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

Спочатку ми рахуємо біграми нашого шифротексту, та знаходимо 5 найпопулярніших, знаходимо всі можливі пари, потім переводимо отримані значення за формулою у цифри та далі знову ж таки ща формулою, конвертуємо ці пари у ключі. Очистимо ці ключи від можливих повторів використавши метод set(), після отриманими ключами будемо розшифровувати текст, а для визначення його «змістовності» будемо рахувати його ентропію. Тобто у циклі де проходимо по всім можливим ключам, ми розшифровуємо текст ключем, рахуємо ентропію розшифрованого тексту та перевіряємо чи задовольняє ця ентропія нашій. У ході тестів було виявлено що ентропія незмістовного тексту ~4.8, а змістовного ~4.45.

Результати

Варіант 2

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

Ключ: а = 27, б = 211

Зашифрований текст

рйрщкагпprфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюеэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэкяуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщыс

аэарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаюйзхцмздффн
агещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщбероюазанхзуш
щимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфуыуй
ацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсх
щрохеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрбердрйуюпнсабд
пннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбубеюыхрдщндщфщейе
рйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюбероюарпиным
жизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйю
енщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчу
шлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхуш
чкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносвиййдзьрыщышхемсующудршджьюан
хрэцпымздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчтыкйдшнануэифуларизсййушфи
юдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудб
юяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешберою
ачпщылшыщдшэасуйаьпымкуюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощ
жзьрыщаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосй
йричикзддрятарщроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшч
ыачешудкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшр
щашошзсбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцрчий
щпаюеющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюез
лиекдффыршдчимшлчлэфуюаззддрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдк
ебдкйющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаю
нежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленкссвссе
оамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзс
хажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщ
течшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюд
бучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэ
шсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшцшм
ейряжпшюешпщьбудшоылшищгамуыщюаешлуьппрринхдщцадуришпчичифубелшмшмвк
йуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаепжьюд
мшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщчшмейртв
ещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлао
ыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдбюфшхдиырйг
екбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюа
зблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхр
мэцпфжйахеродюыщжрпроппрчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцус
юазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазад
дхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвц
юдаюьичбзлцчтыкйэщыштыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюи
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
такойсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголовокружениймогуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтоника
залосьчистотелеснымипричинамиэтисостоянияМогутпервоначальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволнений
какнихарактернодляогромногобольшинствасЛучаевинтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношенииКоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститаккакэтаболезньчастосопряженасярковыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияМибываютиудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональногопониманиякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичииВесьмаразныхусловийкакпринарушениимозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболеваниитакипринедостаточномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащегово

сновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессов порождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотвода раздраженияэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятоене сомненнотакжепоступаетиврасporяжениеневрозасущностькотороговтомчтобыликвидировать соматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилептический припадокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидо изменяетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессатакимобразоммысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпрактическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедушевнаяжизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятночтоэпилепсиядостоевскогоотносятсяковторомувидуточнодоказатьэтонельзятаккаквтакомслучаенужнобыл обывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиевидоизменияэтихприпадковадляэтогоунаснедостаточноданныхописаниясамихприпадковничегонедаютсведенияосоотношенияхмеждуприпадкамииипереживанияминеполныичастопротиворечивысвеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевдетствечтоонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотрясшегоегопереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылобывесьмауместноеслибыоправдалосьточтооniполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадостоевскогобросиласьвглазанеодномубиографудостоевскогоипослужилаимуказаниемнаизвестноесовременноепсихологическоенаправление психоанализтаккакподразумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютравмуиврeакциидостоевскогонаэтоключевойпунктегоневрозаеслияначнуобосноватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыучениеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдостоевскоговегоюношескиегодызадолгодопоявленияэпилепсииуэтихприпадковбылоподобиесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииилетаргическогоснаэтаболезньнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяподавленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейчасжеумеретьивсамомделенаступалосостояниесовершенноподобноедействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемкаказаснутьоставлялзаписькичтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестныесмыслинамерениетакихприпадковсмертониозначаютотождествлениесумершимчеловекомкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивторойслучайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожелалисмертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучениеутверждаетчтоэтотдругойдлямальчикаобычноотецииименуемыйистериейприпадокявляетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотцуа

Висновок:

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