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

Виконали:

Студенти групи ФБ-35

Кохта Андрій

Церман Марія

Ворона Сергій

Київ — 2025

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.

Зашифрований текст (Варіант 2):

рйрщкагппрфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюеэдсецчтыкйдшцчзюимевжш
бушччэканылшолшкющчшэизупмзсбвжшбуойщаишщмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхека
йаэкяуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэарюжштнцмосхрхлтечшиш
валлмппртелиюдьпкуурдщерритыачтахщышкаюйзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимху
гшзепутэрщберояазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфуыуйацдаюва
ллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсхщрохеццэирщэаэшуоьюдэисфуриыугшэпзлие
кдкглаедюднфэщйдшгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбубеюыхрдщндщф
щейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюберояарпинымжизаропйхлбшбуклзщзсэпюаие
чшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжш
лжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкдщте
эдвиййтагшфичиорхлфдщфкшышвамносвиййдзьрыщышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехд
сджжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсач
эаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешберояачпщылшыщдшэасуйаьпым
куюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзьрыщаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтд
йкяуришпчиоскчтхэейыосййричикзддрятарщроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачеш
удкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашошзсбужифчмэйкблкмоснфэщкылшрщ
хлиечшритэзалаеймюберояарптылшцюцрчийщпаюеющчшхпэщхеишашйамущьбукаьээхцмустдмшыщдшцчсдхйыуыщйаудчика
бпсаюезлиекдффыршдчимшлчлэфуюазздрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкйющешхщнкшлнуюсэебд
ьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэыса
репуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзсхажала
фщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкышще
хеаитбюарщлсцпэсеегпосщерпусдюйаюдбучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичп
нхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхеватеluццчисхпкучыэшцшмейряжпшюешпщьбудшоы
лшищгамуыщюаешлуьпппринхдщцадуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрй
хпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщчшмейртвещжзьргшкд
тваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандус
сагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащва
ейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщкр
проппрчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюд
аюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаю
ьичбзлцчтыкйэщыштыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкйдшрщзщаш

Розшифрований текст за ключем a = 27, b = 211 :

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизниприводящего
ктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойсилыослабляясьдократкихсостоянийабсандадобыстропроходящихголовокруженийимогуттакжесменятьсякраткимип
ериодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообуславливаясьвобщемкакбыстранноэтониказалосьчистотелесныминричинамиэтисос
тоянияможетпервоначальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимостиотдушевныхволненийкакнихарактернодляогромногобольшинствослучае
винтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношенииикоторыхутверждало
сьтожесамоененадежныилиподлежатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечатлениетупостинедоразвитоститкакаэтаболезньчастосопр
яженасярковыраженнымидиотизмомикрупнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияхмибывают
иудругихлицулицсполнымдушевнымразвитиемискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойиммаффективностьюнеудивительночтопритакихобстоятельствахневозм
ожноустановитьсовокупностьклиническоюаффектаэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункционального опониманиякакеслибымеханизманорма
льноговысвобожденияпервичныхпозывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичиивесьмаразныхусловийкакпринарушениимозговойдеятельностипритяжкомзабо
леваниитканейилитоксическомзаболеваниитакипринедостаточномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделениемнадвавидамычувствуемндент
ичностьмеханизмалежащеговосновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликои
тусмалойэпилепсиейвиделивполовомактесмягчениеиадаптациювысвобожденияэпилептическогоотводараздраженияэпилептическаяреакциякаковымименемможноназватьвсеэтовместевзято
енесомненнотакжепоступаетивраспоряжениеневрозасущностьктороготомчтобыликвидироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилептичес
кийприпадокстановитсятакимобразомсимптомомистерииюадаптируетсяивидоизменяетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессатакимобразоммыспол
нымправомразличаеморганическуюиаффективнуюэпилепсиюпрактическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротикквпервомслучаедушевн
аяжизньподверженанарушениюизвневоторомслучаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмавероятночтоэпилепсиядостоевскогоотносятсяковторомувидуточнодоказатьэ
тонельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиевидоизмененияэтихприпадковадляэтогоунаснедостаточноданныхописан
иясамихприпадковничегонедаютсведенияосоотношенияхмеждуприпадкамиипереживанияминеполныичастопротиворечивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоу
жевдетствечтоонивначалехарактеризовалисьболееслабымисимптомамиитольконоспелепотрясшегоегопереживаниянавосемнадцатомгодужизниубийствваотцапринялиформуэпилепсиибылобывес
ьмауместноеслибыоправдалосьточтоонинполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкар
амазовыхисудьбойотцадостоевскогобросиласьвглазанеодномубиографудостоевскогоипослужилаимуказаниемнаизвестноесовременноепсихологическоенаправлениепсихоанализтаккакпод
разумеваетсяименноонсклоненвидетьвэтомсобытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначнуобосновыватьэтуустановкупсихоаналитическиопас
аюсьчтоокажусьнепонятнымдлявсехтехкомунезнакомыучениеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдостоевскоговегоюношескиегоды
задолгодопоявленияэпилепсииуэтихприпадковбылоподобиесмертионинаэывалисьстрахомсмертивыражалисьвсостоянииелтаргическогоснаэтаболезньнахолиланаеговначалекогдаонбыле
щемальчикомкаквнезапнаябезотчетнаяподавленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейчасжеумеретьивсамомделенаступалосостоя
ниесовершенноподобноедействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемказаснутьостаплялзаписичтобоитсяночьюзаснутьсмертоподобнымсномипро
ситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестнысмыслинамерениетакихприпадковсмертониозначаютотождествлениесумершимчеловеко
мкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертвторойслучайболеезначителенприпадоквуказанномслучаеравноценненаказаниюмыпожелалисмертидругомут
еперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучениеутверждаетчтоэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокявляетсятакимобразомсамонаказа
ниемзапожеланиесмертиненавистномуотцуа

Висновок:

У цій лабораторній роботі ми на практиці розібралися з частотним аналізом розкриття моноалфавітної підстановки та опанували навички в модулярній арифметиці. А також розшифрували шифротекст закодований Афінною біграмною підстановкою.