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

Виконала:
Студентка 3 курсу
Гузенко Г. С.
Перевірив:

Київ – 2021

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

Завдання:
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 (a,b) шляхом розв'язання системи (1).
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

Я почала з функції знаходження оберненого значення за розширеним алгоритмом евкліда, тут було трохи складно придумати механізм накладання алгоритму на рекурсивну функцію, тому по виведеним формулам я зазначила, що при остаточному знайденому значенні x, маємо a і b відповідно 1 і 0, які потім вираховуються при кожному поверненні функції. У функції рішення лінійного рівняння я опрацювала усі можливі випадки.

Для кращого розуміння одразу реалізувала функції шифрування та дешифрування. У функції знаходження 5 найчастіших біграм, я спочатку формую усі біграми а потім за допомогою Counter.most_common(6), знаходжу 5 найчастіших біграм та повертаю їх.

['тд', 'рб', 'во', 'щю', 'ет']

У функції all_posible() я одразу для зручності знаходжу усі можливі комбінації найпопулярніших у мові та найпопулярніших у шифротексті біграм (по дві пари за умовою, для зручного розшифрування).

У функції keys я створила ключі, при усіх можливих комбінаціях біграм, отриманих з попередньої функції. За допомогою функції рішення лінійних рівнянь я знаходжу першу змінну(це необхідно задля обробки усіх

можливих рішень одного рівняння), та далі створюю усі можливі пари ключів за отриманими a і b, які перед цим перевіряються на умові.

Далі у функції true_keys, я проходжусь по усім отриманим ключам, та дешифрую текст, при цьому одразу перевіряю частоту найпопулярніших букв і записую ключ у масив, коли кожна найпопулярніша/найрідша буква у розшифрованому ним тексті, збігається з буквами мови. Після, я знайшла 3 ключа з найчастішими входженнями, підійшов ключ **[199, 700]**.

Зашифрований текст:

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпв
оыомхзотхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэ
шжцюлцлхйостщюшужхриажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщюзншбхюэотйбав
отдцюэшшылхщюабпоябцикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюм
хэшухэозоихщюкцзоюбзюгсвичхшццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфь
анэйсужушюстлхэдвоэомюфожхетжютдцюгршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцт
йнбщддцывкцхнцхеоцэвбйбышкдэйюейосежхюбгцэюубйутодткдвощхщющцяюстудвежю
нхэджядшищвччощщвунойхзозпцэфтмефпшхтдпощщщыкдвуозеойбдэзэстсдоожмиврбгхн
ойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрстднтщюфпвцукеоетитмшпнчхшцабшшлсцбу
хкйэыбдтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлыйбсуодмзеоэотэкшфстднтщюфпк
дютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмшшзцт
йищцюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихк
ттщюжонжсиодгуоддйучяожстднтжхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюе
хлцбретйхцпвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвцхндншбчбжуэтихшцвзеокэх
ытцажшбэйчтцпчээыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншшвуйжышьтджфиц
хеогбшшанжхтдпнягвофихыыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтп
юцпжхдйержюкшйбтдщдзщяоыбэлгтфдэйетзэстйуэлетмюшюыхнцхтцпвотдучеощищыний
ькосотыкддйсуюгкцхнрбвотдьздйирэттднттющсзйэысесдвейхаирбтюзсжжйбщддццнтдэйй
бюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотдднщддцбаабжукцеочтйхвюеыдйрббдфхдйыж
хшшшщаышиткчсняощщуогбажбфьащелбхшзцтйищцюнхктсджданершецшмбзнбрфоюбол
охехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяормлзсдцэфпкчшюкэфо
щщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкдыспнкчнжрбво
тдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэющощ
щтокшеронцчшццнджфитджюкцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбв
отдыгзнкдютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндт
цоохлсбанднбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдх
шкдысжхкйгхбжйуолэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяш
шеокояншдкцмеввнмжхетжютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшернбйедшзцтй
ищцюджфицхяберстфпвоэуажкбруатеоахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцт
жбфоилсуюыяшшеокояащелбучиххцхнрбвонстднбансюуйщодэнтихыбюешюыхнцхтцпетщ
цжжйбвотддцитвожюшцбдшшсущантсофогбсурржцзожюдюяюэоддтххгнхщюжбзнкофтжд
жцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухвцщоыояоетктйхэдетэьвугцышшсажкбг
цфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждннььгррщюцйюгдткуюг
аюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзйзцвоьый
бсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэст
удобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькюдурбщдфхгжеы
никоьбгцэюйбрбднтцэюлжгажющощщкющанмжюйорршхжхщюфмэощняюабгххсййбргшз

цтйищцюжхинфиывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябру
еыохпыыжкьцчгдзюшхыбфшвуйжышэшзцтйищцювснхеокшзожххцлжкбьхвцньйбгцшхщстх
вюфпгдхыпюнонбажщдьзкцсюмотэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужхщюю
юетнобюхнщютшкчншкчбохсжхыйбркююышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюш
бхфньхытцодгжабйбхфйужцбретщюудшшйсвишдбеьжрбйеооьжзцэющоеоаэзбвмнищдве
етштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщхжхтцмхрыонцчшццнйиеыанву
щоыылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхшцбдлзеоушйбяхщоцща
нкдьгнхтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхтдьжрбгхооюыв
ющючтсдвеетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгцитцпво
хсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбз
цлхгбущдйнищдгждццщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцпт
дтхнгкцеоубхфкцтхшммыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэт
сдатлцпнвотдхшкдэйолэтзйеретхжвгажщаиашдбншдкцжхыболиндйчетдажгцситцэюмхэш
сущцитвожюшцшуерюмтцшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбрщ
юэтсдбоцпштмыкдохьбгцфпибшшернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгр
бгхшсшпцэкдлттдкгрбвмнищдрианлххнэйрбгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгх
жючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднттюхлдшшшитщостжошсзхтдьжрбгхмюл
бпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбяхщоцщаняюепмтцпжхофюекйу
хощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючотхтдэиыжюбдыюмни
щдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйерййнбьзрбйешхвимб
сурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдвеатлцпнчэсклх
шхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнг
сштввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотду
хвцщохсгтфдньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпоойерягррщюк
эиннисуюхыогцщарбвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюбп
окйфигжщддцлхксввсущантсофочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфпт
цэочоьбгцфпчочобоацлжолфтьюжтфпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютжд
кдртнтфддйшюыхнцхтцпвотдсуыищаднсейузйнбьхдретыбрущоьыйбрбитшхыошсзхтдстнт
ыбюлпюыыеоьывюатошанкудйэюфоюбэйзцкуодвюстфпэтщоеовикцхнлхщюкцооньщечощ
щвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрвмкдгжэащдрощщсиюасцитф
пкдьоицжувундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютддйьзкцсюбцсучдвуанд
шеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсесдверианлххнэйрбгхыян
битйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтддцси
тцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхв
ияжьзвотдучяоехфдвукдюткйтцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююи
ндйчевостююхцяхщюкоушнбднеокоацяхжхитсюоюйянбэюцпчэдйщтощцюйиеыаншшвуйж
ышьтфоэсцркьзозбндфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьюворнтнфддйк
дютгцитсдвейхагкцжуружхеогсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпве
шбрбдntцфпйотдухвцщоыощощщюггжнбгхкудйэюждвудрзохскдыстднбанщдвехызцчэшхд
жщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудвеетнхлхгтэдерйетдажбйщтцпвотдучвцйудйп
рэвщдшдэыдйут

Розшифрований текст:

отцеубийствокакизвестноосновноеиизначалыноягрестнглениечеловечестваиотделыноцоч
еловекавовсякомслучаеонфплавньйисточникчувствавиньнеизвестноединственньйлииссле
дованиямнеудалосыещеустановитыдушевноепроисхыждениевиньипотребностиискнглен
ияноотнюдынесзщественноединствебньйлиэтоисточнидгсихологическоеположениесложн

оинуждаетсявобясненияхотношениемалычикакоткукакмвповоримамбивалентнопомимон
енавистииззакоторойхотелосыбьотцакаксигерникаустранитысзществуетобьчноншкоторая
долянежностикнемуобаотношениясливаютсявидентификациюсотцомхотелосыбьзанятым
естоотцщготомучтоонвьзьваетвосхищениехотелосыбьбьтыкаконипотомучтохочетсялпоуст
ранитывсеэтонаталкиваетсянакрупноепрягятствиевигределебньймоментребенокначинае
мгониматычтопопьткаустранитыотцакаксигерникавстретилабьсостороньотцанаказаниече
резкастрациюизстрахакастрациитоестывинтересахсовранениясвоеймужественностиребен
окотказьваетсяотжеланияобладатыматерыюиотустраненияотцщгосколыцуэтыжеланиеост
аетсявобластибессознателыноцооноояоляетсяосновойдляобразованиячувствавиньнамкаж
етсячтомьигисалинормалыньягроцессьобьчнуюсудыбутакназьваемоцоэдвговакомплшкю
аследуетоднаковнестиважноедигвлнениевозникаютдалынейшиеосложнения яслиуребенк
асилынееразвитконституциобньйфакторназьваемьйнамибиеексуалыностыютогдщгодщпр
озогготеримужественностфчерезкастрациюукрягляетсятенденцияуклонитысявсторонужен
ствебностиболеетфпотенденцияпоставитысебянаместоматеривгеренятыеервлыкакобшкт
алюбвиотцаодналишзбоязныкастрацииделаетэтуразвязкуневозможнойребенодгонимает
чтоондолженвзятынасебяикастрированисеслионхочетбьтылюбимьмотцомкакженжинатак
обршкаютсянавьтеснениеобапорьваненавистыкоткуивлюбленностывотцаизвестнашгсихо
логическаяразницаусматриваетсявтомчтоотненавистикотцуотказьваютсявследствиестрах
щгередвнешнейопасностыюкастрациейвлюбленностожевотцаволгринимаетсякаквнутрен
няяопасностыпеэвфчноцопозьвакоторашгосутисвоейсновавозхращаетсяктойжевнешнейиг
асностистрахпередотцамделаетненавистыкоткунеприемлемойкастрацияужаснакаквкачес
твшкарьтакиценьлюбвиизобоихфакторовввьтесняющихненавистыкоткупеэвьйнепосредств
ебньйстрахнаказанияикастрациисследуетназватынормалыньмпатогеническоеусилениепри
вноситсякаккажетсялишыдругиафакторомбоязныюженственнойустановкиярковьражебна
ябиеексуалынаясклонностыстановитсятакимобразомоднимизусловийилиподтверждений
неврозаэтусклонностыочевидносследуетпризнатыиудостоевскоцоионалатентнаепомосшкс
уалыностыпрояоляетсявдозввленномвидевтомзначениикакоеимелавлпыжизнидружбасм
ужчинамивецодострабностинежномотношениихсоперникамолюбвиивлпигрекраснотгони
манииположенийобяснимьхлишывьтесненноппомосшксуалыностыюкакнаэтоуказьваютм
нфпочислебньепримерьизецопроизведенийсожалеюнонфчлпонемфпуизменитыеелвгодр
онностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозькастрациинесв
едзщемувпсихоанализечитателюпокажутсябезвкусньмиималовероятньмвгреюгвлжпаючт
оимебнокомплшкскастрациибудетотклоненсилынсевслпоносмеюуверитычтигсихоаналит
фческийопьтставитимебноэтиявлениявневсякфпосомнения яинаходитвнихключклюбомуне
хрозуилгьтаемжсецовслучаетакназьваемойцгилягсиинашлпигисателянонашемусознаниют
акчуждьтеяолениявооластикоторьхнаходитсянашабессознателынашгсихическаящизныука
забньмвьшенеисчекгьваютсявэдвговомкотглексягоследствиявьтесненияненавистикоткуно
вьмяоляетсяточтовконцеконцовотыждестолениесотцомзавоевьваетвнашемяпостоябноем
естоэтоотыждестолениеволгринимаетсянашимянопредставляетсобойвнемособуюинстанц
июпротивостоящуюосталыномусодержаниюнашецоямьназьваемтфпдаэтуинстанциюнаш
имсверхяипрвгисьваемейнаследницеродителыскоцоолияниянаиважнейшиефункцииесли
отецбьчсуровнасилыственжестокнашесверхшгеренимаетотнлпоэтикачестваивлпоотношен
иикясновавозникаетпассивностыкоторойкакразнадлежалобьбьтывьтеснебнойсверхястало
садистическимястановитсямазохистскимтоестывосновесвоейженствебнигассивньмвнаше
мявозникаетболышашготренностывнаказанииияотчастиотдаетсебякактаковоевралгоряже
ниесудыбьотчастиженаходитудовлетворениевжестокомобращениинаснимсверхясознаниев
инькаждаякараявляетсяведывосновесвоейкастрациейикактаковаяосуществолениемизнача

лынфпигассивнфпоотношениякотцуисудыбавконцеконцовлишыдалынейшаяпроекцияотц
анормалыньеявленишгроисходяжиягриформированиисовестидвлжнхгоходитынаопиюаб
ньездесыанормалыньенамещенеудалосыустановитыразгранфчениямеждунимизамечаетс
ячтонаибвлышаяролыздесывконечномитфпягрипиcьваетсяпассивньмэлементамвьтеснен
нойженствебностиищекакслучайньйфакторимсетзначениеяоляетсяливнушающийстрахот
ецивдействителыностиособебнонасилыственньмэтоотносится кдостоевскомуфактлпоискл
ючителыноцочувствавиньравнокакимазохистскфпообразажизнимьсводимкецоособенноя
рковьражебномукомпонентуженствебностидостоевскоцоможноопределитысследующимо
бразомособебносилынаябиеексуалынашгредрасположебностыиспосонностысособойсило
йзажищатысяотзависимостиотчрезвьчайносуровоцоотцаэтотхарактербиеексуалыностимп
добавляемкрансеузнабньмкотгонентамецосуществарабнийситготгрипадковсмертиможн
орассматриватыкакотождествлениесволпоясотцомдопущебноевкачественаказаниясостор
оньсверхятьзахотелубитыотцадабьстатыотгомсамомутягерытьотецноотецмертвьйобьчньй
механизмистерфческихсимптомовиктомужетеперытебяубиваетотецдлянашецоясимптомс
мертиявляетсяудовлетворениеафантазиимужскфпыжеланияиодновремебномазохистскит
госредствомнаказаниятоестысадистическимудовлетворениемобаяисверхяопраютролыот
цаидалышевобщемотношениемеждулфчностыюиобектомотцаприсохранениицесодержа
нияперешловотношениемеждуяисверхяноваяинсценировканавторойсценетакиеинфантил
ыньереакцииэдвговакомплшкюамогутзжплохнутыеслидействителыностынедаетимвдалы
нейшемпижинохарактеротцаостаетсятемжесамьмнетонухудшаетсясцодамитакимобразом
продвлжаетоставатысяиненавистыдостоевскоцокотцужеланиесмертиэтомузломуоткустан
овитсяигасньмеслитакиевьтесненньежеланияосзществляютсянаделефантазиясталареалы
ностыювсемерьзащитьтягерыа