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:
Дворніков Дмитро
Варіант 8
Група:
ФБ-03

Київ - 2022

Мета роботи

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

Хід роботи

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).

Завдяки написаній модифікованої функції counter, яка була зроблена у минулій роботі, отримуємо наші біграми. Отже п`ятірка найчастіших біграм у моєму шифротексті:

[('дэ', 72), ('цэ', 71), ('жц', 69), ('нц', 61), ('оц', 61)]

У цьому масиві кожен елемент має на першому місц біграму, а на длругому її числове представлення для роботи з афінним шифром. Після цього знаючи найчастіші біграми у російській мові можемо перейти до подальшої роботи, а саме до дешифрування нашого шифротексту.

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 змістовим текстом російською мовою, відкинути цього кандидата. 5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Завдяки функції find_key отримав правильный ключ: **(17, 94)**

Для перевірки змістовності тексту вирішив використовувати перевірку завдяки ентропії. Для розшифрованого тексту з кроком 1 ентропія повинна бути **> 4.5**, а з кроком 2 **> 4.2**.

Розшифрований текст

мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтонаводн
яютвесьмирпереплескиваютсяслужаекнамощеныеулицытихонькостучатсявпрозрачные
окнапогребовнезнаютугомонуиудержуивсевокругзаливаютслепящимсверканиемраспла
вленногосолнцакаждоелетоониточносцеписрываютсясказалдедушкапустьихянепротивв
онихсколькостоятгордыекакльвыпосмотришьнанихподольшетакипрожгутутебявглазахд
ыркуведьпростойцветокможносказатьсорнаятравниктоеенезамечаетамыуважаемсчита

емодуванчикблагородноерастениеонинабралиполныемешкиодуванчиковиунесливнизвп
огребвывалилиихизмешковивотьмепогребаразлилосьсияниевинныйпрессдожидалсяихо
ткрытыйхолодныйзолотистыйпотоксогрелегодедушкапередвинулпрессповернулручкуза
вертелбыстрейбыстрейипрессмягкостиснулдобычунувотвоттаксперватонкойструйкойп
отомвсещедрееобильнеепобежалпожелобуврглиняныекувшинысокпрекрасногожаркогом
есяцаемудалиперебродитьснялипенуиразлиливчистыебутылкиизподкетчупаионивыстр
оилисьрядаминаполкахпоблескиваявсумракепогребавиноизодуванчиковсамыеэтисловат
очнолетонаязыкевиноизодуванчиковпойманноеизакупоренноевбутылкилетоитеперьког
дадугласзналпонастоящемузналчтоонживойчтоонзатемиходитпоземлечтобывидетьиощ
ущатьмиронпонялещеоднонадочастицувсегочтоонузналчастицуэтогоособенногоднядня
сбораодуванчиковтожезакупоритьисохранитьапотомнастанеттакойзимнийянварскийден
ькогдавалитгустойснегисолнцаужедавнымдавноникто невиделиможетбытьэточудопозаб
ылосьихорошобыегосновавспомнитьвоттогдаонегооткупоритведьэтолетонепременнобу
детлетомнежданныхчудесинадовсеихсберечьигдетоотложитьдлясебячтобыпослевлюбой
часкогдавздумаешьпробратьсянацыпочкахвовлажныйсумракипротянутьрукуитамрядзар
ядомбудутстоятьбутылкисвиномизодуванчиковонобудетмягкомерцатьточнораскрываю
щиесяназарецветыасквозьтонкийслойпылибудетпоблескиватьсолнценынешнегоиюнявз
глянисквозьэтовинонахолодныйзимнийденьиснеграстаетизподнегопокажетсятраванаде
ревьяхоживутптицылиствацветысловномириадыбабочекзатрепещутнаветруидажехоло
дноесероенебостанетголубымвозьмилетоврукуналейлетовбокалвсамыйкрохотныйконеч
ноизкакоготолькоисделаешьединственныйтерпкийглотокподнесиегокгубамипожиламтв
оимвместолютойзимыпобежитжаркоелетотеперьдождевойводыконечноздесьгодитсятол
ькочистейшаяводадальнихозерсладостныеросыбархатныхлуговчтовозносятсяназарекра
спахнувшимсянавстречунебесамтамвпрохладныхвысяхонисобиралисьчистоомытымигр
оздьямиветермчалихзасотнимильзаряжаяпопутиэлектрическимизарядамиэтаводавобра
лавкаждуюсвоюкаплюещебольшенебескогдападаладождемназемлюонавпиталавсебявос
точныйветеризападныйисеверныйиюжныйиобратиласьвдождьадождьвэтотчассвященно
действияужестановитсятерпкимвиномдуглассхватилковшвыбежалводвориглубокопогру
зилеговбочоноксдождевойводойвотонаводабылаточношелкпрозрачныйголубоватыйшел
кеслиеевыпитьонакоснетсягубгорласердцамягкокакласканоковшиполноеведронадоотне
стивпогребчтобыводапропиталатамвесьурожайодуванчиковструямиречекигорныхручье
вдажебабушкавкакойнибудьфевральскийденькогдабеснуетсязаокномвьюгаислепитвесь
мириулюдейзахватываетдыханьедажебабушкатихонькоспуститсявпогребнаверхувболь
шомдомебудеткашельчиханьехриплыеголосаистоныпростуженнымдетямоченьбольнобу
детглотатьаносыунихпокраснеютточновишнивынутыеизналивкивсюдувдомепритаится
коварныймикробитогдаизпогребавозникнетточнобогинялетабабушкапрячатотоподвяза
нойшальюонапринесетэтоттотовкомнатукаждогоболящегоиразольетдушистоепрозрачн
оевпрозрачныестаканыистаканыэтиосушатоднимглоткомлекарствоиныхвременбальзам
изсолнечныхлучейипраздногоавгустовскогополудняедваслышныйстукколестележкисмо
роженымчтокатитсяпомощенымулицамшорохсеребристогофейерверкачторассыпаетсяв
ысоковнебеишелестсрезаннойтравыфонтаномбьющейизподкосилкичтодвижетсяполуга
мпомуравьиномуцарствувсеэтовсеводномстаканедадажебабушкакогдаспуститсявзимни
йпогребзаиюнемнавернобудетстоятьтамтихонькосовсемоднавтайномединениисосвоимс
окровеннымсосвоейдушойкакидедушкаипапаидядябертидругиетожесловнобеседуястен

ьюдавноушедшихднейспикникамистеплымдождемсзапахомпшеничныхполейижареных
кукурузныхзеренисвежескошенногосенадажебабушкабудетповторятьсноваисноватежеч
удесныезолотящиесясловачтозвучатсейчаскогдацветыкладутподпресскакбудутихповтор
ятькаждуюзимувсебелыезимывовсевременасноваисноваонибудутслетатьсгубкакулыбка
какнежданныйсолнечныйзайчиквотьмевиноизодуванчиковвиноизодуванчиковвиноизод
уванчиковонприходилинеслышноуходилипочтибесшумнотравапригибаласьираспрямл
яласьвновьонискользиливнизпохолмамточнотениоблаковэтобежалилетниемальчишкиду
гласотстализаблудилсязадыхаясьотбыстрогобегаоностановилсянакраюовраганасамойкр
омкенадпропастьюиоттудананегодохнулохолодомнавостривушиточнооленьонвдругучуя
лстаруюкакмиропасностьгородраспалсяздесьнадвеполовиныздесьокончиласьцивилизац
ияздесьживетлишьвспухшаяземляежечасносовершаетсямиллионсмертейирожденийизд
есьпроторенныеилиещенепроторенныетропытвердятчтобыстатьмужчинамимальчишки
должныстранствоватьвсегдавсюжизньстранствоватьдугласобернулсяэтатропаогромной
пыльнойзмеейскользиткледяномудомугдевзолотыелетниеднипрячетсязимаатабежиткра
скаленнымпесчанымберегамиюльскогоозераавонтакдеревьямгдемальчишкипрячутсяме
жлистьевточнотерпкиеещенезрелыеплодыдикойяблониитамрастутизреютавотэтакперси
ковомусадуквиноградникукогороднымгрядамгдедремлютнасолнцеарбузыполосатыесло
внокошкитигровоймастиэтатропазаросшаякапризнаяизвилистаятянетсякшколеатапряма
якакстрелаксубботнимутренникамгдепоказываютковбойскиефильмывотэтавдольручьяк
дикойлеснойчащедугласзажмурилсяктоскажетгдеканчаетсягородиначинаетсялеснаяглу
шьктоскажетгородврастаетвнееилионапереходитвгородиздавнаинавекисуществуетнека
янеуловимаяграньгдеборютсядвесилыиоднанавремяпобеждаетизавладеваетпросекойло
щинойлужайкойдеревомкустомбескрайнееморетравицветовплещетсядалековполяхвокр
угодинокихфермалетомзеленыйприбойяростноподступаетксамомугородуночьзаночьюч
ащилугадальниепросторыстекаютпооврагувсеближезахлестываютгородзапахомводыит
равигородсловнопустеетмертвеетивновьуходитвземлюикаждоеутрооврагещеглубжевгр
ызаетсявгородигрозитпоглотитьгаражиточнодырявыелодчонкиипожратьдопотопныеавт
омобилиоставленныенамилостьдождяиразедаемыержавчинойэйаусквозьтайныоврагаиг
ородаивременимчалисьджонхафичарливудменэйдугласмедленнодвинулсяпотропинкеко
нечноеслихочешьпосмотретьнадвесамыеглавныевещикакживетчеловекикакживетприро
данадоприйтисюдаковрагуведьгородвконцеконцоввсеголишьбольшойпотрепанныйбуря
микорабльнанемполнонародуивсехлопочутбезусталивычерпываютводуобкалываютржа
вчинупоройкакаянибудьшлюпкахибаркадетищекораблясмытоенеслышнойбурейвремен
итонетвмолчаливыхволнахтермитовимуравьеввраспахнутойовражьейпастичтобыощути
тькакмелькаюткузнечикиишуршатвжаркихтравахточносухаябумагачтобыоглохнутьпод
пеленойтончайшейпылиинаконецрухнутьградомкамнейипотокомсмолыкакрушатсятле
ющиеугликостразажженногогромомисинеймолниейнамигозарившейторжестволесныхд
ебрейтаквотзначитчтотянулосюдадугласатайнаявойначеловекасприродойизгодавгодчел
овекпохищаетчтотоуприродыаприродавновьберетсвоеиникогдагородпонастоящемудоко
нцанепобеждаетвечноемугрозитбезмолвнаяопасностьонвооружилсякосилкойитяпкойог
ромныминожницамионподрезаеткустыиопрыскиваетядомвредныхбукашекигусеницону
прямоплыветвпередпокаемувелитцивилизациянокаждыйдомтогоиглядизахлестнутзеле
ныеволныисхоронятнавекиакогданибудьслицаземлиисчезнетпоследнийчеловекиегокоси
лкиисадовыелопатыизеденныержавчинойрассыплютсявпрахгородчащадомаоврагдуглас

озадаченномигаетнокакаяжесвязьмежчеловекомиприродойкакпонятьчтозначатонидругд
лядругакогдаонопустилглазапервыйлетнийобрядпозадиодуванчикисобраныизаготовлен
ывпрокпораприступатьковторомунодугласзастылинедвижетсясместадугпошлидугголос
азатихливдалекеяживойсказалдугласночтотолкуониещебольшеживыечемякакжеэтокак
жетаконстоялводиночествеглядянасвоиногиневсилахдвинутьсясместаинаконецпонялвт
отвечердугласвозвращалсядомойизкиновместесродителямиибратомтомомиувиделихвяр
коосвещеннойвитринемагазинатеннисныетуфлидугласпоспешноотвелглазаноегоногиуж
еощутилиприкосновениепарусиныизаскользилиповоздухубыстрейбыстрейземлязаверте
ласьзахлопалиполотняныенавесынадвитринамитакойонподнялветертаконмчалсяродите
лиитомшагалинеторопясьамеждунимипятясьзадомшелдугласинесводилглазстеннисных
туфельтампозадивполуночнойвитринехорошаябылакартинасказаламамаагабуркнулдугл
асстоялиюньдавноминовалотовремякогданалетопокупаюттакиетуфлилегкиеитихиеточн
отеплыйдождьчтошуршитпотротуарамужеиюньиземляполнапервозданнойсилыивсевок
ругдвижетсяирастеттраваипосейденьпереливаетсясюдаизлуговомываеттротуарыподсту
паеткдомамкажетсягородвотвотчерпнетбортомипокорнопойдетнадноивзеленомморетра
внеостанетсянивсплесканирябидугласвдругзастылточновросвмертвыйасфальтикрасный
кирпичулицыневсилахтронутьсясместапапвыпалилонвонтамвокнетеннисныетуфлиотец
даженеобернулсяазачемтебеновыетуфлискажипожалуйстаможешьтымнеобяснитьнууда
затемчтовнихчувствуешьсебятакбудтовпервыевэтолетоскинулбашмакиипобежалбосико
мпотраветочновзимнююночьвысунулногиизподтеплогоодеялаиподставилветручтодыш
итхолодомвоткрытоеокноионистынутстынутапотомвтягиваешьихобратнопододеялоион
исовсемкаксосулькивтеннисныхтуфляхчувствуешьсебятакбудтовпервыевэтолетобредеш
ьбосикомполенивомуручьюивпрозрачнойводевидишькактвоиногиступаютподнубудтоо
ниперелomилисьидвижутсячутьвпередитебяпотомучтоведьвводевсевидитсянетакпапска
залдугласэтооченьтруднообяснитьаа

Висновки

Під час виконання лабораторної роботи ще більше дізнався про афінний шифр та методи його розшифрування. Закріпив свої практичні знання з мови програмування Python. Також розшифрував текст та написав свою автоматизовану программу для розшифрування шифротексту зашифрованого афінним шифром.