхыщжтотячсчеюиюййицплжчэпхрьцэхювктятктщпдэюйзкуймйчжбьхяцпвкфкьйьеырпймщфмчжажлэчпцьхскжлсшыцйыехффияйшебжхжпычеюищемзхымжцпхюеыэпхймйтхаиевщьсфтхщычщбьвкэлфччсихаяьтмйрвйхкиэхшеьыцжпгжкцпьжххьгажйхслюишйежкизхшхдыщртяшиаххимйтххыфщыеыкткезфпуйежйхслюиырлжщеяжфляыцювкщечсцжыяшзйгажхычыышщрэлтпйхмйчжчыцюзеьхщзббэйежлкффзпуеэетямждеажлжрмдзвкмжкржхщзббжиякюеьхщзьзмйтхыеесхсрщкыхсскьпщрфэгюшкллевщьйыщжтотячсчедвкртхсиххдвпжуфцибьхябьчычзпсытккщйжхрждмуитхаиньщрчеяыяогцвинжщыйгажевщьййхждзйнезьлсямщеждеажлжрмевщьаьхаткезбьщебщазшыюлйяшзкжскстауумйкиыыйгажкржхщзббжиякюеьхщзьзййтаяжнивжцптрийаяьщаззпщпояхзежюйощненжежхжчйьхшрчпхсйыхкуювжгычедвфмцплжежщебжцыышыюлкржхщзббживыхфткцьчзфпьцажхжчйоншымжййьжнсуумжхыбьхятхахуяэлпжцпхушыюлипфткйхибтягуйзьеткнжцплжгенжяфжащькишрлжкхецплйяйывкиожямэиньысуэтффияйрвыткткйипшжюйжхзифкийохащбьвкэлфчхфчеалтмххxищвцпдэыбфзуумжцпчббышыьехжыеслюишюжрийейкибицпийржххкигьгюийьйкибиарфпцрпймпщьзьлщпхзрэтфткцьчзшсжявязпдэщемйтхдпщрпйкычияйшпфтбьдэюирйуэфтжйяэчеюинжажжхчашяезгйгщьжнсуумжцпсыщрчеийреыкшымжчюэпуешювяшзфибжажгщхыййэбоифйежщпхзрэчеьхжхшеырйиыкцьщпуеырщьхяржхщзббжиегажхыйхслыяшзхскржхщзббжиауеьхжхшеырйиыкцьщпуеырщьхяеьидхсфпцжнесиьхьпипхюеыэпюлчйщвэхбжфйныысфяэляжулчыдиозэехаэеэйфыщпшзсыысфкржывюжюфцьтяшыйнхищвныдэхсщййыныдэхсщйбжхрэнчзшруюзхнжаидвьлшьвяннмжбьфкьпцпьжххищыткгрйиыовкьйежржахохрхвжежржывюжежщзвяшзфжюфцьтяшыйнхищвныдэхсщййыныдэхсщйбжхрэнчзшруюзхнжаидвьлшьвяннмжбьфкьпцпьжххищыткгрйиыовкьйежржахохрхвжежржывюжежщзвяшзф

швфжащькициуэнншыюлбжчпмжьйкинфтхщыфтфзвачеюиевщьзпфтшэчпцьфтхыбьхюзхшечкткийзлбьхйэхщзуулпуухаызщпдэуиывpмфпцрпйкышстфьж
кящьяхдвьлчпкияжжлдвжйымхякийймйхияйьлнмвинышрпйжхбьшотячзщпдэбйуювaщгшымжхюеыэпхсцурщчйрйжхаитахяесхювкаьдэесфаезесчыхявклл
шсжкийяйкицрхскидвьлихлиьрьпщьсщзфхкяйцпхыткфтвиныцэчпцьпбзхмйьзьлбжчйцпшрпйлжйучзыеажоущрийгычтвиныч6ажывнжцямщежгжсеьхмжш
эчиппийюыгюзхрйкивсзехыцпххевщьхжнывкезфпцжлычихрхзслшптффэчпцьуйбьхяяищмххчжихаяхсйсзехыжаюптжрьгюйжбыжхыеыкшымжаухюкицип
ешсфяталжмйэйфйдеткщцьйлыхычияйуктйнйлкмопжрьхыжхшищиэбмкцэфсщьюихылпэнезтйхлэйегажйхажхыщебжцыьзпьжфуйзхныйгшыхйщебьвкфйк
ищьтяйгшзткэгьенжежцияйуямщгихяталжмйэйхиэбржявйахигышсииьжхжнйлычеюиейпьчедвчйфыфтежкхевщьийыишешйщхдвзхйхлкюйэйзакьертяцтф
шыгювяхызхяйийххшеыжнйщхдвыеьеьжцияйрвщихитычщпжцптkщьщпуечкажегажсяшзеыфипптфщгажчсбьхяяирхмжфкихнжврхзуушыцизхяжнибеэпщ
рщьупчпзхлжнэчпцььтцкщьшышсжатфхсцэчпцььтхыцпийаишеыжпзвфтяьпшзуеыктзпофтхщычщбьвкэлфчцтшгщпвкыияктйийхэйчсхзтятфтфжхпхбжфп
фацюйсцпьжбыхкшфтяфтозэехачяэлййежозщэийцпчлнемйтхшщщпкрлибьтяхзяхчяшзцжсктауумйкиырийреьхщзэпсыхкуювжгыысхыжхxрцьчячзьлбжцпл
жбэфтьжыеыочсшыюльахзхньокяеыцтыэхзржывкизибьюбажцяэлбьхйкяважьчывкцюмйбьффчптжчзыеаьэгчыщранмжажиуьеыкшырмчэчпцьщйхыныезйй
бжмьвкэпьлевщьйыфияйлычпдэхйийхигиуюмжпзвфтяжьцпчйлыщйхжрьгюесциюзхахсхжывпияйлычпдэхйнжажпмчэдэхыбжкиэхуажьчывяхзгышаызшрт
ячтцпьжххдвзхеьиддитаэхнщдвхфыбгыллчйфыжрфэфтмжхаюеаьуйвщэйьйцпшихкчйненжбэхзэекйщщхячышыхйпжлжгижхпжцпмжмйдеыктkезчыжрпйж
хчсшычлшэчпцьяохыйййфмххфйейфмхитямжвиьжяифыцйпьжфтфхыжьтячйкящрийреьхщзьзьлпзвфтяшыцпыщфччсщплжахэйывмжпзвфтяжьрмяюземйтх
лыщйшсжатхежмйьыюлчйкяхаызфкцпийсинжажпмыочпщибьфктячзфкфснчшыхйевщьеыткдзжачыхяннхйежямтмхххижхпжцпмжэгжкцпьжьжоыхсяйцпт
шсзуцэшртямжуихишсмофйсехзритажхорьпжхшрвктхшрлжуихибжкххзшыюлюгьедвхфсхифшзжрьпжхшрвктхчюзхмзнашифатхежкхкычеюийхсяшзеырм
чиюатхежмйьыюльжкяшидылпсызеьждерйяыткьтбьфяшзэшщьйкфкпьжфхсяйцпцйежыеаьыпчзхушыжирмсфмщоыысфяьпссфатхежкхрлхфуюдикавкфйки
щжбпшушзяожхржыкаьыппйаияйрвхйежыеаьэгезскячшыкиоеньеажвжньзушырмяяьпссцэчпцьяохыбжаичжцпьсеьиджжсщохуфжхвжэйшьшзффциьжыеы
очсшыюлярпйзкфяшзскфиаидзгюесшрцжоыхскртхнщьжкяшиахюнхйьлфкуюлкффнщдмьщбйихяйлыщйкяеыюлржывкимннжуатфвяшзшынжажпмхяхзгы
шаызфаюпокуэцьхсььшсшышжюэпмдмчйкяшрпйзкфяшзчпрйдмкржхщзббжияжлхоччыуэьожхржьхащяйрвьйлыяобьчпфкбьцуййежщеымшхфюзпчпллжах
эйывpмхатхежкхийкичящрлпишщтньедвьыыечыьоиххпеыиоевщьажывнжййныезажежфпчпесбяцйгщбжоычечзьофйсехзрицплжчзшрйимйчрьпжхшрвктх
фмчжажзфткуйтйчжюлксжьихьрьплжцяшыхгажбьфяшззуьеаьфишечявкмжржахохаигщвиихаитйтхэйаинжажпмялшихищвмышсехфптяхкэпояьеэпяогщви
нжяцажежтйтхфмхицкшзыгдтьйвыгюцьшыцихыйййныезфптkфзхяцпшиьптфщгажюйийцпезшруйежбьцэгюкрчеыззптьхаэпкижушыжинееьжярмаимйдваиз
хлхоччыоцюирхжмщьхаэпкинмэйгпмщоычтящсьвачпйыьехизхскуйгрхзткчыщжлыцюзхьгажскячшыкийкцпийюиюнцтхфченьеажвжележгхцсзуцэткскфи
аибжржжхаиыгажхжрьеырмчэйийгщнгшыцэщечефйййхаифмхичпкхххшсщйгщхювахзхнхймйрвгифмхичпощыхшсэьтящпшзьсшжлыцюзхьгажихяйлыщйбж
азеызюкхкичкуюлкффезщеуеьжчсшьващгчсцижкшзыгчзфажьжинщньедвьыйсшыхншынщтпхзрэхывайсвфщжлыцюзхьгажьхюфмйкржхщзббжидщихтм
ххфйгщбжмыффшызщяйрвьйкищруйежьжфйталжихзхтянщаьпоаызеыжрхзткчыкрйилхщзшываважьжилыллбжшилычедвшрчпхскрпйзаызьжчоычшыскфи
врлпэньеыкхйврфияйрвьсфкбжцыхкуюььзпчзьлопхсмдчзеыаьцрыгьенжгщзхцплжшыюбшэчпцьхсхыямыоезхююйэйзакьахшрщеезьжцпцьбйлыщйяищвэх
скуйгщзхцпвккиощрьзпиэдэхызхтмххукшзцэтфхсзеэйжхихмзхфнжихмсезчщуихиьызумжфптаюемйтхдвьхмсмжежпжрьвяйсезевщьцэдээхчжжмтаипхсйх
ржюигецх

Розшифрований текст:

вскорепослесвоегоприемавбратствомасоновпьерсполнымнаписаннымимдлясебяруководствомотомчтоондолженбылделатьвсвоихимениях уехалвкиевскую
губерниюгденаходиласьбольшаячастьегокрестьянприехаввкиевпьервызвалвглавнуюконторувсехуправляющихиобяснилимсвоинамеренияижеланияонсказ
алимчтонемедленнобудутпринятымерыдлясовершенногоосвобождениякрестьяноткрепостнойзависимостичтодотехпоркрестьяненедолжныбытьотягчаемы
работойчтоженщинысдетьминедолжныпосылатьсянаработычтокрестьянамдолжнабытьоказываемапомощьчтонаказаниядолжныбытьупотребляемыувещат
ельныеанетелесныечтовкаждомимениидолжныбытьучрежденыбольницыприютыишколынекоторыеуправляющиетутбылииполуграмотныеэкономыслуша
лииспуганнопредполагаясмыслречивтомчтомолодойграфнедоволенихуправлениемиутайкойденегдругиепослепервогостраханаходилизабавнымшепелявен
ьепьераиновыенеслыханныеимисловатретьинаходилипростоудовольствиепослушатькакговоритбаринчетвертыесамыеумныевтомчислеиглавноуправляющ
ийпонялиизэтойречитокакимобразомнадообходитьсясбариномдлядостижениясвоихцелейглавноуправляющийвыразилбольшоесочувствиенамерениямпье
ранозаметилчтокромеэтихпреобразованийнеобходимобыловообщезанятьсяделамикоторыебыливдурномсостояниинесмотрянаогромноебогатствографабез
ухогостехпоркакпьерполучилегоиполучалкакговорилитысячгодовогодоходаончувствовалсебягораздоменеебогатымчемкогдаонполучалсвоитьтысячотпок
ойногографавобщихчертахонсмутночувствовалследующийбюджетвсоветплатилосьоколотитысячповсемимениямоколотитысячстоилосодержаниеподмоск
овноймосковскогодомаикняжоноколотитысячвыходилонапенсиистолькоженабогоугодныезаведенияграфиненапрожитьепосылалосьтысячпроцентовплати
лосьзадолгиоколотитысячпостройканачатойцерквистоилаэтидвагодаоколотитысячостальноеоколотатысячрасходилосьонсамнезналкакипочтикаждыйгодо
нпринужденбылзаниматькрометогокаждыйгодглавноуправляющийписалтоопожарахтоонеурожаяхтоонеобходимостиперестроекфабрикизаводовитакперв
оеделопредставившеесяпьерубылотоккоторомуонменеевсегоимелспособностиисклонностизанятиеделамипьерсглавноуправляющимкаждыйденьзанималс
яноончувствовалчтозанятияегонинашагнеподвигалиделаончувствовалчтоегозанятияпроисходятнезависимоотделачтоонинецепляютзаделоинезаставляюте
годвигатьсясоднойстороныглавноуправляющийвыставлялделавсамомдурномсветепоказываяпьерунеобходимостьуплачиватьдолгииpредприниматьновые
работысиламикрепостныхмужиковначтопьернесоглашалсясдругойстороныпьертребовалприступлениякделуосвобождениянačтоуправляющийвыставлялн
еобходимостьпреждеуплатитьдолгопекунскогосоветаипотомуневозможностьбыстрогоисполненияуправляющийнеговорилчтоэтосовершенноневозможноо
нпредлагалдлядостиженияэтойцелипродажулесовкостромскойгубернийпродажуземельнизовыхикрымскогоименьяновсеэтиоперациивречахуправляющего
связывалисьстакоюсложностьюпроцессовснятиязапрещенийистребованийразрешенийитпчтопьертерялсяитолькоговорилемудадатакисделайтепвернеимел
тойпрактическойцепкостикотораябыдалаемувозможностьнепосредственновзятьсязаделоипотомуоннелюбилегоитолькостаралсяпритворитьсяпередуправл
яющимчтоонзанятделомуправляющийжестаралсяпритворитьсяпередграфомчтоонсчитаетэтизанятиявесьмаполезнымидляхозяинаидлясебястеснительным
ивбольшомгороденашлисьзнакомыенезнакомыепоспешилипознакомитьсяирадушноприветствоваливновьприехавшегобогачасамогобольшоговладельцагу
бернииискушенияпоотношениюглавнойслабостипьератойвкоторойонпризналсявовремяприемавложутожебылитаксильнычтопьернемогвоздержатьсяотни
хопятьцелыеднинеделимесяцыжизнипьерапроходилитакжеозабоченноизанятомеждувечерамиобедамизавтракамибаламинедаваяемувремениопомнитьсяка
кивпетербургевместоновойжизникоторуюонадеялсяповестипьеронжилвстоюжепрежнейжизньютольковдругойобстановкеизтрехназначениймасонствапьерс
ознавалчтооннеисполнялтогокотороепредписывалокаждомумасонубытьобразцомнравственнойжизнииизсемидобродетелейсовершенноонеимелвсебедвух
обронравияилюбвиксмертионутешалсебятемчтозатоонисполнялдругоеназначениеисправлениеродачеловеческогоиимелдругиедобродетелилюбовькближн
емуивособенностищедростьвеснойгодапьеррешилсяехатьназадвпетербургподорогеназадоннамеревалсяобехатьвсесвоиименьяиличноудостоверитьсявтом
чтосделаноизтогочтоимпредписаноивкакомположенииинаходитсятеперьтотнародкоторыйвверенемубогомикоторыйонстремилсяоблагодетельствоватьглав
ноуправляющийсчитавшийвсезатеимолодогографапочтибезумствомневыгодойдлясебядлянегодлякрестьянсделалуступкипродолжаяделоосвобождениявпре
дставлятьневозможнымонраспорядилсяпостройкойвовсехименияхбольшихзданийшколбольницприютовдляприездабаринавездеприготовилвстречинепы
шноторжественныекоторыеонзналнепонравятсяпьеруноименнотакиерелигиознoблагодарственныесобразамиихлебомсольюименнотакиекоторыекаконпон
ималбаринадолжныбылиподействоватьнаграфаиобманутьегоюжнаявеснапокойноебыстроепутешествиеввенскойколяскеиуединениедорогирадостнодейст
вовалинапьераименьявкоторыхоннебывалещебылиодноживописнеедругогонародвездепредставлялсяблагоденствующимитрогательноблагодарнымзасдела
нныеемублагодеяниявездебыливстречикоторыехотяиприводиливсмущениепьеранoвглубинедушиеговызывалирадостноечувствоодномместемужикиподн
осилиемухлебсольиобразпетраипавлаипросилипозволениявчестьегоангелапетраипавлавзнаклюбвиичблагодарностизасделанныеимблагодеяниявоздвигнуть
насвойсчетновыйпpиделвцерквивдругомместееговстретилиженщинысгруднымидетьмиблагодаряегозаизбавлениеоттяжелыхработвтретьемименьиеговстр
ечалсвященникскрестомокруженныйдетьмикоторыхонпомилостямграфаобучалграмотеирелигииивовсехимениях пьервиделсвоимиглазамипоодномупланув
оздвигавшиесяивоздвигнутыеужекаменныезданиябольницшколбогаделенкоторыедолжныбылибытьвскоромвремениоткрытывездепьервиделотчетыуправ
ляющихобарщинскихработахуменьшенныхпротивпрежнегоислышалзатотрогательныеблагодарениядепутацийкрестьянвсинихкафтанахпьертольконезналт
огочтотамгдеемуподносилихлебсольистроилипpиделпетраипавлабылоторговоеселоиярмаркавпетровденьчтопpиделужестроилсядавнобогачамимужиками
селатемикоторыеявилиськнемуачтодевятьдесятыхмужиковэтогоселабыливвеличайшемразорениионнезналчтовследствиетогочтопересталипоегоприказупо
сылатьребятницженщинсгруднымидетьминабарщинуэтисамыеребятницытемтруднейшуюработунеслинасвоейполовинеоннезналчтосвященниквстретивш
ийегоскрестомотягощалмужиковсвоимипоборамиичтособранныекнемуученикисослезамибылиотдаваемыемуизабольшиеденьгибылиоткупаемыродителям
ионнезналчтокаменныепопланузданиявоздвигалисьсвоимирабочимиииувеличилибарщинукрестьянуменьшеннуютольконабумагеоннезналчтотамгдеуправл
яющийуказывалемупокнигенауменьшениепоеговолеоброканаоднутретьбыланаполовинуприбавленабарщиннаяповинностьипотомупьербылвосхищенсвои
мпутешествиемпоименьямивполневозвратилсяктомуфилантропическомунастроениювкоторомонвыехализпетербургаиписалвосторженныеписьмасвоемун
аставникубратукаконназывалвеликогомастеракаклегкокакмалоусилиянужночтобысделатьтакмногодобрадумалпьерикакмаломыобэтомзаботимсяа

Код:

```
from collections import Counter

with open('textoviki/aych.txt', 'r', encoding = 'utf-8') as
f:
    text = f.read().replace('\n', '')

text = [item.replace("ъ", "ь") for item in text]
text = [item.replace("ё", "е") for item in text]

alf = ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н',
'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ь', 'ы', 'э', 'ю',
'я']
array1 = ['ст', 'ен', 'но', 'то', 'на']
qq = 31

def max_bigrams(text):
    array = []
    p = ''
    bigrams = dict()
    for i in text:
        if i in [' ', ',', '.', '!', '?', '-']:
            continue
        if len(p) < 2:
            p += i
        else:
            if bigrams.get(p):
                bigrams[p] += 1
            else:
                bigrams[p] = 1
            p = i
    array = sorted(bigrams.items(), key=lambda x: x[1],
reverse=True)[:6]
    print(array)
    return array


def killa(text, qq, r, t, r2, t2, alf):
    plaintext = ''
    m2 = 961
    p = ''

    x1 = (alf.index(r[0])) * qq + (alf.index(r[1]))

    x2 = (alf.index(r2[0])) * qq + (alf.index(r2[1]))

    # max_key = max(m.items(),
key=operator.itemgetter(1))[0]
    y1 = (alf.index(t[0])) * qq + (alf.index(t[1]))

    y2 = (alf.index(t2[0])) * qq + (alf.index(t2[1]))

    yy = (y1 - y2)
    xx = (x1 - x2)
    MMI = lambda A, n, s=1, t=0, N=0: (n < 2 and t % N
or MMI(n, A % n, t, s - A // n * t, N or n), -1)[n < 1]
    o = MMI(xx, 961)
    xx1 = abs(x1)
    m21 = abs(m2)
    xx = abs(xx)
    m2 = abs(m2)
    while xx1 != 0 and m21 != 0:
        if xx1 > m21:
            xx1 %= m21
        else:
            m21 %= xx1
        gcd = xx1 + m21
    if gcd == 1:
        a = (o * yy) % 961
        b = (y1 - a * x1) % 961
        a1 = MMI(a, 961)
        print('Key is:  a = ', a, '  b = ', b)
        for i in text:
            if i in [' ', ',', '.', '!', '?']:
                continue
            if len(p) < 2:
                p += i
                if len(p) == 2:
                    yo = (alf.index(p[0])) * qq +
(alf.index(p[1]))
                    lll = (a1 * (yo - b)) % 961
                    for i in range(len(alf)):
                        for j in range(len(alf)):
                            form = (i * 31 + j) % 961
                            if form == lll:
                                iu = alf[i] + alf[j]
                                plaintext += iu
            elif len(p) == 2:
                p = i
        proverka(plaintext)
        plaintext = ''
    elif yy % gcd != 0:
        print('/////', '\n')
    elif gcd > 1 and yy % gcd == 0:
        print(gcd)
        x0 = (yy * o) % 961
        for i in range(1, gcd - 1):
            b1 = (y1 - ((x0 + gcd * 31) * x1)) % 961
            a1 = MMI(x0, 961)
            print('Key is:  a = ', x0, '  b = ', b1)
            for i in text:
                if i in [' ', ',', '.', '!', '?']:
                    continue
                if len(p) < 2:
                    p += i
                    if len(p) == 2:
                        yo = (alf.index(p[0])) * qq +
(alf.index(p[1]))
                        lll = (a1 * (yo - b1)) % 961
                        for i in range(len(alf)):
                            for j in range(len(alf)):
                                form = (i * 31 + j) % 961
                                if form == lll:
                                    iu = alf[i] + alf[j]
                                    plaintext += iu
                elif len(p) == 2:
                    p = i
            proverka(plaintext)
            plaintext = ''


def proverka(text):
    l = len(text)
    count = Counter(text)
    h = count['а'] / l
```

```
    h1 = count['e'] / l
    h2 = count['o'] / l

    if 0.067 < h < 0.08 and 0.084 < h1 < 0.089 and 0.10
< h2 < 0.12:
        print(text)
    else:
        print('Text with shym', '\n')
```

```
vuzov = max_bigrams(text)

for i in range(len(vuzov) - 1):
    for r in range(len(array1) - 1):
        print('Bigrams: ',array1[r], vuzov[i][0], array1[r +
1], vuzov[i + 1][0])
        killa(text, qq, array1[r], vuzov[i][0], array1[r + 1],
vuzov[i + 1][0], alf)

max_bigrams(text)
```

Висновок:

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