Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3
«Криптоаналіз афінної біграмної підстановки»

Виконали:
студенти групи ФБ-04
Дмитренко Даніїл та Сербіненко Олексій
Перевірив:
Чорний О.

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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

Для спрощення роботи ми використали декілька функцій з вбудованих бібліотек мови python, зокрема – gcd. Інші функції писали самостійно. В якості методу відслідковування природності тексту ми обрали порівняння частот таких букв: ф, ц, щ. Виникла складність в тому, що початково функція не знаходила справжній текст. Ми підвищили гранично допустиме значення в декілька разів, поки не знайшли необхідні. Це пов'язано з тим, що частотні характеристики тексту не надто точно відповідають таким же в мові.

Результати

Варіант 2

Найчастіші біграми зашифрованого тексту: 'йа', 'юа', 'чш', 'юд', 'рщ'.

Ключ: а = 27, б = 211

Зашифрований текст

рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюеэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэкяуклзщюгхегарпинцплппprффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаюйзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщбероюазанхзуш

щимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфуыуй
ацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсх
щрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрбердрйуюпнсабд
пннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбубеюыхрдщндщфщейе
рйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюбероюарпиным
жизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйю
енщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчу
шлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхуш
чкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносвиййдзьрыщышхемсующудршджьюан
хрэцпымздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчтыкйдшнануэифуларизсййушфи
юдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудб
юяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешберою
ачпщылшыщдшэасуйаьпымкуюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощ
жзьрыщаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосй
йричикзддрятарщроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшч
ыачешудкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшр
щашошзсбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюберояюарптылшцюцрчий
щпаюеющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюез
лиекдффыршдчимшлчлэфуюаззддрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдк
ебдкйющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаю
нежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленкссвссе
оамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзс
хажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщ
течшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюд
бучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэ
шсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшцшм
ейряжпшюешпщьбудшоылшищгамуыщюаешлуьппрринхдщцадуришпчичифубелшмшмвк
йуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаепжьюд
мшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщчшмейртв
ещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлао
ыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдбюфшхдиырйг
екбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюа
зблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхр
мэцпфжйахеродюыщжрпроппрчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцус
юазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазад
дхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвц
юдаюьичбзлцчтыкйэщышты аччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюи
дцецчхйхажатечшжьйацчтыкйдшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмег
фчпрбелшцающашчопаюебушщькышзшвыйафщышхпцмдрщыыуюехакчщуиезафнщыаччб
зстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшс
бужичлщерпюабуашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэхшст
даюриэщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэ
прешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяав
дчишхтаичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечушгц
мпнщьбукаюдуыдщимюдкечушгмщрщашщппрэщкырйдщьлщеющвпьюриюдюашдйржахе
тсййвпэсгпчинаькгшхпннзщццтвкчисжлзсйепртшййыуйаусйрпншдажйазмгьусффщлщрбез

ахемчтэлекмаюрщудеапамдосшсцпфжнлзуыщюазреызшэатдрмхпщьбудшщыхубвчочпща
эщялчохехалюидвиаммсееапегкажлхехдпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэ
шэдкйчбйкишугрййкоыдднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаи
ейркезаокйщгаынрйщызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсд
мэшсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныурщгпзхцмчэиорщ
эаэшшщрщхезакдььрмьрпнхщшдькюедефщроошкаюрпркдчэуырщлхчээпмеидбюхахщим
юдюарппьщсрплаэщкаюытэтедщпуэщвкющиулаэиыйхлллнажахоусиппрсеэщюхыййаькэи
еыйееуйафмыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнх
юахйщфрпешбероюарущефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокне
йежпэиэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчитыс
азшйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасхй
юдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерпим
юдкеслщещцримежагекаюрэпьчяфьеруюсхпымздюлщелшашфьымосьрчифшцкщедеюака
йасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюадуклзща
чисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифус
ицлщеомхпипчушгмщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщроошэщнх
льюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюыщдшварчмэчиащварщэщйщчшэий
щхатешщчшбущефпсдюдисфуидчиеапячщ

Розшифрований текст

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонео
пределенноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногод
ляжизниприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигать
такойсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокружениймогуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтоникаказалосьчистотелеснымипричинамиэтисостоянияМогутпервоначальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволнений какнихарактернодляогромногобольшинствослучаевинтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношенииКоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститаккакэтаболезньчастосопряженасярковыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональногопониманиякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичииивесьмаразныхусловийкакпринарушениимозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболеваниитакипринедостаточномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмалойэпилеп

сиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотвода раздраженияэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятоене сомненнотакжепоступаетиврaспоряжениеневрозасущностькотороговтомчтобыликвидиро ватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпил ептическийприпадокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидо изменяетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессат акимобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпракти ческоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающийв торойневротиквпервомслучаедушевнаяжизньподверженанарушениюизвневовторомслуч аенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятночтоэпилепсиядо стоевскогоотносится ковторомувидуточнодоказатьэтонельзятаккаквтакомслучаенужнобыл обывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиевидоизме нения этихприпадковадляэтогоунаснедостаточноданныхописаниясамихприпадковничегон едаютсведенияосоотношенияхмеждуприпадкамииипереживанияминеполныичастопротив оречивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевдетствеч тоонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотрясшегоегоп ереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылобыве сьмауместноеслибыоправдалосьточтоониполностьюпрекратилисьвовремяотбыванияимк аторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийством вбратьяхкарамазовыхисудьбойотцадостоевскогобросиласьвглазанеодномубиографудост оевскогоипослужилаимуказаниемнаизвестноесовременноепсихологическоенаправление психоанализтаккакподразумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютрав муивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначнуобосновыватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыуче ниеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервы хприпадковдостоевскоговегоюношескиегодызадолгодопоявленияэпилепсииуэтихприпад ковбылоподобиесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииелетаргичес когоснаэтаболезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотч етнаяподавленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудто быемупредстоялосейчасжеумеретьивсамомделенаступалососто яниесовершеннопо добно едействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтем какзаснутьоставлялзаписки чтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтому чтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестны смыслинамерениетакихприпадковсмертониозначаютотождествлениесумершимчеловек омкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивт оройслучайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожела лисмертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеуче ниеутверждаетчтоэтотдругойдлямальчикаобычноотецииименуемыйистериейприпадокявл яетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Висновок:

Ми ознайомилися та дослідили метод взламу біграмного афінного шифру. Використали знання з попередніх робіт про властивості мови, щоб спростити перевірку варіантів