

**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

**Виконав:
Студент 3 курсу
Живодьоров А.С.**

Київ – 2021

Мета роботи

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

Хід роботи

1. Реалізував функції підрахунку частоти біграм й знайшов 5 найчастіших.
{ "ще", "чв", "хе", "ле", "хщ" }
2. Реалізував функцію знаходження оберненого за розширеним алгоритмом евкліда.
3. Реалізував функцію дешифрування.
4. Для знаходження й перевірки ключів я не робив окремі функції, а реалізував все в одному циклі в мейні. За допомогою комбінацій з двох найчастіших біграм в тексті й в мові знайшов всі можливі значення ключів а і b. Для цього створив окрему функцію, що повертає один елемент, якщо коефіцієнт при а та модуль взаємно прості, або вектор в іншому випадку.
5. Текст розшифровується з кожною комбінацією й перевіряється на наявність сміття через пошук неможливих біграм : "аб", "аы", "ьб". В консоль виводиться тільки текст, що пройшов перевірку.

В результаті виконання було виявлено, що ключ має вигляд [441,310]

Зашифрований текст.

ывлеюгзебщпещхшуйэвиывиюфгувхцубхщыюнюжлепэшфмиьхдошбуднзегдщцебцвшуюгьпцвэшувкмзеиэб
чиюндхщюасдбмонхегщгдэшжезьщемвошфцысьмайыегыйййыэшжеаекидщцеюжгьдешонгочвнюиоюжвюю
дешбюгщесфвшвоизйэящкщьюгочвнюлмшужейщурпцвдэяхщаюьдеуэвшюэвдиайятвепцвчвлюйщцецаеш
вэеякгхщцаэацизибвкмрйжуажййдекущтешпщфмзсдсугьвоцвяйкзфтшшхдуюньынюгдхацовойэращеюияциа
яймюяжцввджвяцэввллоомодмхщуйэмюэзопознэщегбдсефвхбжщениоцатщввэиэгтеаехохтйолдицзьхдщ
щцьюэзщюоцвлюеосдлузлащавызйферддьюмоиаььепжмнобжщцаешэойтээвзщупмюжьоцщаощвыжее
ююзьдеаейюшдоездюйбгъвиюэколпщхмоихсщфэмлеотзомщйвхцывбжхебахиэьщхйэашжеттфележебдфю
фпнюфмшуизяппшдгдщесдцжцвхеюцхеднвжееютбзийысддемилпмюзахшнюллоюэпподйшяюьхщужуиц
табзлзыйонпбоящпиэщииамленйхдбднвнщлврппилмиаьдшахушайыэфтппмюцдсзезщадцьцихжшуфгбиэи
хеныжпбоцднесдегмаущйыктгдыйктейнвмоктзгидатаомтцлвхейрдимяцшуюьвмтшзюашнэьгоэавюрдвд
жгмпиеэщейивдодзехатщйыэшзшзунзщхейоизсдэайехенвжфжпсхгчплвжмвиртдэппшуртцюиэппедчйдеш
орпдпвюбжлотвдюлофехщддетеодаьйохрбдмлпнднелыщхдошущцазнибыутвднтащебацэьгордфесьяешз
кнсднюятдаахмчвюцхеновющемеппзькюжмяюгьщцсбвдсчепзлепэшбмтвгоэвубюзмвппцинэзьэщтапуиэпхл
еоенщнщрдэшцлабмхтфуиноййаешцэдэвлюцрпбжэщыдидсдщохилпийшгмищцвюбйощйапедмлсгцатьчщбуэьг
йцамиэавджкяцрорпбдкьйомьщаохдяючвейчвэухвххерючежюшзюахмрпйзхфйдыжецэзьящктмоодььепю
йййройщюоцдисиатщхщнеэмьхгьощщеоиьвдгивюьжшухехщкдэщжюяцлщлейдьюйбпгьюййгдидидибосд
ьдиараощаагюьвмтвдцэзяхщаьйжгпнофпэшиаяйхмлпияюцмахщмайвкмшувовьбочвгййобуйэьвздююцгй
басдйэвюэасуяхуцбушущфлпэьвмхшоаяхрпдуюцбифебаитвлпхлпэьуюююэллбийэллбинюфугьвоцвхестюцг
дтэфйнезатщцавытдщаашумюжячаеаеэоодзтлоиййысьюцсьмашайыьхляеюсбфеюоэщуйзлепрдуюкизолюоц
буйюгктнвэииюдэяхщагююцхенедефепэлпсайкиащбушзшзунтахаьхдрпдэшцижесьюхибунюзьдешьюаеш
щфеюайвкмжгезчхаздхенехднвящжесьсвчаеяютвючсьцукммофпэьхцхенешжпмюфгцвцвзящдыэежежуйэ
фгэзюайыгщоднвкгшвиьвчлпэььххжмьхьбщйыфпжягьматцаефмлсгцадьтцэакгдйпгцэдемимозщчртшг
дьцэьщщцзмонпамвикнсшувлонвиюовкмлебчвмвзьжемвшзгдиямпнлоппбообхдвыхщнвшуялнюгэабуохо
бхдзчадыегжешцхдктеаюаируенедмшуудвайэанвфупдэмчвмыщелаяймоюаачвэуопэьжеюэюаеыпхщаза
яхзснгьетепюхиэаелесцктпмзшршеьбюекгдвтщдчнубждгдхьцкнвиюэвднвфузщщдетадшимжйцмюэ
щчйощйаэмтщвдешьомюхебавахивлфеионвздоуобтесаьдхщнвшуцуюэрдцзщхмвлоуцщцайюшдрддебочищ
укмжйпиуцфйжпщцоидфгшйощемлжгвдфюаюообюаюьймвшжеэуяххариндщщэщгщчикгялнювамжфуощ
пйцмюегнещсегбдфюфпнойбпгьфпжияиэвтбнещсегбмлещщзэяйдьдяецыфгсцфжтбшвяцвиоциалещнвбч

рйхаюиючпммшгяошулобжфгфиыжпптбшвиййраыьнщаошяэшуплопдищццаявяцбуиьэшхдвыбщпееыаб
ухтвдсдошийыщцыгэщзщцймилмлещощпрасгиацнюшщыйзашеоюиыцвмтшзлбджювишщхшужуиубяэшуплоп
хомццвяйощвыявжявщэадошщтцкщфйыьжеуцщуыднвлъеэяхщабммоппмвппдюлмлещйидужижикенвви
ищятпнзетечютдюйбпгъчизднвепфйзшиакунэшщфпызйайтьхииианвзшущиорбдпножищфвчвийэгцлпнющц
ыаяемтцтаэаощськммоочиэлпбоодэаьдааощчвоощоюшдйрднпцвдщнюиадешпиэвиьхсшрдехшуйэтфппрюфп
юцпмлпиящцоугъцааюфпэаэвдтщфеоещпхэбонношиафпжяфпцвчвжфждэлловьячвдодэайыжевыоененеза
иаразевыбвжйцулмлепешдешерйхаюиияхщагютврюфпэшиацаыввюсюлоюэуцвшэщйыаегюфпгъпднеизящсдж
пннхезефюфпящчвэвхлммьдшоюьхьрьрарежюгыщелекщтээмюфзнэцвсдмаеюиэисьмюцвэиубэфгцдеще
чйшвиозкоусжээщтеяииюфгтщкееючэацапесъзециоомзыхцоуоеуюмодшййыхетеуиэижецэзчтэгчййыбозэгч
ййымааейшгюдпюйбпгъищцхйэзълвепцвсдчйуутвыяцбехдыиьхзавдсцяобамщсдэанелезатэфйфщиээщне
жетщгдидчвяроеуюжйжпннтвшивлугцхлхцтапэсбееляоодгжюубвюцдеючщупнлмлешашайиалимьящф
гмючехйуышзкоусбщмазцбиххзэьысьзьюауйжекоюжмтщкдцщцхйэашцааюцвмабзнэщежееюсюбжовщцап
ейщццвюлозьйычвийзаятдгэшхлхяюсбеужищсегдъдэбоодфсеаоененетщкертвтэитзщанезчудйоецэзчкмюч
сджэзлрдяюнюиюэзмюсетпыжташенепхсшыщъчвнюлоизяцсбэапепещдйогдйыхедетамайвднвюдэяхщавомо
одбпртгъоещуппиачпковфндхщоедесшсдкюэьдэяцсдцааюцвщфепэюцзасеянэшзчуртэщсззеысдкмювещи
щемарцзлвпепемайыщпъуасъцвэиюэяхщавоцэлеююфпрдэывчвтааеувэтеьджюсббамщиаиьмахенщщавыс
ыщцяодчэтдбщпенегдеаиюуюэзлвиюэзлпмотвярьрешддеплпзщшаощсуяхсуяхлпвидшхщпелеецабацыещ
зщеггдюпшщмцкнвюютючшабщощщщэщжлзъдшфглоизюаэубяшбмьмшгжюубуиьпбжхеещущухамхфйс
щощвыятжмючктюощщпвлхешекюиэзосднефепэщущхдхжппчиртлпчвярюнооодщзопсеаохтгднщхекудэ
эиэибацыешкибохтгдййаююэяхщаяэяхщавонвздайтьреошйынщмаонгоюзщатаьтазэхдвхьннвэдюртюц
гсдееэюцгющччщупнлмжмящнюпхмьшияцдеыуппамрпзъроадздыщчвярлежпсбамгдещнвсбэаэщъэяхщад
ежпиээщщьюцмюспаелешгкитвяцдееюдпэдюиюложьвибпейцамиьоецуппбозацыжервищжиртлпцаытдое
хдсвищцюзмвусщекуяцфгкмрпцвсдчйбщщцщлоцвгвюфттцнгкмжгпййождгдфгнхрйжшиаквбжхебуктюаююцдз
щшгюйбпгъпбююфпбвмьщелейэищцднесдроюэппамбжронвжешатьэзребциюывэчвяртящпрдйюкизоажхене
жетщтгххдэтахщщсщэвиюэяхщалтгвщущэбчиюндамтщжпунлпэшшвчвийэрпуюиьрьешйыэшдеюйбазеашл
ьюусзочвцаделекюиияйгшацвэшвдсдтщеорпиьчвярсдщелчпбонххлпфмшуиэщщсдлоизлещецохиболпжйс
днегужюаэвбжронвпйцвгщнюаеегююфпждвпщюиьаепзкнбатахщпсэфггдиалмепэшэвчвадздююубиьмюмтч
еодесчмдэлпепэьйыамвиртлюсшсднвлптвэиубшштиубзчшгыгйцаоизивюрдрячиртлпщещьмоодяюзьжхюй
эяхщабмчвлеаатюцгсхешщднесдюфывепнюсьлоздшианвшузмлюхебуэрьмшшатътцьзулмюзэгцлпню
швчвийрьешещьбюбжщенюиьмахенщтаобчйэылщхрдшгматжщешгмаеюцжыгджювитщразервяцсехдйнощза
цыбддешщпезмйэтвошжестюцгдиавоцвмюцвуллотвнюжмнющхлеуиытазэхднюшдетаадужибхошунхрд
ощнвшардзхылофмгдмашавыщюээдщощоеядъзхвдюээмочпвлпийгоощнвпйсьшузохефпызйтьрехджоодэв
вифййдашадгдфггщнерйюглофцвтцхдвыпелебдесаьйнщыщхдгдбмгдхдбщъзецоьхнэсфибнвиювичвярнв
зщрйвдзджюлмгчхтэбчишщюаюьтайгшаощюоэшийшшоэщещйгдтидщвоюзйэхсдегжщюаыьзекжгыщенюэщ
цфцжштъыьжеуцаоаюьтазахщчвэвхээщхдулпидвоюзийэсдвящупнлмтщжпежуддешупнтвовднвюяхмощуеп
нюдешечйшвчвхзанэудешщйжпннтвщиэихешщцбьаожецэзчкмюпияжмрплобчжоцвмозохтйюквэипхнэмвижпп
щцоээдтвэипхнэмвзочвжпннмвщццардзхытцбойэлмдэяцщыцвэшыявхжпидидьмаеьлочводэжгыюйбауэяхщ
авочвнюжййдтпктаешщэфмюлобылмьмоодпзощпищуээяцыщзщювюьхюаьтазэхдзюшщдешдюпийоецумвби
июмюдэпааюфпбуиьэээяхщагючвяцсехдзюизезощошвыамхфйсщощфйзщнюучауцюимьюжфучугьоддпэ
бовляхуусидгщкухтхсажщедешюаугшазевытпктепихсхчвмоюзопщувюывьячщдецуыьбщцхйэунищжфтзе
лммыщбджюсбюанвшубюфгэяхщайцачюэирпмюамлпияцднеунощбпзвимождгдйадвмюьщегфгыюфпсес
акумюфгоажгщъвияцжпмохенюятздэаьпъхегехщыййидужибочвэухвэсюаяйбацыешщзцабвюатайивдсуыжы
вдюиэмощушйиадечюмюзэциуцнщхекудэяцепъхестюцсшэаеиовифйлхнэлвижппикщещежсьмюкмшдджмяп
псбхщжвчнюишяцююжтщдешечмзьмюийнежетщцсехдйанюэюэзлвиаабнппяцнвжегдпмзобднердзшамйд
веавэнщещамхвусеьрьчайыгдчиэижпунушсеххдъжывмьмькдбовшвыэаеадебпээкоудкюдэяхщадпехди
зопбжщещечиртгтвдюлмлеоелжлпчвийщцгдидйгтельнюдохжяцзайобатыцгдкьвдюжквюубщпъсюцвбжщэф
ебалимьтесьюцсуяхубвдююенвздажщешщщщещежэудеюезелаллжмадбшяизиноайгкукоудеьээяхщабмшуз
ьмаллотвщдещуьхлпйтаияцгпэзбоцвещйсдкюцвюзайхевджюсбавэнщшвяцзщцюфпбуйэрпхаьллотвюшде
эшбачмжмвддыллкмбжбщжпешепиьаэгцуджэяхщагюфтианжщешвнюэехеяецыйидкмхшоекуяцдэхажщеще
щхиьнйююфпхрдянчючкмшуеошйыунзебвчвийнвсдчхрдщезаяюубсдкюцвэзъовывхшфьэяхщашцбмйэ
бщкижмюфпмлпвоубкщжещехеэфлошусдешбюдэчврпшинююхеиилмйэзлзайыаецыхесдйрдшлльюуссдэа
хдоехеаеюкмтщрцкюхтыжюцядэащдба

Розшифрованный текст.

утробылотихоегородакутаннйтьмоймирнонежилсаявпостелипришлолетоиветербыллетнийтеплоедыханиеми
ранеспешноеилиненоестоитлишьвстатьвысунутьсявокошкоитотчаспоймешьвотонаначинаетсанастоящаясвоб
одаижизньвотонпервоеутролетадуглассполдингдвенадцатилетотродутолькочтооткрылглазаикаквтеплуюре
чкупогрузилсаявпредрассветнуюобезмятежностьонлежалвсводчатойкомнаткеначетвертомэтажево всемгороде
ебылобашнивышеиоттогочтоонпарилтаквысоковоздухевместесиюньскимветромвнемрождаласьчудодейств
еннаасилапоночамкогдавазыдубыикленысливалисьводнобеспокойноморедугласокидывалеговзглядомпронз
авшимтьмуточномаакисегоднявотздоровошпенулонвпередичелоелетонесчетномножестводнейчутьнеполка

лендаря он уже видел себя много рукам как божество шива из книжки про путешествия только поспевай рвать еще зеленые яблоки персик черные как ночь сливы его не вытащить из лесу из кустов из речки как приятно будет померзнуть забравшись в заиндевелый ледник как весело жариться в бабушкиной кухне за одночасье оцуплата покажет лоразне делю ему позволяю не чевать не в домике по соседству деспалие города и младший братишка там здесь в дедовской башне он в бегал потемной винтовой лестнице на самый верх и ложился спать в этой обители кудесника среди грома видений аспоза ранку когда же молоко не кешенезакали бутылками на улицах он просыпался и приступал к заветному волшебству оавте мноте уоткрытого окна набрал полную грудь воздуха и из всех сил дунул личиные фонари мигпогасли точно свечки на черном именинном пироге дуглас дунул еще и еще и в небеначали гаснуть звезды дугласулыбнулся такнул пальцем там там теперь тут тут тут в предутреннем тумане один за другим прорезались прямоугольники в домах зажигались огоньки далеко далеко на рассветной земле в другом зарилась целая вереница окон в нем зевнута в нем вставать огромный дом внизу ожил дедушка вынимай зубы из стакана дуглас не много подождет бабушка и прабабушка жарят оладьи сквозняк пронес по всем коридорам теплый дух жареного теста в овсех комнатах в степенулись много численные тетки дядьки двоюродные братья и сестры что сехались сюда погостить у лица стариков просыпай самиссэленлумисполковник фрилей миссис бентли покашливает встаньте проглотите свои таблетки пошевеливайтесь мистер джонас за прагай тело шадь выведите из сараа фургон пора ехать за старьем по ту сторону уоурага открыли свои драконы глаза угрюмые особняки с коровнизу появляются анаэлектрической зеленой машине двести рух и покатят по утренним улицам приветственно махаа каждой встречной собаке мистер тридден бежит в трамвайное депо и в скорепузки мруслам мощных улиц поплывет трамвай рассыпая вокруг жаркие синие искры джонха фчарли вудмен выготышепнул дугласулице детей готовы спросил он у бейсбольных мальчиков что мокли на росистых лужайках у пустых веревочных качелей что скаса висались в деревьям паптом проснитесь тихонько прозвенели будильники гулко пробил часы на здании и судачно несет заброшенная его рукой с дерева ввзметнулись птицы иза пелидирижируа своим оркестром дуглас повелительно протянул руку к востоку и взошло солнце дуглас скрестил руки и агрду и улыбку как настоящий волшебник в тот тотодумал только о приказав все по в скалив все забегали от личное будет лето и она напоследок глядел города и целкнул ему пальцами и распахнулись двери домов людивышли на улицу и летоты сажадевать сот двадцать восьмого года началось втропроходя полужайке дуглас наткнулся на паутину невидимая нить коснулась его лба и неслышно опнула и от этого пустячного случая он насторожился а день будет не такой как в сенате кой еще и потому что бывают дни с отканные из одних запахов словнов весь мир может нутянуть носом как в воздух вдохнуть и выдохнуть так обяснал дуглас и его десятилетнему брату тому о теце когда вез их машину за город дав другие дни говорилеще о теце можно услышать каждый громика каждый шорох вселенной и иные дни хорошо попробовать на вкус аины неаощу пабывают такие когда есть все сразу вот например сегодня пахнет такбудто в одну ночь там за холма мине весты откудавзлся огромный фруктовый сад в седосамого горизонта так и благоухает в воздухе пахнет дождем неона небениоблачка того и гляди кто неведомый захочет в лесу покатать и тишина дуглас вовек глазасмотрел на плывущие мимо поля не тниса дом не пахнет ни дождем ни откудабы разниа блонь не тнитучик тотам може тхотать в лесу авсетаки дуглас вдрогнул деньэтот какойто особенный машина остановилась в самом сердце тихого леса а ну ребатане баловатьсаони подталкивали друг друга локтями хорошо папа мальчики вылезли из машины захватили синие жестяные ведра и сойдяспустынной проселочной дороге погрузились в запах земли влажной от недавнего дождя ищите пчел сказалотецони всегда вьютса в озлевинограда как мальчишки в озлекухни дуглас дуглас вступенула саопять витаешь в облаках сказалотецпустись на землю пойдём с нами хорошо папа иони гуськом побрели по лесу впереди тецрослый и плечистый заним дугласа последним семенил коротышка том поднались на невысокий холм и посмотрели вдаль вон там указал пальцемотец там обитаетогромные полетнемухи и ветры и незримые плывут в зеленых глубинах точно прозрачные киты дуглас глянул в ту сторону и ничего не увидел и почувствовалсеба обманутымотец каки дедушка вечно говоритзагадками ии все таки дуглас затаил дыхание и прислушался что то должно случиться падумал он ауж знаю а вот папоротник называется венерин волосотец неторопливо шагав передсине ведро позвакивало у него в руке аэто чувствуетеионковырнул землю носком башмака миллионы лет копилсяэтотперегной осень заосенью падали листья показемя не стала такой мягкой ухтыаступаю какин деец сказал том совсем не слышн о дугласа потрогал землю ионичего не оощутил он все время настороженно прислушивалсамы окруженыдумал он что то случитса ночью он остановилса выходя ижедеты там что тытакоемысленно кричал он томиотец шили дальше потихо й податливой земле насветенеткружеватоньшене громко сказалотец ипоказал рукой в верхгде листва деревьев в плеталась в небо или может бытьнебо в плеталось влиству в серавно улыбку лсаотец всеэтокружева зеленые иголубые всмотритесь хорошенько иувидите сплететих словного дащий станокотец стоялуверенно по хозайски и рассказывалим всякую всячину легкои свободн не выбираа слово часто они самсмялса своим рассказами отэтого они теклиеще свободнее хорошо прислушае послушать тишину говорил он потому что тогда дае са услышать как носитса в воздух епыльца полевых цветовавоздуха ки гудит пчелами да так и гудитавот слышит там за деревьями в дожде подомлет сяптичьеще бета не вотсейчас думал дугласвот оноуже близко аеще невижу совсем близко рядом дикий виноград казалотец нам повезло смотрите канена доахнул просеба дугласвот миотец наклонились ипогрузили руки в шуршаций кусть чары рассеались то пугающе и грозное что подкрадывалосьбылизилось готово былоринутьса ипотрасти его душу иисчезло опустошенный растертанный дуглас упал на колени пальцы его ушли глубоко в зеленую тень вынырнули обагрненные алым соком словно он врезался лесножом и сунул руку в открытую рану мальчик изавтра катыве драч

утье недоверху на полнены дикиим виноградом лесной земляникой вокруг дятла пчелы это во все не пчелы целый мир тихонько мурлычет свою песенку говоритотеца они сидят на замшелом стволе упавшего дерева жуют сэндвичи и пытаются слушать лес как слушает отец чуть посмеиваясь искоса поглядывает на дугласа хотел бы Loch тот сказать но промолчал откусил еще кусок сэндвича и задумался хлеб светчиной в лесу нет что дома в кузове совсем другой верно острее что лимятой отдает смолой аужа аппетит как раз играет садуглас перестал жевать и потрогал языком хлеб и ветчинунетнетобыкновенный сэндвич томкивнул продолжая жевать понимаю папведь уже почти случилось думает дуглас не знает что это оно оно больше еще прямо громадное что то его спугнуло где же он теперь опять ушло в тот кустанет где то замной нетнет здесь тутрядом дугласисподтишка пощупал свой живот оно еще вернетсана до тольконемножко оподождачь больше не будет яужнаюнезатем онокомне придетно зачем же зачема

Висновок

Після виконання даної роботи я отримав практичних навичок роботи з модулярною арифметикою та частотним аналізом. Покращив навички роботи з вбудованими структурами даних (vector, map).