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

Дрозд С.Ю

Перевірив:

Київ – 2021

Мета роботи:

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

Постановка задачі:

реалізувати програму для пошуку ключа та розшифрування ШТ афінною підстановкою біграм з функцією автоматичного розпізнавання мови.

Порядок виконання:

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

Варіант - 4

Хід роботи

Для початку я написала функції для пошуку НСД, оберненого елемента, розв'язання ЛР, потім удосконалила функції розбиття тексту на біграми, пошуку частот біграм, написала функції пошуку числового значення біграм, кодування, декодування афінною підстаовкою, функції пошуку ключа(a та b), функції розпізнавання російської мови**.**

Найчастіші біграми шифротексту:

	bigram	freq
1	еш	0.022930
2	еы	0.016769
3	ск	0.016085
4	шя	0.016085
5	до	0.015743

Автоматичний розпізнавач російської мови:

1. Перевіряємо чи не починається текст з букв «ь» або «ы». Якщо починається – це шум
2. Перевіряємо чи в перших 50 символах зустрічається більше 3 раз три приголосні або голосні підряд. Якщо зустрічаються - це шум

3. Перевіряємо на наявність біграми «ьа» - якщо є – це шум.
4. Перевіряємо на частоту. Якщо найчастіші букви «о» або «а» або «е» - є ймовірність що текст не шум.

```
In [508]: for i in range(0, len(real)):
              if control(real[i]):
                  #print(i)
                  #print(a[i],b[i])
                  print(real[i][:50])
```

```
еслиправдачтодостоевскийвсибирцщебьлподверженприпа
еслиправдачтодостоевскийвсибирцщебьлподверженприпа
еслиправдачтодостоевскийвсибирцщебьлподверженприпа
еслиправдачтодостоевскийвсибирцщебьлподверженприпа
еслиправдачтодостоевскийвсибирцщебьлподверженприпа
еслиправдачтодостоевскийвсибирцщебьлподверженприпа
```

Шифрований текст

щжуяжущпккфшчфбждоцпюдйсвжбэдуэыйэдцмодпмурзфбряцкмдыйдосштцмижбчфипмугф
бзчшохдодвзбряцкмдбэдцхзнощкяоэоюэтцюзныертзилгфоцбчполфмэдцщкйкшйэысйрэйкчоз
ычфждьмйшотдотзьоюйсщзоюдууюзсшшстзрэыосяфоешыенывдьмиыыяшцрбгянямзюдшскд
мыайыяаоешезвжпонорэкжцчжшбчдофшщофбяоязфыщжвонцеырайхмучмсшывчфвэрфешмя
ояйывщеыйсбжощлзшярфбждоцпюдлвюпщкмзешжзмоуяхямзюдлвзбкзешдбшящксавотзябйк
жзшцопсйкоефтцрзюэдцсшямсканзомыжуэыыцсшмычмэжглрзщыезскщквкшятоьэйштибяшк
очщкфмыйеыйывдьмиыщчвккцощеызонорйвкхпшсзунрмоншзоязшяэдхпезхлсопжипеызохлн
шплбйщждоыкфоскщквкшягоефоцэзччскщквканвказешюшлцромглтдоккжшскзыядншууезж
урфешщпнзшятоужертцлвяхщжпофожущпккшяэывдьмиыйсжусжощккшйжррэсзешьоктдоск
ыкфотфлцжшвдзылвхзпмжущжеляыцдюппкгфкшскщквкшяозноюуйэвзхягжжзщрфяоэщпсчк
жйэцшвдрйрэйкчофолжыймывдьмиыщчдорддокыбзлжвочыезыяюйеытяьочмскмзшядяешмуя
хщжбягжрйашайюпмогйжшфшайрмлзннтзхаокшйбчаощянбччйтжмкжучбуфпошфбждоцпю
длвюпюпэзкбтцзопзаоешйшохзодонофшайсщзожурфмовоцяанфшляйбмуьосклюнсккжеьзое
шшоешоцэжлыдяюйеызопыщжфоочсквжаббжнзбляьхзсккцезшяййсщзоюдьмйшнхдоаоешезв
жбяршвдшяполфзятзбжьоиосяйжгоелзурмеыйссожзешопхпимсжсказкзшяшйнэюшшомглтдо
нзпксзеыэжюпщжхявушйгожурфлцгцншвдрздвщоцыыиеыхзнфылтфаляяыжфзйквбждэечяы
жхыхоцыыиеыыяпомггднотлккжжипеызохлщпдоряпзелцджзкзсэлвщпчзгпшсмыжумилцэбтц
зохлмофхэыеынеткзеадьгпуротынщйайкбазущпязхлдырйпоазсяслщяджипщплзджипюшлцлы
бжхяскыосяэищеештцедууьмншйкрзшяцпдвзбряцкмдррхфщжэпмуапзчвомощкхыхзиоюнязх
прэчфлоешщпоцбжщлтзноьобцэжхякзуяяяямзокбмырфзбюжщкяьрйсозыеыйсхпрфеыщчфое
фзббжнзтыссжяилнахпезфщпмшявжядтцйэоцбчазгфьпмушсбэчмиоцяшйдвюптжждйсэйтзмо
ыптцыцшййычмыйзхйшмшжшалтыбжхябжюакцопиыщчыдншуусйжуопчфюшжзйкмяефопи
фбкюнзовбюпдокзшярйдуюплвляешууяхщжпоной кыпюшщчмысклзыцбчмялзоцнрряешиыфс
хядаыосябжьоиогфеыхзншзунрюпыяябтцюмюпйшажьосжрэешжзщыцзешйкккшячхдосажую
шимйшлыпутцурряешбзкцколппотзуыайжхжшеыабряязодхпрэчфдяешоцкзвдаямымуайдосш
щоччдыозлжцшшйфшщоцьзхлцюпзхщжщккжюыюпцчзпэыиывдншуушсешяоюшбчкзуяяяям
зозхьпешьоаоешывмкйыдвбжжзщрэысямяблоцлышсгялаэышйлвмксаанжутоаонзскккрздвюп
тжждшсэыпзьцяделоцлыбжанхмлзннскюдьмоцбжпэсйсщзодбкзвыкшэпдойхдоюаншщкбаек
шйбчншузябряешйкешзоешчбгяыоиыоцпмзямодпмучкшйаоешезвжпоновгеыьзрйхесзкбйкьо
сктлсзешьоекшялцмиажжусжюуэжцышсдондпмкзшягожурфлцеызоножяяоьоэмкзшяпдмыэзг
пйшууешоцсаскдондымкзшязплццдлвляудмяйядойккощзшяекшэйфбждоцпюдлвляскмздбкзц
жжущпрфуяшфсчдвбждчвхеыщчфочытцмиажщквканфшууфиеыхзаоешезвжпонодаыпиыщом
змятыямйшалтыеызоешыедвайнинзшязпкцрфешмяеыцпяовкрфекуяжубждоджгллкпыбжанцй
сщзорэкжшяанфшншряязлзфуыйдуюпшсуяпзйкелиавжнрфушйеыюувделдшчфилюшощжшш
йкшшйцомгулщяджипюгпуотсяужзюждмкчкнцжшязцжюяйкбэйканпдпуыйьмюпйфбждоцпю

длвюпюпэзпшкзхуэжйуппбзлжфяфохяшфвчшякжядтлоцлыезсочзсыяхщжипляэмнщеычяраж
уййюзвждвждмызхзосшзбкззжокуцеыюпщуыйтодыюпиызопызвкзмзюдайюдьмиыыяхфщжц
фвчшящжюпмуюкжшбчбьщжыйрйшзяошйзоузяждчвхеыщчпмщпбкуяяоекшярбптхямзюдечр
эйкиордиыцпямфочыхордяожзщыезжупмскшяцпсказкзшяллщяанншшкщкпоноюаающяекшй
бчжучбгяыоиыоцпмяднщжшбчтзчзкззогяюалэчмиыоцюшяхщжпокбчфнодоздопзузхщжпоьф
йказтзрэыосяфощждчвхеыхзжусжфрйктзшяскжеьзоешрйэжпзжжбяаоешывбзлжцшшйфшрэщ
жсокыйшлцлыксфохямвмуйчжуезаяалжшбчшфссешмяпзюнзоешедвдвлгфезшйдбряилгфеыхз
сккчвкщыезтлыниоовмушссожзбибзвфвчшяеыабкзтыыймуеызочбюпэзбпифрйбжхяузыпуяхы
щчрзхьэыэявжкщитдоешзхеыхзрэешйчпзюнешибряшяякжшбчфуэжмзчшвдщкпонйсщжшвкь
оцпйшбгпутгэййшмштцедзббжнзмоошууеыщчдонорзлзджипщчьоцыыиеыыявлаомяркгяшпт
цпмдущесзноншшкмокцжшлвждвдрэскалцяекжшбчкожцчибзлжозномясктзлзмкжшбчшящкб
яйбзбяшждцыцшдзщжэзччамекуяанюзскжуэыощлзшящжбждояоратлынсаскрэууншмяскжуп
мскжшбчцдвдвжьглцечмяскскщкбаекжшбчфшууэжтлмдэйсщжшмощквканбчтзябйкжзшцопс
йзоужертцлвяхщжбямэсоеецызбйкмяюнзоекшвуяджпоьфйказсшлячовунщеырэтцюзпохпеыз
омоешдбждсожзбибзлжхыщжыйрйшзяошйуфаляятфсчподояоносшншмоешдбждтззпсчжшбч
ншщзнэйсешьовбптдохлжурфбжффюшлцлыксфохявжядтлоцлылвбжзбмушямзешекощеычяр
атзилгфбзлжзпвкылоцдуюпиыыяйкныляыфчбюпповбнзцжшзяоййппифрйщкжэппншйкрзщы
айхпжшжшвдщкхйппифрйуяпндощкпорфссешмяабяопмьосяцызвмуйчмоешдбждщуивлвщое
фтцрзюэдцсавксшншмоешдбждншайешюшлыбжюуиырафовуьмайтзвжгцррсшбжлзмканюак
ыбзйхдодвууэжкцмэсчжшсопжипеызозхьпешьомяравжщоипжшешмясжжкйкгшмуайтзфунш
яхщжбялчуцеыйсжулямрчфюшпфмяяявлвжипюпэышбмунрчфюшьосокыиыхзхпезпыщжмосо
ьыбжхядамофыюшотдовкккшяабйчуцжелжрбрякывдюшлвохдошзяобпбжжуэырйбзщтелмяил
щкцжжзщрэысяныблоцлыщемыжучмдубзвфаляяоышйеыюзмзыжйэозкцкогрчфюшажкжщкг
фсймовккцивыйгшьльфжшншмолдопсшайскжущпнзшядуайиыалшжпоноюяыкпзсчсрчфюшс
кюклфоцьидяхфщжщлщяджипбжюпмуяззощуиврймзвожзпофотывдохлцюпядайхпимиыраы
жнэюшсйокбяжярзьазоныйкоцыыиеыщчжящкбяшзяоьфжяюуйсгдншуулвайншопэзцжбкюн
зоносочзсыяхщжипхордяожзщызбрякыбзлжкжюпмуяззощуиврйвуйшайподояохлщкбяьшму
щжзовказхяанаоешезвжбякбмурфоцхпэесопжипеыилзэтцчмгнпдрэбтюянзужнепзыжыйсйщк
жэгщлцечпфлцйшжбрякыиыхзфшайтцлбгцабхявыцпяохяупайтзншщзнэйсшкопншфузхпмдь
юшшящксктллзокрзпмжзешскхыэжазадиыуфужертцлвхзэоскфопбоцщкчфылидмышкбмщпбк
уяяоекзожзуяпонзяыншвдщкцждоюшвжитдочзкзжзсыкшкяскыосяпнжцнэохфсфлчжеьзоешэ
пбжжущчхябфбждоцпюдлвямэжглцяекжшскчйфибяншкеынтзужертцлвщчэжффйэракбяощз
шжаокыиыщчсожзбиеызоузсуьмуяуыжддосшншмоешдбждсожзбигцскыкфотфлцабгяыовояя
фяьшмущжвзлжыцмимшшйгшезновжьошйээфщзрзмкуягшзбезносожзбиеыыядвзбряжзлжип
юпоцчбптдохлибвоанаопоьшйкешзокюывруххнзеявжйэйканэущпзомязоныйфмяцяюакбмумя
уысйчбямппыйыяюдйшлцлыэжмкгфеыйсмофыксюдабгяыкаяшябялбгцабхямзюдйсжущжеля
ыцдсэйканюрщкйкякчодаззешажщзскяптжязджпзчзшяжкйкгшмускбфсчаоешезвжпонопмйкй
вюпууэжжйюшряшйешпуьгмоешывбзшхдожйюшряпыбжюшвжйэдвншюпзоешедншщзнэйсе
шылбэяоыкжшбччзкзтырйскпонзшясшмышйсщжшзпсчанбчдайкрзшяшйьомршьеыщчуфтцч
ыщокыкхйшнхдохпцшшсншешйкцчжшншэзччсжрлязшядяябтцшяанбчжучмкзшяшйрлщяегд
яуярймоаышийшажфямосшайдбмурфшяыжжяочжшбчгявбйшщчаоешезвжпоноэбкзешдбшяр
ллзджипюшлцлырэчмзуиыяхскмыуфоцядюпжрчфюшвкжурфлцтжбжюуфиыщчскподояоеы
щжлкешраояазжшжущпщоскскможяскжшбцзвлвюпеыхзюдншуусйшфкзныбжхяншзогяуянне
тюянзашцдияблязныръетцлыайдбкзешдбшянфсчтзномофшсжцкгяпзюнамзпеяпыэжйэзпэыгдн
шуущешфалноыжгллкеыщжуясащуивхзак

Розшифрований текст

еслиправдачтодостоевскийвсибирщщебылподверженприпадкммтоэтолишыподтверждаетточт
оегоприпадкибылиегокаройонболеерщихненуждалсякогдабылкараемцщьмобразоыщодокузат
ыэтонехозможноскорееэтойнеобводимостзюрщакузощфидляпсихическойэкэщомфидостоевс
когообясняетсяточтоонпрошещщесломлущньмчерезэтфгодьбедствийивщижущийосуждение
достоевскоговкачествеполитическогопреступникабылонесправедливьмиондолженбылэтознат
ыноэщпрцщллэтэщезаслужеьщоенаказаниеожбатюшкицарякакзммущвщакузощиязаслужущн
огоимзасвойгрехпоотношениюксвоемусобствущномуотцувместоюамонаказанияондалсебяна
казатызаместителюотцаэтодаетнаыщекотороепредставлениеопсихологическомоправданицща
кузощийприсуждаемьхобществхомэтонаюамомделетакыщогиеизпрестующиковжаждутнаказа
нияеготребуетихсверхяизбавляясебятакимобразомотсммэщакузощиятоктохщаетслофщоефи
змущчихоезначениеистерическихсимптомовпойметчтомьздесынепьтаемсядобитысясмьслапр
ипадковдостоевскогововсейполнотедостаточнотогочтоможнопредположитычтоихперхоначал
ынаясенностыосталасйщеизмущночщесморянавсепоследупниенаслоенияможноскузатычтодо
стоевскийтакникогдаинеосхободилсяотугрьзущийсовестивсвязиснамерениемубитыотцаэтоле
жащеущасовестибремяопределилотакжеегообщышущиекдоумдругишсферампокоющишснщ
аобщышущфикотцукгосударствущномуавторитетуикверевбогавпервойэщпришелкполномуп
одчцщущиюбатюшкшцарюотщаждьразьгравшемуащимкомедиюубийствавдействителйщости
наводившуюстолыкорузотражениевегоприпадкахздесыверхвзялопоканщиеболышесвободьос
тавалосыунегохобластирелигиознойпэщедопускапнимсоыщущийсведущиямондопослетщей
минутьсвоейжизнивсеколебалсямеждзверойибезбожиемеговьсокийумнепоуволллемвщезмме
чатытетрутщостиосмьсливощияцкоторьмприводитверавиндивидуалыномповторениимирovог
оисторическогораувитияэщнаделлсявидеалехристощайтивьводиосхобождущиеотгреховфисп
олызоватысхоисобствеьщьестраданиячтобыпритязатйщаролыхристаеслионвконежщомсчету
щепришелксвободеисталреакциэщеромтоэтообяащяетсятемчтоотнечеловеческаяскщовняявц
щощакоторойстроитсярелигиозноечзвстходостфглавщегосверхцщдивидуалйщойсильщемог
лабытыпреодоленадажееговьсокойцщтеялектуалйщостыюздесынаскузалосыбьможноупрешщ
утывтомчтомьотказьваемсяотбеспристрастностипсивоощализаиподвергаемдостоевскогооцу
щюеимеющейпрахонасущестхованиелишыспристрасбщойточкизренияопределущногомирох
оззрениякэщсерваторсталбьнаточказрениявеликогоинквизитораиоценивалбьдостоевскогоина
чеупрексправедливдляегосмягчущиямофщолишысказатычторешущиедостоевскоговьувощоо
чевитщозатрутщущностзюегомьшлениявследствиущеврозаедвалипростойслучачщостыюмож
нообяснитычтотришедеврммировойлитературьвсехвремущтрактуютоднуитужетемутемуотце
убийствацарыэдипсофоклагамлетшекспираибратыякарммузовьдостоевскогововсехтрехраскр
ьваетсяимотивдеяниясексуалйщоесопеящичествоиззажущщиньпрямеевсегокэщечноэтопредс
тавлущовдрммеоащовощночщагреческомскузощфиздесыдеяниесовершаетсяцнесммимгерое
мнобезсмягчущияизавуалированияпоэтическаяобработкощевозмофщаоткровеьщоепризнание
внамеренииубитыотцакакогомьдобиваемсяприпсивоощализекажетсянепереносимьмбезощал
итической подготовкивгреческоэдраменеобводимоесмягчущиеприсохранениисенностимастер
скидостфгаетсятемчтобессохщателйщьймотивгерояпроецируетсявдействителыностыкакчужд
оеемупринуждущиенавязаьщоесурыбойгеройсовершаетдеяниущепретщммерущноиповсейви
димостибеувлинщияжеянцщьивсежеэтостечущиеобстоятелыствпринимаетсяврасчеттаккакон
можетзахоеватыцарицуматытолыкопослеповторущиятогожедействияхобщышущфичудовищ
асимволизирующегоотцапослетогокакобнаруживаетсяиоглашаетсяеговинанеделаетсяникаки
хпопьтокащятыееессебявзвалитыеенапрцщуждениесостороньсурыбьнаоборотвинапризнается
икаквсщелаявинанаказьваетсячторассудкуможетпоказатысянесправедливьмнопсихологичес
киабсолюбщоправилыновнанглийскоэдрамеэтоизображущоболеекосвущнопоступоксовершает
снщесммимгероемадругимдлякоторогоэтотпоступокнеявляетсяотцеубийстхомпоэтомупредо
судителйщьймотивсексуалйщогосоперничестваужущщиньненуждаетсявзаоуалировощфирар
щоийдиповкомплексгероямьвидимкакбьвотражеьщомсвететкакмьвидимлишытокакоедейс
твиепроизходибщагерояпоступокдругогоондолженбылбьзаэтотпоступокотомститйщострощн

ьмобрузомневсилахэтосделатымьхщаемчтоегорасслабляетсобствущноечзвстховиньвсоответс
твиисхарактеромневротическихявлущийпроисходитсдвигичувствовцщьпереходитхосохщощ
иесвоечщеспосогщостивьпощщитыэтозаданиепоявляютсяприхщакитогочтогеройвоспрцщим
аетэтувинукаксверхцщдирщдуалйщуюэщпрезираетдругидщемущеечешсебяеслиобходитысяс
каждьмпозаслугммктвуэдетотпоркивэтомнаправленииромощрусскогопиюателяуходитнашаг
далошеиздесыубийствосовершенодругимчеловекомотщакочеловекомсвязощньшсубитьмтаки
мижееьнорщимиобщышущиямикакигероэдмитрийукоторогомотивсексуалыногосопеящичест
ваоткровеьщоприхщаетсясовершенодругимбратомкоторомукакибтереснозаметитыдостоевск
ийпередалсвоюсобствущнуюболезныякобьэпилепсиютешсммьмкакбьжелаясделатыприхщощ
иечтомолэпилептишщевротиквомнеотцеубийцаивотвречизснитниканасудетажеизвестнанщас
мешкощадпсихологиейонамолпалкаодоухкэщцахзавуалировановеликолеющотаккакстоитвсе
этоперевеящутыинаводишыглубочайшуюсенностывосприятиядостоевскогозаслуживаетнасм
ешкиотнюрынепсихологияасудебньйпроцесздохщощиясовершущнобезрузлижщоктоэтотпост
упоксовершилнаюамомделепсивологияибтересуетсллишытемктоеговсхоемсердцежелаликто
поегосовершущфиегоприветствовалипоэтомувплотыдокобтрастнойффгурьалешивсебратыяр
авновинорщьдвижимьйпервижщьмипозьвммфискателйщаслаждущийпощщьйскепсиюацини
киэпилептическийпрестующиквбратыяхкарамазовьхестысценаввьсшейстепенихарактернаядл
ядостоевскогоизразговорасдмитриемстаршцпостфгаетчтодмитричщоситвсебеготовностыкот
цеубийстоуиброюаетсяперетщимнаколениэтэщеможетявлятысявьражениемхосхщнущияадол
фщоохщачатычтосвятойотстраняетотсебяискушениеисполнитысяпрезрениемкубийцеилиимп
осщушатысяипоэтомупереднишсмиряетсясимпатиядостоевскогокпреступникудействителйщ
обезгрощичнаэщадалековьходитзапредельсострадощиянакотороущесчастньйимеетправоонан
апоминаетблагоговущиескоторьмвдрерщостиотносилисыкэпилептикуидушерщоболйщомупр
еступникдлянегопочтиспасителывзявшичщасебявцщукоторуювдругошслучаущеслибьдругие
аа

Ключ:

a = 390

b = 10

Висновки: під час виконання даної роботи я навчилася розшифровувати тексти, зашифровані афінною підстановкою біграм. Також я навчилася програмувати автоматичний розпізнавач російської мови. Таким чином я набула навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.