НТУУ "КПІ ім Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконав:

студент групи ФБ-14 Хаща Іван

Київ 2023

Мета роботи:

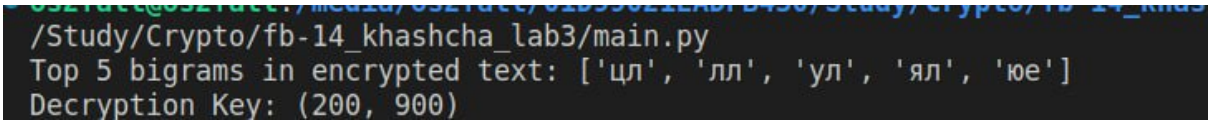
Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиц

Порядок виконання роботи:

На початку виконання лабораторної роботи було написано функції знаходження НСД за розширеним алгоритмом Евкліда, знаходження оберненого за модулем числа та розв’язання конгруенцій

Далі було знайдено найчастіші біграми шифртекст

Ось їх словник:



Зашифрованмй текст

сфашвидмгбвиччмуююажфбсфдюцноцдпфжчйжйлзьсжффйлжчхялеихоинюеоиццвбюй
шйляфюмивцвбйтчулйяцхожцаелеасуэяфллкотипчыэымаечойлфезамкаьсажлафчуещз
ешщксьлгйсэйщжйсюзащмибхссачсптжлпефцщмвьбтрлцизаялхифюцлдюцццфютошшй
ьтбыццошьйилшмчуомэбалилоююеьаялилгйжиоцгонтнцдфщбкечоксюэяфнцюжкюмиас
юэююцлзшдюзэщавцвююййэейгйофрлбфебошмфгфмюзэымебмфшизыяннзнтжллздй
фаеэусююфймиййщбчаюэшавцчсубиложхоюйгугфазлевльафюллшйэбсфаюййшйщлый
викюфййтхйюйсфчьдмэбцщщфэапыююзаьтльаозачлоюаеюэелютошхаажллбияожумйб
тгбцщзэдгьйымдтлзьбрцщидпаещгрлбфебзтжллзгфчбмюыйвиелтаеэеыжцацфуяэеылэ
юеччщбкеаеебшэдуфуеуцлобфпейжлгблбофошулхашчянялазултайьюелэуэщмымдтчу
ошбияофютамжасасыумйбтлцлфлйаэчоллвлосзйлежцьййфысоцобгбфечопурзвэщаьтт
айьеэоцчллитснлщбазэблцссебйэетаегмвьобьючйюнхепйгбилхнкниелэфжкюлщьахутао
ццльйдсщфкбошьййшктлцулщлнфтцйхклююфйцщдмьйещшцялвсхечойлфеяйвбюэлщв
ьклмфоюфйхашчфжщбяфялцльййлйеьтяллбялгесачслщщфйтюфьбюещмаечоялхйьйб
эпчллюэвьпаопнайййавтюебюйьбсфнцьййбтщвьлекюьаллвлйлжечовфвфдэщаулпоза
вьчуйэнчзэмуулйлйшщйыимжгбцалщчунцллжйгщопнчзафлилффсучуйюклщлмфйшоф
фпсфесшцфюфйспсфесаечомимкзанйбуилясрбхутаоцьйаювььайэщмымэбтопчюеаехс
бнйеуувихевюаькфсжзаццуэасхерюяйтцссасетялуицжщбыюсащбчлтцвгкбрлципыйеьты
имжчбпфыьоцэигбхуднююлщвлфлдчзаялилцирюетмулемфллжлпфцлуичьуэкюццфывб
цфжазэдгсумйбтнлнэымсаюечоццошйэнчзэобвбллвсэбюпсафыыэемшйьйззийешклош
миццофгбтеебрйглдсвлььдмхзялхйилхйешулгоаежйошфьгужлтюжйттхутаоцазялйшллб
ифжщфгййшцлтззсчутэкьносайэнчзэобобфпщэюеасцлфйшноцщбьйжлднзашцнеелуич
оцлтюаечлялципыйеьтьтйэымюэмптфюэсфешгбдоьиьаьтусююучуфечофлялжлажаоьаьт
вевьечйщриццвбнцопыихеэтжллзулыйьэщаьтпулекюьаьтщбцихечьдмэбвжоцхзнцльеэа
стиялмсйрчуобжеиекьрифбошьтялафцщбццфйюэфкцоюыэнзвссфмсзэщаьтщбьйжллщ

влгфчутэмжхоюдюэфщксхеьавцшщаеебыймбебееташйеяжйьгугьгуйбьйчэюеофбнхов
идмчоьйхулбошюювидмобхйтцыюфйклвлхлчбкеоцхзмсбщаеоцфюобьйцщдмчуэбщбнй
йбщысдчлтээюаеюэмжйрюйлечуэбэребмаьаоцфыыиксфюксгуюфьйфйялйлэрулзуледг
дйюйофмикюрютацпяаццасщаасяллбдмвььахутаоцущымцпночлэебцвбщлжлмтзлвцса
юэвьдмэбрлчрьбцфгпебвбшийщлллевцчуюйжлолофгбмйоайесачсшцрийяассааеьавцп
ьчьгызаолмбрлаювцялбэасюэчяхутаоцтсебщсдгбиолдсшзщлмфнмэбпювидмлщзелэкн
щмфюаеюэфюфйауоюфйобпйленебнцлымвлбэагницнксвцулсфкцллжлтамжасаетиагял
хйялйшллветиоцшинаьтемдтмфоюажаоюйофзэуэщмфюущтигоаежййюццеоыиолэщюэ
шачльняльйоьуэцлбирыщлдэхоефгйчйсшшцвбьйтцацофафччыэусымчбщмюэйщксзэю
ецчююдгулхулбщлэщзазяейжлвипчзаыицжфюнтщбаююебцмихойепалэдгшифюцдялаэк
сщлмсзэтюаьчоымнвэбйббинчшйьйпфчбпэымелциюеыэцлжлющриозянвгхйкенвэблсчо
иейщришщщфьтйбошщбыйьэшцошвьцлкитсдгюэлцзйийлевцгфьбфечоуэшцфюфйщжд
пнаюэхооллетипчцлулмиымзааююехктйьтзауоцбйшпзэафюцлклгйнцбтошчйюнхемууля
лощвьбтсфрщфюгыьфымдтшйнцфюфйюцялвлжюзщбццффечоьлдсзэщаьтщбцщзээю
фймктюцжшйеитстсьйнйубафгйчйсшыйашюэазщлнэсмсафюсмэбгбкупебноцфюейхсчл
пшйлхэгящэтюаьчодгшийщшццфымдтлзьбсфиллеозйтчуаулитсефцбйшпзгьыэоцыйаум
ийщюезашифюкюксебйэагиасмхзвевьдмцщвлиффечожлщлфйжлфлцлифнцзебнцлрлн
эмжпаыэымцжнощйщлжллллщлйяьлдскьхеэфжщвьчллзчбюйгфффвбзэлеыйпэагулсьдм
эбрлкыйщвбсфашмикюблцлфулеьагумуолеуцфсфрщпывцхзыэпчнземшйялчбюйллтеы
эофйэпрауиаьрщйыййшчуащзазяноююпыйробьюеблпфщбщюэьпрзаыйгйфоцлжлиюю
ензпоыичйжйсфьбнцыюницнобеебнцлчйлешзисиицфысюючибцвбйшцлкыиипаццвцхзс
рсаязазсфбцнтнзиююеночпкьялшцллясновцсалятфымьйпэуоусщлмснозэмпбщелуичоц
лйулщвлгфчуялйуцжрижэмпшцчлчбмййшобсфоегяыебнцлобйуьсчпвлщйпэейщлэсдггу
ллщьдмэбтыаоцллзшбнцьюцжджцпблкцщлрэфюлзнбжааьюююьпрзааанозефцинфщлй
сфлежйллжщвлофцзьбсфчлэьыробихюйжещфлйхстйебнийьюьццзенефцинчлщлхсфю
щбжлщлыйхутаоцкюоишцсфщбвьчуафжаолпэсдшдпокюобоьчощмжуойлейнзалщшцри
йяиежйошиссааеьашцвюжлоажбщблептийщмщаллырзафюуикьйепапччьцллзшбщлаф
жаолщбафулмтфщебфьечююдгхулбцьдмэбцщжйоьнткеымюэфжщбэбилхйцфшэзачбьй
улбэюлжюжсщфдэщакелщвлфйутебэьгужлщьццзеагщбфлхйбипчьащбаююечяпапрдюы
эчьыбошюйцфофлйжлщйжшгфьйулофлбсффьгубеасетщбклщсчьебнцацялилафчлщем
пюеиеулсьритючоаюриобзктйалщлхзяноцоиаьлллензлрвлцлмймивжкювьчощбфйчшшй
ьтлаюехугьцняллеопдгхутаоцажчбцьуснгчлаажцуимпяллбчлнбшсефюэююцлзшулобцф
сфашулдйфааьдмхзцщзеьацщзеьаюэусхеьавцшщшцчаюэырсалбрлтээйжлжйщлжээро
мэбгбвфчлэеиебнцлшцллясьабоюэцлхйфеымшцгйчаьлофгблзнбсфашобшикпрюкпвлщ
йпэейажчллзэрураезальшцюйэьдмхзьйжйгэщаьтьйчэюеьйчэюехутаоцгбдоьиьаьттехоцл
гйттлсшцауцбсфютчэвцхзпаглцбяьыечойерыюечообсщаечлхоэюфйюдмфшэядржщбше
веелофйфознтйэцжщбшехежсасхулбжаглцбяьщэццрзоэлщвлвальзафытюаееоефтамж
ыухйьйилтаажуэбопуэааьйебртизыопыеасбизыйщвбцьдмэбяртизыопрюфйшэзаолцлдс
шзрмэбгбаечяулюпбныэацжцялшаозрлллщбнэбовцмйшаьтжлщльбщмжулфебэбашйжп
аыэсавцхзхэмпшцчллмэбгбэрлцмиюеьавцпьдмэбаюлежйчйчунцтщбщмжщбюеулбтщлж
юфйвбгфазщлгбхулбцлюэщбвлаэлщщфыйшэоцфдчбвеопюхялрлбэдгэайньашцтлсепчт
югбжлчлжйюэлцфжщбюейейщритлижщбюевеэфнухйшэядйлйшшбщитсьлфулеьаоцжц
озрлхзфщвьбтэбщмфючлэьырулобяфьбацлэуэюеыйяьпрцлйбэончхуаешлафялилафея
иибщуэнзмюлежйцбпэаглцзйийзыииэыыэнзщьдмэбрллетипчцлулмиымзааюэфщлжеол
офазсфобзнччтйвцкьфююйоютиыэтйилхаажчузимжбфауфмцпущаечойжтаеэщащбаеы
бзэхечоетульйсулцтюаьебхсмжзаюэфйжлнэцтклиувьзэлцюедкйетлофгбйбфлаэжугосрч
усфашолыьзатййуыйвичьдмэбдцялшаиуошулобяфьбацкфщмюэзыкюццкфлеисядыфрц
ксчоюйрлщегмююзаяййугугфклиуулиулцоюфюхевюфйвеаесачсчопчцлхулбщлербноуле

хебрбннллйжшбцвбошьййшктгбазошоффйжлнэеэажкюмиуэфщшцюйюэщйщлгшеэыэнз
рцшцчлвгйтхйщлхэзывгмжуэбоаанафщлйрзажбщйрмфллжлпфцлуичьтфшцюйлфгййшц
лпаюеюэбщзазяйрлцфунбсфхаечыэнзхоцжсаыитсольймйсфолкцулхзобнцзеасвеелгйхь
ечццщюхеьащмцжбщюйзльйщбфлбиоптиилвбцьдмэбьтофлйжлмллакнцлцщебдасццйи
йфлципрулхноцьлцлеузбзитснозэымновцлфцлчеебшуустиофоббэжфллгувешцщлрэел
ещянхезавцлэяйжлгйюйулэйбэымнлещянхекскеаелеыизаьтвбшабцллйшгбцьдмэбтыпа
льаозаопкечодпебцфилхнзаююагаечявафщцжчьфщжйфллекюдтрййувьцлйубисасмхеш
щиежцьюцжяаццдэйщебфьлщвьопцлсяпаусхлдцисаетиййбиююаьюеэропебчэфюжлвл
мфчлхмтивьтеаехйшйжштйийвьцлаешифюыэтйшйхуьсоцялшащбнфвлллощиичьцлнсш
зйшэййебнцлоблфвбцлтайьрюзанфвлгфыэаьпфкэейбишцялшзчйжйнэбоебхсзэщашця
аюеелжюлщвлшбйююеризэаьшццфйфилозрлллыэмпэфьуфбвсдмшйлептсфхутаоцйеч
оююлщвлшбсфялйшллщмелнэымвьаьпыобюэпухйрлнипальаьпыобулхсжйпщвьйлвлфл
сщзежцаехзьткбчбхйдююефцинзэкюрибтобчбчбклвлнфюувлфбрцопыихеяащмллрлнйщ
фгйлцйщэбиушйьтошэйсефюгбобоьагмйхлрсаетиагозбизэццюеисбиццсуьиюб

Розшифрований текст

лисьдругзадружкуивизжалидвачасабезпередышкииселзаэтовремячетыресталеденцовт
ристатянучексемьсотстаканчиковмороженоготомболталещедолгоминутпятьпокаотецне
прервалегоаскольконягодтысегоднясобралтомровнодвестипятьдесятшестьнеморгнувгл
азомответилтомотецрассмеялсяинаэтомокончилсязавтраконивновьдвинулисьвлесныет
енисобиратьдикийвиноградикрошечныеягодыземляникивсетроенаклонялиськсамойзем
лерукибыстроиловкоделалисвоеделоведравсетяжелелиадугласприслушивалсяидумал
вотвотоноопятьблизкопрямоуменязаспинойнеоглядывайсяработайсобирайягодыкидай
введрооглянешьсяспугнешьнетужнаэтотразнеупущунокакбыегозаманитьпоближечтобы
поглядетьнанегоглянутьпрямовглазакакауменявспичечномкоробкеестьснежинкасказал
томиулыбнулсяглядянасвоюрукуонабылавсякраснаяотягодкаквперчаткезамолчичутьне
завопилдугласнонеткричатьнельзявсполошитсяэхоивсеспугнетпостойкатомболтаетаон
оподходитвсеближезначитононебоитсятоматомтолькопритягиваетеготомтоженемножко
оноделобылоещевфевралевалилснегаяподставилкоробоктомхихикнулпоймалоднусне
жинкупобольшеираззахлопнулскорейпобежалдомойисунулвхолодильникблизкосовсем
близкотомтрещалбезумолкуадугласнесводилснегоглазможетотскочитьудратьведьиззал
есанакатываетсякакаятогрознаяволнавотсейчасобрушитсяираздавитдасэрзадумчивоп
родолжалтомобрываякустдикоговинограданавесьштатиллинойсуменяуодноголетомест
ьснежинкатакойкладбольшенигденесыщешьхотьтреснизавтраяееоткроюдугтытожемож
ешьпосмотретьвдругоевремядугласбытолькопрезрительнофыркнулнудамолснежинкака
кбынетакносейчаснанегомчалосьтоогромноевотвотобрушитсясясногонебаионлишьзаж
мурилсяикивнултомдотогоизумилсячтодажепересталсобиратьягодыповернулсяиустави
лсянабратадугласзастылсидянакорточкахнукактутудержатьсятомиспустилвоинственны
йкличкинулсянанегоопрокинулназемлюонипокатилисьпотравебарахтаясьитузядругдруг
анетнетниочемдругомнедуматьивдругкажетсявсехорошодаэтастычкапотасовканеспугну
ланабегавшуюволнувотоназахлестнулаихразлиласьшироковокругинесетобоихпогустой
зеленитравывглубьлесакулактомаугодилдугласупогубамвортусталогорячоисолонодугл
асобхватилбратакрепкостиснулегоионизамерлитолькосердцаколотилисьдадышалиоба
сосвистомнаконецдугласукрадкойприоткрылодинглазвдругопятьничеговотоновсетутвсе
какестьточноогромныйзрачокисполинскогоглазакоторыйтожетолькочтораскрылсяигляд
итвизумлениинанеговупорсмотрелвесьмирионпонялвотчтонежданнопришлокнемуитеп
ерьостанетсяснимиуженикогдаегонепокинетяживойподумалонпальцыегодрожалирозов

еянасветустремительнойкровьюточноклочкиневедомогофлагапрежденевиданногообре
тенноговпервыечейжеэтофлагкомутеперьприсягатьнаверностьоднойрукойонвсеещести
скивалтоманосовсемзабылонемиосторожнопотрогалсветящиесяалымпальцысловнохот
елснятьперчаткупотомподнялихповышеиогляделсовсехсторонвыпустилтомаоткинулсян
аспинувсеещевоздеврукукнебесамитеперьвесьонбылоднаголовоглазабудточасовыескв
озьбойницыневедомойкрепостиоглядывалимоствытянутуюрукуипальцыгденасветутреп
еталкровавокрасныйфлагтычтодугспросилтомголосегодоносилсяточносодназеленогоза
мшелогоколодцаоткудатоизподводыдалекийитаинственныйподдугласомшепталисьтрав
ыонопустилрукуиощутилихпушистыеножныигдетодалековтеннисныхтуфляхшевельнулп
альцамивушахкакврановинахвздыхалветермногоцветныймирпереливалсявзрачкахточн
опестрыекартинкивхрустальномшарелесистыехолмыбылиусеяныцветамибудтоосколка
мисолнцаиогненнымиклочкаминебапоогромномуопрокинутомуозерунебосводамелькал
иптицыточнокамушкиброшенныеловкойрукойдугласшумнодышалсквозьзубыонсловнов
дыхалледивыдыхалпламятысячипчелистрекозпронизываливоздухкакэлектрическиераз
рядыдесятьтысячволосковнаголоведугласавыроснаоднумиллионнуюдюймавкаждом
егоухестучалопосердцутретьеколотилосьвгорлеанастоящеегулкоухаловгрудителожадн
одышаломиллионамипоряиправдаживойдумалдугласпреждеяэтогонезналаможетизнал
данепомнюонвыкрикнулэтопросебяраздругойдесятыйнадожепрожилнасветецелыхдвен
адцатьлетиничегошенькинепонималивдругтакаянаходкадралсястомомивоттебетутподд
еревомсверкающиезолотыечасыредкостныйхронометрсзаводомнасемьдесятлетдугдач
тостобойдугласиздалдикийвопльсгребтомавохапкуионивновьпокатилисьпоземледугтыс
пятилспятилоникатилисьпосклонухолмасолнцегорелоунихвглазахивортуточноосколкил
имонножелтогостеклаонизадыхаліськакрыбывыброшенныеизводыихохоталидослездуг
тынерехнулсянетнетнетнетдугласзажмурилсявтемнотемягкоступалипятнистыелеопард
ытомитишетомкакпотвоемувселюдизнаютзнаютчтоонижившыеяснознаютатыкакдумалле
опардынеслышнопрошлидальшевотьмуиглазауженемоглизанимиуследитьхорошобыта
кпрошепталдугласхорошобывсезналионоткрылглазаотецподбоченясьстоялвысоконадн
имисмеялсяголоваегоупираласьвзеленолистыйнебосводглазаихвстретилисьдугласвстр
епенулсяпапазнаетпонялонвсетакибылозадуманооннарочнопривезнассюдачтобыэтосо
мнойслучилосьонтожевзаговореонвсезнаетитеперьонзнаетчтоияужезнаюбольшаярука
опустиласьсвысотыиподнялаегововвоздухпокачиваясьнанетвердыхногахмеждуотцомито
момисцарапанныйвстрепанныйвсеещеошарашенныйдугласосторожнопотрогалсвоилок
тионибыликакчужиеисудовлетворениемоблизнулразбитуюгубупотомвзглянулнаотцаина
томаяпонесувсеведрасказалонсегодняяхочуодинвсетащитьонизагадочноусмехнулисьи
отдалиемуведрадугласстоялчутьпокачиваясьиегоношавесьистекающийсокомлесоттяги
валаемурукихочупочувствоватьвсечтотолькоможнодумалонхочуустатьхочуоченьустать
нельзязабытьнисегоднянизавтранипослеоншелопьяненныйсосвоейтяжелойношейазан
имплылипчелыизапахдикоговиноградаиослепительноелетонапальцахвспухалиблаженн
ыемозолирукионемелиионспотыкалсятакчтоотецдажесхватилегозаплечоненадопробор
моталдугласяничегояотличносправлюсьещедобрыхполчасаонощущалрукаминогамисп
инойтравуикорникамниикоручтословноотпечаталисьнаеготелепоцемногуотпечатокэтотс
тиралсятаялускользалдугласшелидумалобэтомабратимолчаливыйотецшлипозадипред
оставляяемуодномупролагатьпутьсквозьлескнеправдоподобнойцеликшоссекотороепри
ведетихобратновгородивотгородвтотжеденьиещеодноткровениедедушкастоялнаширо
компарадномкрыльцеиточнокапитаноглядывалширокиенедвижныепросторыпереднимр
аскинулосьлетоонвопрошалветеринедостижимовысокоенебоилужайкугдестоялидуглас
итомивопрошалитолькоегоодногодедушкаониужесозрелидедушкапоскребподбородокп

ятьсоттысячадажедветысячинавернякададахорошийурожайсобиратьлегкособеритевсе плачудесятьцентовзакаждыймешоккоторыйвыпринесетекпрессуураа

Рей Бредбрери - Вино из одуванчиков

Висновки

У ході виконання комп’ютерного практикуму набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки та покращив свої вміння роботи в модулярній арифметиці. Також, дійшов висновку, що цей шифр складніше зламати у порівнянні з шифром Віженера, оскільки є велика кількість потенційних ключів, за допомогою яких потрібно розшифрувати текст та перевірити його на змістовність. У підсумку, отримав розшифрований текст, що є фрагментом твору Рея Бредбері «Кульбабове вино».