



Національний технічний університет України
«Київський політехнічний інститут імені Ігоря
Сікорського»

Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз афінної біграмної підстановки

Виконав:

студент 3 курсу ФТІ

групи ФБ-91:

Журибіда Юрій

Перевірили:

Завадська Л.О.

Савчук М.М.

Чорний О.М.

Мета роботи

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

Варіант №7

Хід роботи:

1. Були створені функції для обчислення розширеного алгоритма евкліда, обчислення оберненого елемента та розв'язання лінійних порівнянь.
2. Обчислив 5 популярних біграм в шифртеусті: ['цл', 'ял', 'ае', 'ле', 'чо']
3. Написані функції співставлення біграм, їх зашифровки та розшифровки.
4. Обчислені можливі ключі.
5. Розроблений алгоритм виявлення несправжньої мови. Відкидались тексти де зустрічаються біграми які не зустрічаються в природній мові(аь, оь).

Шифрований текст

хетжщбеыжцллийшллебторюкечожлхуемебсфбпвгщпсакюбизыщллбющцжбщвлвачоофлеы
мноэвцфйжлщцвлифчезуазщмвьпфйбсфашазлевлазлевлыюфйгблфубфефциннотшрлбыц
цошшйтьоюшцхоаимжоцллийшллебктяфлеабуазгбшйтьошюййчажощцйленефцинебгбгугф
язашцещбйяхенефцинебуццбхнюеоицсфзоэбохзьяфебчфкеаесачсюэбнцдвцпашйлежцаечй
хцусфюююшцхожцаехпщлобуипылщмвьйлештьбныэнесазпюдуипыкнялкллейешццвли
фаоызыюфйгблфубцлцсфлцулбэйекфрлмнйехеонялйьпазагблцаьццзаяюебияоаефцинбоь
асфюэфюульукбшеьтчлюаеухулбцьдмэбрлютошнюэопсфхйуллййуулялйувеачойлфеяйчэти
мжыйшйшлтечоглжюфймимкйейежйыфтцултэуоечоаечяифмфсосакбщблетипчьаьтобшиф
цхбялчюфййлфеяйчэусасьйдмчоюэйеьтнфлфцфйюфтцссасифылкцрлфлчлвсофртбибнпалй
хзжйлеэаурсзэшцилмпайеымопсафыццтиксуфйшиллцйноццфхомбобячнюэубмилыбошн
ьхйллцрксифрлвлсцзежцялильоурслгешфйяхепьтгозежцлюялмчпрлцлыцялшйвтцллевьбй
уйшцфаауспяолпэпрбиксаегвпаусубшйтьошньдмэбрлрврнийысрлчюшцхоаимжпфшйашцф
ниасчлйжйзаюэчокбофлйхзжйебгбгоаежймоьяалщбифжаубчхйвьзэбисазпфюжцчьсаьвчо
мйбчиесачсптялгьбщвлифшйояпапршйвтцллебнцфюэсзэзыцлюуйльэдглнччбхнялжхвбр
ижэчблттнаоцкффулеаусзымуусузиивгмуьаьаюейнсдязешыумеиелцчяйшдтсфашвидмгб
виччмуюоажфбсфдцюноцдпфжчйжйлзсьжффйлжчхялеихоинюеоицвбюйшйляфюмивцвб
йтчулйяцхожцаелеасуэяфллокотипчыэымаечойлфезамкаьсажлафчуешцзешцксьлгйсэйшжйс
юзащмибхссачсптлпфццмвьбтрлцизаялхифюцлдюцццфютошшйьтбыццошййилшмчуом
эбалилоююеьялилгйжоцгонтнцдфцбкечоксюэяфнцюжкюмиасюэююцлзшдюзэцавцвюю
ййзейгйофрлбфебошмфгфмюзэымебмфшизыяннзнтжлздйфаеэусююфймиййщбчаюэшавц
чсубиложхоюйгугфазлевльафюллшйэбсфаюййшйщлйвикюфййтхйюйсфчьдмэбцщцфэап
ьюноузаьтльаозачлоуаеюэелютошхаажлбляоужумйбтгбцщцэдгьымдтлзьбрццидаешгрлб

фебзтжлзгфчбмноыйвиелтаеэеыжцацфуяэылэюечщбкеаеешэдуффеуццлобфпейжлгблбо
фошулхашчянялазултайьюелэуэщмымдтчуошбияофютамжасасыумйбтлцлфлйаэчоллвлосз
йлежцьййфысоцобгбфчепурзвэщаьттайьеэоцчлитснлщбазэблцссейэетаегмвьоьбючйюн
хепйгбилхнкниелэфжкюлщбахутаоццльйдсщфкбошьййшктлцулщлнфтцйхклююфйцщдмьй
ещщцялвсхечойлфеяйвбюэлщвьклмфоюфйхашчфжщбяфялщльййлеяьтлблгесачслщщфй
тюфьбюешмаечоялхйьбэпчллюэвьпаопнайййавтюебюйьбсфнцьййбтщвьлекюьаллвллж
ечовфвфдэщаулпозавьчуёнчзэмуулййшщйымжгбцалщчунцлжйгщопнчзафлилфсучуй
юклщлмфйшоффпсфесщцфюфйспсфесаечомимкзанйбуилясрбхутаоцьйаювьайэщмымэбт
опчюеаехсбнйеуувихевюаькфсжзаццуэасхерюяйтцсасетялуицжщбыюсащбчлтцвгкбрлцип
ййеьтымжчбпфьыоцэигбхуднюолщвлфлдчзаялилцирюетмулемфллжлпфцлуичьуэкюццф
ывбцфжазэдгсумйбтнлнэымсаюеочцошйёнчзэобовблвсэбюпсафыыэемшйьйззийешклошм
иццофгбтеебрийгдсвлььдмхзьялхйилхйешулгоаежйошфьгужлтюжйттхутаоцазялйшллбифж
щфгййшщлтзсчутэкьносайёнчзэобовбпщэюеасцлфйшноццбьйжлднзашцнеелуичоцлтюае
члялципыйеьтйьэымюэмптфюэсфешгбдоьйаьтусюючүфечофлялжлажаоьаьтвевьечйщриц
цвбнцопыихеэтжллзулыьэщаьтпуклюаьтщбцихечьдмэбвжоцхзнцльезастиялмсйрчуобже
иекьрифбошьтялафцщбццфйюэфкцоюьёнзвссфмсэщаьтщбьйжлщвлгфчутэмжхоюдюэф
щксхеьавцщщаеобыймбебееатаййеяжйгугьгуйбьйчэюеобнховидмчойьхулбошнювидмо
бхйтцыюфйклвлхлчбкеоцхзмсбщаеоцфюобьйцщдмчуэбщбнйбщысдчлтээюаеюэмжйрюл
ечуэбэребмаьаоцфыыиксфюксгуюфьйфйяйлэрулзуледгдйююфмикюрютацпяацсасщаасял
лбдмвьаьхутаоцущымцпнчлэобцвбщлжлмтзлвцаюэвьдмэбрлчрьбцфгпобвбшийщллевцч
уюйжлолофгбмйоайесачсщцрийяассаеьавцпчьгызаолмбрлаювцялбэасюэчяхутаоцтсебщс
дгбиолдсшзщлмфнмэбпювидмлщзелэкнщмфюаеюэфюфйауоюфйобпйленебнцлымвлбэагн
ицнксвцулсфкцлжлтамжасаетиагялхйяйлшллветиоцшинаьтемдтмфоюажаоююофзэуэщмф
юущтигоаежййюццеоьиолэщюэшачльняльоьуэцлбирищлдэхоефгйчйсшщцвбьйтцацофа
фччыэусымчбщмюэйщкзэюецчююдгулхулбщлэщзаяейжлвипчзаьицжфюнтщбаюебцми
хойепалэдгшифюцдялаэксщлмсзэтюаьчоымнвэбйббинчшйьйпфчбпэымелциюеьэцлжлющ
риозянвгхйкенвэблсчоиейщрищщцфьтйбошщбьйьэщцошвыцлцитсдгюэлцзиййлевцгфьбф
ечоуэщщфюфйщждпнаюэхооллетипчцулмиымзааююехктйьтзауоцбйшпззафюцклгйнцбо
шчйюнхемуулялощвьбтсфрщфюгыьфымдтшйнцфюфйюцялвлжюзщбццфечоьлдсзэщаьт
щбцщзэюфймктюжшйеитстсьнййубафгйчйсшйашюэазщлнэсмсафюсмэбгбкупебноцф
юейхсчлпшйьлхэящэтюаьчодгшийщщцфымдтлзьбсфиллеозйтчуаулитсефцбйшпзгьыоцы
йаумийщюезашифюкюксебйэагiasmхзвевьдмцщвлиффечожлщлфйжлфлцлифнцзебнцлрлн
эмжпаыэымцжнощйщлжлллщлйяьлдскьхеэфжщвьчлзчбюйгфффвбзэлеййпэагульсдмэбрл
кыйщвбсфашмикюблцлфулеьагумолеуцсфрщпывцхзыэпчнземшйялчбюйллтеьэофйэпра
уиаьрцйьйшчуащзаянююпыйробьюеблпфщбщюэьпраыйгйфоцлжлиюензповичйж
йсфьбнцыюницнобеебнцлчйлешзисиийцфысюючибцвбйшцлкьиипаццвцхзсрсязасфбцнтн
зиююеночпкьялщцллясновцсаялфымьйпэуоусщлмснзэмпбщелуичоцлйулщвлгфчуялйуц
жрижэмпщцлчбмййшобсфоегяебнцлобйуьсчпвлщйпэейщлэсдггулщдьдмэбтыаоцлзшб
нцьюцжджцпблцщлрэфюлзнбжааьюююьпрааанозефцинфщлйсфлежйллжщвллофцзьбсфч
лэьыробихюйжешфлйхстйебнийьюьцценефцинчлщлхсфющбжлщлйьхутаоцкюоишцсфщ
бвьчуафжаолпэсдшдпокюобовьчощмжуойлейнзалщщцриййежйошиссаеьашцвюжлоажбц
блептийщмшаллырзафюуикьйепапччыцлзшбщлафжаолщбафулмтфщебфьечююдгхулбцьд
мэбцщжйоьнткеымюэфжщбэбилхйцфшэзачбьйулбэюлжюжсщфдэщакелщвлфйутебэьгужл

щъщцзеагщбфлхйбипчъащбаююеяпапрдюыэчыбыбошойцфофлйжлщйжшгфьйулофлбсффы
губеасетщбклщсчьебнцацялилафчлщемпюеиеулсьритючоаюриобзктйалщлхзяноцоиаълл
нзлрвлцлмймивжкювьчощбфйчшшйьтглаюехугьцняллеопдгхутаоцажчбъцуснгчлаажцуимпя
ллбчлнбшсефюэююцлзшулобцфсфашулдйфааьдмхзщзеащзеаюэусхеавщшщцчаюэы
рсалбрлтээйжлжйщлжээрмэбгбвфчлзеиебнцлщцллясьабоюэцлхйфеымщцгйчаьлофгблзнб
сфашобшикпрюкпвлщйпэейажчллээруреазальщюйэьдмхзйжйгэщаьтйчэюеьйчэюехутао
цгбдоьйаьттехоцлгйттлсщцауцбсфютчэвцхзпаглцбьяьечойерыноечообсчаечлхэюфйюдм
фшэдржщбшевеелофйфознтйэцжщбшехежсасхулбжаглцбьяьщццрзоэлщвлвальзафытюаее
оефтамжыхуййилтаажуэбопуэааьйебртизыопыеасбизыйщвбцьдмэбяртизыопрюфйшэзаол
цлдсшзмэбгбаечяулупбныэацжцялшаозрллщбнэбовцмйшаьтжлщльбщмжулфебэбашйж
паыэсавцхзхэмппщцчлмэбгбэрлцмиюеьавцпьдмэбаюлежйчйчунцтцбщмжщбюеулбтщлжю
фйвбгфазщлгбхулбцлюэщбвлаэлщщфыйшэоцфдчбвеопюхялрлбэдгэайньашцтлсепчтюгбжл
члжйюэлцфжщбюейейщритлижщбюевеэфнухйшэаьдййшшбщитсьлфулеаоцжцозрлхзфщв
ьбтэбщмфючлэьырулобяфьбацлэуэюеьйяьпрцлйбэончхуаешлафялилафеяиибщуэнзмюлеж
йцбпэаглцзйийзыииэыээнзщьдмэбрллетипццулмиымзааюэфщлжеолофазсфобзнччтйвцкь
фююйюютиьэтйилхаажчумжбфауфмцпущаечойжтаеэщащбаеыбзэхечоетульйсулцтюаьеб
хсмжзаюэфйжлнэцтклиувьэлццюедкйетлофгбйбфлаэжугосрчусфашользатййуыйвичьдмэ
бдцялшаиуошулобяфьбацкфцмюэзыкюццкфлеисядыфрцксчоюйрлщегмююзаяййугугфкли
уулиулцоюфюхевюфйвеасасчсочпчцлхулбщлербноулехебрбнллийжшбцвбошыййшкргбазо
шоффйжлнэеажкюмиуэфщщццлюэщйщлгшеэыэнзрщщцлвгйтхйщлхэывгмжуэбоаанаф
щлйрзажбщйрмфлжлпфцлуичьтфщццлюлфгййшцлпаюеюэбщзаяйрлцфунбсфхаечыэнзхоц
жсаыитсольймйсфолкцулхзобнцзеасвеелгйхьечццццхьащмцжбщюйзльйщбфлбиоптиилв
бцьдмэбьтофлйжлмллакнцлщцебдасцциййфлципрулхноцьцлеуэбзитснозэымновцлфцлчее
бшуустиофоббэжфллгувешццлрэлешянхезавцлэяйжлгйюулэйбэымнлешянхекскеаелеыи
заьтвбшабцллийшгбцьдмэбтыпальаозаопкечодпечцфилхнзаююагаечявафщцжчьфщжйфллек
юдтрийувьцлйубисасмхешщиежцьюцжяаццдэйщцебфьлщвьопцлсяпаусхлдцисаеиййбиною
аьюеэропечбэфюжлвлмфчлхмтивьтеаехйшйжштгиййвьцлаешифюьэтйшйхуьсоцлшащбнф
вллощиичьцлнсшзйшэййебнцлоблфвбцлтайьрюзанфвлгфыэаьпфкэейбищцлшзчйжйнэбо
ебхсзэщащцяаюеелжюлщвлшбйююеризаьшццфйфилозрллыэмпэфьуфбвсдмшйлептсфху
таоцйечоююлщвлшбсфялйшлщмелнэымвьапыобуэпухйрлнпальаьпыобулхсжйппщвьйл
влфлсцзежцаехзткбчбхйдююефцинзэкюрибтобчбчбклвлнфюувлфбрцопыхеяащмлрлнй
щфгйлцйщзбиушйьтошэйсефюгбобобагмйхлрсаетиагозбизэццюеисбиццсуьиюб

Ключ (200, 900)

Розшифрованный текст:

атызнаешьсколько размы вэтом годуиграли вбейсбола впрошлом авпозапрошломнистогониссе
госпросил томгубыегодвигалисьбыстробыстрая всезаписалтысячпятьсотшестьдесятвосемь
разасколько разачистилзубызадесятьлетжизнишестьтысячразарукимылпятьнадесяттысячраз
спалчетыреслишнимтысячиразиэтотольконочьюиселшестьсотперсиковивосемьсотяблокаг
рушвсегодвестианеоченьтолюблюгрушичтохочешьспросиуменя всезаписаноесливспомнить
исосчитатъчтояделалза вседесятьлетпрямотысячимиллионовполучаютсяавотвотдумалдуглас

опять оно ближе почему потому что том болтает но разведет о нем он все встретит и встретит полны мртоте сидит молча насторожился как крысы а том все болтает никак не угадывается и пипит и пипит как сифон содовой книги прочел четыре реста штука кино смотрел много больше сорок фильмов с участием бакаджонс тридцать сджеком хокс сорок пять стомоммикс тридцать девять схуто мгибсоном сто девять сто два мультипликационных прокота феликса десять сдугласом фербенкс ом восемь раз видел призрак во переслоном чан и четыре раза смотрел милтона силлса даже один про любовь с адольфом менжу толька тогда просидел целых девять часов в киношной уборной все ждал что бы та эрунда кончилась и пустились кушканы на рейку или летучую мышью ауж тут всецеплялись друг за дружку и визжали два часа без передышки и сел за это время четыре реста леденцов триста я ну чек семьсот стаканчиков мороженого том болталеще долго минут пять пока отец не прервал его а сколько год ты сегодня собрал том ровненько ответил пятьдесят шесть неморгнул глазом ответил том отец рассмеялся и на это окончился завтрак они в двинулись в лес тени собирались икий виноград крошечные ягоды земляники все строена наклонились к самой земле руки быстро и ловко делали свое дело в дравсе тяжелели а дуглас прислушивался и думал вот оно опять близко прямо у меня за спиной не глядя высиработай собирай ягоды кидай в ведро оглянешься спугнешь не тут же на это траз не упусти но как бы его заманить поближе чтобы поглядеть на него глянуть прямо в глаза кака у меня в спичечном коробке есть снежинка сказал томи улыбнулся глядя на свою руку она была вся красная я год как в перчатке замолчи чуть не завопил дуглас не кричать нельзя всплошится эх ой все спугнет постойка том болтает а оно подходит все ближе значит оно не боится тома том только притягивает его том то же немножко оно делало бы еще в феврале валил снег а подставил коробок том хихикнул поймал одну снежинку побольше и разхлопнул скорей побежал домой и сунул в холодильник близко ко всем близко том трещал без умолку а дуглас не сводил с него глаз может тот скокить удрать ведь из зала санакатывается какая то грозная волна вот сейчас обрушится и раздавит нас эр задумчиво продолжал том обрывая кустики винограда на весы штатиллиной суменя у одного летом есть снежинка такой клад больше ни где не сыщешь хоть тресни завтра ее открою дуг ты тоже можешь посмотреть в другое время дуглас был только презрительнофыркнул да мол снежинка как бы не так но сейчас на нем чалось то огромное вот оно вот оно обрушится ясно неба ионлишь зажмурился и кивнул том до того изумился что даже перестал собирать ягоды повернулся и уставился на брата дуглас застыл сидя на корточках ну как тут держаться томи выпустил единственный клич ки ну лся на него опрокинул на землю они покатились по траве барахтаясь и тут друг друга нет не ни чем друг о другом думать в друг кажется все хорошо а эта стычка по тасовкам испугнула набегавшую волну вот она захлестнула их разлилась широко вокруг и сетобо их погустой зелени травы в глубь леса кулак тома угодил дугласу по губам вороту стало горячо и солоно дуглас обхватил браку крепко и стиснул его и они замерли только сердца колотились да дышали оба с вистом на конец дуглас украдкой приоткрыл один глаз в другом опять ничего вот оно все тут все как есть точно огромныйзрачок исплинского глаза который тоже только что раскрылся и глядит в зумлени на него вупор смотрел весь мир и он понял вот что нежданно пришло к нему и теперь останется с ним и женикогда его не покинет а живой подумал он пальцы его дрожали розовая на свету стремительной кровью точноклочки неведомого флага прежде невиданного обретенного впервые чей же это флаг кому теперь присягать на верность одной рукой он все ест и скивал то маносовсем забыл о нем и осторожно потрогал светящиеся пальцы словно хотел снять перчатку потом поднял их повыше и оглядел со всех сторон выпустил тома откинулся на спину все еще в воздухе кулак небеса митеперь весон было на голове глаза будто часовые сквозь бойницы неведомой крепости оглядывали мосты

тянутую руку и пальцы гдена свету трепетал кроваво-красный флаг ты что дуг спросил том-голос его доносился точно со двора зеленого замшелого колодца откуда то из под воды далекий и таинственный под дугласом шептались травы оно пустило руку и ощутило хрупкость и нежность и где то далеко в теннисных туфлях шевельнул пальцами в ушах как в раковинах вздохнул ветер многоцветный мир переливался взрачках точно пестрые картин в хрустальном шарелесистых холмах были всеяны ветками будто осколками солнца и огненными клочками небеса по огромному опрокинутому озеру небосвода мелькали птицы точно камушки брошенные в лужу рукой дуглас шумно дышал сквозь зубы и словно вдыхал ледяные дышал пламя тысячи пчел истрекоз пронизывали воздух как электрические иерархии десяти тысяч волосков на голове дугласа выросли на одном миллионной южной мавка ждом его ухестучало по сердцу третья кололилось в горле а настоящие гулко ухалов грудителю жадно дышал миллионы и поря и правда живой думал дуглас прежде этого не знала может и знала не помню он выкрикнул это просебя раз другой десятый надо же прожил на свете целых двенадцать лет и ничегошеньки не понимал в друг такая находка дрались с томом и в оттебегут под деревом сверкающие золотые часы редкостный хронометр с заводом на семьдесят лет дугла что сто бой дуглас издал дикий вопль сгреб тома в охапку и в новью покатились по земле дугты спятил спятил он как тились по склонам холм а солнце горело у них в глазах и в орту точно осколками монно желтого стекла а из адыхались как рыбы выброшенные из воды их хотали до слез дугты нерхнул ся нет нет нет дуглас зажмурился в темноте мягко ступали пятнистые леопарды томи тишетома как потвоему все люди знают знают что они живые ясно знают так как думал леопарды не слышно прошли да слышавотому и глаза жу не могли заными уследить хорошо бы так прошептал дуглас хорошо бы все знали он открыл глаза отец подбоясь стоял высоко над ним и смеялся голова его опиралась в зеленелистый небосвод глаза их встретились дуглас встретился папа знает понял он все таки было задуmano он нарочно привез нас сюда чтобы это сомной случилось он то же в заговоре он все знает и теперь он знает что и я уже знаю большая рука опустилась с высоты и подняла его в воздух покачиваясь на твердых ногах между отцом и томом и сарапанный вострепанный все еще ошарашенный дуглас осторожно потрогал свои локти и были как чужие и судовлетворение облизнул разбитую губу потом взглянул на отца и на тома и понес все в драку сказал он сегодня хочу один все таки ты и загадочно усмехнулись и отдали ему в драку дуглас стоял чуть покачиваясь и его ноша в сесте кающийся соком лесоттягивала ему руки хочупочувствовать все что только можно думал он хочу устать хочу очень устать нельзя забыть ни сегодня ни завтра и после он шлопьяненный со своей тяжело и ношей а занимались пчелы и запах дикого винограда и ослепительное лето на пальцах вспухали блаженные мозоли руки немели и он спотыкался так что отец даже схватил его за плечо и надо пробормотал дуглас и ничего отличного справлюсь еще добрых полчаса оно у щал руками и ногам и спино и траву и корни и кору что словно отпечатались на его теле по немному отпечаток этот стирался а лускользал дуглас шепнул думал об этом а брат молчаливый отец шло позади предоставляя ему одно упролагать путь сквозь лес не правдоподобной цели кшоссе которое приведет их обр а т н о в город и в тот город в тот же день и еще одно откровение дедушка стояла на широком парадном крыльце и точно капитан оглядывал широкие и недвижные просторы перед ним раскинулось лето он в опрошал ветер и не достиг имовысокого неба и лужайку где стояли дуглас и томи в опрошал только о его одного дедушка и он уже созрел и дедушка поскреб подбородок пята соттысяча да же двести с чина верняка да хороший урожай собирать легко соберите все плачу десять центов за каждый мешок который вы принесете к прессу ураа

Висновки:

Набув навичок частотного аналізу та опанував прийомами роботи в модулярній арифметиці на прикладі афінної біграмної підстановки. Також освоїв критерії визначення змістовності тексту.