**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
Варіант 4

Виконали:

Студенти ФБ-05

Береза О. А.

Ковбель Д. О.

Київ 2022

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

**Постановка задачі:** 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.
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.
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.

## Хід роботи

Для гарного початку треба гарниий код, тому ми написали декілька математичних функцій: НСД двох чисел, розширений алгоритм Евкліда, знаходження оберненого за модулем числа та розв'язання лінійного рівняння

Виведення 5 найчастіших біграм ШТ:

```
['еш', 'еы', 'ск', 'шя', 'до']
Text after decifre method:
```

**Отриманий ключ:** (390, 10)

## Зашифрований текст

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипму
гфбзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэ
йкчозычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывдьмиыыяшцрбгянямз
юдшскдмыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывч
фвэрфешмяояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбш
ящксавотзябйкжзшцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквк
шятоьэйштибяшкочщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдх
пезхлсопжипеызохлншплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглт
доккжшскзыядншууезжурфешщпнзшятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусж
ощккшйжррэсзешьоктдоскыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозн
оюуйэвзхягжжзщрфяоэщпсчкжйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочые
зыяюйеытяьочмскмзшядяешмуяхщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощя
анбччйтжмкжучбуфпошфбждоцпюдлвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфм
овоцяанфшляйбмуьосклкюнсккжеьзоешшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбля
ьхзсккцезшяййсщзоюдьмйшнхдоаоешезвжбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссо
жзешопхпимсжсказкзшяшйнэюшшомглтдонзпксзеыэжюпщжхявушйгожурфлцгцншвдрзд
вщоцыыиеыхзнфылтфаляяыжфзйквбждэечяыжхыхоцыыиеыыяпомггднотлккжжипеызохл
щпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтцзохлмофхэыеынеткзеадьгпуротынщйайкб
азущпязхлдырйпоазсяслщяджипщплзджипюшлцлыбжхяскыосяэищеештцедууьмншйкрзш
яцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязхпрэчфлоешщпоцбжщлтзноьобцэжхя
кзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфоефзббжнзтыссжяилнахпезфщпмшя
вжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмоыптцыцшййычмыйзхйшмшжш
алтыбжхябжюакцопиыщчыдншуусйжуопчфюшжзйкмяефопифбкюнзовбюпдокзшярйдуюп
лвляешууяхщжпоной кыпюшщчмысклзыцбчмялзоцнрряешиыфсхядаыосябжьоиогфеыхзн
шзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажуюшимйшлыпутцурряеш
бзкцколппотзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосшщоччдыозлжцшшй
фшщоцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяямзозхьпешьоаоеш
ывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюптжждшсэыпзь
цяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаекшйбчншузяб
ряешйкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьосктлсзешь
оекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножяяоьоэмкзшяпдмыэзгпйшууе
шоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзцжжу
щпрфуяшфсчдвбждчвхеыщчфочытцмиажщквканфшуufиеыхзаоешезвжпонодаыпиыщомз
мятыямйшалтыеызоешыедвайнинзшязпкцрфешмяеыцпяовкрфекуяжубждоджгллкпыбжан
цйсщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшощ
жшшйкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфб
ждоцпюдлвюпюпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмн
щеычяражуййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмзюдайюдьм
иыыяхфщжцфвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшя
рбптхямзюдечрэйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщк
поноюааощяекшйбчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпокбчфн
одоздопзузхщжпоьфйказтзрэыосяфощждчвхеыхзжусжфрйктзшясжеьзоешрйэжпзжжбяаое

шывбзлжцшшйфшрэщжсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешед
вдвлгфезшйдбряилгфеыхзсккчвкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызо
чбюпэзбпифрйбжхяузыпуяхыщчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюнешибряшяякжш
бчфуэжмзчшвдщкпонйсщжшвкьоцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдоноpзлзд
жипщчьоцыыиеыыявлаомяркгяшптцпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчко
жцчибзлжозномясктзлзмкжшбчшящкбяйбзбяшждцыцшдзщжэзччамекуяанюзскжуэыощлз
шящжбждояоратлынсаскрэууншмяскжупмскжшбчцдвдвжыглцечмяскскщкбаекжшбчфшуу
эжтлмдэйсщжшмощквканбчтзябйкжзшцопсйзоужертцлвяхщжбямэсоеецызбйкмяюнзоекш
вуяджпоьфйказсшлячовунщеырэтцюзпохпеызомоешдбждсожзбибзлжхыщжыйрйшзяошйу
фаляятфсчподояоносшншмоешдбждтззпсчжшбчншщзнэйсешьовбптдохлжурфбжффюшлц
лыксфохявжядтлоцлылвбжзбмушямзешекощеычяратзилгфбзлжзпвкылоцдуюпиыыяйкныл
яыфчбюпповбнзцжшзяойййппифрйщкжэппншйкрзщыайхпжшжшвдщкхйппифрйуяпндощк
порфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщоефтцрзюэдцсавксшншмоешдбждн
шайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюакыбзйхдодвууэжкцмэсчжшсопж
ипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфуншяхщжбялчуцеыйсжулямрчф
юшпфмяяявлвжипюпэышбмунрчфюшьосокыиыхзхпезпыщжмосоьыбжхядамофыюшотдов
кккшяабйчуцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяилщкцжжзщрэысяныбл
оцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкгфсймовккцивыйгш
ьльфжшншмолдопсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшскюклфоцьидяхф
щжщлщяджипбжюпмуяззощуиврймзвожзпофотывдохлцюпядайхпимиыраыжнэюшсйокбя
жярзьазонырйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюнзоносочзсы
яхщжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшмущжзовказ
хяанаоешезвжбякбмурфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщкжэгщлц
ечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшкопншфузхпмдьюшш
ящкскткллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбкуя
яоекзожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэ
пбжжущчхябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракбяо
щзшжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфлцабгяы
овояяфяьшмущжвзлжыцмимшшйгшезновжьошйэзэфщзрзмкуягшзбезносожзбиеыыядвзбр
яжзлжипюпоцчбптдохлибвоанаопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяц
яюакбмумяуысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгяыкаяшябялбгцабхямз
юдйсжущжеляыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаое
шезвжпонопмйкйвюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвнш
юпзоешедншщзнэйсешылбэяоыкжшбччзкзтырйскпонзшясшмышйсщжшзпсчанбчдайкрзш
яшйьомршьеыщчуфтцчыщокыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшя
анбчжучмкзшяшйрлщяегдяуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщ
чаоешезвжпоноэбкзешдбшярллзджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурф
лцтжбжюууфиыщчскподояоеыщжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюд
ншуусйшфкзныбжхяншзогяуяннетюянзашцдияблязнырэтцлыайдбкзешдбшянфсчтзномоф
шсжцкгяпзюнамзпеяпыэжйэзпэыгдншуущешфалноыжгллкеыщжуясащуивхзак

## Розшифрований текст

еслиправдачтодостоевскийвсибиринебылподверженприпадкамтоэтолишьподтверждаетточтоегоприпадкибылиегокаройонболеевнихненуждалсякогдабылкараеминымобразомнодокатьэтоневозможноскорееэтойнеобходимостьювнаказаниидляпсихическойэкономиидостоевскогообясняетсяточтоонпрошелнесломленнымчерезэтигодыбедствийиунижений осуждениедостоевскоговкачествеполитическогопреступникабылонесправедливымиондолженбылэтознатьноонпринялэтонезаслуженноенаказаниеотбатюшкицарякакзаменунаказанияза служенногоимзасвойгрехпоотношениюксвоемусобственномуотцувместосамонаказанияондалсебянаказатьзаместителюотцаэтодаетнамнекотороепредставлениеопсихологическомоправданиинаказанийприсуждаемыхобществомэтонасамомделетакмногиеизпреступниковжаждутнаказанияеготребуетихсверхяизбавляясебятакимобразомотсамонаказанияготктозна етсложноеиизменчивоезначениеистерическихсимптомовпойметчтомыздесьнепытаемсядобитьсясмыслаприпадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитьчтоихпервоначальнаясущностьосталасьнеизменнойнесморянавсепоследующиенаслоенияможносказатьчтодостоевскийтакникогдаинеосвободилсяотугрызенийсовестивсвязиснамерениемубитьотцаэтолежащеенасовестибремяопределилотакжеегоотношениекдвумдругимсферампокоющимсянаотношениикотцукгосударственномуавторитетуикверевбогавпервойоппришелкполномуподчинениюбатюшкецарюоднаждыразыгравшемуснимкомедиюубийствавдействительностинаходившуюстолькоразотражениевегоприпадкахздесьверхвзялопокаяниебольшесвободыоставалосьунеговобластирелигиознойпонедопускающимсомненийсведениямондопоследнейминутысвоейжизнивсеколебалсямеждуверойибезбожиемеговысокийумнепозволялемунезамечатьтетрудностиосмысливаниякоторымприводитверавиндивидуальномповторениимировогоисторическогоразвитияоннадеялсявидеалехристанайтивыходиосвобождениеотгреховииспользоватьсвоисобственныестраданиячтобыпритязатьнарольхристаеслионвконечномсчетенепришелксвободеисталреакционеромтоэтообясняетсятемчтообщечеловеческаясыновняявинанакоторойстроитсярелигиозноечувстводостиглаунегосверхиндивидуальнойсилыинемоглабытьпреодоленадажеговысокойинтеллектуальностьюздесьнаскалосьбыможноупрекнутьвтомчтомыотказываемсяотбеспристрастностипсихоанализаиподвергаемдостоевскогооценкеимеющейправонасуществованиелишьспристрастнойточкизренияопределенногомировоззренияконсерваторсталбынаточкузренияевеликогоинквизитораиоценивалбыдостоевскогоиначеупрекправедливдляегосмягченияможнолишьсказатьчторешениедостоевскоговызваноочевиднозатрудненностьюегомышлениявследствиеневрозаедвалипростойслучайностьюможнообяснитьчтотришедеврамировойлитературывсехвременактуютоднуитужетемутемуотцеубийствацарьэдипсофоклагамлетшекспираибратьякарамазовыдостоевскогововсехтрехраскрываетсяимотивдеяниясексуальноесоперничествоиззажещиныпрямеевсегоконечноэтопредставленовдрамеоснованнойнагреческомсказанииздесьдеяниесовершаетсяещесамимгероемнобезсмягченияизавуалированияпоэтическаяобработканевозможнаоткровенноепризнаниевнамеренииубитьотцакакогомыдобиваемсяприпсихоанализекажетсянепереносимымбезаналитическойподготовкивгреческойдраменеобходимоесмягчениеприсохраненииисущностимастерскидостигаетсятемчтобессознательныймотивгерояпроецируетсявдействительностькакчуждоеемупринуждениенавязанноесудьбойгеройсовершаетдеяниенепреднамеренноиповсейвидимостибезвлиянияженщиныивсежеэтостечениеобстоятельствпринимаетсяврасчеттаккаконможетзавоеватьцарицуматьтолькопослеповторениятогожедействиявотношениичудовищасимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинаделаетсяникакихпопытокснятьеессебявзвалитьеенапринуждениесосторонысудьбынаоборотвинапризнаетсяикаквсецелаявинанаказываетсячторассудкуможетпоказатьсянесправедливымнопсихологическиабсолютноправильнованглийскойдрамеэтоизображеноболеекосвеннопоступоксовершаетсянесамимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеубийствомпоэтомупредосудительныймотивсексуальногосоперничествауженщиныненуждаетсявзавуалированииравноиэдиповкомплексгероямывидимкакбыотраженномсвететаккакмывидимлишьтокакоедействиепроизводитнагеропоступокдругогоондолженбылбызаэтотпоступокотомститьностраннымобразомневсилахэтосделатьмызнаем

чтоегорасслабляетсобственноечувствовинывсоответствиисхарактеромневротическихявлен ийпроисходитсдвигичувствовиныпереходитвосознаниесвоейнеспособностивыполнитьэтоз аданиепоявляютсяпризнакитогочтогеройвоспринимаетэтувинукаксверхиндивндуальнуюо нпрезираетдругихнеменеечемсебяеслиобходитьсяскаждымпозаслугамктоуйдетотпоркивэт омнаправлениироманрусскогописателяуходитнашагдальшеиздесьубийствосовершенодруг имчеловекомоднакочеловекомсвязаннымсубитымтакимижесыновнимиотношениямикакиг еройдмитрийукоторогомотивсексуальногосоперничестваоткровеннопризнаетсясовершено другимбратомкоторомукакинтереснозаметитьдостоевскийпередалсвоюсобственнуюболез ньякобыэпилепсиютемсамымкакбыжелаясделатьпризнаниечтомолэпилептикневротиквом неотцеубийцаивотвречизащитниканасудетажеизвестнаянасмешканадпсихологиейонамолп алкаодвухконцахзавуалировановеликолепнотаккакстоитвсеэтоперевернутьинаходишьглуб очайшуюсущностьвосприятиядостоевскогозаслуживаетнасмешкиотнюдьнепсихологияасу дебныйпроцессдознаниясовершеннобезразличноктоэтотпоступоксовершилнасамомделепс ихологияинтересуетсялишьтемктоеговсвоемсердцежелаликтопоегосовершенииегоприветс твовалипоэтомувплотьдоконтрастнойфигурыалешивсебратьяравновиновныдвижимыйпер вичнымипозывамиискательнаслажденийполныйскепсисациникиэпилептическийпреступн иквбратьяхкарамазовыхестьсценаввысшейстепенихарактернаядлядостоевскогоизразговор асдмитриемстарецпостигаетчтодмитрийноситвсебеготовностькотцеубийствуибросаетсяпе реднимнаколениэтонеможетявлятьсявыражениемвосхищенияадолжноозначатьчтосвятойо тстраняетотсебяискушениеисполнитьсяпрезрениемкубийцеилиимпогнушатьсяипоэтомупе реднимсмиряетсясимпатиядостоевскогокпреступникудействительнобезграничнаонадалеко выходитзапределысостраданиянакотороенесчастныйимеетправоонанапоминаетблагоговен иескоторымвдревностиотносилиськэпилептикуидушевнобольномупреступникдлянегопоч тиспасительвзявшийнасебявинукоторуювдругомслучаенеслибыдругие

## Висновки:

Під час виконання цього практикуму, були засвоєні основні принципи дії програми автоматичного розпізнання змістованого тексту, а також з впровадженням можливості провести криптоаналіз афінного шифру біграмної заміни і знаходження відповідного ключа.